OPAP LHDTSV-5
APR 10 2023
PATENT & TRADEMARK OFFICE

4-13-23 IR

PTO/AIA/123 (08-12)
Approved for use through 09/30/2025. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

CHANGE OF CORRESPONDENCE ADDRESS
Patent

Address to:
Mail Stop Post Issue
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Patent Number	9894100
Issue Date	2/13/2018
Application Number	14/566,403
Filing Date	12/30/2014
First Named Inventor	Pernicha
Attorney Docket Number	FORT-012500

Please change the Correspondence Address for the above-identified patent to:

☐ The address associated with Customer Number: [ ]

OR

☑ **Firm *or* Individual Name**

Fortinet, Inc.
Attention Attorney in Charge of Patent Litigation
899 Kifer Road

Address

City	Sunnyvale	**State**	CA	**ZIP**	94086
Country	USA				
Telephone	1-408-235-7700	**Email**	patent_dept@fortinet.com; dhamilton@hdciplaw.com		

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

This form will not affect any "fee address" provided for the above-identified patent. To change a "fee address" use the "Fee Address Indication Form" (PTO/SB/47).

I am the:

☑ Patentee.

☐ If the Patentee was not the applicant for patent (37 CFR 1.42), then a Statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is enclosed or was filed on _____. See 37 CFR 3.71.

☐ Attorney or agent of record. Registration Number _____.

☐ Patent practitioner acting in a representative capacity whose correspondence address is the correspondence address of record. Notice has been given to the patentee or owner. Registration Number _____

Signature	/Will Cooper/
Typed or Printed Name	Will Cooper, Senior Vice President of Litigation and Compliance, Fortinet,Inc.
Date	04/08/2023
Telephone	

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-00**. Public burden for this form is estimated to average ** hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **If filing this completed form by mail, send to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/566,403	02/13/2018	9894100	FORT-012500	7209

64128 7590 01/24/2018

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
12640 W. Cedar Drive, Suite 1
LAKEWOOD, CO 80228

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 119 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Hugo Filipe Parreira Pernicha, Venda do Pinheiro, PORTUGAL;
Fortinet, Inc., Sunnyvale, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

64128 7590 10/31/2017
MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
12640 W. Cedar Drive, Suite 1
LAKEWOOD, CO 80228

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/566,403	12/30/2014	Hugo Filipe Parreira Pernicha	FORT-012500	7209

TITLE OF INVENTION: DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	01/31/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
CHANG, KENNETH W	2438	726-001000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Hamilton, DeSanctis & Cha LLP
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Fortinet, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Sunnyvale, CA

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☒ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ☐ A check is enclosed.
- ☒ Payment by credit card. ~~Form PTO-2038 is attached.~~ (via EFS-Web)
- ☐ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ☐ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ☐ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Michael A DeSanctis/ Date December 28, 2017

Typed or printed name Michael A. DeSanctis Registration No. 39957

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Electronic Patent Application Fee Transmittal					
Application Number:	14566403				
Filing Date:	30-Dec-2014				
Title of Invention:	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT				
First Named Inventor/Applicant Name:	Hugo Filipe Parreira Pernicha				
Filer:	Michael A. DeSanctis				
Attorney Docket Number:	FORT-012500				
Filed as Large Entity					
Filing Fees for Utility under 35 USC 111(a)					
Description		**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:					
Pages:					
Claims:					
Miscellaneous-Filing:					
Petition:					
Patent-Appeals-and-Interference:					
Post-Allowance-and-Post-Issuance:					
UTILITY APPL ISSUE FEE		1501	1	960	960

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**960**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Electronic Acknowledgement Receipt	
EFS ID:	31366827
Application Number:	14566403
International Application Number:	
Confirmation Number:	7209
Title of Invention:	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT
First Named Inventor/Applicant Name:	Hugo Filipe Parreira Pernicha
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-012500
Receipt Date:	29-DEC-2017
Filing Date:	30-DEC-2014
Time Stamp:	13:46:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$960
RAM confirmation Number	010218INTEFSW13471000
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	Issue_Fee.pdf	86673 479532f03eb18e1b084f757d253e4d4a6a253a9e	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30352 a97e23af83e55f3bfe32b3619acc044894379a54	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	117025		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

64128 7590 10/31/2017

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
12640 W. Cedar Drive, Suite 1
LAKEWOOD, CO 80228

EXAMINER
CHANG, KENNETH W

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 10/31/2017

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/566,403	12/30/2014	Hugo Filipe Parreira Pernicha	FORT-012500	7209

TITLE OF INVENTION: DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	01/31/2018

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

64128 7590 10/31/2017
MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
12640 W. Cedar Drive, Suite 1
LAKEWOOD, CO 80228

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/566,403	12/30/2014	Hugo Filipe Parreira Pernicha	FORT-012500	7209

TITLE OF INVENTION: DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	01/31/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
CHANG, KENNETH W	2438	726-001000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/566,403	12/30/2014	Hugo Filipe Parreira Pernicha	FORT-012500	7209

64128 7590 10/31/2017

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
12640 W. Cedar Drive, Suite 1
LAKEWOOD, CO 80228

EXAMINER	
CHANG, KENNETH W	
ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 10/31/2017

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Notice of Allowability	Application No. 14/566,403	Applicant(s) PERNICHA, HUGO FILIPE PARREIRA	
	Examiner Kenneth Chang	Art Unit 2438	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the filing on 09/29/2017*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-26*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/Kenneth Chang/
Primary Examiner, Art Unit 2438

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

DETAILED ACTION

1. This Reasons for Allowance is in response to applicant's amendment and remarks filed on 09/29/2017. Claims 1, 3, 13, and 23 have been amended. **Claims 1-26** are currently pending and have been considered as follows.

2. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action.

3. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

4. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Allowable Subject Matter

5. **Claims 1-26** are allowed.

Examiner's Statement of Reasons for Allowance

6. The following is an examiner's statement of reasons for allowance:

In interpreting the claims in light of the specification, the Examiner finds the claimed invention to be patentably distinct from the prior art of record.

Claims 1-26 are allowed in light of applicant's amendment to the claims filed on 09/29/2017 and remarks filed therewith. Regarding the 35 U.S.C. §103 rejection of Claims 1-26, applicant's amendment to independent Claims 1, 13, and 23 and the corresponding remarks on pages 9-10 have been fully considered, and they are persuasive in that the prior art of record does not disclose the amended features.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Although the prior art **Kanada (US 20010039576 A1)** teaches "a method **(e.g. Kanada FIG. 5; [0002] methods; [0093])** comprising: receiving, by a network security management device **(e.g. Kanada policy server with operator console [0066]; [0067])**, a request to add a new traffic flow policy rule to a plurality of policy rules **(e.g. Kanada rule specified to be added [0021]; receiving input to add policy rule [0067])** managed by the network security management device; automatically determining, by the network security management device, dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules **(e.g. Kanada detects policy rules that the new policy rule depends on [Abstract]; analyzing policy rules for dependence of policy rule data on another policy rule data [0028]; [0068]; [0099]; [0103]; [0167])**",

None of the prior art of record teaches individually or in combination at least the limitations listed below as recited in Applicant's amended independent Claims:

- [Claim 1] "***automatically optimizing, by the network security management device, the updated set of policy rules by grouping*** a first sub-set of policy rules of the updated set of policy rules, ***reordering*** a second sub-set of policy rules of the updated set of policy rules, ***and deleting*** a third sub-set of policy rules of the updated set of policy rules, ***wherein the optimizing is based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules, wherein the optimizing by the network security management device is performed in real***

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

time, wherein the network security management device is configured to maintain a log of changes to the policy rules enabling the optimizing to be undone";

- [Claim 13] "a policy rule optimization module configured to ***automatically optimize the updated set of policy rules by grouping*** a first sub-set of policy rules of the updated set of policy rules, ***reordering*** a second sub-set of policy rules of the updated set of policy rules, ***and deleting*** a third sub-set of policy rules of the updated set of policy rules, ***wherein the optimizing is performed in real-time based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules, and wherein the policy rule optimization module is configured to maintain a log of changes to the policy rules enabling the optimizing to be undone***";
- [Claim 23] "***optimize the current set of policy rules by grouping a first sub-set of policy rules of the current set of policy rules, reordering a second sub-set of policy rules of the current set of policy rules, and deleting a third sub-set of policy rules of the current set of policy rules, wherein the optimizing is performed in real-time based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and usage statistics for each policy rule of the current set of policy rules, wherein the policy rule optimization module***

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

is configured to maintain a log of changes to the policy rules enabling the optimizing to be undone".

The **closest** prior art made of record and cited consisted of the following references.

Kanada (US 20010039576 A1) disclosed a policy server that assigns an identifier to each of a plurality of policy rules in each of which condition and action are described and transmits these policy rules to a network node. When transmitting new policy rules to the network node as additional ones, the server detects policy rules that depend on a newly entered policy rule or on which a newly entered policy rule depends. As for the policy rules that depend on a new policy rule or on any of which a new policy rule depends, if the policy rule has not been transmitted to the network node, the identifier thereof and the condition and action described therein are transmitted to the network node; if the policy rule has been transmitted to said network node, the identifier thereof is transmitted to the network node, but the condition and action described therein are not transmitted.

Cooper et al. (US 20020069200 A1) disclosed a method and apparatus that uses a proprietary algorithm for organizing network security policy rules in a way that minimizes the number of rules considered when determining the set of rules applicable to a given protocol event.

Sheikh et al. (US 20020078382 A1) disclosed a security software methodology and system that takes an internal approach to mitigating security risks from authorized and unauthorized users. The security software system uses the methodology of monitoring, in great detail, any configuration changes made to information systems

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

within a network. These systems and applications include web servers, firewalls, proxy servers, log servers, intrusion detection software systems, routers and any other device or application which can be considered a part of the enterprise information system infrastructure.

Merugu et al. (US 20020152209 A1) disclosed a packet classification system to select representative bits from a packet to look up a set of rules. The per-flow classification works with a large set of rules, where each rule comprises of multiple fields and also allows fast dynamic variation in the rule set. A lookup process includes a simple and finite set of instructions that can be efficiently implemented as pipelined hardware and support very high packet arrival rates

Liu (US 20020154635 A1) disclosed systems for enabling communications between a first private network and a second private network configured from nodes in a public network. When communicating a packet from the first private network to the second private network, a computer receives a packet from a source node in the first private network. The computer then determines whether the packet is destined for the second private network. Thereafter, if the packet is destined for the second private network, the computer forwards the packet to a destination node in the second private network. When communicating a packet from the second private network to the first private network, a computer receives a packet from a source node in the second private network. The computer then determines whether the packet is destined for the second private network. Thereafter, if the packet is not destined for the second private network, the computer forwards the packet to a destination node in the first private network.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Corl et al. (US 20020198981 A1) disclosed system for determining whether to enforce a plurality of filter rules for a packet including a key in a computer network is disclosed. Each of the plurality of filter rules has a priority. The method and system include accumulating statistics for each of the plurality of filter rules. The statistics indicate a frequency of enforcement for each of the plurality of filter rules. The method and system also include placing the plurality of filter rules in an order for testing against the key. The order is based on the frequency of each filter rule of the portion of the plurality of filter rules. Consequently, more frequently enforced filter rules may be tested first.

Levy et al. (US 20030179703 A1) disclosed a policy manager that automatically generates configuration file updates for the routers in the network, as necessary, sends those updates to the appropriate routers, and causes the routers to install the configuration file updates in real-time. The automatic generation of configuration file updates is carried out in response to information that is delivered to the policy manager from a traffic measurement and flow analysis system that replaces the prior art analyzer system. The information that is generated by the traffic measurement and flow analysis system is sensitive to thresholds that the policy manager installs in the traffic measurement and flow analysis system.

Schuba et al. (US 20040177139 A1) disclosed a system that resolves conflicts between rules for network services. During operation, the system receives a set of network service rules for network data traffic from multiple network services, wherein network service rules from different network services can possibly conflict. Next, the

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

system identifies conflicts between pairs of network service rules in the set of network service rules. The system then determines a priority relationship between each pair of conflicting network service rules, and assigns priorities to the network service rules in a manner consistent with the determined priority relationships. This allows conflicts between network service rules to be subsequently resolved based on the assigned priorities.

Goldschmidt et al. (US 20060013136 A1) disclosed a flow manager that may receive packet flow rules from one or more network services and may generate a unified rule set according to the received packet flow rules. A flow manager may additionally split the unified rule set into subsets for enforcement by one or more flow enforcement devices and may install the rule subsets onto the flow enforcement devices. When splitting the unified rule set into subsets, a flow manager may analyze a network topology connecting the flow enforcement devices. A flow manager may also receive additional packet flow rules, integrate them into the unified rule set, update the rule subsets according to the additional rules, and install the updated subsets onto the flow enforcement devices.

Fulp et al. (US 20060248580 A1) disclosed a firewall policy including an ordered list of firewall rules is defined. For each rule, a probability indicating a likelihood of receiving a packet matching the rule is determined. The rules are sorted in order of non-increasing probability in a manner that preserves the firewall policy.

Nguyen et al. (US 20070115916 A1) disclosed a method for optimizing a network based on a performance knowledge base is provided. The network comprises a

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

plurality of network elements. The method includes analyzing raw performance data for each of the network elements in real-time to generate processed data based on network policies and optimization rules stored in the performance knowledge base and optimizing the network based on the processed data.

Porat (US 20080062994 A1) disclosed a method for relaying Ethernet frames over an Ethernet network, the method including adding a tag that provides an address from a hierarchical address scheme to an Ethernet frame; and relaying the Ethernet frame through the network according to the tag. There is also provided a configurable Ethernet bridge having a filtering database including a plurality of subnet masks for relaying frames according to a hierarchical address scheme.

Shah et al. (US 20090125470 A1) disclosed updating access control list (ACL) rule entries in a ternary content addressable memory (TCAM). In a firewall, ACL rules are scanned for each packet arriving in a router or switch to determine if a match exists between the packet and any of the patterns. Depending on the pattern matched, the corresponding action may be either to accept or to deny the packet. These rules are stored in a TCAM, and new or updated rules may be added to the TCAM. Systems and methods consistent with the present invention determine whether the new or updated rule has a dependency conflict with existing rules in the TCAM. If not, the rule can be inserted anywhere in the TCAM. Accordingly, the TCAM associated with a firewall's ACL can be updated more quickly and efficiently.

YANG (US 20100100954 A1) disclosed a method and apparatus for reducing obsolete firewall rules by existing network routing information as well as firewall rule

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

configuration information to help analyze firewall access logs to identify obsolete and unused firewall rules so that these obsolete firewall rules can be removed. In one embodiment, the present invention is capable of periodically identifying the unused rule set for each external partner network and removing these obsolete rules with no impact to the current operation.

SPECTOR et al. (US 20100100468 A1) disclosed a system and method for processing a digital transaction using a layered rule architecture. Any number of rules may be applied to or tested against a transaction record. Rules and associated actions may be associated with priorities. A conflict resolution method or logic may be used to select one or more actions from a set of actions resulting from applying a set of rules to a transaction record.

Ling et al. (US 20100199346 A1) disclosed analyzing and modifying access control lists that are used in computer networks. Access control lists may have many individual rules that indicate whether information can be passed between certain devices in a computer network. The access control lists may include redundant or conflicting rules. An aspect of the invention determines whether two or more access control lists are equivalent or not. Order-dependent access control lists are converted into order-independent access control lists, which enable checking of semantic equivalence of different access control lists. Upon conversion to an order-independent access control list, lower-precedence rules in the order-free list are checked for overlap with a current higher precedence entry. If overlap exists, existing order-free rules are modified so that spinoff rules have no overlap with the current entry.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

However, the prior art of record, taken by itself or in any combination, **do not** anticipate or make obvious the invention of the present application and in particular the claim features listed above.

7. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicants' disclosure.

a. **Chen et al., ("Cross-Domain Privacy-Preserving Cooperative Firewall Optimization", October 2012, IEEE/ACM Transactions on Networking, Vol. 21, No. 3, pp. 857-868)**

b. **Martinez et al. (US 20120185913 A1)**

c. **Roy et al. (US 8478852 B1)**

d. **Gao et al. (US 20150033285 A1)**

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kenneth Chang whose telephone number is (571)270-7530. The examiner can normally be reached on Monday-Friday 8:30am-5pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kenneth Chang/
Primary Examiner, Art Unit 2438
UNITED STATES PATENT AND TRADEMARK OFFICE
10/10/17

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Notice of References Cited	Application/Control No. 14/566,403	Applicant(s)/Patent Under Reexamination PERNICHA, HUGO FILIPE PA	
	Examiner Kenneth Chang	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2012/0185913 A1	07-2012	Martinez; Frank R.	G06F9/455	726/1
*	B	US-8,478,852 B1	07-2013	Roy; Alka	H04L12/6418	709/223
*	C	US-2015/0033285 A1	01-2015	Gao; Bo	H04L63/0263	726/1
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Chen et al., ("Cross-Domain Privacy-Preserving Cooperative Firewall Optimization", October 2012, IEEE/ACM Transactions on Networking, Vol. 21, No. 3, pp. 857-868
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

IEEE.org | IEEE *Xplore* Digital Library | IEEE-SA | IEEE Spectrum | More Sites Cart (0) | Create Account | Personal Sign In

Access provided by:
United States Patent and Trademark Office
Sign Out

Browse My Settings Get Help

Displaying results 1-23 of 23 for **optimize rule firewall network** and refined by
Year: 2004-2013

Show All Results Per Page 25 Sort By Relevance

Select All on Page Download PDFs | Export | Set Search Alerts | Search History

Search within results

Content Type

- Conference Publications (20)
- Journals & Magazines (3)

Year

Author

Affiliation

Publication Title

Conference Location

1. **Cross-Domain Privacy-Preserving Cooperative Firewall Optimization**
   Fei Chen; Bezawada Bruhadeshwar; Alex X. Liu
   IEEE/ACM Transactions on Networking
   Year: 2013, Volume: 21, Issue: 3
   Pages: 857 - 868
   Cited by: Papers (2)
   IEEE Journals & Magazines
   Abstract (3298 Kb)

2. **An online response system for anomaly traffic by incremental mining with genetic optimization**
   Ming-Yang Su; Sheng-Cheng Yeh
   Journal of Communications and Networks
   Year: 2010, Volume: 12, Issue: 4
   Pages: 375 - 381
   Cited by: Papers (2)
   IEEE Journals & Magazines
   Abstract (1287 Kb)

3. **ParaSplit: A Scalable Architecture on FPGA for Terabit Packet Classification**
   Jeffrey Fong; Xiang Wang; Yaxuan Qi; Jun Li; Weirong Jiang
   2012 IEEE 20th Annual Symposium on High-Performance Interconnects
   Year: 2012
   Pages: 1 - 8
   Cited by: Papers (15)
   IEEE Conference Publications
   Abstract (392 Kb)

4. **Firewall packet matching optimization using network traffic behavior and packet matching statistics**
   Zouheir Trabelsi; Hishem El Sayed; Safaa Zeidan
   Third International Conference on Communications and Networking
   Year: 2012
   Pages: 1 - 7
   IEEE Conference Publications
   Abstract (935 Kb)

5. **A Design and Implement of IPS Based on Snort**
   Jianrong Xi
   2011 Seventh International Conference on Computational Intelligence and

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Measuring firewall security
Saeed Al-Haj; Ehab Al-Shaer
2011 4th Symposium on Configuration Analytics and Automation (SAFECONFIG)
Year: 2011
Pages: 1 - 4
IEEE Conference Publications

Abstract (165 Kb)

On synthesizing distributed firewall configurations considering risk, usability and cost constraints
Bin Zhang; Ehab Al-Shaer
2011 7th International Conference on Network and Service Management
Year: 2011
Pages: 1 - 8
IEEE Conference Publications

Abstract (209 Kb)

A cross-domain privacy-preserving protocol for cooperative firewall optimization
Fei Chen; Bezawada Bruhadeshwar; Alex X. Liu
2011 Proceedings IEEE INFOCOM
Year: 2011
Pages: 2903 - 2911
Cited by: Papers (2)
IEEE Conference Publications

Abstract (638 Kb)

Using Genetic Algorithm to Improve an Online Response System for Anomaly Traffic by Incremental Mining
Ming-Yang Su; Sheng-Cheng Yeh; Chun-Yuen Lin; Chen-Han Tsai
International Symposium on Parallel and Distributed Processing with Applications
Year: 2010
Pages: 582 - 587
IEEE Conference Publications

Abstract (281 Kb)

Lightweight Traffic-Aware Packet Classification for Continuous Operation
Shariful Hasan Shaikot; Min Sik Kim
2010 10th IEEE/IPSJ International Symposium on Applications and the Internet
Year: 2010
Pages: 59 - 67
Cited by: Papers (1)
IEEE Conference Publications

Abstract (713 Kb)

Dynamic Policy-Based Routing Using Firewall Rules
Kavin Tantipongsakul; Akharin Khunkitti
2009 Third UKSim European Symposium on Computer Modeling and Simulation
Year: 2009
Pages: 540 - 545
IEEE Conference Publications

Abstract (574 Kb)

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Firewall Policy Queries
Alex X. Liu; Mohamed G. Gouda
IEEE Transactions on Parallel and Distributed Systems
Year: 2009, Volume: 20, Issue: 6
Pages: 766 - 777
Cited by: Papers (32)
IEEE Journals & Magazines

Abstract (1800 Kb)

Taichi: An Open Intrusion Automatic Response System Based on Plugin
Hong Han; Xian-liang Lu; Li-yong Ren; Bo Chen
2006 International Conference on Machine Learning and Cybernetics
Year: 2006
Pages: 68 - 77
Cited by: Papers (1)
IEEE Conference Publications

Abstract (319 Kb)

Firewall Rule Ordering Based on Statistical Model
Weiping Wang; Heran Chen; Jiayao Chen; Bowen Liu
2009 International Conference on Computer Engineering and Technology
Year: 2009, Volume: 2
Pages: 185 - 188
Cited by: Papers (3)
IEEE Conference Publications

Abstract (140 Kb)

Adaptive optimization of packet filtering devices performance ensuring a conflict-free network configuration
Gianluca Maiolini; Lorenzo Cignini; Andrea Baiocchi
IEEE INFOCOM Workshops 2008
Year: 2008
Pages: 1 - 6
Cited by: Patents (1)
IEEE Conference Publications

Abstract (257 Kb)

Dynamic Balancing of Packet Filtering Workloads on Distributed Firewalls
Guannua Yan; Songqing Chen; Stephan Eidenbenz
2008 16th International Workshop on Quality of Service
Year: 2008
Pages: 209 - 216
Cited by: Papers (1)
IEEE Conference Publications

Abstract (232 Kb)

Network Security Policies: Verification, Optimization and Testing
E. Al-Shaer
2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006
Year: 2006
Pages: 584 - 564
Cited by: Papers (2)
IEEE Conference Publications

(80 Kb)

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Abstract

Barbarians in the Gate: An Experimental Validation of NIC-based Distributed Firewall Performance and Flood Tolerance
M. Ihde, W. H. Sanders
International Conference on Dependable Systems and Networks (DSN'06)
Year: 2006
Pages: 209 - 216
Cited by: Papers (2)
IEEE Conference Publications

Abstract (199 Kb)

A multi-dimensional packet classifier for NP-based firewalls
M. J. Rashti; H. R. Rabiee; A. Foroutan; M. Lavasani
2004 International Symposium on Applications and the Internet. Proceedings.
Year: 2004
Pages: 250 - 254
Cited by: Patents (13)
IEEE Conference Publications

Abstract (246 Kb)

Multilevel early packet filtering technique based on traffic statistics and splay trees for firewall performance improvement
Zouheir Trabelsi; Safaa Zeidan
2012 IEEE International Conference on Communications (ICC)
Year: 2012
Pages: 1074 - 1078
Cited by: Papers (6)
IEEE Conference Publications

Abstract (487 Kb)

« First < 1 > Last »

IEEE Account
» Change Username/Password
» Update Address

Purchase Details
» Payment Options
» Order History
» View Purchased Documents

Profile Information
» Communications Preferences
» Profession and Education
» Technical Interests

Need Help?
» **US & Canada:** +1 800 678 4333
» **Worldwide:** +1 732 981 0060
» Contact & Support

About IEEE *Xplore* | Contact Us | Help | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2017 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L18	16	l15 or l16 or l17	US-PGPUB	ADJ	ON	2017/10/10 11:07
L17	5	(US-20060248580-$ or US-20070115916-$ or US-20030179703-$ or US-20100100468-$).did. or (US-8397282-$).did.	US-PGPUB; USPAT	ADJ	ON	2017/10/10 11:07
L16	5	(US-20020069200-$ or US-20100100954-$ or US-20020078382-$ or US-20020152209-$ or US-20080062994-$).did.	US-PGPUB	ADJ	ON	2017/10/10 11:07
L15	7	(US-20010039576-$ or US-20090125470-$ or US-20100199346-$ or US-20040177139-$ or US-20020154635-$ or US-20020198981-$ or US-20060013136-$).did.	US-PGPUB	ADJ	ON	2017/10/10 11:07
L14	8	(US-20020069200-$ or US-20120185913-$ or US-20150033285-$ or US-20100100954-$ or US-20020078382-$ or US-20020152209-$ or US-20080062994-$).did. or (US-8478852-$).did.	US-PGPUB; USPAT	ADJ	ON	2017/10/10 10:45
L13	55	H04L63/20.CPC. and (policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall or traffic) with (reorder$9 or delet$9 or remov$9 or replac$9) with (realtime or real time OR DYNAMIC)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/10 10:44
L11	637	(policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall or traffic) with (reorder$9 or delet$9 or remov$9 or replac$9) with (realtime or real time OR DYNAMIC$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/10 10:43
L10	471	(policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall or traffic) with (reorder$9 or delet$9 or remov$9 or replac$9) with (realtime or real time OR DYNAMIC)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/10 10:43
L9	11356	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/10 10:43
S59	1	"20060248580" .PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 11:37
S58	32	("20020038339" | "7089581" | "20050125697" | "20050251570" | "7227842" | "7237267" | "20100199346" | "20110055923" | "20060195896" | "7237267" | "20040010712" | "20040177139" | "7107613" | "20020198981" | "20100303240" | "6662235" | "20080301765" | "20090138938" | "7954143" | "20020165949" | "20030120622" | "6484261" |	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 11:36

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

		"20110055916" | "6098172" | "6484261" | "7089581" | "7299353" | "7331061" | "20100011433" | "20060070122" | "20040193943" | "7263099" | "20050010765" | "20050229246" | "20060104202" | "6662235").PN.				
S57	147	(policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall or traffic) with (reorder$9 or delet$9 or remov$9 or replac$9) with (realtime or real time)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:49
S56	667	(policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall or traffic) with (reconfigur$9 or updat$9 or reorder$9 or delet$9 or remov$9 or replac$9) with (realtime or real time)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:49
S55	36	(policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall or traffic) with (reorder$9 or reconfigur$9 or updat$9) with (realtime or real time) with (delet$9 or remov$9 or replac$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:44
S54	1570	(policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall or traffic) with (reorder$9 or configur$9 or updat$9) with (realtime or real time)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:43
S53	7	H04L63/20.CPC. and (policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall or traffic) with optimiz$9 with (realtime or real time)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:27
S52	0	H04L63/0263.CPC. and (policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall or traffic) with optimiz$9 with (realtime or real time)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:27
S51	10806	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:27
S50	2404	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:27
S49	233	(policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall or traffic) with optimiz$9 with (realtime or real time)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:26
S48	214	(policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall) with optimiz$9 with (realtime or real time)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:26
S47	1784	(policy or policies or filter$9 or rule) with (traffic or firewall) with optimiz$9	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:09
S46	876	(policy or policies or filter$9 or rule) with (traffic or firewall) with (updat$9 or optimiz$9 or adjust$9 or reorder$9) with (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:09
S45	9	("20020038339" | "7089581" | "20050125697" | "20050251570" | "7227842" | "7237267" | "20100199346" |	US-PGPUB; USPAT;	ADJ	ON	2017/05/24 10:01

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

		"20110055923" | "20060195896" | "7237267" | "20040010712" | "20040177139" | "7107613" | "20020198981" | "20100303240" | "6662235" | "20080301765" | "20090138938" | "7954143" | "20020165949" | "20030120622" | "6484261" | "20110055916" | "6098172" | "6484261" | "7089581" | "7299353" | "7331061" | "20100011433" | "20060070122" | "20040193943" | "7263099" | "20050010765" | "20050229246" | "20060104202" | "6662235").PN. and (realtime or real time)	EPO			
S44	27	("20020038339" | "7089581" | "20050125697" | "20050251570" | "7227842" | "7237267" | "20100199346" | "20110055923" | "20060195896" | "7237267" | "20040010712" | "20040177139" | "7107613" | "20020198981" | "20100303240" | "6662235" | "20080301765" | "20090138938" | "7954143" | "20020165949" | "20030120622" | "6484261" | "20110055916" | "6098172" | "6484261" | "7089581" | "7299353" | "7331061" | "20100011433" | "20060070122" | "20040193943" | "7263099" | "20050010765" | "20050229246" | "20060104202" | "6662235").PN. and (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:01
S43	32	("20020038339" | "7089581" | "20050125697" | "20050251570" | "7227842" | "7237267" | "20100199346" | "20110055923" | "20060195896" | "7237267" | "20040010712" | "20040177139" | "7107613" | "20020198981" | "20100303240" | "6662235" | "20080301765" | "20090138938" | "7954143" | "20020165949" | "20030120622" | "6484261" | "20110055916" | "6098172" | "6484261" | "7089581" | "7299353" | "7331061" | "20100011433" | "20060070122" | "20040193943" | "7263099" | "20050010765" | "20050229246" | "20060104202" | "6662235").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 09:59
S42	20	(policy or policies or filter$9) with (packet or flow or traffic) with rule with (optimiz$9) with (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 09:54
S41	36	(policy or policies or filter$9 or rule) with (packet or flow or traffic) with firewall with (updat$9 or optimiz$9 or adjust$9) with (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 09:42
S40	110	(policy or policies or filter$9) with (packet or flow or traffic) with rule with (updat$9 or optimiz$9 or adjust$9) with (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 09:41
S39	642	(policy or policies or filter$9) with (packet or flow or traffic) same rule same (updat$9 or optimiz$9 or adjust$9) same (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 09:41
S38	1276	(policy or policies or filter$9) same (packet or flow or traffic or firewall) same rule same (updat$9 or optimiz$9 or adjust$9) same	US-PGPUB; USPAT;	ADJ	ON	2017/05/24 09:41

		(realtime or real time or dynamic$9)	EPO			
S37	1201	(policy or policies or filter$9) same (packet or flow or traffic) same rule same (updat$9 or optimiz$9 or adjust$9) same (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 09:41
S36	35	H04L63/20.CPC. and (policy or policies) and (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 21:59
S35	89	(policy or policies) WITH (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:32
S34	84	(policy or policies) WITH (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical) and network$9	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:18
S33	89	(policy or policies) WITH (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:18
S32	24	(policy or policies) and (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical) with (parameter oR (source adj3 address$5) or (destination adj3 address$5))	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:15
S31	635	(policy or policies) and (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:11
S30	22	(policy or policies or filter$9) same (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical) with (parameter or address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 16:57
S29	1	"20100100954".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:34
S28	6	(policy or policies or filter$9) same (packet or flow or traffic) same rule same (delet$5 or remov$9) same (obsolete or redundan$5 or old) same (optimiz$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:33
S27	87	(policy or policies or filter$9) same (packet or flow or traffic) same rule same (delet$5 or remov$9) same (obsolete or redundan$5 or old)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:33
S26	10052	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:32
S25	1	"8478852".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:31
S24	1	"20100318812".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/11 16:14

S22	1	"20150033285".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 18:02
S21	1	"20120185913" .pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 17:56
S20	1	"20020069200".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 17:56
S19	60	H04L63/20.CPC. and (policy or policies or filter$9) same (packet or flow or traffic) same (group or grouped or grouping or delet$5 or remov$9 or reorder$9) with (rule) same (use or usage or statistic or weight)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 17:53
S18	409	(policy or policies or filter$9) same (packet or flow or traffic) same (group or grouped or grouping or delet$5 or remov$9 or reorder$9) with (rule) same (use or usage or statistic or weight)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 16:48
S17	2458	(policy or policies or filter$9) same (packet or flow or traffic) same (group or grouped or grouping or delet$5 or remov$9 or reorder$9) with (rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 16:47
S16	11	H04L63/0263.CPC. and (rule) same (depend$9) same (compatib$9 or conflict$9) and (packet or flow or traffic) and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5) and order$5	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/23 00:02
S15	1	"20060013136".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 22:07
S14	1	"20020198981".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 21:15
S13	14	(supernet$9) same (ip or internet protocol) same address$5 same source same destination	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 20:50
S12	281	(rule) same (depend$9) same (compatib$9 or conflict$9) and (packet or flow or traffic) and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5) and order$5	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:22
S11	185	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5) and order$5	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:21
S10	185	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:20

S9	212	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:20
S8	10	H04L63/0263.CPC. and (rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 14:10
S7	311	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 14:10
S6	9	("5889953" | "6041347" | "6170009" | "6418468" | "6463470" | "6587466" | "6601082" | "6611863").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 12:22
S5	1	"20010039576".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 12:20
S4	1	"7441022".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 12:11
S3	2021	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/20 14:34
S2	590	fortinet.as.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/20 14:33
S1	1	(pernicha adj3 hugo).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/20 14:33

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L8	4	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND (revers$9 or undo or undone or undoing) AND (delet$9 or remov$9 or eras$9 or updat$9)).CLM.	US-PGPUB; USPAT	ADJ	ON	2017/10/10 10:42
L7	2	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND (revers$9 or undo or undone or undoing) AND (delet$9 or remov$9 or eras$9)).CLM.	US-PGPUB; USPAT	ADJ	ON	2017/10/10 10:42
L6	1	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND log AND (delet$9 or remov$9 or eras$9) AND updat$9).CLM.	US-PGPUB; USPAT	ADJ	ON	2017/10/10 10:42
L5	1	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND log AND (delet$9 or remov$9 or eras$9) AND depend$9 AND (rout$9 or	US-PGPUB; USPAT	ADJ	ON	2017/10/10 10:42

		flow)).CLM.				
L4	2	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND log AND (delet$9 or remov$9 or eras$9) AND depend$9).CLM.	US-PGPUB; USPAT	ADJ	ON	2017/10/10 10:41
L3	3	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND log AND (delet$9 or remov$9 or eras$9 or reduc$9 or group or grouped or grouping) AND (reorder$9 or priori$9)).CLM.	US-PGPUB; USPAT	ADJ	ON	2017/10/10 10:41
L2	4	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND log AND (delet$9 or remov$9 or eras$9)).CLM.	US-PGPUB; USPAT	ADJ	ON	2017/10/10 10:40
L1	1	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND log AND (undone or undo or revers$5)).CLM.	US-PGPUB; USPAT	ADJ	ON	2017/10/10 10:40

10/ 10/ 2017 11:35:08 AM
C:\ Users\ kchang3\ Documents\ EAST\ Workspaces\ 14566403_APP.wsp

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 7209

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/566,403	12/30/2014	726	2438	FORT-012500

APPLICANTS
Fortinet, Inc., Sunnyvale, CA;

INVENTORS
Hugo Filipe Parreira Pernicha, Venda do Pinheiro, PORTUGAL;

**** CONTINUING DATA ***************************

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****
12/23/2014

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ Yes ☑ No	☐ Yes ☑ No	/KENNETH W CHANG/ Examiner's Signature	Initials	PORTUGAL	9	26	3

ADDRESS

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
12640 W. Cedar Drive, Suite 1
LAKEWOOD, CO 80228
UNITED STATES

TITLE

DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

FILING FEE RECEIVED		
2080	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14566403	PERNICHA, HUGO FILIPE PARREIRA
	Examiner	Art Unit
	KENNETH CHANG	2438

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/0263	7/20/2016	KC
H04L63/20	1/24/2017	KC
H04L63/0263	5/24/2017	KC
H04L63/20	5/24/2017	KC
H04L63/20	10/10/2017	KC

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

SEARCH NOTES		
Search Notes	Date	Examiner
Searched Inventors' Names and Assignee on eDan and EAST.	7/20/2016	KC
Searched IEEE NPL Xplore Database online.	7/20/2016	KC
Completed Limited Classified Search in CPC on EAST USPAT, PGPUB, and EPO databases with Keywords.	7/22/2016	KC
Keywords Searched: See East search history.	7/22/2016	KC
H04L63/20	1/24/2017	KC
Updated Limited Classified Search in CPC on EAST USPAT, PGPUB, and EPO databases with Keywords. See East Search History.	1/28/2017	KC
Updated Keywords: See East search history.	1/28/2017	KC
Updated NPL search on IEEE Xplore Database online	5/24/2017	KC
Updated Limited Classified Search in CPC on EAST USPAT, PGPUB, and EPO databases with Keywords. See East Search History.	5/24/2017	KC

	/KENNETH CHANG/ Primary Examiner.Art Unit 2438

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
Updated Limited Classified Search in CPC on EAST USPAT, PGPUB, and EPO databases with Keywords. See East Search History.	10/10/2017	KC
Updated NPL search on IEEE Xplore Database online.	10/10/2017	KC
Interference Search Completed on US-PGPUB and USPAT with claim language search. See EAST SEARCH HISTORY for interference searches.	10/10/2017	KC

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND log AND (undone or undo or revers$5)).CLM.	10/10/2017	KC
	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND log AND (delet$9 or remov$9 or eras$9 or reduc$9 or group or grouped or grouping) AND (reorder$9 or priori$9)).CLM.	10/10/2017	KC
	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND log AND (delet$9 or remov$9 or eras$9)).CLM.	10/10/2017	KC
	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND log AND (delet$9 or remov$9 or eras$9) AND depend$9).CLM.	10/10/2017	KC
	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND log AND (delet$9 or remov$9 or eras$9) AND depend$9 AND (rout$9 or flow)).CLM.	10/10/2017	KC
	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND log AND (delet$9 or remov$9 or eras$9) AND updat$9).CLM.	10/10/2017	KC
	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND (revers$9 or undo or undone or undoing) AND (delet$9 or remov$9 or eras$9)).CLM.	10/10/2017	KC
	(traffic AND (policy or policies) AND rule AND (set or subset) AND optimiz$9 AND security AND network AND (revers$9 or undo or undone or undoing) AND (delet$9 or remov$9 or eras$9 or updat$9)).CLM.	10/10/2017	KC

	/KENNETH CHANG/ Primary Examiner.Art Unit 2438

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14566403	PERNICHA, HUGO FILIPE PARREIRA
	Examiner	**Art Unit**
	KENNETH CHANG	2438

CPC						
Symbol					**Type**	**Version**
H04L		63	/	20	F	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	26	
/KENNETH CHANG/ Primary Examiner.Art Unit 2438	10/10/2017	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5A

U.S. Patent and Trademark Office — Part of Paper No. 20171010

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14566403	PERNICHA, HUGO FILIPE PARREIRA
	Examiner	**Art Unit**
	KENNETH CHANG	2438

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
		H 0 4 L 29 / 06 (2006.01.01)	

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 26	
/KENNETH CHANG/ Primary Examiner.Art Unit 2438 (Primary Examiner)	10/10/2017 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 5A

U.S. Patent and Trademark Office — Part of Paper No. 20171010

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14566403	PERNICHA, HUGO FILIPE PARREIRA
	Examiner	**Art Unit**
	KENNETH CHANG	2438

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	26	
/KENNETH CHANG/ Primary Examiner.Art Unit 2438	10/10/2017	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5A

U.S. Patent and Trademark Office Part of Paper No. 20171010

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/566,403	Filing Date 12/30/2014	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 09/29/2017

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 26	Minus	** 26	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
NICOLE NICHOLSON

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Fortinet, Inc.	Examiner: Chang, Kenneth W
Inventons: Pernicha et al.	Group Art Unit: 2438
App. No.: 14/566,403	Conf. No.: 7209
Filed: December 30, 2014	Docket No.: FORT-012500
For: DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT	

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO OFFICE ACTION

Sir/Madam:

In response to the Office Action having a notification date of May 30, 2017 (the "Office Action"), the Applicant respectfully requests the Examiner to enter the following amendment and to consider the following remarks:

Amendments to the Claims are reflected in the listing of claims, which begins on page 2 of this paper.

Remarks begin on page 8 of this paper.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Amendments to the Claims

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. **(Currently amended)** A method comprising:

receiving, by a network security management device, a request to add a new traffic flow policy rule to a plurality of policy rules managed by the network security management device;

automatically determining, by the network security management device, dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules;

forming, by the network security management device, an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules based on the determined dependencies; and

automatically optimizing, by the network security management device, the updated set of policy rules by ~~one or more of~~ grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein the optimizing is based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules, wherein the optimizing by the network security management device is performed in real time, wherein the network security management device is configured to maintain a log of changes to the policy rules enabling the optimizing to be undone.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

2. **(Original)** The method of claim 1, wherein said determining dependencies comprises evaluating dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules.

3. **(Currently amended)** The method of claim 1, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging is conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules, and wherein the network security management device is configured to demerge at least some of the merged policy rule from the single policy rule.

4. **(Original)** The method of claim 3, wherein the merging of combinable policy rules is conducted based on superneting of one or more of the source IP addresses and the destination IP addresses.

5. **(Original)** The method of claim 1, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of policy rules based on one or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters.

6. **(Original)** The method of claim 5, wherein the order of the policy rules of the second sub-set of policy rules is changed based on frequency of usage thereof.

7. **(Original)** The method of claim 1, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

8. **(Original)** The method of claim 7, wherein the one or more conflicts include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules.

9. **(Original)** The method of claim 7, wherein the one or more conflicts include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule.

10. **(Original)** The method of claim 1, wherein the one or more weights are defined manually based on scope and attributes of policy rule.

11. **(Original)** The method of claim 1, wherein the one or more weights are defined automatically.

12. **(Original)** The method of claim 1, wherein said forming an updated set of policy rules is conducted based on the one or more weights, the preference settings, the priority settings for the policy rules, network traffic characteristics, and network usage statistics.

13. **(Currently amended)** A network security policy management system comprising:

one or more processors; and

one or more internal data storage devices operatively coupled to the one or more processors and storing:

a business traffic flow input module configured to receive a request to add a new traffic flow policy rule to a plurality of policy rules managed by the system;

a dependency detection module configured to automatically determine dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules;

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

a traffic flow policy rule incorporation module configured to form an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules based on the determined dependencies; and

a policy rule optimization module configured to automatically optimize the updated set of policy rules by ~~one or more of~~ grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein the optimizing is performed in real-time based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules, and wherein the policy rule optimization module is configured to maintain a log of changes to the policy rules enabling the optimizing to be undone.

14. **(Original)** The system of claim 13, wherein the dependency detection module is further configured to evaluate dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules.

15. **(Original)** The system of claim 13, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging is conducted based on matching of one or more of source IP addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

16. **(Original)** The system of claim 15, wherein the merging of combinable policy rules is conducted based on superneting of one or more of the source Internet Protocol (IP) addresses and the destination IP addresses.

17. **(Original)** The system of claim 13, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

policy rules based on one or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters.

18. **(Original)** The system of claim 13, wherein said deleting the third sub-set of policy rules comprises deleting the policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules.

19. **(Original)** The system of claim 18, wherein the one or more conflicts include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules.

20. **(Original)** The system of claim 18, wherein the one or more conflicts comprise one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule.

21. **(Original)** The system of claim 13, wherein the one or more weights are defined manually based on scope and attributes of the policy rule.

22. **(Original)** The system of claim 13, wherein the one or more weights are defined automatically.

23. **(Currently amended)** A network security policy management system comprising:

one or more processors; and

one or more internal data storage devices operatively coupled to the one or more processors and storing a policy rule optimization module configured to retrieve information regarding a current set of policy rules and optimize the current set of policy rules by grouping a first sub-set of policy rules of the current set of policy rules, reordering a second sub-set of policy rules of the current set of

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

policy rules, and deleting a third sub-set of policy rules of the current set of policy rules, wherein the optimizing is performed in real-time based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and usage statistics for each policy rule of the current set of policy rules, wherein the policy rule optimization module is configured to maintain a log of changes to the policy rules enabling the optimizing to be undone.

24. **(Original)** The system of claim 23, wherein said grouping the first sub-set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging is conducted based on matching of one or more of source IP addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

25. **(Original)** The system of claim 23, wherein said reordering the second sub-set of policy rules comprises changing an order of the policy rules of the second sub-set of policy rules based on one or more of their source Internet Protocol (IP) addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters.

26. **(Original)** The system of claim 23, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the retrieved set of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Remarks

The Applicant respectfully requests reconsideration of this application in view of the following remarks. Claims 1-26 are pending, with claims 1, 13 and 23 being independent. Claims 1, 3, 13 and 23 have been amended. Support for the amendments can be found at least in paragraphs [0056] and [0058]. No new subject matter has been added.

Claims 1, 2, 5, 13, 14, and 17 stand rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada (US 20010039576 A1) in view of Yang (US 20100100954 A1), and further in view of Fulp et al. (US 20060248580 A1, hereinafter Fulp).

Claims 3 and 15 stand rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Yang and Fulp as applied to Claims 1 and 13, and further in view of Porat (US 20080062994 A1).

Claims 4 and 16 stand rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Yang, Fulp and Porat as applied to Claims 3 and 13, and further in view of Liu (US 20020154635 A1).

Claim 6 stands rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Yang and Fulp as applied to Claim 1, and further in view of Corl et al. (US 20020198981 A1, hereinafter Corl).

Claims 7-11 and 18-22 stand rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Yang and Fulp as applied to Claims 1 and 13, and further in view of Goldschmidt et al. (US 20060013136 A1, hereinafter Goldschmidt).

Claim 12 stands rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Yang and Fulp as applied to Claim 1, and further in view of Goldschmidt and Corl.

Claims 23-25 stand rejected under 35 U.S.C. 103 as allegedly being unpatentable over Yang in view of Porat, and further in view of Fulp.

Claim 26 stands rejected under 35 U.S.C. 103 as allegedly being unpatentable over Yang in view of Porat and Fulp, and further in view of Goldschmidt.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

The independent claims, as amended, include a device or module that is configured to maintain a log of changes to the policy rules, enabling the optimizing to be undone. The Office Action acknowledges that Kanada does not disclose a network security management device automatically optimizing a set of policy rules. The undersigned does not find any teaching or suggestion in Kanada directed to undoing optimization of asset of policy rules, nor to maintaining a log that enables such undoing to be performed.

The Office Action alleges that Yang discloses a network security management device automatically optimizing an updated set of policy rules, referring to Yang, ¶ [0014] which teaches a method for parsing firewall configuration and security policy files to enable firewall rule reduction, and ¶ [0029] which teaches the removal, after 90 days, of unused firewall rules of each external partner network, and ¶ [0030] which teaches placing a more frequently used firewall rule at a higher position in a firewall access list in firewall configuration and security policy files.

However, Yang does not teach or suggest the undoing of any of these operations, nor maintaining a log that enables the undoing of any of these operations. As presently understood by the undersigned, Yang does disclose the use of firewall access logs which can be analyzed to identify obsolete and unused firewall rules so that these obsolete firewall rules can be removed. (See Yang, Abstract) While Yang's firewall access logs are used to "enable firewall rule reduction" (Yang, ¶ [0019]), the log tracks accesses to the firewall, not changes to firewall rules. For example, Yang ¶ [0022] teaches that entries in the firewall access logs represent accepted and rejected firewall access sessions. Entries in the firewall access logs are then matched to firewall rules to generate a count of the usage frequency of matched rules (¶¶ [0024]-[0025]) It is clear that Yang's firewall access logs are not a log of changes to the policy rules which enable optimizations of the policy rules to be undone.

As presently understood by the undersigned, Fulp teaches firewall policy optimization that sorts firewall policies in order of non-increasing probability of receiving a packet matching the rule. (Fulp, Abstract) Fulp does disclose a rule list (see ¶ [0050]), but this is an ordered set of rules in a policy, not a log of optimizations made to

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

the policy. Fulp ¶ [0109] teaches that "firewall policy optimizer 1514 may utilize any of the methods described herein to rearrange rules and improve firewall performance. Rules may be tested for rearrangement at user-specified intervals or when average number of packet comparisons increases by a user-specified amount." While Fulp could perform repeated optimizations which would change the rules in a policy, this is not an undo or a return to a prior state as taught in ¶ [0058] of the specification, nor does it teach a log of changes to policy rules made during optimization.

For at least these reasons, the independent claims are believed allowable over the cited references. Reconsideration and allowance are respectfully requested.

The dependent claims depend upon independent claims which are allowable over the cited art as discussed above. These dependent claims are likewise in condition for allowance at least because they depend on allowable independent claims. However, the dependent claims are believed independently allowable at least in that they recite particular features which, when combined with the elements of the independent claim, are not disclosed or suggested in the cited references.

For example, claim 3, as amended, requires that the network security management device be configured to demerge at least some of the merged policy rules from the single policy rule. As discussed above, the cited references do not disclose reversing or undoing policy optimizations. They also do not disclose or suggest demerging policy rules that have been merged during optimization.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Conclusion

The undersigned respectfully submits that the amendments and remarks presented herein have overcome the rejections, and that the pending claims are in condition for allowance. Accordingly, the undersigned requests that the rejections be withdrawn and that a Notice of Allowance be promptly issued for claims 1-26.

By responding in the foregoing remarks only to particular positions taken by the Examiner, the Applicant does not acquiesce with any other positions that have not been explicitly addressed. Applicant's arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist. The absence of a reply to a specific rejection, issue or comment set forth in the Office Action does not signify agreement with or concession of that rejection, issue or comment. In addition, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, and the amendment of any claim does not necessarily signify any concession of unpatentability of the claim prior to its amendment.

In view of the foregoing, the Applicant respectfully asserts that all claims now pending in the application are in condition for allowance. Hence, an early allowance of all such claims is earnestly requested.

Respectfully submitted,
Hamilton, DeSanctis & Cha LLP

By /Guy K. Clinger/
Guy K. Clinger
Reg. No. 42,422
Customer No. 64128
Ph: 720-446-1888

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Electronic Acknowledgement Receipt	
EFS ID:	30529834
Application Number:	14566403
International Application Number:	
Confirmation Number:	7209
Title of Invention:	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT
First Named Inventor/Applicant Name:	Hugo Filipe Parreira Pernicha
Customer Number:	64128
Filer:	Guy Kenneth Clinger
Filer Authorized By:	
Attorney Docket Number:	FORT-012500
Receipt Date:	29-SEP-2017
Filing Date:	30-DEC-2014
Time Stamp:	22:49:20
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		FORT-012500Response3.pdf	42130 163bfd03dd34daad92497cd126d65779f25b0785	yes	11

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	7
	Applicant Arguments/Remarks Made in an Amendment	8	11
Warnings:			
Information:			
	Total Files Size (in bytes):	42130	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Electronic Patent Application Fee Transmittal					
Application Number:	14566403				
Filing Date:	30-Dec-2014				
Title of Invention:	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT				
First Named Inventor/Applicant Name:	Hugo Filipe Parreira Pernicha				
Filer:	Michael A. DeSanctis				
Attorney Docket Number:	FORT-012500				
Filed as Large Entity					
Filing Fees for Utility under 35 USC 111(a)					
Description		**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:					
Pages:					
Claims:					
Miscellaneous-Filing:					
Petition:					
Patent-Appeals-and-Interference:					
Post-Allowance-and-Post-Issuance:					
Extension-of-Time:					

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 1 month with $0 paid	1251	1	200	200
Miscellaneous:				
		Total in USD ($)		**200**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Electronic Acknowledgement Receipt	
EFS ID:	30510359
Application Number:	14566403
International Application Number:	
Confirmation Number:	7209
Title of Invention:	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT
First Named Inventor/Applicant Name:	Hugo Filipe Parreira Pernicha
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-012500
Receipt Date:	28-SEP-2017
Filing Date:	30-DEC-2014
Time Stamp:	17:08:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$200
RAM confirmation Number	092917INTEFSW17092900
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Fee Worksheet (SB06)	fee-info.pdf	30542 5466c9dd89046e071e61e8af7bcda961f09eb871	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	30542		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/566,403	12/30/2014	Hugo Filipe Parreira Pernicha	FORT-012500	7209

64128 7590 05/30/2017

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

EXAMINER	
CHANG, KENNETH W	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
05/30/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mdesanctis@hdciplaw.com
docket@hdciplaw.com

PTOL-90A (Rev. 04/07)

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Office Action Summary	Application No. 14/566,403	Applicant(s) PERNICHA, HUGO FILIPE PARREIRA	
	Examiner Kenneth Chang	Art Unit 2438	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05/02/2017*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-26* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-26* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

1. This non-final office action is in response to applicant's Request for Continued Examination filed on 05/02/2017. Claims 1, 13, and 23 have been amended. **Claims 1-26** are currently pending and have been considered as follows.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/02/2017 has been entered.

Notice of Pre-AIA or AIA Status

3. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

4. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Response to Arguments

5. Applicant's amendment of independent Claims 1, 13, and 23 have changed the scope of the claimed invention thereby necessitating new ground(s) of rejection.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Therefore, Applicant's arguments on page 9 of the remarks filed on 05/02/2017 with respect to the 35 U.S.C. §103 rejections have been fully considered but are moot because the arguments do not apply to the updated reference(s) being used in the current rejection.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

7. **Claims 1, 2, 5, 13, 14, and 17** are rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** (US 20010039576 A1) in view of **YANG** (US 20100100954 A1), and further in view of Fulp et al. (US 20060248580 A1, hereinafter **Fulp**).

As to Amended Claim 1:

Kanada discloses a method **(e.g. Kanada FIG. 5; [0002] methods; [0093])** comprising:

- receiving, by a network security management device **(e.g. Kanada policy server with operator console [0066]; [0067])**, a request to add a new traffic flow policy rule to a plurality of policy rules **(e.g. Kanada rule specified to be added [0021]; receiving input to add policy rule [0067])** managed by the network security management device;
- automatically determining, by the network security management device, dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules **(e.g. Kanada detects policy rules that the new policy rule**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

depends on [Abstract]; analyzing policy rules for dependence of policy rule data on another policy rule data [0028]; [0068]; [0099]; [0103]; [0167]);

- forming, by the network security management device, an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules **(e.g. Kanada add and store input policy rules into policy repository [0067]; [0070]; [0071]; rule table contains all input rules [0087]; list of rule identifiers and added rule sent to router [0099])** based on the determined dependencies;

But **Kanada** does not specifically disclose:

- automatically optimizing, by the network security management device, the updated set of policy rules by **one** or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, ***wherein the optimizing is based on one*** or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules;
- wherein the optimizing by the network security management device is performed in real time.

However, the analogous art **YANG** does disclose automatically optimizing, by the network security management device, the updated set of policy rules **(e.g. YANG firewall rule reduction [0014] for performance enhancement [0029] and reducing**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

overall parsing time [0030]; by the firewall rules reduction module [0032]) by **one** or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules **(e.g. YANG removing unused obsolete rules [0005]; [0029]; placing order of the rules in the firewall configuration [0029]; more frequently used firewall rule placed higher position [0030])**, wherein the optimizing is based on **one** or more of weights assigned to particular types of traffic, preference settings, priority settings **(e.g. YANG placing order of the rules in higher position is based on access count for each rule [0029]; more frequently used firewall rule placed higher position [0030])**, network traffic characteristics **(e.g. YANG identifies existing firewall rules that have been used recently and marked valid on a per external partner network basis [0029]; firewall rule network attributes including source IP, destination IP address, direction, incoming or outgoing [0016]; identified IP addresses [0017])** and usage statistics for each policy rule **(e.g. YANG access count for each valid rule [0029]; [0030])** of the updated set of policy rules. Furthermore, the analogous art **Fulp** does disclose wherein the optimizing by the network security management device is performed in real time **(e.g. control node includes a firewall policy optimizer that measures current rule configuration and dynamically reorders firewall rules to rearrange rules and improve firewall performance [0109])**. **Kanada**, **YANG**, and **Fulp** are analogous art because they are from the same field of endeavor in management of network firewall rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

- (e.g. see **YANG**, "In step 220, the method uses the parsed information to identify all existing firewall rules on a per external partner network basis. In other words, the method identifies, for each external partner network, its routable network address space and all the existing firewall rules associated with that particular external partner network. Firewall rule may comprise attributes that includes, but are not limited to, source IP address, destination IP address, protocol used (e.g., TCP or UDP, etc), protocol port number, direction (e.g., incoming or outgoing) etc" **[0016]**; see also "the method uses the parsed information to identify the permitted IP address space on a per external partner network basis. In other words, the method identifies, for each external partner network, all the valid IP source and destination addresses permitted for access by that particular external partner network" **[0017]**; see also "Once method 300 is executed, it produces an output that identifies all existing firewall rules that have been used recently and marked valid on a per external partner network basis. Therefore, for the existing firewall rules of each external partner network that have not been marked valid, they are considered obsolete or unused rules. In one embodiment, it is reasonable to assume that an unused rule for a predefined period of time, e.g., 90 days or more should be removed. The length of the unused period of time threshold of an unused rule is a configurable parameter set by the network operator. The output also produces the access count for each valid rule for each external partner network. The access count for each individual rule can be used as a reference for the activities associated to the rule as well as the placing order

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

of the rule in the firewall configuration and security policy files for performance enhancement" **[0029]**; see also "For instance, more frequently used firewall rule should be placed at a higher position in the firewall access list in the firewall configuration and security policy files to reduce overall parsing time during normal operations of the firewall system" **[0030]**);

- (e.g. see **FuIp**, "A firewall rule set that is optimized using the subject matter described herein may be implemented on any firewall system that includes one or more firewalls. For example, an optimized firewall rule set according to embodiments of the subject matter described herein may be implemented using any of the hierarchical, multi-node firewall systems… A control node 1512 may include a firewall policy optimizer 1514 that measures the average number of comparisons per packets for the current rule configuration and may dynamically reorder the rules to reduce the average number of comparisons per packet. For example, firewall policy optimizer 1514 may utilize any of the methods described herein to rearrange rules and improve firewall performance" **[0109]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, and **FuIp** before him or her, to modify the invention of **Kanada** with the teachings of **YANG** and **FuIp** to include *automatically optimizing, by the network security management device, the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the*

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

updated set of policy rules, wherein the optimizing is based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules and wherein the optimizing by the network security management device is performed in real time as claimed because **Kanada** provides a network system including a server and routers for management of network policy rules that may be added, deleted, and/or updated **(Kanada [0021]-[0137])** which could include automatic optimization by ordering more frequently used firewall rules in higher positions and removing obsolete or unused rules based on access counts and external partner network attributes **(YANG [0016]; [0017]; [0029]; [0030])** and dynamically optimizing based on measuring current rule configuration and comparing to rearranged rules performance **(FuIp [0109])**. The suggestion/motivation for doing so would have been for performance enhancement and to reduce overall parsing time during normal operations of the firewall system **(YANG [0029]; [0030])** and to significantly improve firewall performance and lower packet delay **(FuIp [0010]; [0109])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, and **FuIp** to obtain the invention as specified in the instant claim(s).

As to Claim 2:

Kanada in view of **YANG** and **FuIp** discloses the method of claim 1, wherein said determining dependencies comprises evaluating dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules **(e.g. Kanada "By referring to the policy repository 211 and the variable reference table 214, the**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

policy rule dependence analyzer 204 analyzes the relation between the rules entered to be added or removed and the relation between these rules and the existing rules to find dependence of a rule on another rule. This analyzer 204 then delivers at a time the rule identifiers of all interdependent rules to the policy scheduler 205" [0068]).

As to Claim 5:

Kanada in view of **YANG** and **Fulp** discloses the method of claim 1, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of policy rules based on **one** or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters **(e.g. YANG placing order of the rules in higher position is based on access count for each rule [0029]; more frequently used firewall rule placed higher position [0030]; see also Kanada rules can be rearranged such that defined variable always precede those that are used as a condition [0106])**. The Examiner supplies the same rationale for the combination of references **Kanada**, **YANG**, and **Fulp** as in Claim 1 above.

As to Amended Claim 13:

Kanada discloses a network security policy management system **(e.g. Kanada FIG. 1 [0060]-[0072])** comprising:

- one or more processors **(e.g. Kanada processor [0066])**; and

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

- one or more internal data storage devices **(e.g. Kanada hard disk or main storage [0066]; [0134])** operatively coupled to the one or more processors and storing:
- a business traffic flow input module **(e.g. Kanada software unit [0066])** configured to receive a request to add a new traffic flow policy rule to a plurality of policy rules managed by the system **(e.g. Kanada rule specified to be added [0021]; receiving input to add policy rule [0067])**;
- a dependency detection module **(e.g. Kanada software unit [0066])** configured to automatically determine dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules **(e.g. Kanada detects policy rules that the new policy rule depends on [Abstract]; analyzing policy rules for dependence of policy rule data on another policy rule data [0028]; [0068]; [0099]; [0103]; [0167])**;
- a traffic flow policy rule incorporation module **(e.g. Kanada software unit [0066])** configured to form an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules based on the determined dependencies **(e.g. Kanada add and store input policy rules into policy repository [0067]; [0070]; [0071]; rule table contains all input rules [0087]; list of rule identifiers and added rule sent to router [0099])**;

But **Kanada** does not specifically disclose:

- automatically optimize the updated set of policy rules by **one** or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, ***wherein the optimizing is based on*** **one** or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules;

- wherein the optimizing is performed in real-time.

However, the analogous art **YANG** does disclose automatically optimize the updated set of policy rules **(e.g. YANG firewall rule reduction [0014] for performance enhancement [0029] and reducing overall parsing time [0030]; by the firewall rules reduction module [0032])** by **one** or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules **(e.g. YANG removing unused obsolete rules [0005]; [0029]; placing order of the rules in the firewall configuration [0029]; more frequently used firewall rule placed higher position [0030])**, wherein the optimizing is based on **one** or more of weights assigned to particular types of traffic, preference settings, priority settings **(e.g. YANG placing order of the rules in higher position is based on access count for each rule [0029]; more frequently used firewall rule placed higher position [0030])**, network traffic characteristics **(e.g. YANG identifies existing firewall rules that have been used recently and marked valid on a per external partner network basis [0029]; firewall rule network attributes including source IP, destination IP address, direction, incoming or outgoing [0016]; identified IP**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

addresses [0017]) and usage statistics for each policy rule **(e.g. YANG access count for each valid rule [0029]; [0030])** of the updated set of policy rules. Furthermore, the analogous art **Fulp** does disclose wherein the optimizing by the network security management device is performed in real-time **(e.g. control node includes a firewall policy optimizer that measures current rule configuration and dynamically reorders firewall rules to rearrange rules and improve firewall performance [0109])**. **Kanada**, **YANG**, and **Fulp** are analogous art because they are from the same field of endeavor in management of network firewall rules.

- (e.g. see **YANG**, "In step 220, the method uses the parsed information to identify all existing firewall rules on a per external partner network basis. In other words, the method identifies, for each external partner network, its routable network address space and all the existing firewall rules associated with that particular external partner network. Firewall rule may comprise attributes that includes, but are not limited to, source IP address, destination IP address, protocol used (e.g., TCP or UDP, etc), protocol port number, direction (e.g., incoming or outgoing) etc" **[0016]**; see also "the method uses the parsed information to identify the permitted IP address space on a per external partner network basis. In other words, the method identifies, for each external partner network, all the valid IP source and destination addresses permitted for access by that particular external partner network" **[0017]**; see also "Once method 300 is executed, it produces an output that identifies all existing firewall rules that have been used recently and marked valid on a per external partner network basis. Therefore, for the existing

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

firewall rules of each external partner network that have not been marked valid, they are considered obsolete or unused rules. In one embodiment, it is reasonable to assume that an unused rule for a predefined period of time, e.g., 90 days or more should be removed. The length of the unused period of time threshold of an unused rule is a configurable parameter set by the network operator. The output also produces the access count for each valid rule for each external partner network. The access count for each individual rule can be used as a reference for the activities associated to the rule as well as the placing order of the rule in the firewall configuration and security policy files for performance enhancement" **[0029]**; see also "For instance, more frequently used firewall rule should be placed at a higher position in the firewall access list in the firewall configuration and security policy files to reduce overall parsing time during normal operations of the firewall system" **[0030]**);

- (e.g. see **FuIp**, "A firewall rule set that is optimized using the subject matter described herein may be implemented on any firewall system that includes one or more firewalls. For example, an optimized firewall rule set according to embodiments of the subject matter described herein may be implemented using any of the hierarchical, multi-node firewall systems… A control node 1512 may include a firewall policy optimizer 1514 that measures the average number of comparisons per packets for the current rule configuration and may dynamically reorder the rules to reduce the average number of comparisons per packet. For

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

example, firewall policy optimizer 1514 may utilize any of the methods described herein to rearrange rules and improve firewall performance" **[0109]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, and **Fulp** before him or her, to modify the invention of **Kanada** with the teachings of **YANG** and **Fulp** to include *automatically optimize the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein the optimizing is based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules and wherein the optimizing is performed in real-time* as claimed because **Kanada** provides a network system including a server and routers for management of network policy rules that may be added, deleted, and/or updated **(Kanada [0021]-[0137])** which could include automatic optimization by ordering more frequently used firewall rules in higher positions and removing obsolete or unused rules based on access counts and external partner network attributes **(YANG [0016]; [0017]; [0029]; [0030])** and dynamically optimizing based on measuring current rule configuration and comparing to rearranged rules performance **(Fulp [0109])**. The suggestion/motivation for doing so would have been for performance enhancement and to reduce overall parsing time during normal operations of the firewall system **(YANG [0029]; [0030])** and to significantly improve

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

firewall performance and lower packet delay **(Fulp [0010]; [0109])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, and **Fulp** to obtain the invention as specified in the instant claim(s).

As to Claim 14:

Kanada in view of **YANG** and **Fulp** discloses the system of claim 13, wherein the dependency detection module is further configured to evaluate dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules. **(e.g. Kanada "By referring to the policy repository 211 and the variable reference table 214, the policy rule dependence analyzer 204 analyzes the relation between the rules entered to be added or removed and the relation between these rules and the existing rules to find dependence of a rule on another rule. This analyzer 204 then delivers at a time the rule identifiers of all interdependent rules to the policy scheduler 205" [0068])**.

As to Claim 17:

Kanada in view of **YANG** and **Fulp** discloses the system of claim 13, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of policy rules based on **one** or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters **(e.g. YANG placing order of the rules in higher position is based on access count for each rule [0029]; more frequently used firewall rule placed higher position [0030]; see also Kanada rules can be rearranged such that defined variable always precede those that are used as a**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

condition [0106]). The Examiner supplies the same rationale for the combination of references **Kanada**, **YANG**, and **Fulp** as in Claim 13 above.

8. **Claims 3 and 15** are rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of **YANG** and **Fulp** as applied to Claims 1 and 13 above, and further in view of **Porat** (US 20080062994 A1).

As to Claim 3:

Kanada in view of **YANG** and **Fulp** discloses the method of claim 1, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule **(e.g. Kanada plurality of rules are merged into one rule [0021]; rules on lines 1302 and 1303 are merged into one rule [0139]; in a form that can be executed [0147]; [0179])**, but does not specifically disclose:

- wherein the merging is conducted ***based on matching of one*** or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

However, the analogous art **Porat** does disclose wherein the merging is conducted **(e.g. Porat combining the rules of several HVIDs into one rule [0046])** based on matching of **one** or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules **(e.g. Porat combining the rules into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

the same rule). **Kanada**, **YANG**, **Fulp**, and **Porat** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Porat**, "The use of subnet masks enables pruning of the filtering database according to the address scheme by combining the rules of several HVIDs into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using the same rule)" **[0046]**; see also "In addition, the subnet mask can be used to filter and prune MAC address rules in the filtering database" **[0047]**; see also "Thus, the bridge 50 is pre-programmed to know which bits of the HVID or MAC must be read for forwarding information, and which can be ignored for that particular hop. Preferably, an algorithm for best match or longest prefix (similar to that used in IP routing) runs in switching processor 52. It will be appreciated that an address can have different subnet masks, i.e., one can look at the first three bits, while another only looks at the first two bits. The algorithm for best match utilizes the rule that has the most bits in the subnet mask, e.g., the longest matching address with the highest number of matching bits, or any other rule used to define best match, such as least cost, etc" **[0048]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, **Fulp**, and **Porat** before him or her, to modify the combination of **Kanada**, **YANG**, and **Fulp** with the teachings of **Porat** to include *wherein the merging is conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination IP*

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules as claimed because **Kanada** already teaches management of network policy rules that may be added, deleted, updated, and merged **(Kanada [0021]-[0137]; [0139])** which could be based on matching subnet prefixes **(Porat [0046]-[0048])**. The suggestion/motivation for doing so would have been to enable pruning of the filtering database according to an address scheme **(Porat [0046])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, **Fulp**, and **Porat** to obtain the invention as specified in the instant claim(s).

As to Claim 15:

Kanada in view of **YANG** and **Fulp** discloses the system of claim 13, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule **(e.g. Kanada plurality of rules are merged into one rule [0021]; rules on lines 1302 and 1303 are merged into one rule [0139]; in a form that can be executed [0147]; [0179])**, but does not specifically disclose:

- wherein the merging is conducted ***based on matching of one*** or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

However, the analogous art **Porat** does disclose wherein the merging is conducted **(e.g. Porat combining the rules of several HVIDs into one rule [0046])** based on matching of **one** or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

combinable policy rules **(e.g. Porat combining the rules into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using the same rule)**. **Kanada**, **YANG**, **Fulp**, and **Porat** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Porat**, "The use of subnet masks enables pruning of the filtering database according to the address scheme by combining the rules of several HVIDs into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using the same rule)" **[0046]**; see also "In addition, the subnet mask can be used to filter and prune MAC address rules in the filtering database" **[0047]**; see also "Thus, the bridge 50 is pre-programmed to know which bits of the HVID or MAC must be read for forwarding information, and which can be ignored for that particular hop. Preferably, an algorithm for best match or longest prefix (similar to that used in IP routing) runs in switching processor 52. It will be appreciated that an address can have different subnet masks, i.e., one can look at the first three bits, while another only looks at the first two bits. The algorithm for best match utilizes the rule that has the most bits in the subnet mask, e.g., the longest matching address with the highest number of matching bits, or any other rule used to define best match, such as least cost, etc" **[0048]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, **Fulp**, and **Porat** before him or her, to modify the combination of **Kanada**, **YANG**, and **Fulp**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

with the teachings of **Porat** to include *wherein the merging is conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules* as claimed because **Kanada** already teaches management of network policy rules that may be added, deleted, updated, and merged **(Kanada [0021]-[0137]; [0139])** which could be based on matching subnet prefixes **(Porat [0046]-[0048])**. The suggestion/motivation for doing so would have been to enable pruning of the filtering database according to an address scheme **(Porat [0046])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, **Fulp**, and **Porat** to obtain the invention as specified in the instant claim(s).

9. **Claims 4 and 16** are rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of **YANG**, **Fulp**, and **Porat** as applied to Claims 3 and 15 above, and further in view of **Liu** (US 20020154635 A1).

As to Claim 4:

Kanada in view of **YANG**, **Fulp**, and **Porat** discloses the method of claim 3, but does not specifically disclose:

- superneting of one or more of the source IP addresses and the destination IP addresses.

However, the analogous art **Liu** does disclose superneting of one or more of the source IP addresses and the destination IP addresses **(e.g. Liu Supernet security layer prepends real source and destination IP addresses [0062]; [0076])**. **Kanada**,

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

YANG, **Fulp**, **Porat**, and **Liu** are analogous art because they are from the same field of endeavor in network traffic management.

- (e.g. see **Liu**, "a Supernet security layer (SNSL) 532, acting as the conduit for all Supernet communications. To conserve memory, both inner IP layer 530 and outer IP layer 534 may share the same instance of the code of an IP layer. SNSL 532 performs security functionality as well as address translation. It also caches the most recently used channel keys for ten seconds. Thus, when a channel key is needed, SNSL 532 checks its cache first, and if it is not found, it requests KMD 520 to contact the appropriate KMC to retrieve the appropriate channel key. Two IP layers 530, 534 are used in the TCP /IP protocol stack 524 because both the internal addressing scheme and the external addressing scheme are IP-based. Thus, for example, when a packet is sent, inner IP layer 530 receives the packet from TCP/UDP layer 528 and processes the packet with its node ID address before passing it to the SNSL layer 532, which encrypts it, prepends the real source IP address and the real destination IP address, and then passes the encrypted packet to outer IP layer 534 for sending to the destination" **[0062]**; see also **[0076]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, **Fulp**, **Porat**, and **Liu** before him or her, to modify the combination of **Kanada**, **YANG**, **Fulp**, and **Porat** with the teachings of **Liu** to include *superneting of one or more of the source IP addresses and the destination IP addresses* as claimed because **Kanada** provides a

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

policy rule controlled network with server and routers **(Kanada [0021]-[0137])** which could include implement a Supernet security layer that translates source and destination IP addresses of communicated packets **(Liu [0062]; [0076])**. The suggestion/motivation for doing so would have been to allow utilization of public-network infrastructure without the need to maintain a private network to be able to use resources securely and without geographical restriction **(Liu [0020])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, **Fulp**, **Porat**, and **Liu** to obtain the invention as specified in the instant claim(s).

As to Claim 16:

Kanada in view of **YANG**, **Fulp**, and **Porat** discloses the system of claim 15, but does not specifically disclose:

- superneting of one or more of the source Internet Protocol (IP) addresses and the destination IP addresses.

However, the analogous art **Liu** does disclose superneting of one or more of the source IP addresses and the destination IP addresses **(e.g. Liu Supernet security layer prepends real source and destination IP addresses [0062]; [0076])**. **Kanada**, **YANG**, **Fulp**, **Porat**, and **Liu** are analogous art because they are from the same field of endeavor in network traffic management.

- (e.g. see **Liu**, "a Supernet security layer (SNSL) 532, acting as the conduit for all Supernet communications. To conserve memory, both inner IP layer 530 and outer IP layer 534 may share the same instance of the code of an IP layer. SNSL 532 performs security functionality as well as address translation. It also caches

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

> the most recently used channel keys for ten seconds. Thus, when a channel key is needed, SNSL 532 checks its cache first, and if it is not found, it requests KMD 520 to contact the appropriate KMC to retrieve the appropriate channel key. Two IP layers 530, 534 are used in the TCP /IP protocol stack 524 because both the internal addressing scheme and the external addressing scheme are IP-based. Thus, for example, when a packet is sent, inner IP layer 530 receives the packet from TCP/UDP layer 528 and processes the packet with its node ID address before passing it to the SNSL layer 532, which encrypts it, prepends the real source IP address and the real destination IP address, and then passes the encrypted packet to outer IP layer 534 for sending to the destination" **[0062]**; see also **[0076]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, **Fulp**, **Porat**, and **Liu** before him or her, to modify the combination of **Kanada**, **YANG**, **Fulp**, and **Porat** with the teachings of **Liu** to include *superneting of one or more of the source IP addresses and the destination IP addresses* as claimed because **Kanada** provides a policy rule controlled network with server and routers **(Kanada [0021]-[0137])** which could include implement a Supernet security layer that translates source and destination IP addresses of communicated packets **(Liu [0062]; [0076])**. The suggestion/motivation for doing so would have been to allow utilization of public-network infrastructure without the need to maintain a private network to be able to use resources securely and without geographical restriction **(Liu [0020])**. Therefore, it would have

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

been obvious to combine **Kanada**, **YANG**, **Fulp**, **Porat**, and **Liu** to obtain the invention as specified in the instant claim(s).

10. **Claim 6** is rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of **YANG** and **Fulp** as applied to Claim 1 above, and further in view of Corl et al. (US 20020198981 A1, hereinafter **Corl**).

As to Claim 6:

Kanada in view of **YANG** and **Fulp** discloses the method of claim 5, but does not specifically disclose:

- wherein the order of the policy rules of the second sub-set of policy rules is changed based on frequency of usage thereof.

However, the analogous art **Corl** does disclose wherein the order of the policy rules of the second sub-set of policy rules is changed based on frequency of usage thereof **(e.g. Corl placing the plurality of filter rules in an order based on frequency of reach filter rule [Abstract]; statistics of frequency [0024]; placing higher frequency filter rules first [0028])**. **Kanada**, **YANG**, **Fulp**, and **Corl** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Corl**, "Each of the plurality of filter rules has a priority. The method and system include accumulating statistics for each of the plurality of filter rules. The statistics indicate a frequency of enforcement for each of the plurality of filter rules. The method and system also include placing the plurality of filter rules in an order for testing against the key. The order is based on the frequency of each filter rule of the portion of the plurality of filter rules" **[Abstract]**; see also "The

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

statistics indicate a frequency of enforcement for each of the plurality of filter rules. The method and system also comprise placing the plurality of filter rules in an order for testing against the key. The order is based on the frequency of each filter rule of the portion of the plurality of filter rules" **[0024]**; see also "The order preferably places higher frequency filter rules first, so that the filter rules that are enforced more often will be tested first. The order preferably places the remaining rules in order of their frequency" **[0028]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, **Fulp**, and **Corl** before him or her, to modify the combination of **Kanada**, **YANG**, and **Fulp** with the teachings of **Corl** to include *wherein the order of the policy rules of the second sub-set of policy rules is changed based on frequency of usage thereof* as claimed because **Kanada** provides a policy rule controlled network with server and routers **(Kanada [0021]-[0137])** which could accumulate frequency statistics for each rule and place higher frequency filter rules first **(Corl [0062]; [0076])**. The suggestion/motivation for doing so would have been to save time and allow network processing to function more efficiently **(Corl [0029])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, **Fulp**, and **Corl** to obtain the invention as specified in the instant claim(s).

11. **Claims 7-11 and 18-22** are rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of **YANG** and **Fulp** as applied to Claims 1 and 13 above, and further in view of Goldschmidt et al. (US 20060013136 A1, hereinafter **Goldschmidt**).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

As to Claim 7:

Kanada in view of **YANG** and **Fulp** discloses the method of claim 1, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules **(e.g. deleting policy rules and checks consistency Kanada [0069]; [0096]; [0097])**, but does not specifically disclose:

- based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. although Kanada does teach a policy consistency checker that checks rules for being exclusive with each other [0109]-[0111])**.

However, the analogous art **Goldschmidt** does disclose based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt determining whether rules of updated rule subset have equal conflict relationship, then delete the lower priority rule [0061])**. **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "A flow manager may also receive additional packet flow rules, integrate them into the unified rule set, update the rule subsets according to the additional rules, and install the updated subsets onto the flow enforcement devices" **[Abstract]**; see also "After determining the relationship between two conflicting packet flow rules, flow manager 120 may be configured to determine whether the two rules have an equal relationship, as illustrated by decision block 440. If the two rules do have an equal conflict relationship, flow manager 120

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

may, according to one embodiment, append the actions of the lower priority rule to the actions of the higher priority rule, as illustrated by block 460. According to certain embodiments, if flow manager 120 appends the actions of the lower priority rule to the actions of the higher priority rule, flow manager 120 may be configured to delete the lower priority rule, since is may now be redundant" **[0061]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **])**. **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** before him or her, to modify the combination of **Kanada**, **YANG**, and **Fulp** with the teachings of **Goldschmidt** to include *based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules* as claimed because **Kanada** provides a policy rule controlled network with a policy server that deletes rules **(Kanada [0021]-[0137])** which could be based on conflicting relationship of rules **(Goldschmidt [0061])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **])**. **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 8:

Kanada in view of **YANG**, **Fulp**, and **Goldschmidt** discloses the method of claim 7, wherein the one or more conflicts include existence of a duplicate policy rule in the

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt "resolving a conflict between two packet flow rules that comprise identical packet filters. For example, in one embodiment, a flow manager, such as flow manager 120, may be configured to determine the relationship between the data packet flow specified by the packet filters of the conflicting rules, as illustrated by block 420" [0056]; see also "two rules conflict if their packet filters specify overlapping, or identical, data flow packets" [0057])**. The Examiner supplies the same rationale for the combination of references **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** as in Claim 7 above.

As to Claim 9:

Kanada in view of **YANG**, **Fulp**, and **Goldschmidt** discloses the method of claim 7, wherein the one or more conflicts include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule **(e.g. Kanada policy consistency checker that checks rules for being exclusive with each other [0109]-[0111]; Goldschmidt two or more rules may conflict by having packet filters that match the same data packets [0046]; [0051]; [0055])**. The Examiner supplies the same rationale for the combination of references **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** as in Claim 7 above.

As to Claim 10:

Kanada in view of **YANG** and **Fulp** discloses the method of claim 1, but does not specifically disclose:

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

- wherein the one or more weights are defined manually based on scope and attributes of policy rule.

However, the analogous art **Goldschmidt** does disclose wherein the one or more weights are defined manually based on scope and attributes of policy rule **(e.g. Goldschmidt rules are prioritized using prefix or ordered precedence, actions specified are prioritized [0038]; priority order for rules as specified by network service [0039]; administrator may provide the priorities [0047])**. **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** before him or her, to modify the combination of **Kanada**, **YANG**, and **Fulp** with the teachings of **Goldschmidt** to include *wherein the one or more weights are defined manually based on scope and attributes of policy rule* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 11:

Kanada in view of **YANG** and **Fulp** discloses the method of claim 1, but does not specifically disclose:

- wherein the one or more weights are defined automatically.

However, the analogous art **Goldschmidt** does disclose wherein the one or more weights are defined automatically **(e.g. Goldschmidt rules are prioritized using prefix or ordered precedence, actions specified are prioritized [0038]; policies are received that express priorities between network services and their supplied packet flow rules [0047])**. **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** before him or her, to modify the combination of **Kanada**, **YANG**, and **Fulp** with the teachings of **Goldschmidt** to include *wherein the one or more weights are defined manually based on scope and attributes of policy rule* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order based on received policies **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 18:

Kanada in view of **YANG** and **Fulp** discloses the system of claim 13, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules **(e.g. deleting policy rules and checks consistency Kanada [0069]; [0096]; [0097])**, but does not specifically disclose:

- based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. although Kanada does teach a**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

policy consistency checker that checks rules for being exclusive with each other [0109]-[0111]).

However, the analogous art **Goldschmidt** does disclose based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt determining whether rules of updated rule subset have equal conflict relationship, then delete the lower priority rule [0061 Kanada**, **YANG**, **Fulp**, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "A flow manager may also receive additional packet flow rules, integrate them into the unified rule set, update the rule subsets according to the additional rules, and install the updated subsets onto the flow enforcement devices" **[Abstract]**; see also "After determining the relationship between two conflicting packet flow rules, flow manager 120 may be configured to determine whether the two rules have an equal relationship, as illustrated by decision block 440. If the two rules do have an equal conflict relationship, flow manager 120 may, according to one embodiment, append the actions of the lower priority rule to the actions of the higher priority rule, as illustrated by block 460. According to certain embodiments, if flow manager 120 appends the actions of the lower priority rule to the actions of the higher priority rule, flow manager 120 may be configured to delete the lower priority rule, since is may now be redundant" **[0061]**).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** before him or her, to modify the combination of **Kanada**, **YANG**, and **Fulp** with the teachings of **Goldschmidt** to include *based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules* as claimed because **Kanada** provides a policy rule controlled network with a policy server that deletes rules **(Kanada [0021]-[0137])** which could be based on conflicting relationship of rules **(Goldschmidt [0061])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 19:

Kanada in view of **YANG**, **Fulp**, and **Goldschmidt** discloses the system of claim 18, wherein the one or more conflicts include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt "resolving a conflict between two packet flow rules that comprise identical packet filters. For example, in one embodiment, a flow manager, such as flow manager 120, may be configured to determine the relationship between the data packet flow specified by the packet filters of the conflicting rules, as illustrated by block 420" [0056]; see also "two rules conflict if their packet filters**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

specify overlapping, or identical, data flow packets" [0057]). The Examiner supplies the same rationale for the combination of references **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** as in Claim 18 above.

As to Claim 20:

Kanada in view of **YANG**, **Fulp**, and **Goldschmidt** discloses the system of claim 18, wherein the one or more conflicts comprise one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule **(e.g. Kanada policy consistency checker that checks rules for being exclusive with each other [0109]-[0111]; Goldschmidt two or more rules may conflict by having packet filters that match the same data packets [0046]; [0051]; [0055])**. The Examiner supplies the same rationale for the combination of references **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** as in Claim 18 above.

As to Claim 21:

Kanada in view of **YANG** and **Fulp** discloses the system of claim 13, but does not specifically disclose:

- wherein the one or more weights are defined manually based on scope and attributes of the policy rule.

However, the analogous art **Goldschmidt** does disclose wherein the one or more weights are defined manually based on scope and attributes of the policy rule **(e.g. Goldschmidt rules are prioritized using prefix or ordered precedence, actions specified are prioritized [0038]; priority order for rules as specified by network service [0039]; administrator may provide the priorities [0047])**. **Kanada**, **YANG**,

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Fulp, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** before him or her, to modify the combination of **Kanada**, **YANG**, and **Fulp** with the teachings of **Goldschmidt** to include *wherein the one or more weights are defined manually based on scope and attributes of policy rule* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

As to Claim 22:

Kanada in view of **YANG** and **Fulp** discloses the system of claim 13, but does not specifically disclose:

- wherein the one or more weights are defined automatically.

However, the analogous art **Goldschmidt** does disclose wherein the one or more weights are defined automatically **(e.g. Goldschmidt rules are prioritized using prefix or ordered precedence, actions specified are prioritized [0038]; policies are received that express priorities between network services and their supplied packet flow rules [0047])**. **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** before him or her, to modify the combination of **Kanada**, **YANG**, and **Fulp** with the teachings of **Goldschmidt** to include *wherein the one or more weights are defined manually based on scope and attributes of policy rule* as claimed because

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Kanada provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order based on received policies **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, **Fulp**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

12. **Claim 12** is rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of **YANG** and **Fulp** as applied to Claim 1 above, and further in view of **Goldschmidt** and **Corl**.

As to Claim 12:

Kanada in view of **YANG** and **Fulp** discloses the method of claim 1, wherein said forming an updated set of policy rules is conducted **(e.g. Kanada add and store input policy rules into policy repository [0067]; [0070]; [0071]; rule table contains all input rules [0087]; list of rule identifiers and added rule sent to router [0099])** based on the preference settings and network traffic characteristics **(e.g. Kanada cross-reference relations between variables in policy rules [0067]; consistency checker of conditions of the rules being exclusive with each other or not [0110])**, but does not specifically disclose:

- based on the one or more weights, the priority settings for the policy rules, and network usage statistics.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

However, the analogous art **Goldschmidt** does disclose based on the one or more weights **(e.g. Goldschmidt longest prefix or ordered precedence [0038])**, the priority settings for the policy rules **(e.g. Goldschmidt priority order for rules [0039]; [0040]; [0041])**. Furthermore, the analogous art **Corl** does disclose network usage statistics [for each policy rule] **(e.g. Corl statistics of frequency of enforcement for reach of the plurality of filter rules [0024])**. **Kanada**, **YANG**, **Fulp**, **Goldschmidt**, and **Corl** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**);
- (e.g. see **Corl**, "Each of the plurality of filter rules has a priority. The method and system include accumulating statistics for each of the plurality of filter rules. The statistics indicate a frequency of enforcement for each of the plurality of filter rules. The method and system also include placing the plurality of filter rules in an order for testing against the key. The order is based on the frequency of each filter rule of the portion of the plurality of filter rules" **[Abstract]**; see also "The statistics indicate a frequency of enforcement for each of the plurality of filter

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

rules. The method and system also comprise placing the plurality of filter rules in an order for testing against the key. The order is based on the frequency of each filter rule of the portion of the plurality of filter rules" **[0024]**; see also "The order preferably places higher frequency filter rules first, so that the filter rules that are enforced more often will be tested first. The order preferably places the remaining rules in order of their frequency" **[0028]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, **Fulp**, **Goldschmidt**, and **Corl** before him or her, to modify the combination of **Kanada**, **YANG**, and **Fulp** with the teachings of **Goldschmidt** and **Corl** to include *based on the one or more weights, the priority settings for the policy rules, and network usage statistics* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order based on received policies **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])** and accumulating frequency statistics for each rule and placing higher frequency filter rules first **(Corl [0062]; [0076])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])** and to save time and allow network processing to function more efficiently **(Corl [0029])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, **Fulp**, **Goldschmidt**, and **Corl** to obtain the invention as specified in the instant claim(s).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

13. **Claims 23-25** are rejected under 35 U.S.C. 103 as being unpatentable over **YANG** in view of **Porat**, and further in view of **Fulp**.

As to Amended Claim 23:

YANG discloses a network security policy management system **(e.g. YANG method and apparatus for reducing obsolete firewall rules [Abstract]; parsing firewall configuration and security policy files [0014]; [0015]; FIG. 4 system [0031])** comprising:

- one or more processors **(e.g. YANG processor element [0031])**; and
- one or more internal data storage devices **(e.g. YANG memory, RAM, ROM, [0031])** operatively coupled to the one or more processors and storing a policy rule optimization module **(e.g. YANG firewall rules reduction module [0031]; [0032])** configured to retrieve information regarding a current set of policy rules **(e.g. YANG parsing firewall security policy files [0014]; [0015])** and optimize the current set of policy rules **(e.g. YANG firewall rule reduction [0014] for performance enhancement [0029] and reducing overall parsing time [0030]; by the firewall rules reduction module [0032])** by reordering a second sub-set of policy rules of the current set of policy rules, and deleting a third sub-set of policy rules of the current set of policy rules **(e.g. YANG removing unused obsolete rules [0005]; [0029]; placing order of the rules in the firewall configuration [0029]; more frequently used firewall rule placed higher position [0030])**, wherein the optimizing is based on **one** or more of weights assigned to particular types of traffic, preference settings, priority settings **(e.g.**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

YANG placing order of the rules in higher position is based on access count for each rule [0029]; more frequently used firewall rule placed higher position [0030]), network traffic characteristics **(e.g. YANG identifies existing firewall rules that have been used recently and marked valid on a per external partner network basis [0029]; firewall rule network attributes including source IP, destination IP address, direction, incoming or outgoing [0016]; identified IP addresses [0017])** and usage statistics for each policy rule **(e.g. YANG access count for each valid rule [0029]; [0030])** of the current set of policy rules.

But **YANG** does not specifically disclose:

- grouping a first sub-set of policy rules of the current set of policy rules based on **one** or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and usage statistics for each policy rule of the current set of policy rules;
- wherein the optimizing is performed in real-time.

However, the analogous art **Porat** does disclose grouping a first sub-set of policy rules of the current set of policy rules **(e.g. Porat combining the rules of several HVIDs into one rule [0046])** based on **one** or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics **(e.g. Porat combining the rules into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using the same rule)**, and usage statistics for each policy rule of the current set of policy rules. . Furthermore, the analogous art **Fulp**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

does disclose wherein the optimizing by the network security management device is performed in real-time **(e.g. control node includes a firewall policy optimizer that measures current rule configuration and dynamically reorders firewall rules to rearrange rules and improve firewall performance [0109])**. **YANG**, **Porat**, and **Fulp** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Porat**, "The use of subnet masks enables pruning of the filtering database according to the address scheme by combining the rules of several HVIDs into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using the same rule)" **[0046]**; see also "In addition, the subnet mask can be used to filter and prune MAC address rules in the filtering database" **[0047]**; see also "Thus, the bridge 50 is pre-programmed to know which bits of the HVID or MAC must be read for forwarding information, and which can be ignored for that particular hop. Preferably, an algorithm for best match or longest prefix (similar to that used in IP routing) runs in switching processor 52. It will be appreciated that an address can have different subnet masks, i.e., one can look at the first three bits, while another only looks at the first two bits. The algorithm for best match utilizes the rule that has the most bits in the subnet mask, e.g., the longest matching address with the highest number of matching bits, or any other rule used to define best match, such as least cost, etc" **[0048]**);

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

- (e.g. see **FuIp**, "A firewall rule set that is optimized using the subject matter described herein may be implemented on any firewall system that includes one or more firewalls. For example, an optimized firewall rule set according to embodiments of the subject matter described herein may be implemented using any of the hierarchical, multi-node firewall systems… A control node 1512 may include a firewall policy optimizer 1514 that measures the average number of comparisons per packets for the current rule configuration and may dynamically reorder the rules to reduce the average number of comparisons per packet. For example, firewall policy optimizer 1514 may utilize any of the methods described herein to rearrange rules and improve firewall performance" **[0109]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **YANG**, **Porat**, and **FuIp** before him or her, to modify the invention of **YANG** with the teachings of **Porat** and **FuIp** to include *grouping a first sub-set of policy rules of the current set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and usage statistics for each policy rule of the current set of policy rules and wherein the optimizing is performed in real-time* as claimed because **YANG** already teaches an apparatus for parsing, identifying, and reducing obsolete firewall rules by reordering and removing **(YANG [Abstract]; [0014]; [0015]; [0029]-[0032])** which could also include combining rules with matching subnet prefixes **(Porat [0046]-[0048])** and dynamically optimizing based on measuring current rule configuration and comparing to rearranged rules performance

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

(Fulp [0109]). The suggestion/motivation for doing so would have been to enable pruning of the filtering database according to an address scheme **(Porat [0046])** and to significantly improve firewall performance and lower packet delay **(Fulp [0010]; [0109])**. Therefore, it would have been obvious to combine **YANG**, **Porat**, and **Fulp** to obtain the invention as specified in the instant claim(s).

As to Claim 24:

YANG in view of **Porat** and **Fulp** discloses the system of claim 23, wherein said grouping the first sub-set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule **(e.g. Porat combining the rules of several HVIDs into one rule [0046])**, wherein the merging is conducted based on matching of **one** or more of source IP addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules **(e.g. Porat combining the rules into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using the same rule)**. The Examiner supplies the same rationale for the combination of references **YANG**, **Porat**, and **Fulp** as in Claim 23 above.

As to Claim 25:

YANG in view of **Porat** and **Fulp** discloses the system of claim 23, wherein said reordering the second sub-set of policy rules comprises changing an order of the policy rules of the second sub-set of policy rules based on **one** or more of their source Internet Protocol (IP) addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters **(e.g. YANG placing order**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

of the rules in higher position is based on access count for each rule [0029]; more frequently used firewall rule placed higher position [0030]). The Examiner supplies the same rationale for the combination of references **YANG**, **Porat**, and **Fulp** as in Claim 23 above.

14. **Claim 26** is rejected under 35 U.S.C. 103 as being unpatentable over **YANG** in view of **Porat** and **Fulp** as applied to Claim 23 above, and further in view of **Goldschmidt**.

As to Claim 26:

YANG in view of **Porat** and **Fulp** discloses the system of claim 23, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules **(e.g. removing obsolete firewall rules YANG [0005]; [0029])**, but does not specifically disclose:

- based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. although Kanada does teach a policy consistency checker that checks rules for being exclusive with each other [0109]-[0111])**.

However, the analogous art **Goldschmidt** does disclose based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt determining whether rules of updated rule subset have equal conflict relationship, then delete the lower priority rule [0061])**. **YANG**, **Porat**, **Fulp**, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

- (e.g. see **Goldschmidt**, "A flow manager may also receive additional packet flow rules, integrate them into the unified rule set, update the rule subsets according to the additional rules, and install the updated subsets onto the flow enforcement devices" **[Abstract]**; see also "After determining the relationship between two conflicting packet flow rules, flow manager 120 may be configured to determine whether the two rules have an equal relationship, as illustrated by decision block 440. If the two rules do have an equal conflict relationship, flow manager 120 may, according to one embodiment, append the actions of the lower priority rule to the actions of the higher priority rule, as illustrated by block 460. According to certain embodiments, if flow manager 120 appends the actions of the lower priority rule to the actions of the higher priority rule, flow manager 120 may be configured to delete the lower priority rule, since is may now be redundant" **[0061]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **YANG**, **Porat**, **Fulp**, and **Goldschmidt** before him or her, to modify the combination of **YANG**, **Porat**, and **Fulp** with the teachings of **Goldschmidt** to include *based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules* as claimed because **YANG** already teaches an apparatus for parsing, identifying, and reducing obsolete firewall rules by reordering and removing **(YANG [Abstract]; [0014]; [0015]; [0029]-[0032])** which could be based on conflicting relationship of rules **(Goldschmidt [0061])**. The suggestion/motivation for doing so would have been to

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **YANG**, **Porat**, **Fulp**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. **Levy et al. (US 20030179703 A1)**

b. **Nguyen et al. (US 20070115916 A1)**

c. **SPECTOR et al. (US 20100100468 A1)**

d. **Turley et al. (US 8397282 B2)**

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kenneth Chang whose telephone number is (571)270-7530. The examiner can normally be reached on Monday-Friday 8:30am-5pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kenneth Chang/
Primary Examiner, Art Unit 2438
UNITED STATES PATENT AND TRADEMARK OFFICE
05/24/17

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Notice of References Cited	Application/Control No. 14/566,403	Applicant(s)/Patent Under Reexamination PERNICHA, HUGO FILIPE PA	
	Examiner Kenneth Chang	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2003/0179703 A1	09-2003	Levy, Yonatan Aharon	H04L41/06	370/230
*	B	US-2006/0248580 A1	11-2006	Fulp; Errin W.	H04L63/20	726/11
*	C	US-2007/0115916 A1	05-2007	Nguyen; Nhut	H04L41/0893	370/351
*	D	US-2010/0100468 A1	04-2010	SPECTOR; Omri	G06Q20/04	705/35
*	E	US-8,397,282 B2	03-2013	Turley; Patrick	H04L63/0263	726/11
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L17	0	H04L63/0263.CPC. and (policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall or traffic) with optimiz$9 with (realtime or real time)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:27
L16	10806	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:27
L15	2404	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:27
L14	233	(policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall or traffic) with optimiz$9 with (realtime or real time)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:26
L13	214	(policy or policies or filter$9 or rule) with (network$9 or rout$9 or firewall) with optimiz$9 with (realtime or real time)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:26
L12	1784	(policy or policies or filter$9 or rule) with (traffic or firewall) with optimiz$9	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:09
L11	876	(policy or policies or filter$9 or rule) with (traffic or firewall) with (updat$9 or optimiz$9 or adjust$9 or reorder$9) with (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:09
L10	9	("20020038339" | "7089581" | "20050125697" | "20050251570" | "7227842" | "7237267" | "20100199346" | "20110055923" | "20060195896" | "7237267" | "20040010712" | "20040177139" | "7107613" | "20020198981" | "20100303240" | "6662235" | "20080301765" | "20090138938" | "7954143" | "20020165949" | "20030120622" | "6484261" | "20110055916" | "6098172" | "6484261" | "7089581" | "7299353" | "7331061" | "20100011433" | "20060070122" | "20040193943" | "7263099" | "20050010765" | "20050229246" | "20060104202" | "6662235").PN. and (realtime or real time)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:01
L9	27	("20020038339" | "7089581" | "20050125697" | "20050251570" | "7227842" | "7237267" | "20100199346" | "20110055923" | "20060195896" | "7237267" | "20040010712" | "20040177139" | "7107613" | "20020198981" | "20100303240" | "6662235" | "20080301765" |	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 10:01

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

		"20090138938" | "7954143" | "20020165949" | "20030120622" | "6484261" | "20110055916" | "6098172" | "6484261" | "7089581" | "7299353" | "7331061" | "20100011433" | "20060070122" | "20040193943" | "7263099" | "20050010765" | "20050229246" | "20060104202" | "6662235").PN. and (realtime or real time or dynamic$9)				
L8	32	("20020038339" | "7089581" | "20050125697" | "20050251570" | "7227842" | "7237267" | "20100199346" | "20110055923" | "20060195896" | "7237267" | "20040010712" | "20040177139" | "7107613" | "20020198981" | "20100303240" | "6662235" | "20080301765" | "20090138938" | "7954143" | "20020165949" | "20030120622" | "6484261" | "20110055916" | "6098172" | "6484261" | "7089581" | "7299353" | "7331061" | "20100011433" | "20060070122" | "20040193943" | "7263099" | "20050010765" | "20050229246" | "20060104202" | "6662235").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 09:59
L7	20	(policy or policies or filter$9) with (packet or flow or traffic) with rule with (optimiz$9) with (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 09:54
L6	36	(policy or policies or filter$9 or rule) with (packet or flow or traffic) with firewall with (updat$9 or optimiz$9 or adjust$9) with (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 09:42
L5	110	(policy or policies or filter$9) with (packet or flow or traffic) with rule with (updat$9 or optimiz$9 or adjust$9) with (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 09:41
L4	642	(policy or policies or filter$9) with (packet or flow or traffic) same rule same (updat$9 or optimiz$9 or adjust$9) same (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 09:41
L3	1276	(policy or policies or filter$9) same (packet or flow or traffic or firewall) same rule same (updat$9 or optimiz$9 or adjust$9) same (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 09:41
L2	1201	(policy or policies or filter$9) same (packet or flow or traffic) same rule same (updat$9 or optimiz$9 or adjust$9) same (realtime or real time or dynamic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/05/24 09:41
S36	35	H04L63/20.CPC. and (policy or policies) and (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 21:59
S35	89	(policy or policies) WITH (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:32
S34	84	(policy or policies) WITH (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical) and network$9	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:18

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

S33	89	(policy or policies) WITH (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:18
S32	24	(policy or policies) and (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical) with (parameter oR (source adj3 address$5) or (destination adj3 address$5))	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:15
S31	635	(policy or policies) and (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:11
S30	22	(policy or policies or filter$9) same (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical) with (parameter or address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 16:57
S29	1	"20100100954".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:34
S28	6	(policy or policies or filter$9) same (packet or flow or traffic) same rule same (delet$5 or remov$9) same (obsolete or redundan$5 or old) same (optimiz$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:33
S27	87	(policy or policies or filter$9) same (packet or flow or traffic) same rule same (delet$5 or remov$9) same (obsolete or redundan$5 or old)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:33
S26	10052	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:32
S25	1	"8478852".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:31
S24	1	"20100318812".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/11 16:14
S22	1	"20150033285".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 18:02
S21	1	"20120185913" .pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 17:56
S20	1	"20020069200".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 17:56
S19	60	H04L63/20.CPC. and (policy or policies or filter$9) same (packet or flow or traffic) same (group or grouped or grouping or delet$5 or remov$9 or reorder$9) with (rule) same (use or usage or statistic or weight)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 17:53
S18	409	(policy or policies or filter$9) same (packet or	US-	ADJ	ON	2017/01/10

		flow or traffic) same (group or grouped or grouping or delet$5 or remov$9 or reorder$9) with (rule) same (use or usage or statistic or weight)	PGPUB; USPAT; EPO			16:48
S17	2458	(policy or policies or filter$9) same (packet or flow or traffic) same (group or grouped or grouping or delet$5 or remov$9 or reorder$9) with (rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 16:47
S16	11	H04L63/0263.CPC. and (rule) same (depend$9) same (compatib$9 or conflict$9) and (packet or flow or traffic) and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5) and order$5	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/23 00:02
S15	1	"20060013136".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 22:07
S14	1	"20020198981".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 21:15
S13	14	(supernet$9) same (ip or internet protocol) same address$5 same source same destination	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 20:50
S12	281	(rule) same (depend$9) same (compatib$9 or conflict$9) and (packet or flow or traffic) and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5) and order$5	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:22
S11	185	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5) and order$5	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:21
S10	185	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:20
S9	212	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:20
S8	10	H04L63/0263.CPC. and (rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 14:10
S7	311	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 14:10
S6	9	("5889953" | "6041347" | "6170009" | "6418468" | "6463470" | "6587466" | "6601082" | "6611863").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 12:22
S5	1	"20010039576".pn.	US-PGPUB;	ADJ	ON	2016/07/22 12:20

			USPAT; EPO			
S4	1	"7441022".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 12:11
S3	2021	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/20 14:34
S2	590	fortinet.as.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/20 14:33
S1	1	(pernicha adj3 hugo).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/20 14:33

5/24/2017 10:27:47 AM
C:\Users\kchang3\Documents\EAST\Workspaces\14566403_APP.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14566403	PERNICHA, HUGO FILIPE PARREIRA
	Examiner	Art Unit
	KENNETH CHANG	2438

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/0263	7/20/2016	KC
H04L63/20	1/24/2017	KC
H04L63/0263	5/24/2017	KC
H04L63/20	5/24/2017	KC

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Searched Inventors' Names and Assignee on eDan and EAST.	7/20/2016	KC
Searched IEEE NPL Xplore Database online.	7/20/2016	KC
Completed Limited Classified Search in CPC on EAST USPAT, PGPUB, and EPO databases with Keywords.	7/22/2016	KC
Keywords Searched: See East search history.	7/22/2016	KC
H04L63/20	1/24/2017	KC
Updated Limited Classified Search in CPC on EAST USPAT, PGPUB, and EPO databases with Keywords. See East Search History.	1/28/2017	KC
Updated Keywords: See East search history.	1/28/2017	KC
Updated NPL search on IEEE Xplore Database online	5/24/2017	KC
Updated Limited Classified Search in CPC on EAST USPAT, PGPUB, and EPO databases with Keywords. See East Search History.	5/24/2017	KC

INTERFERENCE SEARCH	
	/KENNETH CHANG/ Primary Examiner.Art Unit 2438

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/KENNETH CHANG/ Primary Examiner.Art Unit 2438

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14566403	PERNICHA, HUGO FILIPE PARREIRA
	Examiner	**Art Unit**
	KENNETH CHANG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/23/2016	01/28/2017	05/24/2017						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	✓						
	6	✓	✓	✓						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	✓	✓						
	15	✓	✓	✓						
	16	✓	✓	✓						
	17	✓	✓	✓						
	18	✓	✓	✓						
	19	✓	✓	✓						
	20	✓	✓	✓						
	21	✓	✓	✓						
	22	✓	✓	✓						
	23	✓	✓	✓						
	24	✓	✓	✓						
	25	✓	✓	✓						
	26	✓	✓	✓						

IEEE.org | IEEE *Xplore* Digital Library | IEEE-SA | IEEE Spectrum | More Sites Cart (0) | Create Account | Personal Sign In

Access provided by:
United States Patent and Trademark Office
Sign Out

BROWSE MY SETTINGS GET HELP WHAT CAN I ACCESS?

Displaying results 1-6 of 6 for **firewall rule optimization automatic**

Show All Results Sort By Relevance

Select All on Page Download PDFs | Export | Set Search Alerts | Search History

Refine results by

Search within results

Content Type

- Conference Publications (5)
- Journals & Magazines (1)

Year

Single Year Range

2003 2016

From 2008 To 2016

Author

Affiliation

Publication Title

Conference Location

1. **A general framework for benchmarking firewall optimization techniques**
   Ghassan Misherghi; Lihua Yuan; Zhendong Su; Chen-Nee Chuah; Hao Chen
   IEEE Transactions on Network and Service Management
   Year: 2008, Volume: 5, Issue: 4
   Pages: 227 - 238, DOI: 10.1109/TNSM.2009.041104
   Cited by: Papers (13) | Patents (1)
   IEEE Journals & Magazines
   Abstract (355 Kb)

2. **Software-based computing platform as an experimental topology assembled to detect and mitigate DDoS attacks using virtual environments**
   Walter Fuertes; Miguel Morales; Hernán Aules; Theofilos Toulkeridis
   2016 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)
   Year: 2016
   Pages: 1 - 8, DOI: 10.1109/SPECTS.2016.7570512
   IEEE Conference Publications
   Abstract (1571 Kb)

3. **Automatic NIDS Rule Generating System for Detecting HTTP-like Malware Communication**
   Chia-Nan Kao; Yung-Cheng Chang; Nen-Fu Huang; I-Ju Liao; Rong-Tai Liu; Hsien-Wei Hung; Che-Wei Lin
   2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)
   Year: 2015
   Pages: 199 - 202, DOI: 10.1109/IIH-MSP.2015.10
   Cited by: Papers (1)
   IEEE Conference Publications
   Abstract (202 Kb)

4. **On synthesizing distributed firewall configurations considering risk, usability and cost constraints**
   Bin Zhang; Ehab Al-Shaer
   2011 7th International Conference on Network and Service Management
   Year: 2011
   Pages: 1 - 8
   IEEE Conference Publications
   Abstract (209 Kb)

5. **A Fully Automatic Approach for Fixing Firewall Misconfigurations**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Abstract (449 Kb)

An Enhanced Firewall Scheme for Dynamic and Adaptive Containment of Emerging Security Threats
Aniello Castiglione; Alfredo De Santis; Ugo Fiore; Francesco Palmieri
2010 International Conference on Broadband, Wireless Computing, Communication and Applications
Year: 2010
Pages: 475 - 481, DOI: 10.1109/BWCCA.2010.117
Cited by: Papers (2)
IEEE Conference Publications

Abstract (376 Kb)

« First < 1 > Last »

IEEE Account
» Change Username/Password
» Update Address

Purchase Details
» Payment Options
» Order History
» View Purchased Documents

Profile Information
» Communications Preferences
» Profession and Education
» Technical Interests

Need Help?
» **US & Canada:** +1 800 678 4333
» **Worldwide:** +1 732 981 0060
» Contact & Support

About IEEE *Xplore* | Contact Us | Help | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2017 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	14/566,403	Filing Date	2014-12-30	Docket Number (if applicable)	FORT-012500	Art Unit	2438
First Named Inventor	Pernicha			Examiner Name	Chang, Kenneth W		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, to any international application that does not comply with the requirements of 35 U.S.C. 371, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV.

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☐ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No _____

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

Applicant Signature

EFS - Web 2.1.15

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Michael A. DeSanctis/	Date (YYYY-MM-DD)	2017-05-02
Name	Michael A. DeSanctis	Registration Number	39957

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal	
Application Number:	14566403
Filing Date:	30-Dec-2014
Title of Invention:	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT
First Named Inventor/Applicant Name:	Hugo Filipe Parreira Pernicha
Filer:	Michael A. DeSanctis
Attorney Docket Number:	FORT-012500
Filed as Large Entity	
Filing Fees for Utility under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
RCE- 1st Request	1801	1	1200	1200
		Total in USD ($)		**1200**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Electronic Acknowledgement Receipt	
EFS ID:	29096985
Application Number:	14566403
International Application Number:	
Confirmation Number:	7209
Title of Invention:	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT
First Named Inventor/Applicant Name:	Hugo Filipe Parreira Pernicha
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-012500
Receipt Date:	02-MAY-2017
Filing Date:	30-DEC-2014
Time Stamp:	18:11:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1200
RAM confirmation Number	050317INTEFSW18115900
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Amendment_Response_5_2_17.pdf	114533 ca089ad89635ceff0619d4daa9738e990ebc473f	yes	10
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment Submitted/Entered with Filing of CPA/RCE		1	1	
	Claims		2	7	
	Applicant Arguments/Remarks Made in an Amendment		8	10	
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	RCE.pdf	1349859 b87e8722001ae3b081b60704bd8e1018d3fda723	no	3
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30284 7b483d0dcdea4117e15b70651d255de014ff4ee5	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1494676		

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Fortinet, Inc.	Examiner: Chang, Kenneth W
Inventons: Pernicha et al.	Group Art Unit: 2438
App. No.: 14/566,403	Conf. No.: 7209
Filed: December 30, 2014	Docket No.: FORT-012500
For: DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT	

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO OFFICE ACTION

Sir/Madam:

In response to the Office Action having a notification date of February 2, 2017 (the "Office Action"), the Applicant respectfully requests the Examiner to enter the following amendment and to consider the following remarks:

Amendments to the Claims are reflected in the listing of claims, which begins on page 2 of this paper.

Remarks begin on page 8 of this paper.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Amendments to the Claims

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. **(Currently amended)** A method comprising:

receiving, by a network security management device, a request to add a new traffic flow policy rule to a plurality of policy rules managed by the network security management device;

automatically determining, by the network security management device, dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules;

forming, by the network security management device, an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules based on the determined dependencies;

automatically optimizing, by the network security management device, the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein the optimizing is based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules, wherein the optimizing by the network security management device is performed in real time.

2. **(Original)** The method of claim 1, wherein said determining dependencies comprises evaluating dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

3. **(Original)** The method of claim 1, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging is conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

4. **(Original)** The method of claim 3, wherein the merging of combinable policy rules is conducted based on superneting of one or more of the source IP addresses and the destination IP addresses.

5. **(Original)** The method of claim 1, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of policy rules based on one or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters.

6. **(Original)** The method of claim 5, wherein the order of the policy rules of the second sub-set of policy rules is changed based on frequency of usage thereof.

7. **(Original)** The method of claim 1, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules.

8. **(Original)** The method of claim 7, wherein the one or more conflicts include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

9. **(Original)** The method of claim 7, wherein the one or more conflicts include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule.

10. **(Original)** The method of claim 1, wherein the one or more weights are defined manually based on scope and attributes of policy rule.

11. **(Original)** The method of claim 1, wherein the one or more weights are defined automatically.

12. **(Original)** The method of claim 1, wherein said forming an updated set of policy rules is conducted based on the one or more weights, the preference settings, the priority settings for the policy rules, network traffic characteristics, and network usage statistics.

13. **(Currently amended)** A network security policy management system comprising:

one or more processors; and

one or more internal data storage devices operatively coupled to the one or more processors and storing:

a business traffic flow input module configured to receive a request to add a new traffic flow policy rule to a plurality of policy rules managed by the system;

a dependency detection module configured to automatically determine dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules;

a traffic flow policy rule incorporation module configured to form an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules based on the determined dependencies; and

a policy rule optimization module configured to automatically optimize the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein the optimizing is performed in real-time based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

14. **(Original)** The system of claim 13, wherein the dependency detection module is further configured to evaluate dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules.

15. **(Original)** The system of claim 13, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging is conducted based on matching of one or more of source IP addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

16. **(Original)** The system of claim 15, wherein the merging of combinable policy rules is conducted based on superneting of one or more of the source Internet Protocol (IP) addresses and the destination IP addresses.

17. **(Original)** The system of claim 13, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of policy rules based on one or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters.

18. **(Original)** The system of claim 13, wherein said deleting the third sub-set of policy rules comprises deleting the policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

19. **(Original)** The system of claim 18, wherein the one or more conflicts include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules.

20. **(Original)** The system of claim 18, wherein the one or more conflicts comprise one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule.

21. **(Original)** The system of claim 13, wherein the one or more weights are defined manually based on scope and attributes of the policy rule.

22. **(Original)** The system of claim 13, wherein the one or more weights are defined automatically.

23. **(Currently amended)** A network security policy management system comprising:

one or more processors; and

one or more internal data storage devices operatively coupled to the one or more processors and storing a policy rule optimization module configured to retrieve information regarding a current set of policy rules and optimize the current set of policy rules by grouping a first sub-set of policy rules of the current set of policy rules, reordering a second sub-set of policy rules of the current set of policy rules, and deleting a third sub-set of policy rules of the current set of policy rules, wherein the optimizing is performed in real-time based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and usage statistics for each policy rule of the current set of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

24. **(Original)** The system of claim 23, wherein said grouping the first sub-set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging is conducted based on matching of one or more of source IP addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

25. **(Original)** The system of claim 23, wherein said reordering the second sub-set of policy rules comprises changing an order of the policy rules of the second sub-set of policy rules based on one or more of their source Internet Protocol (IP) addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters.

26. **(Original)** The system of claim 23, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the retrieved set of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Remarks

The Applicant respectfully requests reconsideration of this application in view of the following remarks. Claims 1-26 are pending, with claims 1, 13 and 23 being independent. Claims 1, 13 and 23 have been amended. Support for the amendments is found at least in ¶¶ [0028], [0034], [0041], [0044] of the specification. No new subject matter has been added.

Claims 1, 2, 5, 13, 14, and 17 stand rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada (US 20010039576 A1) in view of Yang (US 20100100954 A1).

Claims 3 and 15 stand rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Yang as applied to Claims 1 and 13, and further in view of Porat (US 20080062994 A1).

Claims 4 and 16 stand rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Yang and Porat as applied to Claims 3 and 13, and further in view of Liu (US 20020154635 A1).

Claim 6 stands rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Yang as applied to Claim 1, and further in view of Corl et al. (US 20020198981 A1, hereinafter Corl).

Claims 3 and 15 stand rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Yang as applied to Claims 1 and 13, and further in view of Goldschmidt et al. (US 20060013136 A1, hereinafter Goldschmidt).

Claim 12 stands rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Yang as applied to Claim 1, and further in view of Goldschmidt and Corl.

Claims 23-25 stand rejected under 35 U.S.C. 103 as allegedly being unpatentable over Yang in view of Porat.

Claim 26 stands rejected under 35 U.S.C. 103 as allegedly being unpatentable over Yang in view of Porat, and further in view of Goldschmidt.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

The independent claims, as amended, include optimizing of security policy rules in real-time based for example on network traffic characteristics. Thus, in addition to optimizations which can be performed in response to a request to add a new traffic flow policy rule to a plurality of policy rules managed by a network security management device, such a network security management device or policy rule optimization module can perform security policy rule optimization in real-time. While Yang does disclose periodically removing unused rules (see Yang, Abstract and Summary), Yang does not teach security policy rule optimization in real-time. To illustrate Yang's periodic rule removal, Yang teaches that a rule that has been unused for 90 days should be removed. (Yang, ¶ [0029])

The present specification also discloses an embodiment in which policy rule optimization is configured to run on a periodic basis. (Specification, ¶ [0061]) However, the specification teaches both the periodic optimization of ¶ [0061] and real-time optimization as in ¶¶ [0028], [0034], [0041], [0044], and Yang's teaching of "periodically identifying the unused rule set for each external partner network and removing these obsolete rules" (Yang, Abstract) does not disclose the real-time optimizing of security policy rules as in the amended independent claims.

For at least these reasons, the independent claims are believed allowable over the cited references. Reconsideration and allowance are respectfully requested.

The dependent claims depend upon independent claims which are allowable over the cited art as discussed above. These dependent claims are likewise in condition for allowance at least because they depend on allowable independent claims. However, the dependent claims are believed independently allowable at least in that they recite particular features which, when combined with the elements of the independent claim, are not disclosed or suggested in the cited references.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Conclusion

The undersigned respectfully submits that the amendments and remarks presented herein have overcome the rejections, and that the pending claims are in condition for allowance. Accordingly, the undersigned requests that the rejections be withdrawn and that a Notice of Allowance be promptly issued for claims 1-26.

By responding in the foregoing remarks only to particular positions taken by the Examiner, the Applicant does not acquiesce with any other positions that have not been explicitly addressed. Applicant's arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist. The absence of a reply to a specific rejection, issue or comment set forth in the Office Action does not signify agreement with or concession of that rejection, issue or comment. In addition, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, and the amendment of any claim does not necessarily signify any concession of unpatentability of the claim prior to its amendment.

In view of the foregoing, the Applicant respectfully asserts that all claims now pending in the application are in condition for allowance. Hence, an early allowance of all such claims is earnestly requested.

Respectfully submitted,
Hamilton, DeSanctis & Cha LLP

By /Guy K. Clinger/
Guy K. Clinger
Reg. No. 42,422
Customer No. 64128
Ph: 720-446-1888

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/566,403	Filing Date 12/30/2014	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **05/02/2017**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 26	Minus	** 26	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/DORIS KING/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/566,403	12/30/2014	Hugo Filipe Parreira Pernicha	FORT-012500	7209

64128 7590 02/02/2017

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

EXAMINER	
CHANG, KENNETH W	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
02/02/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mdesanctis@hdciplaw.com
docket@hdciplaw.com

PTOL-90A (Rev. 04/07)

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Office Action Summary	Application No. 14/566,403	Applicant(s) PERNICHA, HUGO FILIPE PARREIRA	
	Examiner Kenneth Chang	Art Unit 2438	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/27/2016*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-26* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-26* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

1. The following is a Final Office action in response to applicant's amendment filed on 10/27/2016. Claims 1, 13, and 23 have been amended with support from ¶ [0029] of the specification. **Claims 1-26** are currently pending and have been considered as follows.

2. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Response to Arguments

3. Applicant's arguments and amendment with respect to the 35 U.S.C. §101 rejection(s) of claims 1-26 on pages 8-14 of the remarks filed on 10/27/2016 have been fully considered and are persuasive. Therefore, the 35 U.S.C. §101 rejection of claims 1-26 is withdrawn.

4. Applicant's amendment of independent Claims 1, 13, and 23 have changed the scope of the claimed invention thereby necessitating new ground(s) of rejection. Therefore, Applicant's arguments on pages 15-19 of the remarks filed on 10/27/2016 with respect to the 35 U.S.C. 102(a)(1) and 102(a)(2) rejections have been fully considered but are moot because the arguments do not apply to any of the updated references being used in the current rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 1, 2, 5, 13, 14, and 17** are rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** (US 20010039576 A1) in view of **YANG** (US 20100100954 A1).

As to Amended Claim 1:

Kanada discloses a method **(e.g. Kanada FIG. 5; [0002] methods; [0093])** comprising:

- receiving, by a network security management device **(e.g. Kanada policy server with operator console [0066]; [0067])**, a request to add a new traffic flow policy rule to a plurality of policy rules **(e.g. Kanada rule specified to be added [0021]; receiving input to add policy rule [0067])** managed by the network security management device;
- automatically determining, by the network security management device, dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules **(e.g. Kanada detects policy rules that the new policy rule depends on [Abstract]; analyzing policy rules for dependence of policy rule data on another policy rule data [0028]; [0068]; [0099]; [0103]; [0167])**;
- forming, by the network security management device, an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules **(e.g. Kanada add and store input policy rules into policy repository [0067]; [0070]; [0071]; rule table contains all input rules [0087]; list of rule identifiers and added rule sent to router [0099])** based on the determined dependencies;

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

But **Kanada** does not specifically disclose:

- automatically optimizing, by the network security management device, the updated set of policy rules by **one** or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, ***wherein the optimizing is based on* one** or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules.

However, the analogous art **YANG** does disclose automatically optimizing, by the network security management device, the updated set of policy rules **(e.g. YANG firewall rule reduction [0014] for performance enhancement [0029] and reducing overall parsing time [0030]; by the firewall rules reduction module [0032])** by **one** or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules **(e.g. YANG removing unused obsolete rules [0005]; [0029]; placing order of the rules in the firewall configuration [0029]; more frequently used firewall rule placed higher position [0030])**, wherein the optimizing is based on **one** or more of weights assigned to particular types of traffic, preference settings, priority settings **(e.g. YANG placing order of the rules in higher position is based on access count for each rule**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0029]; more frequently used firewall rule placed higher position [0030]), network traffic characteristics **(e.g. YANG identifies existing firewall rules that have been used recently and marked valid on a per external partner network basis [0029]; firewall rule network attributes including source IP, destination IP address, direction, incoming or outgoing [0016]; identified IP addresses [0017])** and usage statistics for each policy rule **(e.g. YANG access count for each valid rule [0029]; [0030])** of the updated set of policy rules. **Kanada** and **YANG** are analogous art because they are from the same field of endeavor in management of network firewall rules.

- (e.g. see **YANG**, "In step 220, the method uses the parsed information to identify all existing firewall rules on a per external partner network basis. In other words, the method identifies, for each external partner network, its routable network address space and all the existing firewall rules associated with that particular external partner network. Firewall rule may comprise attributes that includes, but are not limited to, source IP address, destination IP address, protocol used (e.g., TCP or UDP, etc), protocol port number, direction (e.g., incoming or outgoing) etc" **[0016]**; see also "the method uses the parsed information to identify the permitted IP address space on a per external partner network basis. In other words, the method identifies, for each external partner network, all the valid IP source and destination addresses permitted for access by that particular external partner network" **[0017]**; see also "Once method 300 is executed, it produces an output that identifies all existing firewall rules that have been used recently and

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

> marked valid on a per external partner network basis. Therefore, for the existing firewall rules of each external partner network that have not been marked valid, they are considered obsolete or unused rules. In one embodiment, it is reasonable to assume that an unused rule for a predefined period of time, e.g., 90 days or more should be removed. The length of the unused period of time threshold of an unused rule is a configurable parameter set by the network operator. The output also produces the access count for each valid rule for each external partner network. The access count for each individual rule can be used as a reference for the activities associated to the rule as well as the placing order of the rule in the firewall configuration and security policy files for performance enhancement" **[0029]**; see also "For instance, more frequently used firewall rule should be placed at a higher position in the firewall access list in the firewall configuration and security policy files to reduce overall parsing time during normal operations of the firewall system" **[0030]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada** and **YANG** before him or her, to modify the invention of **Kanada** with the teachings of **YANG** to include *automatically optimizing, by the network security management device, the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein the optimizing is based on one or more of weights assigned to*

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules as claimed because **Kanada** provides a network system including a server and routers for management of network policy rules that may be added, deleted, and/or updated **(Kanada [0021]-[0137])** which could include ordering more frequently used firewall rules in higher positions and removing obsolete or unused rules based on access counts and external partner network attributes **(YANG [0016]; [0017]; [0029]; [0030])**. The suggestion/motivation for doing so would have been for performance enhancement and to reduce overall parsing time during normal operations of the firewall system **(YANG [0029]; [0030])**. Therefore, it would have been obvious to combine **Kanada** and **YANG** to obtain the invention as specified in the instant claim(s).

As to Claim 2:

Kanada in view of **YANG** discloses the method of claim 1, wherein said determining dependencies comprises evaluating dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules **(e.g. Kanada "By referring to the policy repository 211 and the variable reference table 214, the policy rule dependence analyzer 204 analyzes the relation between the rules entered to be added or removed and the relation between these rules and the existing rules to find dependence of a rule on another rule. This analyzer 204 then delivers at a time the rule identifiers of all interdependent rules to the policy scheduler 205" [0068])**.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

As to Claim 5:

Kanada in view of **YANG** discloses the method of claim 1, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of policy rules based on **one** or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters **(e.g. YANG placing order of the rules in higher position is based on access count for each rule [0029]; more frequently used firewall rule placed higher position [0030]; see also Kanada rules can be rearranged such that defined variable always precede those that are used as a condition [0106])**. The Examiner supplies the same rationale for the combination of references **Kanada** and **YANG** as in Claim 1 above.

As to Amended Claim 13:

Kanada discloses a network security policy management system **(e.g. Kanada FIG. 1 [0060]-[0072])** comprising:

- one or more processors **(e.g. Kanada processor [0066])**; and
- one or more internal data storage devices **(e.g. Kanada hard disk or main storage [0066]; [0134])** operatively coupled to the one or more processors and storing:
- a business traffic flow input module **(e.g. Kanada software unit [0066])** configured to receive a request to add a new traffic flow policy rule to a plurality of policy rules managed by the system **(e.g. Kanada rule specified to be added [0021]; receiving input to add policy rule [0067])**;

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

- a dependency detection module **(e.g. Kanada software unit [0066])** configured to automatically determine dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules **(e.g. Kanada detects policy rules that the new policy rule depends on [Abstract]; analyzing policy rules for dependence of policy rule data on another policy rule data [0028]; [0068]; [0099]; [0103]; [0167])**;
- a traffic flow policy rule incorporation module **(e.g. Kanada software unit [0066])** configured to form an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules based on the determined dependencies **(e.g. Kanada add and store input policy rules into policy repository [0067]; [0070]; [0071]; rule table contains all input rules [0087]; list of rule identifiers and added rule sent to router [0099])**;

But **Kanada** does not specifically disclose:

- automatically optimize the updated set of policy rules by **one** or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, ***wherein the optimizing is based on* one** or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules.

However, the analogous art **YANG** does disclose automatically optimize the updated set of policy rules **(e.g. YANG firewall rule reduction [0014] for performance**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

enhancement [0029] and reducing overall parsing time [0030]; by the firewall rules reduction module [0032]) by **one** or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules **(e.g. YANG removing unused obsolete rules [0005]; [0029]; placing order of the rules in the firewall configuration [0029]; more frequently used firewall rule placed higher position [0030])**, wherein the optimizing is based on **one** or more of weights assigned to particular types of traffic, preference settings, priority settings **(e.g. YANG placing order of the rules in higher position is based on access count for each rule [0029]; more frequently used firewall rule placed higher position [0030])**, network traffic characteristics **(e.g. YANG identifies existing firewall rules that have been used recently and marked valid on a per external partner network basis [0029]; firewall rule network attributes including source IP, destination IP address, direction, incoming or outgoing [0016]; identified IP addresses [0017])** and usage statistics for each policy rule **(e.g. YANG access count for each valid rule [0029]; [0030])** of the updated set of policy rules. **Kanada** and **YANG** are analogous art because they are from the same field of endeavor in management of network firewall rules.

- (e.g. see **YANG**, "In step 220, the method uses the parsed information to identify all existing firewall rules on a per external partner network basis. In other words, the method identifies, for each external partner network, its routable network address space and all the existing firewall rules associated with that particular

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

external partner network. Firewall rule may comprise attributes that includes, but are not limited to, source IP address, destination IP address, protocol used (e.g., TCP or UDP, etc), protocol port number, direction (e.g., incoming or outgoing) etc" **[0016]**; see also "the method uses the parsed information to identify the permitted IP address space on a per external partner network basis. In other words, the method identifies, for each external partner network, all the valid IP source and destination addresses permitted for access by that particular external partner network" **[0017]**; see also "Once method 300 is executed, it produces an output that identifies all existing firewall rules that have been used recently and marked valid on a per external partner network basis. Therefore, for the existing firewall rules of each external partner network that have not been marked valid, they are considered obsolete or unused rules. In one embodiment, it is reasonable to assume that an unused rule for a predefined period of time, e.g., 90 days or more should be removed. The length of the unused period of time threshold of an unused rule is a configurable parameter set by the network operator. The output also produces the access count for each valid rule for each external partner network. The access count for each individual rule can be used as a reference for the activities associated to the rule as well as the placing order of the rule in the firewall configuration and security policy files for performance enhancement" **[0029]**; see also "For instance, more frequently used firewall rule should be placed at a higher position in the firewall access list in the firewall

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

configuration and security policy files to reduce overall parsing time during normal operations of the firewall system" **[0030]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada** and **YANG** before him or her, to modify the invention of **Kanada** with the teachings of **YANG** to include *automatically optimize the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein the optimizing is based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules* as claimed because **Kanada** provides a network system including a server and routers for management of network policy rules that may be added, deleted, and/or updated **(Kanada [0021]-[0137])** which could include ordering more frequently used firewall rules in higher positions and removing obsolete or unused rules based on access counts and external partner network attributes **(YANG [0016]; [0017]; [0029]; [0030])**. The suggestion/motivation for doing so would have been for performance enhancement and to reduce overall parsing time during normal operations of the firewall system **(YANG [0029]; [0030])**. Therefore, it would have been obvious to combine **Kanada** and **YANG** to obtain the invention as specified in the instant claim(s).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

As to Claim 14:

Kanada in view of **YANG** discloses the system of claim 13, wherein the dependency detection module is further configured to evaluate dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules. **(e.g. Kanada "By referring to the policy repository 211 and the variable reference table 214, the policy rule dependence analyzer 204 analyzes the relation between the rules entered to be added or removed and the relation between these rules and the existing rules to find dependence of a rule on another rule. This analyzer 204 then delivers at a time the rule identifiers of all interdependent rules to the policy scheduler 205" [0068])**.

As to Claim 17:

Kanada in view of **YANG** discloses the system of claim 13, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of policy rules based on **one** or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters **(e.g. YANG placing order of the rules in higher position is based on access count for each rule [0029]; more frequently used firewall rule placed higher position [0030]; see also Kanada rules can be rearranged such that defined variable always precede those that are used as a condition [0106])**. The Examiner supplies the same rationale for the combination of references **Kanada** and **YANG** as in Claim 13 above.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

7. **Claims 3 and 15** are rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of **YANG** as applied to Claims 1 and 13 above, and further in view of **Porat** (US 20080062994 A1).

As to Claim 3:

Kanada in view of **YANG** discloses the method of claim 1, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule **(e.g. Kanada plurality of rules are merged into one rule [0021]; rules on lines 1302 and 1303 are merged into one rule [0139]; in a form that can be executed [0147]; [0179])**, but does not specifically disclose:

- wherein the merging is conducted ***based on matching of one*** or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

However, the analogous art **Porat** does disclose wherein the merging is conducted **(e.g. Porat combining the rules of several HVIDs into one rule [0046])** based on matching of **one** or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules **(e.g. Porat combining the rules into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using the same rule)**. **Kanada**, **YANG**, and **Porat** are analogous art because they are from the same field of endeavor in network rule management.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

- (e.g. see **Porat**, "The use of subnet masks enables pruning of the filtering database according to the address scheme by combining the rules of several HVIDs into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using the same rule)" **[0046]**; see also "In addition, the subnet mask can be used to filter and prune MAC address rules in the filtering database" **[0047]**; see also "Thus, the bridge 50 is pre-programmed to know which bits of the HVID or MAC must be read for forwarding information, and which can be ignored for that particular hop. Preferably, an algorithm for best match or longest prefix (similar to that used in IP routing) runs in switching processor 52. It will be appreciated that an address can have different subnet masks, i.e., one can look at the first three bits, while another only looks at the first two bits. The algorithm for best match utilizes the rule that has the most bits in the subnet mask, e.g., the longest matching address with the highest number of matching bits, or any other rule used to define best match, such as least cost, etc" **[0048]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, and **Porat** before him or her, to modify the combination of **Kanada** and **YANG** with the teachings of **Porat** to include *wherein the merging is conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules* as claimed because **Kanada** already teaches management of network

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

policy rules that may be added, deleted, updated, and merged **(Kanada [0021]-[0137]; [0139])** which could be based on matching subnet prefixes **(Porat [0046]-[0048])**. The suggestion/motivation for doing so would have been to enable pruning of the filtering database according to an address scheme **(Porat [0046])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, and **Porat** to obtain the invention as specified in the instant claim(s).

As to Claim 15:

Kanada in view of **YANG** discloses the system of claim 13, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule **(e.g. Kanada plurality of rules are merged into one rule [0021]; rules on lines 1302 and 1303 are merged into one rule [0139]; in a form that can be executed [0147]; [0179])**, but does not specifically disclose:

- wherein the merging is conducted ***based on matching of one*** or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

However, the analogous art **Porat** does disclose wherein the merging is conducted **(e.g. Porat combining the rules of several HVIDs into one rule [0046])** based on matching of **one** or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules **(e.g. Porat combining the rules into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

the same rule). **Kanada**, **YANG**, and **Porat** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Porat**, "The use of subnet masks enables pruning of the filtering database according to the address scheme by combining the rules of several HVIDs into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using the same rule)" **[0046]**; see also "In addition, the subnet mask can be used to filter and prune MAC address rules in the filtering database" **[0047]**; see also "Thus, the bridge 50 is pre-programmed to know which bits of the HVID or MAC must be read for forwarding information, and which can be ignored for that particular hop. Preferably, an algorithm for best match or longest prefix (similar to that used in IP routing) runs in switching processor 52. It will be appreciated that an address can have different subnet masks, i.e., one can look at the first three bits, while another only looks at the first two bits. The algorithm for best match utilizes the rule that has the most bits in the subnet mask, e.g., the longest matching address with the highest number of matching bits, or any other rule used to define best match, such as least cost, etc" **[0048]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, and **Porat** before him or her, to modify the combination of **Kanada** and **YANG** with the teachings of **Porat** to include *wherein the merging is conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination IP addresses,*

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules as claimed because **Kanada** already teaches management of network policy rules that may be added, deleted, updated, and merged **(Kanada [0021]-[0137]; [0139])** which could be based on matching subnet prefixes **(Porat [0046]-[0048])**. The suggestion/motivation for doing so would have been to enable pruning of the filtering database according to an address scheme **(Porat [0046])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, and **Porat** to obtain the invention as specified in the instant claim(s).

8. **Claims 4 and 16** are rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of **YANG** and **Porat** as applied to Claims 3 and 13 above, and further in view of **Liu** (US 20020154635 A1).

As to Claim 4:

Kanada in view of **YANG** and **Porat** discloses the method of claim 3, but does not specifically disclose:

- superneting of one or more of the source IP addresses and the destination IP addresses.

However, the analogous art **Liu** does disclose superneting of one or more of the source IP addresses and the destination IP addresses **(e.g. Liu Supernet security layer prepends real source and destination IP addresses [0062]; [0076])**. **Kanada**, **YANG**, **Porat** and **Liu** are analogous art because they are from the same field of endeavor in network traffic management.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

- (e.g. see **Liu**, "a Supernet security layer (SNSL) 532, acting as the conduit for all Supernet communications. To conserve memory, both inner IP layer 530 and outer IP layer 534 may share the same instance of the code of an IP layer. SNSL 532 performs security functionality as well as address translation. It also caches the most recently used channel keys for ten seconds. Thus, when a channel key is needed, SNSL 532 checks its cache first, and if it is not found, it requests KMD 520 to contact the appropriate KMC to retrieve the appropriate channel key. Two IP layers 530, 534 are used in the TCP /IP protocol stack 524 because both the internal addressing scheme and the external addressing scheme are IP-based. Thus, for example, when a packet is sent, inner IP layer 530 receives the packet from TCP/UDP layer 528 and processes the packet with its node ID address before passing it to the SNSL layer 532, which encrypts it, prepends the real source IP address and the real destination IP address, and then passes the encrypted packet to outer IP layer 534 for sending to the destination" **[0062]**; see also **[0076]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, **Porat** and **Liu** before him or her, to modify the combination of **Kanada**, **YANG**, and **Porat** with the teachings of **Liu** to include *superneting of one or more of the source IP addresses and the destination IP addresses* as claimed because **Kanada** provides a policy rule controlled network with server and routers **(Kanada [0021]-[0137])** which could include implement a Supernet security layer that translates source and destination IP addresses

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

of communicated packets **(Liu [0062]; [0076])**. The suggestion/motivation for doing so would have been to allow utilization of public-network infrastructure without the need to maintain a private network to be able to use resources securely and without geographical restriction **(Liu [0020])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, **Porat** and **Liu** to obtain the invention as specified in the instant claim(s).

As to Claim 16:

Kanada in view of **YANG** and **Porat** discloses the system of claim 15, but does not specifically disclose:

- superneting of one or more of the source Internet Protocol (IP) addresses and the destination IP addresses.

However, the analogous art **Liu** does disclose superneting of one or more of the source IP addresses and the destination IP addresses **(e.g. Liu Supernet security layer prepends real source and destination IP addresses [0062]; [0076])**. **Kanada**, **YANG**, **Porat** and **Liu** are analogous art because they are from the same field of endeavor in network traffic management.

- (e.g. see **Liu**, "a Supernet security layer (SNSL) 532, acting as the conduit for all Supernet communications. To conserve memory, both inner IP layer 530 and outer IP layer 534 may share the same instance of the code of an IP layer. SNSL 532 performs security functionality as well as address translation. It also caches the most recently used channel keys for ten seconds. Thus, when a channel key is needed, SNSL 532 checks its cache first, and if it is not found, it requests KMD

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

520 to contact the appropriate KMC to retrieve the appropriate channel key. Two IP layers 530, 534 are used in the TCP /IP protocol stack 524 because both the internal addressing scheme and the external addressing scheme are IP-based. Thus, for example, when a packet is sent, inner IP layer 530 receives the packet from TCP/UDP layer 528 and processes the packet with its node ID address before passing it to the SNSL layer 532, which encrypts it, prepends the real source IP address and the real destination IP address, and then passes the encrypted packet to outer IP layer 534 for sending to the destination" **[0062]**; see also **[0076]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, **Porat** and **Liu** before him or her, to modify the combination of **Kanada**, **YANG**, and **Porat** with the teachings of **Liu** to include *superneting of one or more of the source IP addresses and the destination IP addresses* as claimed because **Kanada** provides a policy rule controlled network with server and routers **(Kanada [0021]-[0137])** which could include implement a Supernet security layer that translates source and destination IP addresses of communicated packets **(Liu [0062]; [0076])**. The suggestion/motivation for doing so would have been to allow utilization of public-network infrastructure without the need to maintain a private network to be able to use resources securely and without geographical restriction **(Liu [0020])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, **Porat** and **Liu** to obtain the invention as specified in the instant claim(s).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

9. **Claim 6** is rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of **YANG** as applied to Claim 1 above, and further in view of Corl et al. (US 20020198981 A1, hereinafter **Corl**).

As to Claim 6:

Kanada in view of **YANG** discloses the method of claim 5, but does not specifically disclose:

- wherein the order of the policy rules of the second sub-set of policy rules is changed based on frequency of usage thereof.

However, the analogous art **Corl** does disclose wherein the order of the policy rules of the second sub-set of policy rules is changed based on frequency of usage thereof **(e.g. Corl placing the plurality of filter rules in an order based on frequency of reach filter rule [Abstract]; statistics of frequency [0024]; placing higher frequency filter rules first [0028])**. **Kanada**, **YANG**, and **Corl** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Corl**, "Each of the plurality of filter rules has a priority. The method and system include accumulating statistics for each of the plurality of filter rules. The statistics indicate a frequency of enforcement for each of the plurality of filter rules. The method and system also include placing the plurality of filter rules in an order for testing against the key. The order is based on the frequency of each filter rule of the portion of the plurality of filter rules" **[Abstract]**; see also "The statistics indicate a frequency of enforcement for each of the plurality of filter rules. The method and system also comprise placing the plurality of filter rules in

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

an order for testing against the key. The order is based on the frequency of each filter rule of the portion of the plurality of filter rules" **[0024]**; see also "The order preferably places higher frequency filter rules first, so that the filter rules that are enforced more often will be tested first. The order preferably places the remaining rules in order of their frequency" **[0028]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, and **Corl** before him or her, to modify the combination of **Kanada** and **YANG** with the teachings of **Corl** to include *wherein the order of the policy rules of the second sub-set of policy rules is changed based on frequency of usage thereof* as claimed because **Kanada** provides a policy rule controlled network with server and routers **(Kanada [0021]-[0137])** which could accumulate frequency statistics for each rule and place higher frequency filter rules first **(Corl [0062]; [0076])**. The suggestion/motivation for doing so would have been to save time and allow network processing to function more efficiently **(Corl [0029])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, and **Corl** to obtain the invention as specified in the instant claim(s).

10. **Claims 7-11 and 18-22** are rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of **YANG** as applied to Claims 1 and 13 above, and further in view of Goldschmidt et al. (US 20060013136 A1, hereinafter **Goldschmidt**).

As to Claim 7:

Kanada in view of **YANG** discloses the method of claim 1, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

rules **(e.g. deleting policy rules and checks consistency Kanada [0069]; [0096]; [0097])**, but does not specifically disclose:

- based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. although Kanada does teach a policy consistency checker that checks rules for being exclusive with each other [0109]-[0111])**.

However, the analogous art **Goldschmidt** does disclose based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt determining whether rules of updated rule subset have equal conflict relationship, then delete the lower priority rule [0061])**. **Kanada**, **YANG**, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "A flow manager may also receive additional packet flow rules, integrate them into the unified rule set, update the rule subsets according to the additional rules, and install the updated subsets onto the flow enforcement devices" **[Abstract]**; see also "After determining the relationship between two conflicting packet flow rules, flow manager 120 may be configured to determine whether the two rules have an equal relationship, as illustrated by decision block 440. If the two rules do have an equal conflict relationship, flow manager 120 may, according to one embodiment, append the actions of the lower priority rule to the actions of the higher priority rule, as illustrated by block 460. According to certain embodiments, if flow manager 120 appends the actions of the lower

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

priority rule to the actions of the higher priority rule, flow manager 120 may be configured to delete the lower priority rule, since is may now be redundant" **[0061]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, and **Goldschmidt** before him or her, to modify the combination of **Kanada** and **YANG** with the teachings of **Goldschmidt** to include *based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules* as claimed because **Kanada** provides a policy rule controlled network with a policy server that deletes rules **(Kanada [0021]-[0137])** which could be based on conflicting relationship of rules **(Goldschmidt [0061])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 8:

Kanada in view of **YANG** and **Goldschmidt** discloses the method of claim 7, wherein the one or more conflicts include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt "resolving a conflict between two packet flow rules that comprise identical packet filters. For example, in one embodiment, a flow manager, such as flow manager 120, may be configured to determine the relationship between the data packet**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

flow specified by the packet filters of the conflicting rules, as illustrated by block 420" [0056]; see also "two rules conflict if their packet filters specify overlapping, or identical, data flow packets" [0057]). The Examiner supplies the same rationale for the combination of references **Kanada**, **YANG**, and **Goldschmidt** as in Claim 7 above.

As to Claim 9:

Kanada in view of **YANG** and **Goldschmidt** discloses the method of claim 7, wherein the one or more conflicts include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule **(e.g. Kanada policy consistency checker that checks rules for being exclusive with each other [0109]-[0111]; Goldschmidt two or more rules may conflict by having packet filters that match the same data packets [0046]; [0051]; [0055])**. The Examiner supplies the same rationale for the combination of references **Kanada**, **YANG**, and **Goldschmidt** as in Claim 7 above.

As to Claim 10:

Kanada in view of **YANG** discloses the method of claim 1, but does not specifically disclose:

- wherein the one or more weights are defined manually based on scope and attributes of policy rule.

However, the analogous art **Goldschmidt** does disclose wherein the one or more weights are defined manually based on scope and attributes of policy rule **(e.g. Goldschmidt rules are prioritized using prefix or ordered precedence, actions**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

specified are prioritized [0038]; priority order for rules as specified by network service [0039]; administrator may provide the priorities [0047]). **Kanada**, **YANG**, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, and **Goldschmidt** before him or her, to modify the combination of **Kanada** and **YANG** with the teachings of **Goldschmidt** to include *wherein the one or more weights are defined manually based on scope and attributes of policy rule* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

have been obvious to combine **Kanada**, **YANG**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 11:

Kanada in view of **YANG** discloses the method of claim 1, but does not specifically disclose:

- wherein the one or more weights are defined automatically.

However, the analogous art **Goldschmidt** does disclose wherein the one or more weights are defined automatically **(e.g. Goldschmidt rules are prioritized using prefix or ordered precedence, actions specified are prioritized [0038]; policies are received that express priorities between network services and their supplied packet flow rules [0047])**. **Kanada**, **YANG**, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings **Kanada**, **YANG**, and **Goldschmidt** before him or her, to modify the combination of **Kanada** and **YANG** with

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

the teachings of **Goldschmidt** to include *wherein the one or more weights are defined manually based on scope and attributes of policy rule* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order based on received policies **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 18:

Kanada in view of **YANG** discloses the system of claim 13, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules **(e.g. deleting policy rules and checks consistency Kanada [0069]; [0096]; [0097])**, but does not specifically disclose:

- based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. although Kanada does teach a policy consistency checker that checks rules for being exclusive with each other [0109]-[0111])**.

However, the analogous art **Goldschmidt** does disclose based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt determining whether rules of updated rule subset have**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

equal conflict relationship, then delete the lower priority rule [0061]). **Kanada**, **YANG**, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "A flow manager may also receive additional packet flow rules, integrate them into the unified rule set, update the rule subsets according to the additional rules, and install the updated subsets onto the flow enforcement devices" **[Abstract]**; see also "After determining the relationship between two conflicting packet flow rules, flow manager 120 may be configured to determine whether the two rules have an equal relationship, as illustrated by decision block 440. If the two rules do have an equal conflict relationship, flow manager 120 may, according to one embodiment, append the actions of the lower priority rule to the actions of the higher priority rule, as illustrated by block 460. According to certain embodiments, if flow manager 120 appends the actions of the lower priority rule to the actions of the higher priority rule, flow manager 120 may be configured to delete the lower priority rule, since is may now be redundant" **[0061]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, and **Goldschmidt** before him or her, to modify the combination of **Kanada** and **YANG** with the teachings of **Goldschmidt** to include *based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules* as claimed because **Kanada** provides a policy rule controlled network with a policy server that

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

deletes rules **(Kanada [0021]-[0137])** which could be based on conflicting relationship of rules **(Goldschmidt [0061])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 19:

Kanada in view of **YANG** and **Goldschmidt** discloses the system of claim 18, wherein the one or more conflicts include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt "resolving a conflict between two packet flow rules that comprise identical packet filters. For example, in one embodiment, a flow manager, such as flow manager 120, may be configured to determine the relationship between the data packet flow specified by the packet filters of the conflicting rules, as illustrated by block 420" [0056]; see also "two rules conflict if their packet filters specify overlapping, or identical, data flow packets" [0057])**. The Examiner supplies the same rationale for the combination of references **Kanada**, **YANG**, and **Goldschmidt** as in Claim 18 above.

As to Claim 20:

Kanada in view of **YANG** and **Goldschmidt** discloses the system of claim 18, wherein the one or more conflicts comprise one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule **(e.g. Kanada policy**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

consistency checker that checks rules for being exclusive with each other [0109]-[0111]; Goldschmidt two or more rules may conflict by having packet filters that match the same data packets [0046]; [0051]; [0055]). The Examiner supplies the same rationale for the combination of references **Kanada**, **YANG**, and **Goldschmidt** as in Claim 18 above.

As to Claim 21:

Kanada in view of **YANG** discloses the system of claim 13, but does not specifically disclose:

- wherein the one or more weights are defined manually based on scope and attributes of the policy rule.

However, the analogous art **Goldschmidt** does disclose wherein the one or more weights are defined manually based on scope and attributes of the policy rule **(e.g. Goldschmidt rules are prioritized using prefix or ordered precedence, actions specified are prioritized [0038]; priority order for rules as specified by network service [0039]; administrator may provide the priorities [0047])**. **Kanada**, **YANG**, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, and **Goldschmidt** before him or her, to modify the combination of **Kanada** and **YANG** with the teachings of **Goldschmidt** to include *wherein the one or more weights are defined manually based on scope and attributes of policy rule* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 22:

Kanada in view of **YANG** discloses the system of claim 13, but does not specifically disclose:

- wherein the one or more weights are defined automatically.

However, the analogous art **Goldschmidt** does disclose wherein the one or more weights are defined automatically **(e.g. Goldschmidt rules are prioritized using prefix or ordered precedence, actions specified are prioritized [0038]; policies are**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

received that express priorities between network services and their supplied packet flow rules [0047]). **Kanada**, **YANG**, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings **Kanada**, **YANG**, and **Goldschmidt** before him or her, to modify the combination of **Kanada** and **YANG** with the teachings of **Goldschmidt** to include *wherein the one or more weights are defined manually based on scope and attributes of policy rule* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order based on received policies **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore,

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

it would have been obvious to combine **Kanada**, **YANG**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

11. **Claim 12** is rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of **YANG** as applied to Claim 1 above, and further in view of **Goldschmidt** and **Corl**.

As to Claim 12:

Kanada in view of **YANG** discloses the method of claim 1, wherein said forming an updated set of policy rules is conducted **(e.g. Kanada add and store input policy rules into policy repository [0067]; [0070]; [0071]; rule table contains all input rules [0087]; list of rule identifiers and added rule sent to router [0099])** based on the preference settings and network traffic characteristics **(e.g. Kanada cross-reference relations between variables in policy rules [0067]; consistency checker of conditions of the rules being exclusive with each other or not [0110])**, but does not specifically disclose:

- based on the one or more weights, the priority settings for the policy rules, and network usage statistics.

However, the analogous art **Goldschmidt** does disclose based on the one or more weights **(e.g. Goldschmidt longest prefix or ordered precedence [0038])**, the priority settings for the policy rules **(e.g. Goldschmidt priority order for rules [0039]; [0040]; [0041])**. Furthermore, the analogous art **Corl** does disclose network usage statistics [for each policy rule] **(e.g. Corl statistics of frequency of enforcement for reach of the plurality of filter rules [0024])**. **Kanada**, **YANG**, **Goldschmidt**, and **Corl** are

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, “multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list” **[0038]**; see also “A flow manager may also add rules to the unified rule set according to the particular priority order for those rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**);
- (e.g. see **Corl**, “Each of the plurality of filter rules has a priority. The method and system include accumulating statistics for each of the plurality of filter rules. The statistics indicate a frequency of enforcement for each of the plurality of filter rules. The method and system also include placing the plurality of filter rules in an order for testing against the key. The order is based on the frequency of each filter rule of the portion of the plurality of filter rules” **[Abstract]**; see also “The statistics indicate a frequency of enforcement for each of the plurality of filter rules. The method and system also comprise placing the plurality of filter rules in an order for testing against the key. The order is based on the frequency of each filter rule of the portion of the plurality of filter rules” **[0024]**; see also “The order preferably places higher frequency filter rules first, so that the filter rules that are enforced more often will be tested first. The order preferably places the remaining rules in order of their frequency" **[0028]**).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **YANG**, **Goldschmidt**, and **Corl** before him or her, to modify the combination of **Kanada** and **YANG** with the teachings of **Goldschmidt** and **Corl** to include *based on the one or more weights, the priority settings for the policy rules, and network usage statistics* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order based on received policies **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])** and accumulating frequency statistics for each rule and placing higher frequency filter rules first **(Corl [0062]; [0076])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])** and to save time and allow network processing to function more efficiently **(Corl [0029])**. Therefore, it would have been obvious to combine **Kanada**, **YANG**, **Goldschmidt**, and **Corl** to obtain the invention as specified in the instant claim(s).

12. **Claims 23-25** are rejected under 35 U.S.C. 103 as being unpatentable over **YANG** in view of **Porat**.

As to Amended Claim 23:

YANG discloses a network security policy management system **(e.g. YANG method and apparatus for reducing obsolete firewall rules [Abstract]; parsing firewall**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

configuration and security policy files [0014]; [0015]; FIG. 4 system [0031])

comprising:

- one or more processors **(e.g. YANG processor element [0031])**; and
- one or more internal data storage devices **(e.g. YANG memory, RAM, ROM, [0031])** operatively coupled to the one or more processors and storing a policy rule optimization module **(e.g. YANG firewall rules reduction module [0031]; [0032])** configured to retrieve information regarding a current set of policy rules **(e.g. YANG parsing firewall security policy files [0014]; [0015])** and optimize the current set of policy rules **(e.g. YANG firewall rule reduction [0014] for performance enhancement [0029] and reducing overall parsing time [0030]; by the firewall rules reduction module [0032])** by reordering a second sub-set of policy rules of the current set of policy rules, and deleting a third sub-set of policy rules of the current set of policy rules **(e.g. YANG removing unused obsolete rules [0005]; [0029]; placing order of the rules in the firewall configuration [0029]; more frequently used firewall rule placed higher position [0030])**, wherein the optimizing is based on **one** or more of weights assigned to particular types of traffic, preference settings, priority settings **(e.g. YANG placing order of the rules in higher position is based on access count for each rule [0029]; more frequently used firewall rule placed higher position [0030])**, network traffic characteristics **(e.g. YANG identifies existing firewall rules that have been used recently and marked valid on a per external partner network basis [0029]; firewall rule network attributes**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

including source IP, destination IP address, direction, incoming or outgoing [0016]; identified IP addresses [0017]) and usage statistics for each policy rule **(e.g. YANG access count for each valid rule [0029]; [0030])** of the current set of policy rules.

But **YANG** does not specifically disclose:

- grouping a first sub-set of policy rules of the current set of policy rules based on **one** or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and usage statistics for each policy rule of the current set of policy rules.

However, the analogous art **Porat** does disclose grouping a first sub-set of policy rules of the current set of policy rules **(e.g. Porat combining the rules of several HVIDs into one rule [0046])** based on **one** or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics **(e.g. Porat combining the rules into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using the same rule)**, and usage statistics for each policy rule of the current set of policy rules. **YANG** and **Porat** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Porat**, "The use of subnet masks enables pruning of the filtering database according to the address scheme by combining the rules of several HVIDs into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using the same rule)" **[0046]**; see also "In addition, the subnet mask can be used to filter and prune MAC address rules in the filtering

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

database" **[0047]**; see also "Thus, the bridge 50 is pre-programmed to know which bits of the HVID or MAC must be read for forwarding information, and which can be ignored for that particular hop. Preferably, an algorithm for best match or longest prefix (similar to that used in IP routing) runs in switching processor 52. It will be appreciated that an address can have different subnet masks, i.e., one can look at the first three bits, while another only looks at the first two bits. The algorithm for best match utilizes the rule that has the most bits in the subnet mask, e.g., the longest matching address with the highest number of matching bits, or any other rule used to define best match, such as least cost, etc" **[0048]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **YANG** and **Porat** before him or her, to modify the invention of **YANG** with the teachings of **Porat** to include *grouping a first sub-set of policy rules of the current set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and usage statistics for each policy rule of the current set of policy rules* as claimed because **YANG** already teaches an apparatus for parsing, identifying, and reducing obsolete firewall rules by reordering and removing **(YANG [Abstract]; [0014]; [0015]; [0029]-[0032])** which could also include combining rules with matching subnet prefixes **(Porat [0046]-[0048])**. The suggestion/motivation for doing so would have been to enable pruning of the filtering database according to an

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

address scheme **(Porat [0046])**. Therefore, it would have been obvious to combine **YANG**, and **Porat** to obtain the invention as specified in the instant claim(s).

As to Claim 24:

YANG in view of **Porat** discloses the system of claim 23, wherein said grouping the first sub-set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule **(e.g. Porat combining the rules of several HVIDs into one rule [0046])**, wherein the merging is conducted based on matching of **one** or more of source IP addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules **(e.g. Porat combining the rules into one rule, using a matching subnet (e.g., all HVIDs that have a prefix of 83c will be forwarded using the same rule)**. The Examiner supplies the same rationale for the combination of references **YANG** and **Porat** as in Claim 23 above.

As to Claim 25:

YANG in view of **Porat** discloses the system of claim 23, wherein said reordering the second sub-set of policy rules comprises changing an order of the policy rules of the second sub-set of policy rules based on **one** or more of their source Internet Protocol (IP) addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters **(e.g. YANG placing order of the rules in higher position is based on access count for each rule [0029]; more frequently used firewall rule placed higher position [0030])**. The Examiner supplies the same rationale for the combination of references **YANG** and **Porat** as in Claim 23 above.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

13. **Claim 26** is rejected under 35 U.S.C. 103 as being unpatentable over **YANG** in view of **Porat** as applied to Claim 23 above, and further in view of **Goldschmidt**.

As to Claim 26:

YANG in view of **Porat** discloses the system of claim 23, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules **(e.g. removing obsolete firewall rules YANG [0005]; [0029])**, but does not specifically disclose:

- based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. although Kanada does teach a policy consistency checker that checks rules for being exclusive with each other [0109]-[0111])**.

However, the analogous art **Goldschmidt** does disclose based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt determining whether rules of updated rule subset have equal conflict relationship, then delete the lower priority rule [0061])**. **YANG**, **Porat**, and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "A flow manager may also receive additional packet flow rules, integrate them into the unified rule set, update the rule subsets according to the additional rules, and install the updated subsets onto the flow enforcement devices" **[Abstract]**; see also "After determining the relationship between two conflicting packet flow rules, flow manager 120 may be configured to determine

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

whether the two rules have an equal relationship, as illustrated by decision block 440. If the two rules do have an equal conflict relationship, flow manager 120 may, according to one embodiment, append the actions of the lower priority rule to the actions of the higher priority rule, as illustrated by block 460. According to certain embodiments, if flow manager 120 appends the actions of the lower priority rule to the actions of the higher priority rule, flow manager 120 may be configured to delete the lower priority rule, since is may now be redundant" **[0061]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **YANG**, **Porat**, and **Goldschmidt** before him or her, to modify the combination of **YANG** and **Porat** with the teachings of **Goldschmidt** to include *based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules* as claimed because **YANG** already teaches an apparatus for parsing, identifying, and reducing obsolete firewall rules by reordering and removing **(YANG [Abstract]; [0014]; [0015]; [0029]-[0032])** which could be based on conflicting relationship of rules **(Goldschmidt [0061])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **YANG**, **Porat**, and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. **Cooper et al. (US 20020069200 A1)**

b. **Sheikh et al. (US 20020078382 A1)**

c. **Merugu et al. (US 20020152209 A1)**

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kenneth Chang whose telephone number is (571)270-7530. The examiner can normally be reached on Monday-Friday 10:30am-6:30pm.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kenneth Chang/
Primary Examiner, Art Unit 2438
UNITED STATES PATENT AND TRADEMARK OFFICE
01/27/17

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Notice of References Cited	Application/Control No. 14/566,403	Applicant(s)/Patent Under Reexamination PERNICHA, HUGO FILIPE PA	
	Examiner Kenneth Chang	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2002/0069200 A1	06-2002	Cooper, Geoffrey	H04L12/2602	1/1
*	B	US-2002/0078382 A1	06-2002	Sheikh, Ali	H04L12/2602	726/22
*	C	US-2002/0152209 A1	10-2002	Merugu, Shashidhar	H04L47/10	1/1
*	D	US-2008/0062994 A1	03-2008	Porat; Haim	H04L45/00	370/392
*	E	US-2010/0100954 A1	04-2010	YANG; JAMES H.	H04L63/0263	726/11
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14566403	PERNICHA, HUGO FILIPE PARREIRA
	Examiner	Art Unit
	KENNETH CHANG	2438

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/0263	7/20/2016	KC
H04L63/20	1/24/2017	KC

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Searched Inventors' Names and Assignee on eDan and EAST.	7/20/2016	KC
Searched IEEE NPL Xplore Database online.	7/20/2016	KC
Completed Limited Classified Search in CPC on EAST USPAT, PGPUB, and EPO databases with Keywords.	7/22/2016	KC
Keywords Searched: See East search history.	7/22/2016	KC
H04L63/20	1/24/2017	KC
Updated Limited Classified Search in CPC on EAST USPAT, PGPUB, and EPO databases with Keywords. See East Search History.	1/28/2017	KC
Updated Keywords: See East search history.	1/28/2017	KC

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/KENNETH CHANG/ Primary Examiner.Art Unit 2438

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L5	35	H04L63/20.CPC. and (policy or policies) and (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 21:59
S35	89	(policy or policies) WITH (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:32
S34	84	(policy or policies) WITH (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical) and network$9	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:18
S33	89	(policy or policies) WITH (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:18
S32	24	(policy or policies) and (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical) with (parameter oR (source adj3 address$5) or (destination adj3 address$5))	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:15
S31	635	(policy or policies) and (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 17:11
S30	22	(policy or policies or filter$9) same (merg$9 or combine or combining or combined) with rule with (match$9 or similar or identical) with (parameter or address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/28 16:57
S29	1	"20100100954".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:34
S28	6	(policy or policies or filter$9) same (packet or flow or traffic) same rule same (delet$5 or remov$9) same (obsolete or redundan$5 or old) same (optimiz$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:33
S27	87	(policy or policies or filter$9) same (packet or flow or traffic) same rule same (delet$5 or remov$9) same (obsolete or redundan$5 or old)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:33
S26	10052	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:32
S25	1	"8478852".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/24 17:31

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

S24	1	"20100318812".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/11 16:14
S22	1	"20150033285".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 18:02
S21	1	"20120185913" .pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 17:56
S20	1	"20020069200".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 17:56
S19	60	H04L63/20.CPC. and (policy or policies or filter$9) same (packet or flow or traffic) same (group or grouped or grouping or delet$5 or remov$9 or reorder$9) with (rule) same (use or usage or statistic or weight)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 17:53
S18	409	(policy or policies or filter$9) same (packet or flow or traffic) same (group or grouped or grouping or delet$5 or remov$9 or reorder$9) with (rule) same (use or usage or statistic or weight)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 16:48
S17	2458	(policy or policies or filter$9) same (packet or flow or traffic) same (group or grouped or grouping or delet$5 or remov$9 or reorder$9) with (rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/01/10 16:47
S16	11	H04L63/0263.CPC. and (rule) same (depend$9) same (compatib$9 or conflict$9) and (packet or flow or traffic) and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5) and order$5	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/23 00:02
S15	1	"20060013136".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 22:07
S14	1	"20020198981".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 21:15
S13	14	(supernet$9) same (ip or internet protocol) same address$5 same source same destination	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 20:50
S12	281	(rule) same (depend$9) same (compatib$9 or conflict$9) and (packet or flow or traffic) and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5) and order$5	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:22
S11	185	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5) and order$5	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:21
S10	185	(rule) same (depend$9) same (compatib$9 or	US-	ADJ	ON	2016/07/22

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

		conflict$9) and traffic and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5)	PGPUB; USPAT; EPO			15:20
S9	212	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:20
S8	10	H04L63/0263.CPC. and (rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 14:10
S7	311	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 14:10
S6	9	("5889953" | "6041347" | "6170009" | "6418468" | "6463470" | "6587466" | "6601082" | "6611863").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 12:22
S5	1	"20010039576".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 12:20
S4	1	"7441022".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 12:11
S3	2021	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/20 14:34
S2	590	fortinet.as.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/20 14:33
S1	1	(pernicha adj3 hugo).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/20 14:33

1/28/2017 10:00:35 PM
C:\Users\kchang3\Documents\EAST\Workspaces\14566403_APP.wsp

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14566403	PERNICHA, HUGO FILIPE PARREIRA
	Examiner	**Art Unit**
	KENNETH CHANG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/23/2016	01/28/2017							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							
	21	✓	✓							
	22	✓	✓							
	23	✓	✓							
	24	✓	✓							
	25	✓	✓							
	26	✓	✓							

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Pernicha et al.	**Examiner:** Chang, Kenneth W
App. No.: 14/566,403	Group Art Unit: 2438
Filed: December 30, 2014	Conf. No.: 7209
For: DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT	Docket No.: FORT-012500

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO OFFICE ACTION

Sir:

In response to the Office Action mailed July 27, 2016 (the "Office Action"), the Applicant respectfully requests the Examiner to enter the following amendment and to consider the following remarks:

Amendments to the Claims are reflected in the listing of claims, which begins on page 3 of this paper.

Remarks begin on page 8 of this paper.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Amendments to the Claims

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. **(Currently amended)** A method comprising:

receiving, by a network security management device, a request to add a new traffic flow policy rule to a plurality of policy rules managed by the network security management device;

automatically determining, by the network security management device, dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules;

forming, by the network security management device, an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules based on the determined dependencies;

automatically optimizing, by the network security management device, the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein the optimizing is based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules.

2. **(Original)** The method of claim 1, wherein said determining dependencies comprises evaluating dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

3. **(Original)** The method of claim 1, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging is conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

4. **(Original)** The method of claim 3, wherein the merging of combinable policy rules is conducted based on superneting of one or more of the source IP addresses and the destination IP addresses.

5. **(Original)** The method of claim 1, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of policy rules based on one or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters.

6. **(Original)** The method of claim 5, wherein the order of the policy rules of the second sub-set of policy rules is changed based on frequency of usage thereof.

7. **(Original)** The method of claim 1, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules.

8. **(Original)** The method of claim 7, wherein the one or more conflicts include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

9. **(Original)** The method of claim 7, wherein the one or more conflicts include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule.

10. **(Original)** The method of claim 1, wherein the one or more weights are defined manually based on scope and attributes of policy rule.

11. **(Original)** The method of claim 1, wherein the one or more weights are defined automatically.

12. **(Original)** The method of claim 1, wherein said forming an updated set of policy rules is conducted based on the one or more weights, the preference settings, the priority settings for the policy rules, network traffic characteristics, and network usage statistics.

13. **(Currently amended)** A network security policy management system comprising:

one or more processors; and

one or more internal data storage devices operatively coupled to the one or more processors and storing:

a business traffic flow input module configured to receive a request to add a new traffic flow policy rule to a plurality of policy rules managed by the system;

a dependency detection module configured to automatically determine dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules;

a traffic flow policy rule incorporation module configured to form an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules based on the determined dependencies; and

a policy rule optimization module configured to automatically optimize the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein the optimizing is based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

14. **(Original)** The system of claim 13, wherein the dependency detection module is further configured to evaluate dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules.

15. **(Original)** The system of claim 13, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging is conducted based on matching of one or more of source IP addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

16. **(Original)** The system of claim 15, wherein the merging of combinable policy rules is conducted based on superneting of one or more of the source Internet Protocol (IP) addresses and the destination IP addresses.

17. **(Original)** The system of claim 13, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of policy rules based on one or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters.

18. **(Original)** The system of claim 13, wherein said deleting the third sub-set of policy rules comprises deleting the policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

19. **(Original)** The system of claim 18, wherein the one or more conflicts include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules.

20. **(Original)** The system of claim 18, wherein the one or more conflicts comprise one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule.

21. **(Original)** The system of claim 13, wherein the one or more weights are defined manually based on scope and attributes of the policy rule.

22. **(Original)** The system of claim 13, wherein the one or more weights are defined automatically.

23. **(Currently amended)** A network security policy management system comprising:

one or more processors; and

one or more internal data storage devices operatively coupled to the one or more processors and storing a policy rule optimization module configured to retrieve information regarding a current set of policy rules and optimize the current set of policy rules by ~~one or more of~~ grouping a first sub-set of policy rules of the current set of policy rules, reordering a second sub-set of policy rules of the current set of policy rules, and deleting a third sub-set of policy rules of the current set of policy rules, wherein the optimizing is based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and usage statistics for each policy rule of the current set of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

24. **(Original)** The system of claim 23, wherein said grouping the first sub-set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging is conducted based on matching of one or more of source IP addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

25. **(Original)** The system of claim 23, wherein said reordering the second sub-set of policy rules comprises changing an order of the policy rules of the second sub-set of policy rules based on one or more of their source Internet Protocol (IP) addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters.

26. **(Original)** The system of claim 23, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the retrieved set of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Remarks

The Applicant respectfully requests reconsideration of this application in view of the following remarks. Claims 1-26 are pending, with claims 1, 13 and 23 being independent. Claims 1, 13 and 23 have been amended. Support for the amendments is found at least in ¶ [0029] of the specification. No new subject matter has been added.

Claims 1-26 stand rejected under 35 U.S.C. 101 because the claimed invention is allegedly not directed to statutory subject matter.

Claims 1-3, 5, 13-15, 17, and 23-25 are rejected under 35 U.S.C. 102(a)(1) and 102(a)(2) as allegedly being anticipated by Kanada (US 20010039576 A1).

Claims 4 and 16 stand rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Liu (US 20020154635 A1).

Claim 6 stands rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Corl et al. (US 20020198981 A1, hereinafter Corl).

Claims 7-11, 18-22, and 26 stand rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Goldschmidt et al. (US 20060013136 A1, hereinafter Goldschmidt).

Claim 12 stands rejected under 35 U.S.C. 103 as allegedly being unpatentable over Kanada in view of Goldschmidt and further in view of Corl.

Claim Rejections – 35 U.S.C. § 101

In the Office Action, the Examiner rejected claims 1-26 under 35 U.S.C. §101 as being allegedly directed to non-statutory subject matter. The undersigned respectfully submits, the claims are not "directed to" an abstract idea. Rather, the claims are directed to improved computer networking communications and more specifically to network security policy optimization based on one or more of weights assigned to

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

particular types of traffic, preference settings, priority settings, network traffic characteristics, and usage statistics for each policy rule of the current set of policy rules. See Specification at ¶¶ [0018],[0029].

As an initial matter, the undersigned respectfully suggests the Examiner has asserted too high of a level of abstraction, which poses the all-too-real risk of "the exceptions [i.e., abstractness] to § 101 swallow[ing] the rule." Alice, 134 S. Ct. at 2354. In the Office Action, the Examiner indicates claims 1, 13 and 23 "are directed to the abstract idea of organizing rules based on dependencies (e.g. using categories to organize, store, and transmit information - see Cyber[F]one Sys., LLC v. CNN Interactive (Fed. Cir. Feb. 26, 2014); e.g. comparing new and stored information and using rules to identify options, Smartgene, Inc. v. Advanced Biological Labs., SA, 555 Fed. Appx. 950 (Fed. Cir. 2014))." See Office Action at p. 3. However, the claims are not directed at merely "organizing rules based on dependencies", which is an overly broad generalization of the field of the claims and which does not directly reflect even a single step or element of the claims at issue. As such, it appears the Examiner has improperly applied a high level of abstraction that ignores most of the claim language by simply boiling the claim down to less than a single one of the recited elements.

In CyberFone, claim 1 recited a method having three steps: (1) obtaining data from a telephone transmission, (2) forming multiple data transactions based on the data in the telephone transmission and (3) sending each of those data transactions to a respective destination. Notably, the data that was obtained, formed and sent to respective destinations did not appear to have any connection with any particular telephone system, and could thus presumably be performed on any telephone system. In contrast, the claimed invention is directed to a particular network security policy management system or a method using a particular network security management device that is configured to determine dependencies between traffic flow policy rules, to form updated sets of policy rules, and to automatically optimize the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules. In the present circumstances, the claims are clearly directed to a specific implementation of a network security management device or system, and not to "the abstract idea of organizing rules based on dependencies".

In Smartgene, the claims were directed to a set of expert rules for evaluating and selecting a therapeutic treatment regimen for a disease or medical condition. The court limited the reach of the holding by stating "Our ruling is limited to the circumstances presented here, in which every step is a familiar part of the conscious process that doctors can and do perform in their heads." The claims in Smartgene did not state anything about the details of the rules other than their purpose "for evaluating. . . .", and the court believed that the rules were the very rules normally used by doctors in their practice. In contrast, the claimed invention includes a particular network security policy management device or system, performing functions that are not normally performed by human operators based on information derived from the flow of the traffic in the network.

Again, it appears the Examiner has improperly applied a high level of abstraction that ignores most of the claim language by simply boiling the claim down to less than a single one of the recited elements. In Enfish, LLC v. Microsoft Corp. et al., 2016 WL 2756255 (Fed. Cir. May 12, 2016), the Federal Circuit reversed a similar §101 rejection of claims directed to a specific improvement to the way computers operate, cautioning against describing a claim at a high level of abstraction untethered from the language of the claim when determining the focus of the claimed invention. As in the case of Enfish, the claims of the above-captioned patent application relate to specific asserted improvements in computer-related technology – the way network security management device or system manages traffic in a network.

This is a device, and it is not a general purpose computer. Even if it were, Enfish indicates that the fact that an invention runs on a general computer does not mean

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

that the claims are patent ineligible. However, the claims are not the mere recitation of a generic computer or computer network. The invention claims "automatically optimizing, by the network security management device, the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules". Clearly, a generic computer or computer network doesn't offer that functionality unless there is a program installed that so directs the machine to provide that functionality.

In Ex parte Balestrieri, Appeal No. 2013-007305 (PTAB Oct. 23, 2015), the applicant claimed a method for "establishing an online marketplace for distributing software applications," including "enabling the devices to select respective ones of the software applications and initiate testing of the selected software applications" and "determining whether or not to classify the software application as a certified software application based on an evaluation of the testing data generated during the testing of the software applications." The Office Action alleges that the method steps "could be performed without a machine (e.g. a person can receive a new policy rule, determine if the rule is dependent on other rules, add the rule to a set of rules, and 'optimize' the set of rules by grouping, reordering, or deleting rules in the set)". However, the claim is directed to a method which includes a network security management device that automatically determines dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules, and which incorporates the new traffic flow policy rule within the plurality of policy rules based on the dependencies automatically determined by the network security management device. It is not merely a matter of receiving a new policy rule, determining if the rule is dependent on other rules, adding the rule to a set of rules, and optimizing the set of rules by grouping, reordering, or deleting rules in the set, but of a network security management device that automatically determining dependencies of the new traffic flow policy rule on one or more of the plurality of policy

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

rules, and incorporating the new traffic flow policy rule within the plurality of policy rules based on the dependencies automatically determined by the network security management device. Thus, as in Ex parte Balestrieri in which the PTAB determined that a computer testing step was a necessary precursor to a determining step, the claimed method incorporates a new traffic flow policy based on dependencies automatically determined by the network security management device, thereby solving a network traffic-specific problem. Furthermore, the claimed method does not optimize the set of rules by merely "grouping, reordering, or deleting rules in the set", rather the claimed method optimizes the set of policy rules by "(i) grouping a first sub-set of policy rules of the updated set of policy rules; (ii) reordering a second sub-set of policy rules of the updated set of policy rules; and/or (iii) deleting a third sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules." A person manually inserting a rule into a group of rules and then "grouping, reordering or deleting rules in the set" would not have the claimed "weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules", at least some of which are attributes gathered based on traffic flowing through the network and available to the network security management device, a fact that again illustrates that this is not an abstract idea or problem being solved but a network-related problem being solved by a method using a network security management device that automatically determines dependencies.

As described in the specification, the claimed invention solves problems that occur with manual user-managed rule-based policies, see, for example, the Specification at paragraph [0006]: "Firewall rule-based policy is typically static. As such, once it is configured, it will stay the same, in the same order and not be changed unless explicitly changed by a user/administrator. In practice, large enterprises end up with a substantial set of firewall rule-based policies that are more oriented to user/operator visibility than rule processing efficiency. Furthermore, addition of each

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

new policy rule or modification of an existing rule typically has ripple effects on other existing/stored rules and policies. For instance, a new policy rule may be configured to allow packets of a specific traffic type to a given destination, which otherwise may have been denied by an already existing policy rule in the rule database. Existing security policy management techniques require manual detection of issues, such as duplication of rules, conflicts between rules, dependency between rules, or shadowing of one rule by another and therefore are error prone. These issues are exacerbated in the context of large policy rule databases."

The Office Action alleges that "Claims 1, 13, and 23 would preempt the field of policy rule organization." As discussed above, this is not the case. The claims are directed at a method and systems that are directed at grouping, reordering and deleting policy rules using a network security management device or processors based on weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and usage statistics, information that is generated by traffic in a network and available to the network security management device or processors. This is clearly not an abstract field of policy rule optimization, nor the mere use of a computer as a tool, it is a specific network issue that occurs precisely because manual user management of rule-based policies creates a problem, solved in the claimed invention by special purpose network hardware based on information generated based on traffic flowing in the network. The claimed invention is a solution that is tethered to the technology that created the problem.

The undersigned believes a review of the memo circulated among the Patent Examining Corps by Deputy Commissioner for Patent Examination Policy, Robert W. Bahr on May 19, 2016 (the "Enfish Memo") might inform the Examiner's approach to identifying abstract ideas (Step 2A of the subject matter eligibility examination guidelines). For Example, the claims at issue in Enfish avoided the "significantly more" step of the Alice test (Step 2B) of the subject matter eligibility examination guidelines because they "'improve the functioning of the computer itself,' or 'improve an existing technological process.'" In the present circumstances, the claims are clearly directed to a

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

specific implementation of a solution to a problem relating to network traffic management that allows enhanced computing performance, rule management, policy optimization, and session/network traffic packet flow management (see Specification, ¶ [0018]), thereby improving the existing technological process of firewall rule matching and policy rule addition. As such, the present claims are not directed to an abstract idea under Step 2A of the subject matter eligibility examination guidelines (as clarified by Enfish) and there is no need to analyze the additional elements under Step 2B.

To the extent the Examiner believes analysis of the additional elements under Step 2B is necessary (a conclusion with which the undersigned disagrees), the undersigned respectfully suggests the recent case of BASCOM Global Internet Services Inc. v. AT&T Mobility LLC (Fed. Cir. 2016) is informative. In BASCOM, the CAFC emphasized "[t]he inventive concept inquiry requires more than recognizing that each claim element, by itself was [allegedly] known in the art" and held "an inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces." Slip Op. at 15. The specific method and system recited by the claims of, among other limitations, optimizing a set of policy rules by one or more of grouping a first sub-set of policy rules of the current set of policy rules, reordering a second sub-set of policy rules of the current set of policy rules, and deleting a third sub-set of policy rules of the current set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and usage statistics for each policy rule of the current set of policy rules clearly provide significantly more than simply "organizing rules based on dependencies". For at least these reasons, the undersigned respectfully requests the Examiner to withdraw the 101 rejections of the pending claims.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Claim Rejections – 35 U.S.C. § 102

In the Office Action, the Examiner rejected claims 1-3, 5, 13-15, 17, and 23-25 under 35 U.S.C. 102(a)(1) and 102(a)(2) as allegedly being anticipated by Kanada.

The undersigned respectfully disagrees with the Examiner's characterization of the teachings and/or applicability of the cited references to the claims and requests reconsideration for at least the reasons set forth below.

At the outset it should be noted that a rejection under 35 U.S.C. 102 requires a single prior art reference must teach each and every element of the rejected claim. MPEP §2131 (citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Not only must each of the elements of the claim be shown in the single prior art reference, the "identical invention" must be shown "in as complete detail as contained in the claim." MPEP §2131 (citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989), 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Further, the single prior art reference "must not only disclose all elements of the claim within the four corners of the document, but must also disclose those elements 'arranged as in the claim'" as "the hallmark of anticipation is prior invention." Net MoneyIn v. Verisign, 545 F.3d 1359, 3369 (Fed. Cir. 2008) citing Connell v. Sears, Roebuck & Co., 722 F.2d 1542, 1548 (Fed. Cir. 1983). The outstanding rejections fall short of the established legal standard.

Independent claim 1, as amended, sets forth a method including, among other limitations, automatically optimizing, by a network security management device, an updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein the optimizing is based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

By making the rejection under 35 USC §102(a)(2), the Office Action alleges that Kanada discloses "each and every element" of the rejected claims, and that those elements are disclosed "in as complete detail as contained in the claim", and "arranged as in the claim". See e.g., Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987), Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989), and Net MoneyIn v. Verisign, 545 F.3d 1359, 3369 (Fed. Cir. 2008).

However, Kanada does not disclose a network security management device that automatically optimizes an updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein the optimizing is based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules.

Briefly and by way of background without reference to any particular claim, the undersigned notes that embodiments of the present invention generally relate to methods and systems for creation and modification of firewall/access control policy rules so as to allow enhanced computing performance, rule management, policy optimization, and session/network traffic packet flow management. Methods and systems are further provided for optimizing the security policy rules by performing any or a combination of reordering, grouping, updating, deleting, along with performing any other actions on one or more policy rules based on parameters, including, but not limited to, weights assigned to traffic attributes (e.g., source address, destination address, service, port information, among other such attributes), preference settings, priority settings for the policy rules, network traffic characteristics, network usage statistics, among other optimization parameters. See, e.g., the specification at ¶ [0018].

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

As presently understood by the undersigned, Kanada generally relates to methods of controlling Quality of Service (QoS) over a network such as the Internet in which routers and other network nodes that are controllable on a policy basis are interconnected by media and methods of running distributed rule-based programs over a network in which nodes on which rule-based programs can run are interconnected by media. (Kanada, ¶ [0002]) Kanada teaches that in a network system to which policy control is applied, by specifying setup policies on a computer called a policy server, all devices in the network can be set up accordingly, only requiring the input of a small quantity of information. Such network administrative method enables control duties over the network that is too complicated for human operators to exercise, such as policy change in minute time steps specified and dynamic policy update when requested from an application program. (Kanada, ¶ [0007])

Kanada teaches that policy rules can be transferred from the policy server to a network node as either a block or a single rule, but that adding, removing, or updating a single rule may cause the failure of intended action, because rules are generally interdependent, and adding, removing, or updating a rule changes the meaning of another rule that depends on the rule, and because batch processing of a plurality of essentially independent rules by a router may result in some interdependence. (Kanada, ¶ [0021]) When, for example, rules downloaded from a policy server are converted into those in form that they can be executed on a router, it is required that a plurality of rules are merged into one rule, or inversely, one rule is broken down into a plurality of rules. If one of the rules to be merged is removed or updated, the remaining rules must be reconverted accordingly. (Kanada, ¶ [0021])

Kanada also teaches that when the policy server is requested to send a policy rule to the router, it judges whether the policy rule has been stored in the router. If the policy rule has been stored in the router, the policy server transfers only its identifier to the router instead of transferring its contents. (Kanada, ¶ [0028])

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Thus, while Kanada does teach merging a plurality of rules into one rule, this is done to place them in a form that can be executed on a router (see, e.g., Kanada ¶¶ [0021], [0139], [0147], [0179]), rather than to optimize an updated set of policy rules, and furthermore, Kanada's merging is not done based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules. With respect to the rule form that can be executed on a particular router, Kanada indicates that in some cases, the interface specification prescribes that macro rules be used, and in other cases, the rule can be formatted as shown in Fig. 4, element 1708. Notably, conversion of a rule between a macro rule and another rule format, performed based on interface specification requirements of a router, is explicitly stated by Kanada to be performed to allow the rule to be executed on the router, and is not an optimization of an updated set of policy rules.

The Office Action alleges with respect to claim 3 that Kanada teaches that such merging of rules is conducted based on source IP address of the flow or destination IP address of the flow, citing Kanada ¶¶ [0073], [0088]. The undersigned respectfully disagrees with this characterization of Kanada and requests reconsideration.

> "[0077] The rule represented by the data entered in the template 301 has the following meaning. Flows that are transmitted from the IP address 192.168.4.1 with the TCP protocol are labeled VideoSource during the period from 0:00 on Saturday to 24:00 on Sunday every week. This labeling functions to determine rules that are to be next activated. This label is, however, different from DSCP and MPLS labels which are actually assigned to packets and is virtually assigned to packets and effective within the router. There are two rules with the condition entry containing the label VideoSource in the template 341 and in the first Condition field in the template 321 as will be described later. Thus, only these rules are next activated."
>
> "[0088] On a line 402, a rule with the #1 rule identifier 411 is described and this rule has been entered by using the template 301. The rule type

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

412 is "classification". For the condition, the pointer indicates table (A). This table is filled with null data except that protocol 421 is TCP, source IP address of flow is 192.168.4.1 421, and destination IP address of flow is 192.168.4.1 422. Furthermore, the action is to assign a value of 1 to the label variable."

(Kanada ¶¶ [0073], [0088])

The cited portions of Kanada which mention source IP address of flow and destination IP address of flow are directed at a template displayed on an operator console and used to fill in a rule table. There is no teaching that the merging of rules into a form that can be executed on a particular router is performed based on the source IP address of flow or destination IP address of flow. For at least these reasons, Kanada does not disclose "each and every element" of the rejected claims, disclosed "in as complete detail as contained in the claim", and "arranged as in the claim". See e.g., Verdegaal Bros. v. Union Oil Co. of California, *supra*, Richardson v. Suzuki Motor Co., *supra*, and Net MoneyIn v. Verisign, *supra*.

Independent claims 13 and 23 contain similar limitations and are believed allowable for at least the reasons discussed above with respect to independent claim 1. Such allowance is respectfully requested.

The dependent claims depend upon independent claims which are allowable over the cited art as discussed above. These dependent claims are likewise in condition for allowance at least because they depend on allowable independent claims. However, the dependent claims are believed independently allowable at least in that they recite particular features which, when combined with the elements of the independent claim, are not disclosed or suggested in the cited references.

Conclusion

The undersigned respectfully submits that the amendments and remarks presented herein have overcome the rejections, and that the pending claims are in

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

condition for allowance. Accordingly, the undersigned requests that the rejections be withdrawn and that a Notice of Allowance be promptly issued for claims 1-26.

By responding in the foregoing remarks only to particular positions taken by the Examiner, the Applicant does not acquiesce with any other positions that have not been explicitly addressed. Applicant's arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist. The absence of a reply to a specific rejection, issue or comment set forth in the Office Action does not signify agreement with or concession of that rejection, issue or comment. In addition, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, and the amendment of any claim does not necessarily signify any concession of unpatentability of the claim prior to its amendment.

In view of the foregoing, the Applicant respectfully asserts that all claims now pending in the application are in condition for allowance. Hence, an early allowance of all such claims is earnestly requested.

Respectfully submitted,
Hamilton, DeSanctis & Cha LLP

By /Guy K. Clinger/
Guy K. Clinger
Reg. No. 42,422
Customer No. 64128
Ph: 720-446-1888

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Electronic Acknowledgement Receipt	
EFS ID:	27338098
Application Number:	14566403
International Application Number:	
Confirmation Number:	7209
Title of Invention:	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT
First Named Inventor/Applicant Name:	Hugo Filipe Parreira Pernicha
Customer Number:	64128
Filer:	Guy Kenneth Clinger
Filer Authorized By:	
Attorney Docket Number:	FORT-012500
Receipt Date:	27-OCT-2016
Filing Date:	30-DEC-2014
Time Stamp:	11:42:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		FORT-012500Response1.pdf	88773 73450c4cff32c4ebddde06830aabbdf1557b dcc4	yes	20

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	7
	Applicant Arguments/Remarks Made in an Amendment	8	20
Warnings:			
Information:			
	Total Files Size (in bytes):	88773	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/566,403	Filing Date 12/30/2014	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **10/27/2016**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 26	Minus	** 26	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	**0**

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/RENEE M. COLLINS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/566,403	12/30/2014	Hugo Filipe Parreira Pernicha	FORT-012500	7209

64128 7590 07/27/2016

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

EXAMINER
CHANG, KENNETH W

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
07/27/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mdesanctis@hdciplaw.com
docket@hdciplaw.com

PTOL-90A (Rev. 04/07)

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Office Action Summary	Application No. 14/566,403	Applicant(s) PERNICHA, HUGO FILIPE PARREIRA	
	Examiner Kenneth Chang	Art Unit 2438	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/10/2014*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-26* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-26* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *12/10/2014* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *12/30/2014*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

1. This non-final Office Action is in response to the original filing on 12/10/2014.

Claims 1-26 are currently pending and have been considered as follows.

Notice of Pre-AIA or AIA Status

2. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

3. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Drawings

4. The drawings filed on 12/10/2014 are accepted.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 12/30/2014 has been placed in the application file, and the information referred therein has been considered as to the merits.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. **Claims 1-26** are rejected under 35 U.S.C. § 101 because the claimed invention is not directed to patent eligible subject matter. Based upon consideration of all of the

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

relevant factors with respect to the claims as a whole, claim(s) 1-26 are determined to be directed to an abstract idea (judicially recognized exception). The rationale for this determination is explained below:

Under STEP 1 of the Subject Matter Eligibility Test **(See *2014 Interim Guidance on Patent Subject Matter Eligibility*)**, independent Claims 1, 13 and 23 recite a "method", a "system", and a "system" respectively which are directed to one of the four subject matter categories. Claims 13 and 23 recite systems that comprise one or more processors and one or more internal data storage devices operatively coupled to the one or more processors where the storage devices are construed as machine hardware.

Under STEP 2A of the Subject Matter Eligibility Test, independent Claims 1, 13 and 23 are directed to the abstract idea of organizing rules based on dependencies (e.g. using categories to organize, store, and transmit information - ***see Cyberphone Sys., LLC v. CNN Interactive* (Fed. Cir. Feb. 26, 2014)**; e.g. comparing new and stored information and using rules to identify options ***Smartgene, Inc. v. Advanced Biological Labs., SA*, 555 Fed. Appx. 950 (Fed. Cir. 2014)**). The method of Claim 1 recites steps of "***receiving****… a request to add a new traffic flow policy rule*", "*automatically* ***determining****… dependencies of the … rule on one or more … rules*", "***forming****... an updated set of policy rules by incorporating the new... rule within the plurality of ... rules*", "*automatically* ***optimizing****... the updated set of policy rules* ***by one or more of****... **grouping**... **reordering**... [or]* ***deleting****…rules*". Clearly, this method could be performed without a machine (e.g. a person can receive a new policy rule,

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

determine if the rule is dependent on other rules, add the rule to a set of rules, and "optimize" the set of rules by grouping, reordering, or deleting rules in the set) which is a well-established concept recognized as an abstract idea of organizing information (e.g. ***Cyberphone*** and ***Smartgene*** court decisions). Applicant's method, including the nominal language "*automatically*", is a process that qualifies as an abstract idea for which ***computers are invoked merely as a tool*** (e.g. *automatically, by a network security management device*). Claims 13 and 23 recite systems comprising generic computer elements (i.e. *processor, internal data storage devices storing modules*) for performing the abstract idea of Claim 1, and "*simply implementing an abstract concept on a computer, without meaningful limitations to that concept, does not transform a patent-ineligible claim into a patent-eligible one.*" ***Accenture Global Service v. Guidewire Software, Inc.*, 728 F.3d 1336 (Fed. Cir. 2013) at 1345**. Given the broadest reasonable interpretation, Claims 1, 13, and 23 recite the concept of adding a rule to a set of rules and organizing the rules based on dependency which "*would risk disproportionately tying up the use of the underlying ideas... and are therefore ineligible for patent protection*" (***Alice Corp. v. CLS Bank International* 134 S. Ct at 2354 (2014)**). Claims 1, 13, and 23 would preempt the field of policy rule organization.

Under STEP 2B (Part 2 of the *Mayo* test), Claims 1, 13, and 23 do not recite additional elements that individually or in combination amount to significantly more than the judicial exception. The recited features of the particular data and technological environment (i.e. traffic flow policy rule by network security management device) do not circumvent the prohibition against patenting an abstract principle by attempting to limit

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

the use of the [principle] to a particular technological environment (***see Diehr***, **450 U.S. at 191**; "*attempts to limit the abstract concept to a computer implementation and to a specific industry thus do not provide additional substantive limitations to avoid preempting the abstract idea of [the] system*" ***Accenture Global Service v. Guidewire Software, Inc.***, **728 F.3d 1336 (Fed. Cir. 2013)**). The claims fail to recite any inventive concept that amounts to significantly more than the abstract idea above.

Dependent Claims **2-12, 14-22, and 24-26** when analyzed as a whole are held to be patent ineligible under 35 U.S.C. § 101 because the additional recited limitations fail to establish that the claims are not directed to an abstract idea, and none of the additionally recited limitations amount to significantly more than the abstract idea. For instance, Claims 2-12, 14-22, and 24-26 only recite evaluating dependence, merging combinable policy rules based on matching or superneting, changing an order of policy rules, deleting… rules, and weights are defined which does not amount to significantly more than the abstract idea of organizing a policy rule set.

Therefore, Claims **1-26** when analyzed as a whole are held to be patent ineligible under 35 U.S.C. § 101 because the claims fail to establish meaningful limitations on the abstract idea and fail to transform the abstract idea into a patent eligible application of the abstract idea such that the claims amount to significantly more than the abstract idea itself. ***See 2014 Interim Guidance on Patent Subject Matter Eligibility*** *(Federal Register Vol. 79, No. 241, December 2014) in view of the decisions by the U.S. Supreme Court, including Alice Corp., Myriad, and Mayo.* See also ***July 2015 Update: Subject Matter Eligibility*** *(Federal Register Vol. 80, No. 146, July 2015).*

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

8. **Examiner's Note:** The Examiner has pointed out particular references contained in the prior art of record within the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33,216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275,277 (CCPA 1968)). A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments (see MPEP 2123). Therefore, Applicant, in preparing the response, must fully consider the entire disclosure of the cited references as potentially teaching all or part of the claimed invention, including the context of the cited passages as taught by the prior art disclosed by the Examiner.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a)(1) the claimed invention was patented, described in a printed publication, or in public use, on sale or otherwise available to the public before the effective filing date of the claimed invention.
>
> (a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

10. **Claims 1-3, 5, 13-15, 17, and 23-25** are rejected under 35 U.S.C. 102(a)(1) and 102(a)(2) as being anticipated by **Kanada** (US 20010039576 A1).

As to Claim 1:

Kanada discloses a method **(e.g. Kanada FIG. 5; [0002] methods; [0093])** comprising:

- receiving, by a network security management device **(e.g. Kanada policy server with operator console [0066]; [0067])**, a request to add a new traffic flow policy rule to a plurality of policy rules **(e.g. Kanada rule specified to be added [0021]; receiving input to add policy rule [0067])** managed by the network security management device;
- automatically determining, by the network security management device, dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules **(e.g. Kanada detects policy rules that the new policy rule depends on [Abstract]; analyzing policy rules for dependence of policy rule data on another policy rule data [0028]; [0068]; [0099]; [0103]; [0167])**;
- forming, by the network security management device, an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules **(e.g. Kanada add and store input policy rules into policy repository [0067]; [0070]; [0071]; rule table contains all input rules [0087]; list of rule identifiers and added rule sent to router [0099])** based on the determined dependencies;
- automatically optimizing, by the network security management device, the updated set of policy rules by **one** or more of grouping a first sub-set of policy

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

rules of the updated set of policy rules **(e.g. Kanada plurality of rules are merged into one rule [0021]; rules on lines 1302 and 1303 are merged into one rule [0139]; in a form that can be executed [0147]; [0179])**, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules.

As to Claim 2:

Kanada discloses the method of claim 1, wherein said determining dependencies comprises evaluating dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules **(e.g. Kanada "By referring to the policy repository 211 and the variable reference table 214, the policy rule dependence analyzer 204 analyzes the relation between the rules entered to be added or removed and the relation between these rules and the existing rules to find dependence of a rule on another rule. This analyzer 204 then delivers at a time the rule identifiers of all interdependent rules to the policy scheduler 205" [0068])**.

As to Claim 3:

Kanada discloses the method of claim 1, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule **(e.g. Kanada plurality of rules are merged into one rule [0021]; rules on lines 1302 and 1303 are merged**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

into one rule [0139]; in a form that can be executed [0147]; [0179]), wherein the merging is conducted based on matching of **one** or more of source Internet Protocol (IP) addresses **(e.g. Kanada source IP address of the flow [0073]; [0088])**, destination IP addresses **(e.g. Kanada destination IP address [0073])**, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

As to Claim 5:

Kanada discloses the method of claim 1, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of policy rules based on **one** or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters **(e.g. Kanada rules can be rearranged such that defined variable always precede those that are used as a condition [0106])**.

As to Claim 13:

Kanada discloses a network security policy management system **(e.g. Kanada FIG. 1 [0060]-[0072])** comprising:

- one or more processors **(e.g. Kanada processor [0066])**; and
- one or more internal data storage devices **(e.g. Kanada hard disk or main storage [0066]; [0134])** operatively coupled to the one or more processors and storing:
- a business traffic flow input module **(e.g. Kanada software unit [0066])** configured to receive a request to add a new traffic flow policy rule to a plurality

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

of policy rules managed by the system **(e.g. Kanada rule specified to be added [0021]; receiving input to add policy rule [0067])**;

- a dependency detection module **(e.g. Kanada software unit [0066])** configured to automatically determine dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules **(e.g. Kanada detects policy rules that the new policy rule depends on [Abstract]; analyzing policy rules for dependence of policy rule data on another policy rule data [0028]; [0068]; [0099]; [0103]; [0167])**;
- a traffic flow policy rule incorporation module **(e.g. Kanada software unit [0066])** configured to form an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules based on the determined dependencies **(e.g. Kanada add and store input policy rules into policy repository [0067]; [0070]; [0071]; rule table contains all input rules [0087]; list of rule identifiers and added rule sent to router [0099])**; and
- a policy rule optimization module **(e.g. Kanada software unit [0066])** configured to automatically optimize the updated set of policy rules by **one** or more of grouping a first sub-set of policy rules of the updated set of policy rules **(e.g. Kanada plurality of rules are merged into one rule [0021]; rules on lines 1302 and 1303 are merged into one rule [0139]; in a form that can be executed [0147]; [0179])**, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

As to Claim 14:

Kanada discloses the system of claim 13, wherein the dependency detection module is further configured to evaluate dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules. **(e.g. Kanada "By referring to the policy repository 211 and the variable reference table 214, the policy rule dependence analyzer 204 analyzes the relation between the rules entered to be added or removed and the relation between these rules and the existing rules to find dependence of a rule on another rule. This analyzer 204 then delivers at a time the rule identifiers of all interdependent rules to the policy scheduler 205" [0068])**.

As to Claim 15:

Kanada discloses the system of claim 13, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule **(e.g. Kanada plurality of rules are merged into one rule [0021]; rules on lines 1302 and 1303 are merged into one rule [0139]; in a form that can be executed [0147]; [0179])**, wherein the merging is conducted based on matching of **one** or more of source Internet Protocol (IP) addresses **(e.g. Kanada source IP address of the flow [0073]; [0088])**, destination IP addresses **(e.g. Kanada destination IP address [0073])**, services,

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

As to Claim 17:

Kanada discloses the system of claim 13, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of policy rules based on **one** or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters **(e.g. Kanada rules can be rearranged such that defined variable always precede those that are used as a condition [0106])**.

As to Claim 23:

Kanada discloses a network security policy management system **(e.g. Kanada FIG. 1 [0060]-[0072])** comprising:

- one or more processors **(e.g. Kanada processor [0066])**; and
- one or more internal data storage devices **(e.g. Kanada hard disk or main storage [0066]; [0134])** operatively coupled to the one or more processors and storing a policy rule optimization module **(e.g. Kanada software unit [0066])** configured to retrieve information regarding a current set of policy rules **(e.g. Kanada obtains transition closure regarding reference relations between variables by using the variable reference table 212. The origin of the transition closure is all rules that are new entries or have been edited before being transmitted to the router. Finding all rules before being transmitted to the router can be implemented by providing flag fields for**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

rules in the rule table 401. When the policy server accepts a new rule entry or an edited rule, the flag for the entry is cleared and at transmission of the rule, the flag is set. All unflagged rules are found to be those before being transmitted [0103]) and optimize the current set of policy rules by **one** or more of grouping a first sub-set of policy rules of the updated set of policy rules **(e.g. Kanada plurality of rules are merged into one rule [0021]; rules on lines 1302 and 1303 are merged into one rule [0139]; in a form that can be executed [0147]; [0179])**, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

As to Claim 24:

Kanada discloses the system of claim 23, wherein said grouping the first sub-set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule **(e.g. Kanada plurality of rules are merged into one rule [0021]; rules on lines 1302 and 1303 are merged into one rule [0139]; in a form that can be executed [0147]; [0179])**, wherein the merging is conducted based on matching of **one** or more of source IP addresses **(e.g. Kanada source IP address of the flow [0073]; [0088])**, destination IP addresses **(e.g. Kanada destination IP**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

address [0073]), services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

As to Claim 25:

Kanada discloses the system of claim 23, wherein said reordering the second sub-set of policy rules comprises changing an order of the policy rules of the second sub-set of policy rules based on **one** or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters **(e.g. Kanada rules can be rearranged such that defined variable always precede those that are used as a condition [0106])**.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

12. **Claims 4 and 16** are rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of **Liu** (US 20020154635 A1).

As to Claim 4:

Kanada discloses the method of claim 3, but does not specifically disclose:

- superneting of one or more of the source IP addresses and the destination IP addresses.

However, the analogous art **Liu** does disclose superneting of one or more of the source IP addresses and the destination IP addresses **(e.g. Liu Supernet security layer**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

prepends real source and destination IP addresses [0062]; [0076]). **Kanada** and **Liu** are analogous art because they are from the same field of endeavor in network packet management.

- (e.g. see **Liu**, "a Supernet security layer (SNSL) 532, acting as the conduit for all Supernet communications. To conserve memory, both inner IP layer 530 and outer IP layer 534 may share the same instance of the code of an IP layer. SNSL 532 performs security functionality as well as address translation. It also caches the most recently used channel keys for ten seconds. Thus, when a channel key is needed, SNSL 532 checks its cache first, and if it is not found, it requests KMD 520 to contact the appropriate KMC to retrieve the appropriate channel key. Two IP layers 530, 534 are used in the TCP /IP protocol stack 524 because both the internal addressing scheme and the external addressing scheme are IP-based. Thus, for example, when a packet is sent, inner IP layer 530 receives the packet from TCP/UDP layer 528 and processes the packet with its node ID address before passing it to the SNSL layer 532, which encrypts it, prepends the real source IP address and the real destination IP address, and then passes the encrypted packet to outer IP layer 534 for sending to the destination" **[0062]**; see also **[0076]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada** and **Liu** before him or her, to modify the invention of **Kanada** with the teachings of **Liu** to include *superneting of one or more of the source IP addresses and the destination IP*

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

addresses as claimed because **Kanada** provides a policy rule controlled network with server and routers **(Kanada [0021]-[0137])** which could include implement a Supernet security layer that translates source and destination IP addresses of communicated packets **(Liu [0062]; [0076])**. The suggestion/motivation for doing so would have been to allow utilization of public-network infrastructure without the need to maintain a private network to be able to use resources securely and without geographical restriction **(Liu [0020])**. Therefore, it would have been obvious to combine **Kanada** and **Liu** to obtain the invention as specified in the instant claim(s).

As to Claim 16:

Kanada discloses the system of claim 15, but does not specifically disclose:

- superneting of one or more of the source Internet Protocol (IP) addresses and the destination IP addresses.

However, the analogous art **Liu** does disclose superneting of one or more of the source Internet Protocol (IP) addresses and the destination IP addresses **(e.g. Liu Supernet security layer prepends real source and destination IP addresses [0062]; [0076])**. **Kanada** and **Liu** are analogous art because they are from the same field of endeavor in network packet management.

- (e.g. see **Liu**, "a Supernet security layer (SNSL) 532, acting as the conduit for all Supernet communications. To conserve memory, both inner IP layer 530 and outer IP layer 534 may share the same instance of the code of an IP layer. SNSL 532 performs security functionality as well as address translation. It also caches the most recently used channel keys for ten seconds. Thus, when a channel key

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

> is needed, SNSL 532 checks its cache first, and if it is not found, it requests KMD 520 to contact the appropriate KMC to retrieve the appropriate channel key. Two IP layers 530, 534 are used in the TCP /IP protocol stack 524 because both the internal addressing scheme and the external addressing scheme are IP-based. Thus, for example, when a packet is sent, inner IP layer 530 receives the packet from TCP/UDP layer 528 and processes the packet with its node ID address before passing it to the SNSL layer 532, which encrypts it, prepends the real source IP address and the real destination IP address, and then passes the encrypted packet to outer IP layer 534 for sending to the destination" **[0062]**; see also **[0076]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada** and **Liu** before him or her, to modify the invention of **Kanada** with the teachings of **Liu** to include *superneting of one or more of the source Internet Protocol (IP) addresses and the destination IP addresses* as claimed because **Kanada** provides a policy rule controlled network with server and routers **(Kanada [0021]-[0137])** which could include implement a Supernet security layer that translates source and destination IP addresses of communicated packets **(Liu [0062]; [0076])**. The suggestion/motivation for doing so would have been to allow utilization of public-network infrastructure without the need to maintain a private network to be able to use resources securely and without geographical restriction **(Liu [0020])**. Therefore, it would have been obvious to combine **Kanada** and **Liu** to obtain the invention as specified in the instant claim(s).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

13. **Claim 6** is rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of Corl et al. (US 20020198981 A1, hereinafter **Corl**).

As to Claim 6:

Kanada discloses the method of claim 5, but does not specifically disclose:

- wherein the order of the policy rules of the second sub-set of policy rules is changed based on frequency of usage thereof.

However, the analogous art **Corl** does disclose wherein the order of the policy rules of the second sub-set of policy rules is changed based on frequency of usage thereof **(e.g. Corl placing the plurality of filter rules in an order based on frequency of reach filter rule [Abstract]; statistics of frequency [0024]; placing higher frequency filter rules first [0028])**. **Kanada** and **Corl** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Corl**, "Each of the plurality of filter rules has a priority. The method and system include accumulating statistics for each of the plurality of filter rules. The statistics indicate a frequency of enforcement for each of the plurality of filter rules. The method and system also include placing the plurality of filter rules in an order for testing against the key. The order is based on the frequency of each filter rule of the portion of the plurality of filter rules" **[Abstract]**; see also "The statistics indicate a frequency of enforcement for each of the plurality of filter rules. The method and system also comprise placing the plurality of filter rules in an order for testing against the key. The order is based on the frequency of each filter rule of the portion of the plurality of filter rules" **[0024]**; see also "The order

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

preferably places higher frequency filter rules first, so that the filter rules that are enforced more often will be tested first. The order preferably places the remaining rules in order of their frequency" **[0028]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada** and **Corl** before him or her, to modify the invention of **Kanada** with the teachings of **Corl** to include *wherein the order of the policy rules of the second sub-set of policy rules is changed based on frequency of usage thereof* as claimed because **Kanada** provides a policy rule controlled network with server and routers **(Kanada [0021]-[0137])** which could accumulate frequency statistics for each rule and place higher frequency filter rules first **(Corl [0062]; [0076])**. The suggestion/motivation for doing so would have been to save time and allow network processing to function more efficiently **(Corl [0029])**. Therefore, it would have been obvious to combine **Kanada** and **Corl** to obtain the invention as specified in the instant claim(s).

14. **Claims 7-11, 18-22, and 26** are rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of Goldschmidt et al. (US 20060013136 A1, hereinafter **Goldschmidt**).

As to Claim 7:

Kanada discloses the method of claim 1, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules **(e.g. deleting policy rules and checks consistency Kanada [0069]; [0096]; [0097])**, but does not specifically disclose:

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

- based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. although Kanada does teach a policy consistency checker that checks rules for being exclusive with each other [0109]-[0111])**.

However, the analogous art **Goldschmidt** does disclose based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt determining whether rules of updated rule subset have equal conflict relationship, then delete the lower priority rule [0061])**. **Kanada** and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "A flow manager may also receive additional packet flow rules, integrate them into the unified rule set, update the rule subsets according to the additional rules, and install the updated subsets onto the flow enforcement devices" **[Abstract]**; see also "After determining the relationship between two conflicting packet flow rules, flow manager 120 may be configured to determine whether the two rules have an equal relationship, as illustrated by decision block 440. If the two rules do have an equal conflict relationship, flow manager 120 may, according to one embodiment, append the actions of the lower priority rule to the actions of the higher priority rule, as illustrated by block 460. According to certain embodiments, if flow manager 120 appends the actions of the lower priority rule to the actions of the higher priority rule, flow manager 120 may be

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

configured to delete the lower priority rule, since is may now be redundant" **[0061]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada** and **Goldschmidt** before him or her, to modify the invention of **Kanada** with the teachings of **Goldschmidt** to include *based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules* as claimed because **Kanada** provides a policy rule controlled network with a policy server that deletes rules **(Kanada [0021]-[0137])** which could be based on conflicting relationship of rules **(Goldschmidt [0061])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada** and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 8:

Kanada in view of **Goldschmidt** discloses the method of claim 7, wherein the one or more conflicts include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt "resolving a conflict between two packet flow rules that comprise identical packet filters. For example, in one embodiment, a flow manager, such as flow manager 120, may be configured to determine the relationship between the data packet flow specified by the packet filters of the conflicting rules, as illustrated by block**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

420" [0056]; see also "two rules conflict if their packet filters specify overlapping, or identical, data flow packets" [0057]). The Examiner supplies the same rationale for the combination of references **Kanada** and **Goldschmidt** as in Claim 7 above.

As to Claim 9:

Kanada in view of **Goldschmidt** discloses the method of claim 7, wherein the one or more conflicts include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule **(e.g. Kanada policy consistency checker that checks rules for being exclusive with each other [0109]-[0111]; Goldschmidt two or more rules may conflict by having packet filters that match the same data packets [0046]; [0051]; [0055])**. The Examiner supplies the same rationale for the combination of references **Kanada** and **Goldschmidt** as in Claim 7 above.

As to Claim 10:

Kanada discloses the method of claim 1, but does not specifically disclose:

- wherein the one or more weights are defined manually based on scope and attributes of policy rule.

However, the analogous art **Goldschmidt** does disclose wherein the one or more weights are defined manually based on scope and attributes of policy rule **(e.g. Goldschmidt rules are prioritized using prefix or ordered precedence, actions specified are prioritized [0038]; priority order for rules as specified by network service [0039]; administrator may provide the priorities [0047])**. **Kanada** and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada** and **Goldschmidt** before him or her, to modify the invention of **Kanada** with the teachings of **Goldschmidt** to include *wherein the one or more weights are defined manually based on scope and attributes of policy rule* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada** and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 11:

Kanada discloses the method of claim 1, but does not specifically disclose:

- wherein the one or more weights are defined automatically.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

However, the analogous art **Goldschmidt** does disclose wherein the one or more weights are defined automatically **(e.g. Goldschmidt rules are prioritized using prefix or ordered precedence, actions specified are prioritized [0038]; policies are received that express priorities between network services and their supplied packet flow rules [0047])**. **Kanada** and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada** and **Goldschmidt** before him or her, to modify the invention of **Kanada** with the teachings of **Goldschmidt** to include *wherein the one or more weights are defined manually based on scope and attributes of policy rule* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order based on received policies **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])**. The suggestion/motivation for doing so would have been to provide for the efficient and

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada** and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 18:

Kanada discloses the system of claim 13, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules **(e.g. deleting policy rules and checks consistency Kanada [0069]; [0096]; [0097])**, but does not specifically disclose:

- based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. although Kanada does teach a policy consistency checker that checks rules for being exclusive with each other [0109]-[0111])**.

However, the analogous art **Goldschmidt** does disclose based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt determining whether rules of updated rule subset have equal conflict relationship, then delete the lower priority rule [0061])**. **Kanada** and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "A flow manager may also receive additional packet flow rules, integrate them into the unified rule set, update the rule subsets according to the additional rules, and install the updated subsets onto the flow enforcement

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

devices" **[Abstract]**; see also "After determining the relationship between two conflicting packet flow rules, flow manager 120 may be configured to determine whether the two rules have an equal relationship, as illustrated by decision block 440. If the two rules do have an equal conflict relationship, flow manager 120 may, according to one embodiment, append the actions of the lower priority rule to the actions of the higher priority rule, as illustrated by block 460. According to certain embodiments, if flow manager 120 appends the actions of the lower priority rule to the actions of the higher priority rule, flow manager 120 may be configured to delete the lower priority rule, since is may now be redundant" **[0061]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada** and **Goldschmidt** before him or her, to modify the invention of **Kanada** with the teachings of **Goldschmidt** to include *based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules* as claimed because **Kanada** provides a policy rule controlled network with a policy server that deletes rules **(Kanada [0021]-[0137])** which could be based on conflicting relationship of rules **(Goldschmidt [0061])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada** and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

As to Claim 19:

Kanada in view of **Goldschmidt** discloses the system of claim 18, wherein the one or more conflicts include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules **(e.g. Goldschmidt "resolving a conflict between two packet flow rules that comprise identical packet filters. For example, in one embodiment, a flow manager, such as flow manager 120, may be configured to determine the relationship between the data packet flow specified by the packet filters of the conflicting rules, as illustrated by block 420" [0056]; see also "two rules conflict if their packet filters specify overlapping, or identical, data flow packets" [0057])**. The Examiner supplies the same rationale for the combination of references **Kanada** and **Goldschmidt** as in Claim 18 above.

As to Claim 20:

Kanada in view of **Goldschmidt** discloses the system of claim 18, wherein the one or more conflicts include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule **(e.g. Kanada policy consistency checker that checks rules for being exclusive with each other [0109]-[0111]; Goldschmidt two or more rules may conflict by having packet filters that match the same data packets [0046]; [0051]; [0055])**. The Examiner supplies the same rationale for the combination of references **Kanada** and **Goldschmidt** as in Claim 18 above.

As to Claim 21:

Kanada discloses the system of claim 13, but does not specifically disclose:

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

- wherein the one or more weights are defined manually based on scope and attributes of the policy rule.

However, the analogous art **Goldschmidt** does disclose wherein the one or more weights are defined manually based on scope and attributes of the policy rule **(e.g. Goldschmidt rules are prioritized using prefix or ordered precedence, actions specified are prioritized [0038]; priority order for rules as specified by network service [0039]; administrator may provide the priorities [0047])**. **Kanada** and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada** and **Goldschmidt** before him or her, to modify the invention of **Kanada** with the teachings of **Goldschmidt** to include *wherein the one or more weights are defined manually based on scope and attributes of the policy rule* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

(Kanada [0021]-[0137]) which could include prioritizing rules in a particular order **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada** and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 22:

Kanada discloses the system of claim 13, but does not specifically disclose:

- wherein the one or more weights are defined automatically.

However, the analogous art **Goldschmidt** does disclose wherein the one or more weights are defined automatically **(e.g. Goldschmidt rules are prioritized using prefix or ordered precedence, actions specified are prioritized [0038]; policies are received that express priorities between network services and their supplied packet flow rules [0047])**. **Kanada** and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada** and **Goldschmidt** before him or her, to modify the invention of **Kanada** with the teachings of **Goldschmidt** to include *wherein the one or more weights are defined manually based on scope and attributes of policy rule* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order based on received policies **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada** and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

As to Claim 26:

Kanada discloses the system of claim 23, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules **(e.g. deleting policy rules and checks consistency Kanada [0069]; [0096]; [0097])**, but does not specifically disclose:

- based on one or more conflicts between policy rules of the third sub-set of policy rules and the retrieved set of policy rules **(e.g. although Kanada does teach a policy consistency checker that checks rules for being exclusive with each other [0109]-[0111])**.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

However, the analogous art **Goldschmidt** does disclose based on one or more conflicts between policy rules of the third sub-set of policy rules and the retrieved set of policy rules **(e.g. Goldschmidt determining whether rules of updated rule subset have equal conflict relationship, then delete the lower priority rule [0061])**. **Kanada** and **Goldschmidt** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "A flow manager may also receive additional packet flow rules, integrate them into the unified rule set, update the rule subsets according to the additional rules, and install the updated subsets onto the flow enforcement devices" **[Abstract]**; see also "After determining the relationship between two conflicting packet flow rules, flow manager 120 may be configured to determine whether the two rules have an equal relationship, as illustrated by decision block 440. If the two rules do have an equal conflict relationship, flow manager 120 may, according to one embodiment, append the actions of the lower priority rule to the actions of the higher priority rule, as illustrated by block 460. According to certain embodiments, if flow manager 120 appends the actions of the lower priority rule to the actions of the higher priority rule, flow manager 120 may be configured to delete the lower priority rule, since is may now be redundant" **[0061]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada** and **Goldschmidt** before him or her, to modify the invention of **Kanada** with the teachings of

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Goldschmidt to include *based on one or more conflicts between policy rules of the third sub-set of policy rules and the retrieved set of policy rules* as claimed because **Kanada** provides a policy rule controlled network with a policy server that deletes rules **(Kanada [0021]-[0137])** which could be based on conflicting relationship of rules **(Goldschmidt [0061])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])**. Therefore, it would have been obvious to combine **Kanada** and **Goldschmidt** to obtain the invention as specified in the instant claim(s).

15. **Claim 12** is rejected under 35 U.S.C. 103 as being unpatentable over **Kanada** in view of **Goldschmidt** and further in view of **Corl**.

As to Claim 12:

Kanada discloses the method of claim 1, wherein said forming an updated set of policy rules is conducted **(e.g. Kanada add and store input policy rules into policy repository [0067]; [0070]; [0071]; rule table contains all input rules [0087]; list of rule identifiers and added rule sent to router [0099])** based on the preference settings and network traffic characteristics **(e.g. Kanada cross-reference relations between variables in policy rules [0067]; consistency checker of conditions of the rules being exclusive with each other or not [0110])**, but does not specifically disclose:

- based on the one or more weights, the priority settings for the policy rules, and network usage statistics.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

However, the analogous art **Goldschmidt** does disclose based on the one or more weights **(e.g. Goldschmidt longest prefix or ordered precedence [0038])**, the priority settings for the policy rules **(e.g. Goldschmidt priority order for rules [0039]; [0040]; [0041])**. Furthermore, the analogous art **Corl** does disclose network usage statistics [for each policy rule] **(e.g. Corl statistics of frequency of enforcement for reach of the plurality of filter rules [0024])**. **Kanada**, **Goldschmidt**, and **Corl** are analogous art because they are from the same field of endeavor in network rule management.

- (e.g. see **Goldschmidt**, "multiple rules from a single network service may be prioritized using either longest prefix or ordered precedence and the actions specified by the packet flow rules may be prioritized through their respective order in each rule's action list" **[0038]**; see also "A flow manager may also add rules to the unified rule set according to the particular priority order for those rules as specified by the network service that supplied those rules" **[0039]**; see also **[0040]**; see also **[0041]**);
- (e.g. see **Corl**, "Each of the plurality of filter rules has a priority. The method and system include accumulating statistics for each of the plurality of filter rules. The statistics indicate a frequency of enforcement for each of the plurality of filter rules. The method and system also include placing the plurality of filter rules in an order for testing against the key. The order is based on the frequency of each filter rule of the portion of the plurality of filter rules" **[Abstract]**; see also "The statistics indicate a frequency of enforcement for each of the plurality of filter rules. The method and system also comprise placing the plurality of filter rules in

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

an order for testing against the key. The order is based on the frequency of each filter rule of the portion of the plurality of filter rules" **[0024]**; see also "The order preferably places higher frequency filter rules first, so that the filter rules that are enforced more often will be tested first. The order preferably places the remaining rules in order of their frequency" **[0028]**).

It would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art, having the teachings of **Kanada**, **Goldschmidt**, and **Corl** before him or her, to modify the invention of **Kanada** with the teachings of **Goldschmidt** and **Corl** to include *based on the one or more weights, the priority settings for the policy rules, and network usage statistics* as claimed because **Kanada** provides a policy rule controlled network with a policy server that analyzes policy rules for dependencies **(Kanada [0021]-[0137])** which could include prioritizing rules in a particular order based on received policies **(Goldschmidt [0038]; [0039]; [0040]; [0041]; [0047])** and accumulating frequency statistics for each rule and placing higher frequency filter rules first **(Corl [0062]; [0076])**. The suggestion/motivation for doing so would have been to provide for the efficient and distributed management of heterogeneous sets of flow enforcement policies for homogeneous flow enforcement devices **(Goldschmidt [0011])** and to save time and allow network processing to function more efficiently **(Corl [0029])**. Therefore, it would have been obvious to combine **Kanada**, **Goldschmidt**, and **Corl** to obtain the invention as specified in the instant claim(s).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. **Schuba et al. (US 20040177139 A1)**

b. **Shah et al. (US 20090125470 A1)**

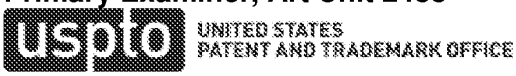
c. **Ling et al. (US 20100199346 A1)**

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kenneth Chang whose telephone number is (571)270-7530. The examiner can normally be reached on Monday-Friday 10:30am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

/Kenneth Chang/
Primary Examiner, Art Unit 2438


07/22/16

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Notice of References Cited	Application/Control No. 14/566,403	Applicant(s)/Patent Under Reexamination PERNICHA, HUGO FILIPE PA	
	Examiner Kenneth Chang	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2001/0039576 A1	11-2001	Kanada, Yasusi	H04L41/0893	709/223
*	B	US-2002/0154635 A1	10-2002	Liu, Yuefeng	H04L63/0428	370/392
*	C	US-2002/0198981 A1	12-2002	Corl, Everett Arthur JR.	H04L29/06	709/224
*	D	US-2004/0177139 A1	09-2004	Schuba, Christoph L.	H04L41/0873	709/223
*	E	US-2006/0013136 A1	01-2006	Goldschmidt; Jason L.	H04L47/10	370/235
*	F	US-2009/0125470 A1	05-2009	Shah; Sandip	H04L63/0263	706/47
*	G	US-2010/0199346 A1	08-2010	Ling; Yibei	H04L63/0263	726/12
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 7209

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/566,403	12/30/2014	726	2438	FORT-012500

APPLICANTS
Fortinet, Inc., Sunnyvale, CA;

INVENTORS
Hugo Filipe Parreira Pernicha, Venda do Pinheiro, PORTUGAL;

**** CONTINUING DATA **************************

**** FOREIGN APPLICATIONS **************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****
12/23/2014

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ Yes ☑ No	☐ Yes ☑ No	/KENNETH W CHANG/ Examiner's Signature	☐ Initials	PORTUGAL	9	26	3

ADDRESS

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228
UNITED STATES

TITLE

DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

FILING FEE RECEIVED		
2080	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed
PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14566403
	Filing Date	2014-12-10
	First Named Inventor	Hugo Filipe Parreira Pernicha
	Art Unit	~~2434~~ 2438
	Examiner Name	Kenneth Chang
	Attorney Docket Number	FORT-012500

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button							Add	

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./
Examiner Signature

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Receipt date: 12/30/2014	Application Number	14566403 14566403 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2014-12-10
(Not for submission under 37 CFR 1.99)	First Named Inventor	Hugo Filipe Parreira Pernicha
	Art Unit	~~2491~~ 2438
	Examiner Name	Kenneth Chang
	Attorney Docket Number	FORT-012500

/K.C./	1	AlgoSec BusinessFlow®. "Data Center Application Connectivity Management." 2013. 2 pages.	☐
	2	AlgoSec. "Managing Security at the Speed of Business." 2014. 6 pages.	☐
	3	EMA. "FireMon's Security Manager V7.0 Release Expands Value to Enterprises and Service Providers." 2013. 4 pages.	☐
	4	Tufin. SecureTrackTM. "Firewall Operations Management, Auditing & Compliance." Feb, 2012. 10 pages.	☐
	~~5~~	~~Ramachandran, V. "HOW TURBO ACL'S WORK." 6 pages.~~	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Kenneth Chang/	Date Considered	07/20/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14566403	PERNICHA, HUGO FILIPE PARREIRA
	Examiner	**Art Unit**
	KENNETH CHANG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/23/2016								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								

IEEE.org | IEEE *Xplore* Digital Library | IEEE-SA | IEEE Spectrum | More Sites Cart (0) | Create Account | Personal Sign In

Access provided by:
United States Patent and Trademark Office
Sign Out

BROWSE | MY SETTINGS | GET HELP | WHAT CAN I ACCESS?

Displaying results 1-22 of 22 for **policy rule network traffic optimize**

Show All Results Per Page 25 Sort By Relevance

Select All on Page | Download Citations | Export to IEEE Collabratec | Set Search Alerts | Search History

Refine results by

Search within results

Content Type

- Conference Publications (19)
- Journals & Magazines (3)

Year

Single Year | Range

1983 2015

From 1989 To 2015

Author

Affiliation

Publication Title

Publisher

Conference Location

1. **Network Security Policies: Verification, Optimization and Testing**
   E. Al-Shaer
   2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006
   Year: 2006
   Pages: 584 - 584, DOI: 10.1109/NOMS.2006.1687592
   Cited by: Papers (2)
   IEEE Conference Publications
   Abstract (80 Kb)

2. **Impact of IP layer routing policy on multilayer design**
   E. Palkopoulou; O. Gerstel; I. Stiakogiannakis; T. Telkamp; V. Lopez; I. Tomkos
   IEEE/OSA Journal of Optical Communications and Networking
   Year: 2015, Volume: 7, Issue: 3
   Pages: A396 - A402, DOI: 10.1364/JOCN.7.00A396
   Cited by: Papers (2)
   IEEE Journals & Magazines
   Abstract (618 Kb)

3. **Dynamic policy and charging control framework**
   Xiang Yang Li; Kim Brouard; Yigang Cai
   Bell Labs Technical Journal
   Year: 2012, Volume: 17, Issue: 1
   Pages: 105 - 123, DOI: 10.1002/bltj.21526
   Alcatel-Lucent Journal
   Abstract (499 Kb)

4. **Firewall packet matching optimization using network traffic behavior and packet matching statistics**
   Zouheir Trabelsi; Hishem El Sayed; Safaa Zeidan
   Third International Conference on Communications and Networking
   Year: 2012
   Pages: 1 - 7, DOI: 10.1109/ComNet.2012.6217735
   IEEE Conference Publications
   Abstract (936 Kb)

5. **Adaptive optimization of packet filtering devices performance ensuring a conflict-free network configuration**
   Gianluca Maiolini; Lorenzo Cignini; Andrea Baiocchi
   INFOCOM Workshops 2008, IEEE
   Year: 2008

Guannua Yan; Songqing Chen; Stephan Eidenbenz
Quality of Service, 2008. IWQoS 2008. 16th International Workshop on
Year: 2008
Pages: 209 - 218, DOI: 10.1109/IWQOS.2008.30
Cited by: Papers (1)
IEEE Conference Publications

Abstract (232 Kb)

☐ **Firewall Policy Queries**
Alex X. Liu; Mohamed G. Gouda
IEEE Transactions on Parallel and Distributed Systems
Year: 2009, Volume: 20, Issue: 6
Pages: 766 - 777, DOI: 10.1109/TPDS.2008.263
Cited by: Papers (21)
IEEE Journals & Magazines

Abstract (1800 Kb)

☐ **Challenges in the design and implementation of wireless sensor networks: A holistic approach-development and planning tools, middleware, power efficiency, interoperability**
George Papadopoulos
2015 4th Mediterranean Conference on Embedded Computing (MECO)
Year: 2015
Pages: 1 - 3, DOI: 10.1109/MECO.2015.7181857
IEEE Conference Publications

Abstract (127 Kb)

☐ **Emulation Performance Study of Traffic-Aware Policy Enforcement in Software Defined Networks**
Isaac Vawter; Deng Pan; Wenrui Ma
2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems
Year: 2014
Pages: 775 - 780, DOI: 10.1109/MASS.2014.62
IEEE Conference Publications

Abstract (598 Kb)

☐ **Dynamic Policy-Based Routing Using Firewall Rules**
Kavin Tantipongsakul; Akharin Khunkitti
Computer Modeling and Simulation, 2009. EMS '09. Third UKSim European Symposium on
Year: 2009
Pages: 540 - 545, DOI: 10.1109/EMS.2009.33
IEEE Conference Publications

Abstract (574 Kb)

« First < 1 > Last »

Personal Sign In | Create Account

IEEE Account
» Change Username/Password
» Update Address

Purchase Details
» Payment Options
» Order History
» View Purchased Documents

Profile Information
» Communications Preferences
» Profession and Education
» Technical Interests

Need Help?
» US & Canada: +1 800 678 4333
» Worldwide: +1 732 981 0060
» Contact & Support

About IEEE *Xplore* | Contact Us | Help | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity
© Copyright 2016 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	11	H04L63/0263.CPC. and (rule) same (depend$9) same (compatib$9 or conflict$9) and (packet or flow or traffic) and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5) and order$5	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/23 00:02
S15	1	"20060013136".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 22:07
S14	1	"20020198981".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 21:15
S13	14	(supernet$9) same (ip or internet protocol) same address$5 same source same destination	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 20:50
S12	281	(rule) same (depend$9) same (compatib$9 or conflict$9) and (packet or flow or traffic) and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5) and order$5	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:22
S11	185	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5) and order$5	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:21
S10	185	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule) and (optimiz$5 or efficient$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:20
S9	212	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies) and (add or added or adding or new$5) with (rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 15:20
S8	10	H04L63/0263.CPC. and (rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 14:10
S7	311	(rule) same (depend$9) same (compatib$9 or conflict$9) and traffic and network$5 and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 14:10
S6	9	("5889953" | "6041347" | "6170009" | "6418468" | "6463470" | "6587466" | "6601082" | "6611863").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 12:22

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

S5	1	"20010039576".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 12:20
S4	1	"7441022".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/22 12:11
S3	2021	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/20 14:34
S2	590	fortinet.as.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/20 14:33
S1	1	(pernicha adj3 hugo).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/07/20 14:33

7/23/2016 12:03:31 AM
C:\Users\kchang3\Documents\EAST\Workspaces\14566403_APP.wsp

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14566403	PERNICHA, HUGO FILIPE PARREIRA
	Examiner	Art Unit
	KENNETH CHANG	2438

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/0263	7/20/2016	KC

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Searched Inventors' Names and Assignee on eDan and EAST.	7/20/2016	KC
Searched IEEE NPL Xplore Database online.	7/20/2016	KC
Completed Limited Classified Search in CPC on EAST USPAT, PGPUB, and EPO databases with Keywords.	7/22/2016	KC
Keywords Searched: See East search history.	7/22/2016	KC

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/KENNETH CHANG/ Primary Examiner.Art Unit 2438

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/566,403	12/30/2014	Hugo Filipe Parreira Pernicha	FORT-012500

CONFIRMATION NO. 7209

64128
MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

PUBLICATION NOTICE

OC000000084072705

Title:DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

Publication No.US-2016-0191466-A1
Publication Date:06/30/2016

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/566,403

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	600
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	26 minus 20 =	* 6			OR	x 80 =	480
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 420 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	2080

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/566,403	12/30/2014	2431	2080	FORT-012500	26	3

CONFIRMATION NO. 7209

UPDATED FILING RECEIPT

64128
MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

OC000000073989897

Date Mailed: 03/17/2015

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)
Hugo Filipe Parreira Pernicha, Venda do Pinheiro, PORTUGAL;

Applicant(s)
Fortinet, Inc., Sunnyvale, CA

Assignment For Published Patent Application
FORTINET, INC., Sunnyvale, CA

Power of Attorney: The patent practitioners associated with Customer Number 64128

Domestic Applications for which benefit is claimed - None.
A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 12/23/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/566,403**

Projected Publication Date: 06/30/2016

Non-Publication Request: No

Early Publication Request: No

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Title

DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Fortinet, Inc.	Examiner: To be assigned
Inventor: Hugo Filipe Parreira Pernicha	Group Art Unit: To be assigned
App. No.: 14/566,403	Conf. No.: 7209
Filed: December 10, 2014	Docket No.: FORT-012500
For: DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT	

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR LATER FILING DATE
under 37 CFR 1.182

Dear Sir/Madam:

The undersigned respectfully requests the Director to accord the above-captioned patent application the filing date of December 30, 2014 in view of the fact that this Petition is being timely submitted within two months of the Notice to File Corrected Application Papers mailed on December 29, 2014 ("**Notice**") concurrently with the omitted item(s) noted by the Notice, this Petition and the petition fee set forth in 37 CFR 1.17(f).

Statement of Facts

1. The above-captioned patent application was original filed on December 10, 2014 via EFS-Web.
2. Subsequently, the USPTO issued the Notice setting a two-month period for response.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

3. The Applicant has elected option II described in the Notice (i.e., supply of the omitted item(s) and acceptance of the date that such omitted item(s) are filed in the USPTO as the filing date for the above-captioned patent application).
4. The omitted item(s) noted in the Notice are submitted concurrently herewith in the form of a substitute specification in clean and redlined form.

Point to be Reviewed

Whether the above-captioned patent application should be accorded a filing date of December 30, 2014 in view of the fact that the omitted item(s) noted in the Notice are submitted concurrently herewith.

Action Requested

The undersigned respectfully requests the Director to accord the above-captioned patent application a filing date of December 30, 2014 (i.e., the date that the omitted item(s) noted in the Notice were filed in the USPTO).

Respectfully submitted,
Hamilton, DeSanctis & Cha LLP

Date December 30, 2014

By /Michael A. DeSanctis/
Michael A. DeSanctis, Esq.
Reg. No. 39,957
Customer No. 64128
Ph: (303) 856-7155

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PTO/AIA/17p (03-13)
Approved for use through 07/31/2014. OMB 0651-0059
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

PROCESSING FEE Under 37 CFR 1.17(f), (g) & (h) TRANSMITTAL

(Fees are subject to annual revision)

[Page 1 of 2]

Send completed form to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Application Number	14/566,403
Filing Date	December 10, 2014
First Named Inventor	Hugo Filipe Parreira Pernic
Art Unit	TBD
Examiner Name	TBD
Practitioner Docket No.	FORT-012500

Enclosed is a petition filed under 37 CFR 1.182 **that requires a processing fee (37 CFR 1.17(f), (g), or (h)).**

Payment of $ 400 **is enclosed.**

This form should be included with the above-mentioned petition and faxed or mailed to the Office using the appropriate Mail Stop (*e.g.*, Mail Stop Petition), if applicable. *For transmittal of processing fees under 37 CFR 1.17(i), see form PTO/SB/17i.*

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

Payment of Fees

☐ The Commissioner is hereby authorized to charge the following fees to Deposit Account No. _____:

☑ petition fee under 37 CFR 1.17(f), (g) or (h) ☐ any deficiency of fees and credit of any overpayments

☐ Check in the amount of $ _____ is enclosed. ☑ Payment via EFS-Web.

☐ Payment by credit card (Form PTO-2038 or equivalent is enclosed). Do not provide credit card information on this form.

Processing Fees Under 37 CFR 1.17(f):

Undiscounted Fee $400 (Fee Code 1462) Small Entity Fee $200 (Fee Code 2462) Micro Entity Fee $100 (Fee Code 3462)

For papers filed under:
§ 1.36(a) - for revocation of a power of attorney by fewer than all of the applicants.
§ 1.53(e) - to accord a filing date.
§ 1.57(a) - to accord a filing date.
§ 1.182 - for decision on a question not specifically provided for.
§ 1.183 - to suspend the rules.
§ 1.378(e) - for reconsideration of decision on petition refusing to accept delayed payment of maintenance fee in an expired patent.
§ 1.741(b) - to accord a filing date to an application under § 1.740 for extension of a patent term.

Processing Fees Under 37 CFR 1.17(g):

Undiscounted Fee $200 (Fee Code 1463) Small Entity Fee $100 (Fee Code 2463) Micro Entity Fee $50 (Fee Code 3463)

For papers filed under:
§ 1.12 - for access to an assignment record.
§ 1.14 - for access to an application.
§ 1.46 - for filing an application on behalf of an inventor by a person who otherwise shows sufficient proprietary interest in the matter.
§ 1.55(f) - for filing a belated certified copy of a foreign application.
§ 1.59 - for expungement of information.
§ 1.103(a) - to suspend action in an application.
§ 1.136(b) - for review of a request for extension of time when the provisions of § 1.136(a) are not available.
§ 1.377 - for review of decision refusing to accept and record payment of a maintenance fee filed prior to expiration of a patent.
§ 1.550(c) - for patent owner requests for extension of time in *ex parte* reexamination proceedings.
§ 1.956 - for patent owner requests for extension of time in *inter partes* reexamination proceedings.
§ 5.12 - for expedited handling of a foreign filing license.
§ 5.15 - for changing the scope of a license.
§ 5.25 - for retroactive license.

This collection of information is required by 37 CFR 1.17. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 5 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PTO/AIA/17p (03-13)
Approved for use through 07/31/2014. OMB 0651-0059
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

PROCESSING FEE
Under 37 CFR 1.17(f), (g) & (h)
TRANSMITTAL

Processing Fees Under 37 CFR 1.17(h):

Undiscounted Fee $140 (Fee Code 1464) **Small Entity Fee $70 (Fee Code 2464)** **Micro Entity Fee $35 (Fee Code 3464)**

For papers filed under:
§ 1.19(g) - to request documents in a form other than provided in this part.
§ 1.84 – for accepting color drawings or photographs.
§ 1.91 – for entry of a model or exhibit.
§ 1.102(d) – to make an application special.
§ 1.138(c) - to expressly abandon an application to avoid publication.
§ 1.313 – to withdraw an application from issue.
§ 1.314 - to defer issuance of a patent.

SUBMITTED BY

Signature		Registration No. (Attorney/Agent)	Telephone
Name (Print/Type)			Date

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Electronic Patent Application Fee Transmittal	
Application Number:	14566403
Filing Date:	10-Dec-2014
Title of Invention:	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT
First Named Inventor/Applicant Name:	Hugo Filipe Parreira Pernicha
Filer:	Michael A. DeSanctis
Attorney Docket Number:	FORT-012500
Filed as Large Entity	
Filing Fees for Utility under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Petition fee- 37 CFR 1.17(f) (Group I)	1462	1	400	400
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**400**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Electronic Acknowledgement Receipt	
EFS ID:	21089221
Application Number:	14566403
International Application Number:	
Confirmation Number:	7209
Title of Invention:	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT
First Named Inventor/Applicant Name:	Hugo Filipe Parreira Pernicha
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-012500
Receipt Date:	30-DEC-2014
Filing Date:	10-DEC-2014
Time Stamp:	15:01:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$400
RAM confirmation Number	15296
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	Notice_to_File_Corrected_Application_Papers.pdf	189790 dc8a4f20668733c736e1955437b7757c97f8457d	no	3
Warnings:					
Information:					
2	Miscellaneous Incoming Letter	Response_to_Notice.pdf	74928 307073065420bd0a651ad833f35d5665528aafbb	no	2
Warnings:					
Information:					
3	Preliminary Amendment	Preliminary_Amendment.pdf	79979 210665c262e9781c6fabab4906bafae2f9ca837f	no	3
Warnings:					
Information:					
4	Specification	Specification_Specification_CLEAN.pdf	281535 a6d72348c39812cd3cffd8a16a0c4fff5fddfecc	no	34
Warnings:					
Information:					
5	Specification	Substitute_Specification_REDLINE.pdf	285339 1d1345ca3eebd3067e9612dfeb75d11c75d5fdfc	no	34
Warnings:					
Information:					
6	Petition for review by the Office of Petitions.	Rule_182_Petition.pdf	76166 f1936f4ad7ce82ce9fe30efb88190ab55c636103	no	2
Warnings:					
Information:					
7	Transmittal Letter	Fee_Transmittal.pdf	214825 b3622c749eff4e65f92cdd7a6ab9c09cc9812f81	no	3
Warnings:					
Information:					

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

8	Fee Worksheet (SB06)	fee-info.pdf	30282 1efba1d51168df3fa25630150443db0f0d36478e	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	1232844	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/566,403	12/10/2014	Hugo Filipe Parreira Pernicha	FORT-012500

CONFIRMATION NO. 7209

64128
MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

FORMALITIES LETTER

OC000000072559100

Date Mailed: 12/29/2014

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Filing Date Granted

An application number and filing date have been accorded to this application. The application is informal since it does not comply with the regulations for the reason(s) indicated below. Applicant is given TWO MONTHS from the date of this Notice within which to correct the informalities indicated below. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

The required item(s) identified below must be timely submitted to avoid abandonment:

- A substitute specification in compliance with 37 CFR 1.52, 1.121(b)(3), and 1.125, is required. The substitute specification must be submitted with markings and be accompanied by a clean version (without markings) as set forth in 37 CFR 1.125(c) and a statement that the substitute specification contains no new matter (see 37 CFR 1.125(b)). The specification, claims, and/or abstract page(s) submitted is not acceptable and cannot be scanned or properly stored because:
  - The application contains drawings, but the specification does not contain a brief description of the several views of the drawings as required by 37 CFR 1.74 and 37 CFR 1.77(b)(9).

The following item(s) appear to have been **omitted** from the application:

- Figure(s) **3** described in the specification.

Applicant must reply to this notice within the time period set forth in this notice to avoid abandonment of this application. Applicant must select one of the three following options and the reply must comply with the requirements set forth in the selected option and any other requirements set forth in this notice. The reply should also indicate which option applicant has selected.

I. Petition for date of deposit: Should applicant contend that the above-noted omitted item(s) was in fact deposited in the U.S. Patent and Trademark Office (USPTO) with the nonprovisional application papers, a copy of this Notice and a petition (and the petition fee set forth in 37 CFR 1.17(f) with evidence of such deposit **must** be filed within **TWO MONTHS** of the date of this Notice. The petition fee will be refunded if it is determined that the item(s) was received by the USPTO. **THIS TWO MONTH PERIOD IS EXTENDABLE UNDER 37 CFR 1.136(a) or (b).**

II. Petition for later filing date: Should applicant desire to supply the omitted item(s) and accept the date that such omitted item(s) was filed in the USPTO as the filing date of the above-identified application, a copy of this Notice, the omitted item(s), and a petition under 37 CFR 1.182 with the petition fee set forth in 37 CFR 1.17(f) requesting the later filing date **must** be filed within **TWO MONTHS** of the date of this Notice. **THIS TWO MONTH PERIOD IS EXTENDABLE UNDER 37 CFR 1.136(a) or (b).**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Applicant is advised that generally the filing fee required for an application is the filing fee in effect on the filing date accorded the application and that payment of the requisite basic filing fee on a date later than the filing date of the application requires payment of a surcharge (37 CFR 1.16(f)). To avoid processing delays and payment of a surcharge, applicant should submit any balance due for the requisite filing fee based on the later filing date being requested when submitting the omitted item(s) and the petition (and petition fee) requesting the later filing date.

III. Acceptance of application as deposited: Applicant may accept the application as deposited in the USPTO by filing an appropriate amendment as set forth in either (A) or (B) below within **TWO MONTHS** of the date of this Notice. **THIS TWO MONTH PERIOD IS EXTENDABLE UNDER 37 CFR 1.136(a) or (b)** . The application will maintain a filing date as of the date of deposit of the application papers in the USPTO, and original application papers (i.e., the original disclosure of the invention) will include only those application papers present in the USPTO on the date of deposit. A petition is not required for this option.

(A) If applicant wants to accept the application as deposited without adding the subject matter that was in the omitted item (e.g., a missing page or figure), applicant is required to submit one or more of the following items without adding any new matter (see 35 U.S.C. 132(a)):

1. For a missing page of the specification,
   a) a substitute specification including claims that amends the specification to renumber the pages consecutively and cancels any incomplete sentences, and
   b) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125;
2. For a missing figure of the drawings,
   a) replacement drawing sheets in compliance with 37 CFR 1.121(d) to renumber the drawing figures consecutively (if necessary),
   b) a substitute specification excluding claims that amends the specification to cancel any references to any omitted drawing(s) and corrects the references in the specification to the drawing figures to correspond with any relabeled drawing figures, and
   c) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125;
3. For a missing page of the claim listing only, a replacement claim listing with the claims renumbered consecutively or, if amendment to the claims is also necessary, then a complete claim listing in compliance with 37 CFR 1.121(c);
4. For a missing or unreadable compact disc,
   a) a substitute specification (excluding the claims) deleting the reference to the compact disc and the files contained on the compact disc, and
   b) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125; and
5. For a missing or unreadable file submitted on a compact disc,
   a) a substitute specification (excluding the claims) deleting the reference to the missing or unreadable file, and a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125; and
   b) a replacement transmittal letter listing all of the files except the missing or unreadable file in compliance with 37 CFR 1.52(e)(3)(ii).

(B) Alternatively, if applicant wants to accept the application as deposited but wishes to add the subject matter in the omitted item (e.g., a missing page or figure) by relying on an incorporation by reference under 37 CFR 1.57 or other portions of the original disclosure, applicant is required to submit one or more of the following items without adding any new matter (see 35 U.S.C. 132(a)):

1. To add the subject matter in a missing page of specification,
   a) a substitute specification excluding claims and
   b) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125;

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

2. To add a missing figure of the drawings, new and replacement drawing sheets in compliance with 37 CFR 1.121(d);
3. To add the subject matter in a missing page of the claim listing, a complete claim listing in compliance with 37 CFR 1.121(c) (e.g., a claim in the missing page should be submitted as a new claim);
4. To add the subject matter in a missing or unreadable compact disc,
   a) a replacement compact disc and a duplicate copy of the compact disc, in compliance with 37 CFR 1.52(e); and
   b) a statement that the replacement compact disc contains no new matter in compliance with 37 CFR 1.52(e)(4); and,
5. To add the subject matter in a missing or unreadable file submitted on a compact disc,
   a) a replacement compact disc that contains all of the files listed in the specification including the missing or unreadable file and a duplicate copy of the compact disc, in compliance with 37 CFR 1.52(e); and
   b) a statement that the replacement compact disc contains no new matter in compliance with 37 CFR 1.52(e)(4).

If applicant is relying on an incorporation by reference under 37 CFR 1.57 to add the omitted subject matter, then applicant must also comply with the requirements of 37 CFR 1.57.

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/kung/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Fortinet, Inc.	Examiner: To Be Assigned
Inventor: Hugo Filipe Parreira Pernicha	Group Art Unit: To Be Assigned
App. No.: 14/566,403	Conf. No.: 7209
Filed: December 10, 2014	Docket No.: FORT-012500
For: DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT	

Mail Stop Missing Parts
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO THE NOTICE TO FILE CORRECTED APPLICATION PAPERS

Dear Sir/Madam:

In response to the Notice to File Corrected Application Papers mailed December 29, 2014 ("**Notice**"), the Applicant selects option II (i.e., petition for later filing date) and provides herewith the omitted item(s).

Submitted concurrently herewith are the following:

- A PDF version of the Notice
- A Preliminary Amendment
- A Substitute Specification (in clean and redlined form) containing proposed amendments to address the deficiencies noted in the Notice;
- A Petition under 37 CFR 1.182 ("**Petition**"); and
- The Petition fee set forth in 37 CFR 1.17(f).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

The undersigned respectfully requests consideration of the Petition and that the above-captioned patent application be accorded a filing date of December 30, 2014.

Respectfully submitted,
Hamilton, DeSanctis & Cha LLP

Date December 30, 2014

By /Michael A. DeSanctis/
Michael A. DeSanctis, Esq.
Reg. No. 39,957
Customer No. 64128
Ph: (303) 856-7155

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Fortinet, Inc.	Examiner: To Be Assigned
Inventor: Hugo Filipe Parreira Pernicha	Group Art Unit: To Be Assigned
App. No.: 14/566,403	Conf. No.: 7209
Filed: December 10, 2014	Docket No.: FORT-012500
For: DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT	

Mail Stop Missing Parts
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

PRELIMINARY AMENDMENT

Dear Sir/Madam:

The Applicant respectfully requests the Examiner to enter the following amendment and to consider the following remarks before acting on the above-referenced patent application:

Amendments to the Specification begin on page 2 of this paper.

Remarks begin on page 3 of this paper.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

AMENDMENT

Amendments to the Specification:

Please replace the specification with the attached substitute specification pursuant to 37 CFR §1.121(b)(3).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Remarks

The Applicant respectfully requests reconsideration of the above-captioned patent application in view of the following remarks. In this Preliminary Amendment, no claims have been added, cancelled or amended. Hence, upon entry of this Preliminary Amendment, claims 1-26 remain for examination.

The undersigned submits herewith a substitute specification (in clean and redlined form) to address the omitted item(s) noted in the Notice to File Corrected Application Papers mailed December 29, 2014 ("Notice").

Request for a Telephone Interview

If the Examiner believes a telephone conference would expedite prosecution of the above-captioned patent application, please telephone the undersigned at (303) 856-7155.

Respectfully submitted,
Hamilton, DeSanctis & Cha LLP

Date December 30, 2014

By /Michael A. DeSanctis/
Michael A. DeSanctis, Esq.
Reg. No. 39,957
Customer No. 64128
Ph: (303) 856-7155

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Atty. Docket No.: FORT-012500 Patent Application
Fortinet Ref. No.: 13048

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TITLE OF THE INVENTION

DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

Inventor:

Hugo Filipe Parreira Pernicha, residing at:
Av. 9 de Julho, nº 12, 3 Dto
2665-520 Venda do Pinheiro
PORTUGAL

Assignee: **FORTINET, INC.**
A Delaware Corporation

Entity: Regular Undiscounted

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

COPYRIGHT NOTICE

[0001] Contained herein is material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction of the patent disclosure by any person as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all rights to the copyright whatsoever. Copyright © 2014, Fortinet, Inc.

BACKGROUND

Field

[0002] Embodiments of the present invention generally relate to network traffic control. In particular, embodiments of the present invention relate to systems and methods for firewall and/or access control policy management and optimization of policy rules to enhance performance of policy rule processing.

Description of the Related Art

[0003] A firewall generally represents an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system. A firewall may assume the form of a flow control device or set of devices configured to permit, deny, encrypt, decrypt and/or proxy computer traffic between different security domains based upon a set of rules and other criteria. Organizations that use Internet Protocol (IP) based communication networks have firewalls or access control devices/mechanisms to control the traffic that crosses into and out of their networks, or between different network segments. Each firewall is basically a special-purpose computer that enforces the organization's traffic filtering policy. Typically, the filtering policy is implemented in a rule base, which is an ordered list of rules, wherein each rule consists of a set of field value-ranges, and an associated action that is generally either “PASS” or “DROP”.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0004] Most firewalls enforce the policy according to "first-match" semantics, wherein for each new IP connection, the firewall checks the rules one by one, according to their order in the rule-base, until it finds a rule that matches the new connection. The first rule that matches the connection determines the firewall's action, wherein if the first matching rule has an action of "PASS" then the firewall will allow the connection to continue, and if the rule's action is "DROP" then the firewall will discard all the packets belonging to the connection. If no rule matches the connection then the firewall uses a default action, which is usually DROP.

[0005] As firewall or access control policies can have numerous rules, searching for a matching rule in sequence can require considerable CPU time. In such an implementation, the computational effort to match a connection to the rule-base is proportional (linearly) to the number of rules the firewall needs to try in sequence until it reaches the first matching rule. If checking a match against one rule typically requires M computer instructions, then checking K rules in sequence requires K times M instructions. If the first-matching rule happens to be one of the first in the rule-base, the firewall will identify the corresponding action quickly and with a low computational effort. Conversely, if the first-matching rule is near the end of the rule-base, the firewall will take longer to identify the corresponding action.

[0006] Firewall rule-based policy is typically static. As such, once it is configured, it will stay the same, in the same order and not be changed unless explicitly changed by a user/administrator. In practice, large enterprises end up with a substantial set of firewall rule-based policies that are more oriented to user/operator visibility than rule processing efficiency. Furthermore, addition of each new policy rule or modification of an existing rule typically has ripple effects on other existing/stored rules and policies. For instance, a new policy rule may be configured to allow packets of a specific traffic type to a given destination, which otherwise may have been denied by an already existing policy rule in the rule database. Existing security policy management techniques require manual detection of issues, such as duplication of rules, conflicts between rules, dependency between rules, or shadowing of one rule by another and therefore are error prone. These issues are exacerbated in the context of large policy rule databases.

[0007] There is therefore a need for systems and methods that allow efficient addition or modification of one or more policy rules by enabling enhanced system performance, manageability and reduced human error. There is also a need for systems and methods that

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

allow dynamic and automatic optimization of policy rules by efficiently grouping/merging, deleting, reordering and otherwise managing policy rules based on defined and configurable optimization criteria so as to enable improved overall performance and significant reduction in session establishment/rule access/rule processing delay.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

SUMMARY

[0008] Methods and systems are described for dynamically optimizing rule-based security policies. According to one embodiment, a security policy optimization method is provided. A request is received by a network security management device to add a new traffic flow policy rule to multiple existing policy rules managed by the network security management device. Dependencies of the new traffic flow policy rule on one or more of the existing policy rules are automatically determined. An updated set of policy rules is formed by incorporating the new traffic flow policy rule within the existing policy rules based on the determined dependencies. The updated set of policy rules is then optimized by (i) grouping a first sub-set of policy rules of the updated set of policy rules; (ii) reordering a second sub-set of policy rules of the updated set of policy rules; and/or (iii) deleting a third sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules.

[0009] Other features of embodiments of the present disclosure will be apparent from accompanying drawings and from detailed description that follows.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] In the Figures, similar components and/or features may have the same reference label. Further, various components of the same type may be distinguished by following the reference label with a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

[0011] FIG. 1 illustrates exemplary security policy architecture in accordance with an embodiment of the present invention.

[0012] FIG. 2 illustrates exemplary functional units of a rule-based security policy management system in accordance with an embodiment of the present invention.

[0013] FIGs. 3A and 3B illustrate addition of a new security policy rule to a policy rule database in accordance with an embodiment of the present invention.

[0014] FIG. 4 illustrates an exemplary snapshot of a security policy rule management system in accordance with an embodiment of the present invention.

[0015] FIGs. 5A to 5E illustrate exemplary optimization of policy rules stored in a rule database based on dependencies, priorities, traffic attributes, hits, sessions, potential of merger/modification/deletion, among other attributes in accordance with an embodiment of the present invention.

[0016] FIG. 6 is a flow diagram illustrating security policy rule management in accordance with an embodiment of the present invention.

[0017] FIG. 7 is an exemplary computer system in which or with which embodiments of the present invention may be utilized.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

DETAILED DESCRIPTION

[0018] Methods and systems are described for dynamically optimizing rule-based security policies. Methods and systems are also provided for creation and modification of firewall/access control policy rules so as to allow enhanced computing performance, rule management, policy optimization, and session/network traffic packet flow management. Methods and systems are further provided for optimizing the security policy rules by performing any or a combination of reordering, grouping, updating, deleting, along with performing any other actions on one or more policy rules based on parameters, including, but not limited to, weights assigned to traffic attributes (e.g., source address, destination address, service, port information, among other such attributes), preference settings, priority settings for the policy rules, network traffic characteristics, network usage statistics, among other optimization parameters.

[0019] In the following description, numerous specific details are set forth in order to provide a thorough understanding of embodiments of the present disclosure. It will be apparent to one skilled in the art that embodiments of the present disclosure may be practiced without some of these specific details. Embodiments of the present disclosure include various steps, which will be described below. The steps may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor programmed with the instructions to perform the steps. Alternatively, steps may be performed by a combination of hardware, software, firmware and/or by human operators.

[0020] Embodiments of the present disclosure may be provided as a computer program product, which may include a machine-readable storage medium tangibly embodying thereon instructions, which may be used to program a computer (or other electronic devices) to perform a process. The machine-readable medium may include, but is not limited to, fixed (hard) drives, magnetic tape, floppy diskettes, optical disks, compact disc read-only memories (CD-ROMs), and magneto-optical disks, semiconductor memories, such as ROMs, PROMs, random access memories (RAMs), programmable read-only memories (PROMs), erasable PROMs (EPROMs), electrically erasable PROMs (EEPROMs), flash memory, magnetic or optical cards, or other type of media/machine-readable medium suitable for storing electronic instructions (e.g., computer programming code, such as software or firmware).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0021] Various methods described herein may be practiced by combining one or more machine-readable storage media containing the code according to the present disclosure with appropriate standard computer hardware to execute the code contained therein. An apparatus for practicing various embodiments of the present disclosure may involve one or more computers (or one or more processors within a single computer) and storage systems containing or having network access to computer program(s) coded in accordance with various methods described herein, and the method steps of the disclosure could be accomplished by modules, routines, subroutines, or subparts of a computer program product.

[0022] In various embodiments, the article(s) of manufacture (e.g., the computer program products) containing the computer programming code may be used by executing the code directly from the machine-readable storage medium or by copying the code from the machine-readable storage medium into another machine-readable storage medium (e.g., a hard disk, RAM, etc.) or by transmitting the code on a network for remote execution. Various methods described herein may be practiced by combining one or more machine-readable storage media containing the code according to the present disclosure with appropriate standard computer hardware to execute the code contained therein. An apparatus for practicing various embodiments of the present disclosure may involve one or more computers (or one or more processors within a single computer) and storage systems containing or having network access to computer program(s) coded in accordance with various methods described herein, and the method steps of the present disclosure could be accomplished by modules, routines, subroutines, or subparts of a computer program product.

[0023] Various embodiments are described assuming rule optimization and/or dependency detection are performed in real-time responsive to the proposed addition of a new traffic flow policy rule to an existing set of policy rules. Those skilled in the art will appreciate, however, that rule optimization and/or dependency detection may also or alternatively be performed in the background.

[0024] Notably, while embodiments of the present disclosure may be described using modular programming terminology, the code implementing various embodiments of the present disclosure is not so limited. For example, the code may reflect other programming paradigms and/or styles, including, but not limited to object-oriented programming (OOP), agent oriented

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

programming, aspect-oriented programming, attribute-oriented programming (@OP), automatic programming, dataflow programming, declarative programming, functional programming, event-driven programming, feature oriented programming, imperative programming, semantic-oriented programming, functional programming, genetic programming, logic programming, pattern matching programming and the like.

[0025] If the specification states a component or feature "may", "can", "could", or "might" be included or have a characteristic, that particular component or feature is not required to be included or have the characteristic.

[0026] Exemplary embodiments will now be described more fully hereinafter with reference to the accompanying drawings, in which exemplary embodiments are shown. This disclosure may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. These embodiments are provided so that this disclosure will be thorough and complete and will fully convey the scope of the disclosure to those of ordinary skill in the art. Moreover, all statements herein reciting embodiments of the disclosure, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future (i.e., any elements developed that perform the same function, regardless of structure).

[0027] Thus, for example, it will be appreciated by those of ordinary skill in the art that the diagrams, schematics, illustrations, and the like represent conceptual views or processes illustrating systems and methods embodying this disclosure. The functions of the various elements shown in the figures may be provided through the use of dedicated hardware as well as hardware capable of executing associated software. Similarly, any switches shown in the figures are conceptual only. Their function may be carried out through the operation of program logic, through dedicated logic, through the interaction of program control and dedicated logic, or even manually, the particular technique being selectable by the entity implementing this disclosure. Those of ordinary skill in the art further understand that the exemplary hardware, software, processes, methods, and/or operating systems described herein are for illustrative purposes and, thus, are not intended to be limited to any particular named.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0028] Aspects of the present disclosure provide a method that can be implemented in a network security management device for automatically optimizing security policy rules in real-time based on traffic conditions or when one or more traffic rules are added/edited/deleted/modified. According to one embodiment, the method includes receiving, by the network security management device, a request to add a new traffic flow policy rule to a repository of existing control rules. In an aspect, such a request can either be manually generated by say a user/administrator or can be automatically generated based on traffic pattern/characteristics, network usage statistics, user activities, among other like actions. One should also appreciate that even though part of the disclosure has been explained with reference to new rules being added, the same systems/methods is also clearly applicable to any other action that needs to be taken place on existing set of traffic flow policy rules such as modification of one or more rules stored in rule repository or even deletion of one or more rules.

[0029] In an aspect, upon receipt of the request to add the new traffic flow policy rule, network security management device can be configured to automatically determine dependencies of the new traffic flow policy rule on one or more policy rules, and form an updated set of policy rules based on the determined dependencies. Methods of the present disclosure can further be configured to automatically optimize, by means of the network security management device, the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein such optimization of the updated set of policy rules can be performed based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

[0030] According to one embodiment, dependencies can be determined by means of evaluation of dependence in execution of the new traffic flow policy rule on one or more policy rules. In another aspect, grouping of the first sub-set of policy rules of the updated set of policy rules can include merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging can be conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination (IP) addresses, services, applications, interfaces, rule

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

tags, priorities, and parameters of the combinable policy rules. According to another embodiment, merging of the combinable policy rules can be conducted based on superneting of one or more of the source IP addresses and the destination IP addresses.

[0031] According to another embodiment, reordering a second sub-set of policy rules can include changing an order of policy rules of the second sub-set of policy rules based on one or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters. According to one embodiment, order of the policy rules of the second sub-set of policy rules can be changed based on frequency of usage thereof.

[0032] According to another embodiment, deleting a third sub-set of policy rules can include deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules. In an exemplary embodiment, the one or more conflicts can include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules. One or more conflicts can also include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule. According to one embodiment, when conflicts exist between a denied traffic flow and an allowed traffic flow, in order to avoid creating a potential security issue, the denied traffic flow will be placed before the allowed traffic flow. Alternatively, if an advantage exists, the allowed traffic flow can be split to suppress the denied traffic flow.

[0033] According to one embodiment, weights assigned to types of traffic can be defined manually based on scope and attributes of policy rule or can be defined automatically. According to another embodiment, formation of the updated set of policy rules can be conducted/performed based on the one or more weights, the preference settings, the priority settings for the policy rules, network traffic characteristics, and network usage statistics.

[0034] Aspects of the present disclosure also provide for a system for automatically optimizing security policy rules in real-time based on network traffic conditions/characteristics/usage in addition to when one or more traffic rules are added/modified. According to one embodiment, system of the present disclosure can include a business traffic flow input module configured to receive a request to add a new traffic flow policy rule to a

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

repository of existing policy rules managed by the system. The system can further include a dependency detection module configured to automatically determine dependencies of the new traffic flow policy rule on one or more policy rules, and a traffic flow policy rule incorporation module configured to form an updated set of policy rules by incorporating the new traffic flow policy rule within the policy rules based on the determined dependencies. System of the present disclosure can further include a policy rule optimization module configured to automatically optimize the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

[0035] FIG. 1 illustrates an exemplary security policy implementation architecture 100 in accordance with an embodiment of the present disclosure. In the context of the present simplified example, a protected network coupled to a public network 112 (e.g., the Internet) includes a firewall/flow control device 108, a policy rule database 110, an access point 106 and a local area network (LAN) 104 containing multiple end points 102-1, 102-2 and 102-3. When a system residing outside of the protected network attempts to communicate with a device on LAN 104 or when end points 102-1, 102-2 or 102-3 attempt to access network 112 or any resource within the network 112 through access point 106, a network security management device, (e.g., firewall/flow control device 108), which is configured to, among other things, monitor and/or filter traffic flow between end points 102 and network 112, determines whether the attempted access/communication is permitted by the enterprise security policy.

[0036] According to one embodiment, the enterprise security policy is represented by a set of rules (e.g., assess control lists (ACLs), traffic flow control rules, etc.) stored within policy rule database 110 that are used for filtering traffic flow (e.g., blocking or allowing packets between LAN 104 and network 112). Those skilled in the art will appreciate that policy rule database 110 may be separate from firewall/flow control device 108 or integral to firewall/flow control device 108.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0037] Those skilled in the art will appreciate, end points 102 may represent a variety of different operating environments. For example, end points 102 may include, but are not limited to, personal computers (PCs), end user workstations, server computers, mobile computer systems (e.g., hand-held devices, tablet computers, laptop devices), multiprocessor systems, microprocessor-based systems, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments and the like.

[0038] According to one embodiment, although the firewall/flow control device 108 in the present illustration is depicted as residing between access point 106 and network 112, in other example implementations, firewall/flow control device 108 may simply be logically interposed between end points 102 and network 112, and therefore various other network architectures/configurations are possible. In an aspect, the monitored network traffic can include, but is not limited to, HyperText Transfer Protocol (HTTP) traffic, File Transfer Protocol (FTP) traffic, Domain Name System (DNS) requests/responses, unclassified (e.g., unknown) or classified (e.g., known) application traffic and/or other types of traffic (e.g., traffic using other types of known or unknown protocols).

[0039] As explained earlier, existing firewall/flow control devices or network security management device use static policy rules to filter/block/allow traffic entering or leaving a protected network and once configured, the firewall/flow control device always searches through the same set of policy rules in the same hierarchical order. This hierarchical based execution of policy rules may delay the decision to allow/block the traffic and may impact the performance of the network. In a typical enterprise set-up, a firewall/flow control device can have thousands of policy rules, some of which may be generic policy rules that are applicable to all the traffic flow from/to network 112 and others of which may be specific to a set or range of source IP addresses, destination IP addresses, applications, ports and/or services. As discussed in the Background, increased network delays are observed for existing firewall/flow control devices or network security management devices when the matching rule of a rule base for the packet at issue is found lower in hierarchy as all policy rules placed higher in the hierarchy must be evaluated before evaluating those rules at the bottom of the hierarchy.

[0040] In order to address certain deficiencies of existing firewall/flow control devices, in an aspect, a network security management device (e.g., firewall/flow control device 108) can be

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

configured to implement systems and methods of the present disclosure and can be configured to optimize security policy rules in real-time based on traffic conditions or when one or more traffic rules within policy rule database 110 are added/edited/deleted/modified. According to one embodiment, network security device 108 can receive a request to add a new traffic flow policy rule to the rules stored in policy rule database 110, based on which firewall/flow control device 108 can be configured to automatically determine dependencies of the new traffic flow policy rule on one or more of the existing policy rules within policy rule database 110 and form an updated set of policy rules based on the determined dependencies. Firewall/flow control device 108 can then automatically optimize the updated set of policy rules grouping one or more policy rules of the updated set of policy rules, reordering one or more policy rules of the updated set of policy rules and/or deleting one or more policy rules of the updated set of policy rules, wherein such optimization of the updated set of policy rules can be performed based on various predetermined or configurable parameters, including, but not limited to, weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and/or network usage statistics for the policy rules of the updated set of policy rules. For example, if redundant rules are found in policy rule database 110 or rules that contradict each other are found in policy rule database 110 the redundancy or conflict can be proactively addressed by deleting one of the redundant or conflicting rules (e.g., manually, automatically or by a combination of manual and automated means).

[0041] As discussed in further detail below, in some embodiments, when a policy rule within policy rule database 110 is modified/amended, all other rules that are impacted by the amended rule can be automatically modified or deleted to maintain consistency with the modified rule. Similarly, when two or more rules are identified as being capable of being merged with each other by virtue of having the same source IP addresses, destination IP addresses, a common intended destination/department and/or any other relevant commonality, such rules can be automatically merged in the background or in real-time so as to avoid unnecessary growth in the size and complexity of policy rule database 110. According to one embodiment, validation and optimization functionality can be performed in the background to identify duplicate entries, mergeable entries, shadowed rules and other usual security rule based errors or sub-optimal configurations.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0042] According to another embodiment, firewall/flow control device 108 provides for dynamic reordering of policy rules within policy rule database 110 based on statistical data or weights assigned to one or more policy rules. Such dynamic reordering of the evaluation sequence of policy rules can be based on the most frequently used or the most recently used policy rule(s), for example. Such reordering will facilitate faster decision making by firewall/flow control device 108 as the rules observed to be used most frequently, for example, will be found faster as a result of being placed earlier in the search sequence of policy rule database 110. Typically, the policy rules will be reordered in accordance with administrator-defined criteria; however, in the absence of such criteria embodiments of the present invention may place less specific rules on top or very specific rules on top. Statistical analysis of the application/usage of existing policy rules may be used to select an appropriate default ordering approach.

[0043] Further, as security requirements change over time, network administrator and/or security provider may want to add new policy rules, in which case, the network security device 108 or any other network security management device (e.g., a firewall, a gateway, an intrusion prevention device, an intrusion detection device, a server, an integrated security appliance, a switch, a unified threat management (UTM) device, among others, can be configured to use the systems and methods of the present disclosure for creation and modification of firewall/access control policy rules so as to facilitate enhanced computing performance, rule management, policy optimization and/or session/network traffic packet flow management. In an aspect, firewall/flow control device 108 can be configured to use the method of present disclosure so as to overcome the limitation of existing static rule based policy by incorporating dynamic addition/modification of one or more policy rules and to create and optimize the new set of policy rules.

[0044] In an aspect, methods of the present disclosure can be used by firewall/flow control device 108 for implementation, execution, and management of policy rules, including but not limited to addition of one or more policy rules, modification of one or more existing policy rules, grouping/merging of one or more existing policy rules, reordering of one or more policy rules, and/or deletion of one or more policy rules in real-time or in the background, without impacting performance of network security device 108. Those skilled in the art will recognize the various

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

purposes of the optimization of flow control policy rules include, but are not limited to, increasing the efficiency of rule scanning/evaluation during packet filtering processing, optimizing storage of policy rule database 110, facilitating management of rules within policy rule database 110 and facilitating fast processing of packets received by firewall/flow control device 108.

[0045] According to one embodiment, firewall/flow control device 108 of the present disclosure can also be operatively coupled with a security service/server/software (not show), for example, using secure communications, such as encrypted communication techniques, to store parameters and/or attributes of incoming and outgoing network traffic packets (such as signatures, heuristics, application ID related information, packet attributes, user ID related information, content ID related information, and trusted/untrusted zone information). Based on heuristic/statistical information regarding such parameters and/or attributes, new flow control policy rules may be automatically conceived/generated and added to policy rule database 110. As another example, firewall/flow control device 108 can communicate with the service (e.g., using secure communications, such as encrypted communication techniques) to provide monitored traffic information (e.g., potential malware samples, such as in the form of subsets of such monitored traffic information, such as a portion of the packet flow, monitored Universal Resource Locator (URL)/DNS information, monitored files requested for upload/download/access, and/or other information, along with possibly other information, such as content information for the client device associated with the traffic flow and possibly user identification and/or application identification information as well), and the service can perform additional real-time and or post analysis (e.g., additional heuristic analysis as described herein with respect to various embodiments for detecting malware, including new malware threats and zero-day attacks, and/or to compare to other samples received and analyzed for other customers of the security cloud service).

[0046] FIG. 2 illustrates exemplary functional modules of a network security policy management system 200 in accordance with an embodiment of the present disclosure. In the context of the present example, system 200 includes a business traffic flow input module 202, a dependency detection module 204, a traffic flow policy rule incorporation module 206 and a policy rule optimization module 208.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0047] In one embodiment, business traffic flow input module 202 can be configured to receive a request to add a new traffic flow policy rule to a repository of policy rules managed by system 200. Such a request can either be generated automatically or can be manually generated by the user/administrator of the network. In another aspect, business traffic flow input module 202 can also be configured to receive a request relating to modification of an existing stored policy rule, wherein the modification can either be suggested by the administrator or can proposed automatically based on observed traffic patterns (e.g., source/destination IP address patterns), protocols being used, rule hits, types of prevalent attacks, frequency of attacks, changes in organization policy, among other like factors. For example, responsive to observing that one or more policies of a rule base have been unused over a configurable or predetermined period of time, a warning may be provided to the network administrator along with one or more suggested changes to be made to the rule base (e.g., removal or editing of such rules). For example, rules or objects (e.g., addresses or services) that are unused for a long period of time may be recommended for removal or, for performance reasons, the traffic flows containing the unused object may be automatically reordered to place them on the bottom of the security policy. If the unused rules or objects are removed (rather than reordered), in one embodiment, a new security policy optimization is performed.

[0048] According to one embodiment, business traffic flow input module 202 can be configured to receive one or more traffic flow policy rules corresponding to a traffic policy control requirement of the business. For example, the enterprise may desire that some traffic be processed faster or given priority over other types of traffic (e.g., a Voice over Internet Protocol (VoIP) provider might choose to have voice sessions be given a higher priority than management sessions). The traffic flow policy rules received by business traffic flow input module 202 may represent new policy rules that needs to be created and added to the policy rule database and can be defined by means of a traffic policy control requirement given as input by a user/administrator. The traffic policy control requirement can be received by a user/administrator in a defined yet flexible format such that the user/administrator may not need to be aware of the already existing policy rules or about the constraints/conflicts that the addition of the new policy rule might create. Adding one or more new policy rules or editing or deleting some preexisting policy rules can have ripple effects on other existing policy rules. As a new policy rule needs to be added and incorporated with the preexisting set of policy rules, automated

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

checks for dependency and shadowing may be implemented by business traffic flow input module 202 or one or more other functional units within system 200.

[0049] In another aspect, dependency detection module 204 can be configured to automatically determine dependencies of a new traffic flow policy rule on one or more existing policy rules. In an aspect, dependency detection module 204 can be further configured to evaluate dependence in execution of the new traffic flow policy rule on one or more existing policy rules. In an example implementation, a dependency can be established between policy rules if one policy rule (R1) partially or completely shadows another policy rule (R2) such that execution of rule R1 directly or indirectly impacts the rule R2. According to one embodiment, two rules are dependent if they mutually exhibit a precedence relationship. Such a dependency may not necessarily be detrimental or contradictory to the execution of rule R1, but may overlap with and/or depend on R2. For instance, rules R1 and R2 may be dependent on each other when they are not disjoint such that R2 cannot be moved before R1 without violating semantic integrity of the rule set. Dependency detection module 204 can therefore be configured to detect whether the newly proposed policy rule (one or more traffic flow policy rules) depends, for its execution, on any preexisting policy rule, so as to understand relationships between the newly proposed policy rule and the stored policy rules.

[0050] In another instance of dependency detection, consider two rules as follows: rule 1 permits packets with characteristic A (source address, for example) and rule 2 denies packets with characteristic B (destination address, for example). A packet with a profile matching both characteristics (from A to B in this case) will match both rules. In such a case therefore, the rules are dependent. In an aspect, dependency can be determined by means of multiple methods. For example, a rule can be selected, e.g., rule 1, for determining whether other rules in a policy rule database (e.g., policy rule database 110) depend on it. In selecting the rule, match types and associated values that would be used to filter packets can be identified, wherein match types are characteristics of packets that are used for comparison to a rule. Packet characteristics can include, for example, the protocol, port, originating IP address, destination IP address, etc. For example, a match type may be "protocol" and the value is "TCP." The rule might also have a match type "port" with a value of "20." The rule might also have a match type "IP" with a value of "123.45.67.89." One of ordinary skill in the art will recognize that a match type may be any

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

characteristic associated with the profile of a packet. A second rule, e.g., rule 2, may then be selected for comparison to rule 1. In selecting the second rule, again match types and associated values that would be used to filter packets may be identified for that rule. The match types of rule 1 can then be compared to rule 2 such that if rule 1 and rule 2 have at least one of the same match types, the values of each of the match types of rule 1 and rule 2 are compared. If all of the match types have different values than their corresponding match types in rule 2, rule 1 and rule 2 may be determined to be order independent. If rule 1 and rule 2 have at least one match type that is not in common, or if at least one match type of rule 1 shares the same value as the corresponding match type in rule 2, or if at least one of the match type of rule 1 is included (e.g., IP address and subnet) on the corresponding match type in rule 2, or or if at least one of the match type of rule 2 is included (e.g., IP address and subnet) on the corresponding match type in rule 1, rule 1 and rule 2 may be determined to be order dependent. This background process can be repeated until each pair of rules has been compared.

[0051] In another aspect, traffic flow policy rule incorporation module 206 can be configured to form an updated set of policy rules by incorporating the new traffic flow policy rule within the policy rules based on the determined dependencies, if any. In an implementation, traffic flow policy rule incorporation module 206 can either be configured to simply incorporate the new traffic flow policy rule into the policy database and leave the dependencies to be evaluated and handled later, or it can be configured to handle the dependencies and accordingly add or remove one or more existing traffic flow policy rules to/from the policy rules database. For instance, the position at which a new traffic flow policy rule is added to the database and the level at which it would be executed can be based on the dependencies computed by dependency detection module 204. Furthermore, an order of the new rule in the existing repository of flow control policy rules can also be accounted for while forming the updated set of policy rules. In an exemplary implementation, when the new rule is found to be dependent on another rule stored in the repository, both the rules can be assigned the same equivalence class.

[0052] In another aspect, policy rule optimization module 208 can be configured to automatically optimize the updated set of policy rules by grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules and/or deleting a third sub-set of policy rules of the updated set of policy rules

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

based on weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and/or network usage statistics for the policy rules of the updated set of policy rules.

[0053] According to one embodiment, grouping policy rules includes identifying potentially combinable policy rules associated with similar allowed flows (e.g., only different sources, only different destinations or only different services) and merging the identified combinable policy rules into a single policy rule. The merging can also be conducted based on matching of source IP addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities and/or parameters of the policy rules. In some embodiment, identifying potentiall combinable policy rules can be based on IP supernetting of the source IP addresses and/or the destination IP addresses. For example, a first traffic flow from source 192.168.0.0/24 to destination 1.1.1.1:80 and a second flow from source 192.168.1.0/24 to destination 1.1.1.1:80 can be merged into a new flow from source 192.168.0.0/25 to destination 1.1.1.1:80. In an instance, multiple parameters of the rule space, including, but not limited to, source, destination, user, service, enterprise firewall ID, and other such parameters can be used to identify rules that may interact or be combinable.

[0054] As a specific non-limiting example for purposes of illustration, assume there are three FTP rules that are candidates for combination, including rules allowing FTP traffic from trusted sources trusted.com and reliableco.com. In various embodiments, these trusted sources would be identified by an IP address or an IP address range. In the context of the present example, rules for both trusted sources allow FTP traffic, but require a virus scan to be performed. A third rule allows FTP traffic from all other sources except for "put" functions that may be used to upload a file. This rule allows unknown sources to log on and download, but not upload, files. As such, no antivirus scan is required for the third rule. While it is evident that the first two rules can be easily combined as they are identical except for a single parameter that does not overlap or interact in identifying two different connection sources, the third rule is distinctly different. Further, the order of the third rule is important, as the rule should be processed only after the first two rules, so that the trusted sources are allowed to FTP and "put" files to the servers protected by the firewall. Adding the third rule to the other two to form a combined rule or otherwise modifying the first two rules based on the third will result in firewall

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

behavior not intended by the administrator for at least some connections. In this example, it may be acceptable to allow FTP access including upload capability for all users, requiring anti-virus scanning for uploads only. The administrator may deem this a reasonable risk to take, or may decide the change to rule set functionality is unacceptable and only allow combination of the first two rules while declining to allow the third rule to be combined with the first two. In an aspect, whether two or more rules can be grouped/merged is determined by examining whether the rules at issue differ in relation to only a single parameter (e.g., source, destination, service), in which case, they are identified as capable of being grouped/merged. In another aspect, whenever possible, rules are grouped by superneting. If two rules differ in two or more elements/parameters, they may be grouped/reordered in such a way that results in more hits in one of the generated rules. Meanwhile, if the scope of one rule is contained entirely by the scope of another rule, the narrower rule may be deleted and the broader rule may be retained.

[0055] In an example implementation, merging of policy rules can be implemented based on superneting of one or more of the source IP addresses and the destination IP addresses, i.e. applying a single policy rule for IP addresses belonging to same class of IP addresses. In an example implementation, one or more parameters can be used to determine the group-able/merge-able policy rules. For example, if two rules differ in just one element (e.g., source, destination, service), they can be grouped together. Similarly, the policy rules applied for a group of network elements can be grouped by superneting. In an example implementation, when the scope of one policy rule is "contained" in another policy rule or all the security checks of the one policy one rule are covered by a broader security rule, then both rules can be merged into the policy rule having broader scope.

[0056] Those skilled in the art will appreciate that policy rule optimization module 208 can also be configured to demerge one or more rules to make them separate in case their order, for instance, plays an important role in deciding how the traffic packets are to be processed, and therefore, although the functions of deletion, grouping, and re-ordering have been mentioned above, any other function that enables optimization of the updated set of rules is completely within the scope of the present disclosure.

[0057] According to one embodiment, reordering of policy rules can include changing an order of policy rules based on their respective source IP addresses, destination IP addresses,

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

network usage statistics, applications, interfaces, rule tags, priorities and/or parameters. In an example implementation, the order of policy rules may be changed based on frequency of past usage, a manual priority set according to the business needs and/or other predefined or dynamically determined criteria. For example, a policy rule that is observed to be used the most frequently can be reordered to be executed first. In an example implementation, a dynamic priority can be assigned to each policy rule and the order of execution can therefore be dynamically changed. In an example implementation, if one policy rules is dependent upon another, then their relative order of execution will be preserved.

[0058] According to one embodiment, deletion of a policy rule or recommendation of deletion of a policy rule to the administrator is as a result of identifying one or more conflicts among policy rules. Conflicts include, but are not limited to, existence of a duplicate policy rule and existence of a policy rule that is contrary to a new traffic flow policy rule, for example. According to one embodiment, new rules may subsume or negate previous rules, or conflicting rules may be present in the rule set. Depending upon the particular implementation, optimization module 208 can be configured to simply bring to the attention of the administration policy rules that have been identified to be in conflict so that the administrator can select which of the rules to apply, what order the rules should be applied, or whether to merge the rules into a single rule if appropriate. In an alternative embodiment, optimization module 208 may implement changes to the policy rule database and maintain a log of changes to allow an administrator to selectively undo certain optimizations and/or revert to a prior state of the policy rule database if desired. When statistical data (e.g., frequency of execution during one or more particular time frames) is tracked and maintained relating to execution of policy rules, optimization module 208 may provide a warning to the administrator regarding any unused policies, suggest changes (e.g., removal, editing or reordering of an unused policy) and/or automatically implement and log changes to the policy rule database deemed to be appropriate.

[0059] Depending upon the particular implementation, the updated set of policy rules may be defined dynamically based on the scope and attributes of policy rules and weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and/or network usage statistics based on automatic or manual criteria, at any given time, with or without administrator intervention. In an aspect, assignment of weights to types of traffic can be

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

conducted manually or automatically or a combination thereof based on scope and/or attributes of the policy rule. In an example implementation, each policy rule can be assigned a dynamic priority/weight for its hierarchical execution. While reordering policy rules, dynamic priority can be used to define the execution order of policy rules. Policy rules can be executed in hierarchical/sequential manner according to their priority such that policy rules with highest priority is executed before execution of policy rules of comparatively lower priority. The priority can be assigned by the user/administrator or can be automatically determined based on statistical and/or historical data regarding the actual use of the policy rules. In an example implementation, an updated set of policy rules can be executed in parallel or in sequence based on the one or more weights assigned, the preference settings, the priority settings for the policy rules, network traffic characteristics, and network usage statistics, among other attributes/parameters.

[0060] Depending upon the particular implementation, network security policy management system 200 may be implemented separately from or integrated within a network security device, for example, comprising one or more processors, a communication interface mechanism, one or more internal data storage devices operatively coupled to the one or more processors and storing policy rule optimization module 208 configured to retrieve a set of policy rules and optimize the retrieved set of policy rules.

[0061] According to one embodiment, policy rule optimization module 208 can also be configured to run on a periodic basis or when one or more optimization parameters are defined/modified so as to ensure that at any given moment, the policy rules are optimally ordered, grouped and managed. Policy rule optimization module 208 may also or alternatively be manually initiated by the network administrator or automatically initiated upon detection of one of a set of predefined events (e.g., a change to the policy rule database or a change to defined business flows, expressing the relative priorities of various types of traffic within the enterprise, for example).

[0062] In an example implementation, network security policy management system 200 can have a front end interface module (not shown) that can be used by user/administrator to create and/or upload one or more new security policy rules. Other modules of the present system can run in the background for validation and optimization of updated policy rules that would

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

identify duplicate entries, merge-able entries, shadowed rules and other usual security rule based errors or non-optimized configurations. Optimization module 208 can, periodically or dynamically or based on user-defined actions, create an optimized version of the policy rules that would effectively reduce the size of the actual security policy being executed by the firewall/flow control device/ network security management device. For example, the network security device may calculate whether the creation of one or more explicit denied flows might be advantageous in connection with reducing the security policy size. In an exemplary embodiment, policy rule optimization module 208 can also reorder security policies based on customer business drivers, thereby reducing the initial rule matching time for network traffic so as to increase the performance of the security system based on automatic and/or user defined criteria. Thus, flow control policy rules can be reordered and/or rebuilt/modified dynamically based on automatic and/or manual criteria at any given time, with or without user intervention.

[0063] In an exemplary implementation, proposed changes to the policy rule database may be brought to the attention of the user/administrator via the frontend interface for further modification and/or confirmation before taking affect. Alternatively, confirmation of optimized policy rules may not require to be confirmed/approved by any user/administrator prior to being implemented and taking affect.

[0064] In accordance with embodiments of the present invention, creation and/or ordering of optimized policy rules can be based on various criteria, including, but not limited to, performance (e.g., rule hits), business flows (e.g., to guarantee one or more types traffic are processed faster) and/or statistical analysis of the actual policy rules being used. The security policy can also self-adjust automatically over time in order to improve performance and further reduce delay for new session establishment.

[0065] In an exemplary implementation, network security policy management system 200 may generate a warning if a rule remains unused over a predetermined or configurable period of time. Network security policy management system 200 may alternatively or additionally suggest re-ordering of rules within the policy rule database (e.g., moving unused or infrequently used rules to the end) or removal of unused rules. Network security policy management system 200 can also be configured to simplify management of policy rules so as to allow the administrator to focus his/her attention on traffic flows that reflect particular business needs. For example,

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

because network security policy management system 200 will take care of evaluating and creating a valid, effective, efficient and optimized security policy, the administrator no longer needs to check the complete rule base before making any changes. In an aspect, higher priority rules can also be identified and re-ordered and/or categorized in order to optimize packet filtering. In another embodiment, priorities of optimization parameters (e.g., network traffic characteristics, source/destination IP addresses, frequency/time aspects of packets, type of traffic, among others) can also be configured/changed based on usage/context/organization policies/objectives. For example, some enterprises may value (and therefore prioritize) increased performance in initial session establishment (e.g., as a result of reordering of rules based on frequency of execution or based on whether they specify one or more specific IP addresses or are subnet based) over a more compact rule set (e.g., as a result of merging rules).

[0066] FIG. 3A illustrates an exemplary representation 300 showing a snapshot of a simplified security policy, and FIG. 3B shows addition of a new security policy rule 399 to the security policy in accordance with an embodiment of the present disclosure. In the present example, representation 300, includes a Host/Network column 310, identify the source host/network(s) with which the policy rule is associated, a Peer Host/Network column, identifying the destination/target peer host/network(s) with which the policy rule is associated, a Ports column 330, identifying particular ports on which the traffic is allowed, a Business Case/tag column 340, identifying a project with which the corresponding policy rule is associated, and a rule ID/seq column 350, potentially indicating an order in which the policy rules are applied. Those skilled in the art will appreciate the exemplary functional modules described herein are for purposes of illustration only and that the functionality described with reference to various of the exemplary functional modules may be combined and/or distributed differently.

[0067] FIG. 3A illustrates a simplified example of preexisting flow control security policy rules having rule identifiers (IDs) 350 ranging from 1 to 15 and representing different policy rules that are defined/configured by the user/administrator/system in order to filter incoming/outgoing traffic/packet/connection requests from/to the network. Rule IDs 350 can also indicate the sequence in which the processing of the network traffic takes place, wherein the traffic would first pass through the entries/flows associated with sequence ID 1 and then to 2 and

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

so on. As can be seen, each rule ID 1-15 can be implemented for one or more projects that correspond to respective business cases/tags 340. Each project can also be associated with multiple sessions between source host and destination/peer host.

[0068] As can be seen in the present example, entry 301a of policy rule 301 relates to all traffic/packet/connection requests sent from host 10.184.17.0/26 to peer host/network 10.135.32.0/26, which, can be sent on any of the ports, wherein the interaction between the source-destination relates to a project referred to as "Initial Project." Similarly, in accordance with entry 303a of policy rule 303, traffic can be sent from buss-server02 to 10.135.35.121 on ports 3315/TCP, 3380/TCP, 3366/UDP, and 3390/TCP. While representation 300 FIG. 3A only shows twenty-one entries representing twelve policy rules, those skilled in the art will appreciate, in practice, there can be hundreds of such entries.

[0069] FIG. 3B illustrates a new rule 399 created by user/administrator, which needs to be incorporated with the existing policy rules of FIG. 3A. New rule 399 may be used for traffic analysis and monitoring of traffic flow, for example, between buss-fe01 and 10.135.35.0/24 through port TCP-1024. Prior to incorporation of new rule 399 into the existing policy rules, various initial checks may be performed to identify policy rules within the existing policy rule database upon which new rule 303 may be dependent, identify duplicate/overlapping/dependent/shadowing rules and/or determine the relative priority of new rule 399, based on which new rule 399 can be incorporated into the policy rule database. Since the project ("Web-API-Integration") with which new rule 399 is associated is business critical, it will be given high priority which should be reflected during reordering of the policy rules.

[0070] If the flow represented by new rule 399 is expected to have many sessions and in view of its high priority, the administrator, without the benefit of performing a detailed analysis of the security policy, may manually create the following flawed security rule entry on top of the security policy represented in FIG. 3A:

Host/Network	Peer Host/Network	Ports	Business Case/tag	rule ID/seq
buss-fe01	10.135.35.0/24	TCP-1024	web_API integration	1

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0071] In existing systems, with the insertion of this new rule, the sequence numbers of subsequent rules would be incremented by one. With this change, the newly defined traffic flow would have the highest priority in relation to new session matching processing, but the security policy may effectively shadow part of rule 305, and allow traffic that should be denied by rule 311, thus creating unnecessary processing on rule 305 and allowing a traffic flow that should have been denied by rule 311. Since traffic meeting rule 311 (which should be denied) is allowed in accordance with the present example, it is unlikely anyone would complain (as end users typically only notice the denial of traffic they desire to be allowed), but a security issue has been created by the introduction of a flawed security rule.

[0072] In accordance with embodiments of the present invention, on the other hand, without analyzing the security policy, the administrator can instruct the security system to create a flow with the characteristics of new rule 399 without concern as network security policy management system 200 would automatically evaluate the existing security policy and reach the following conclusions:

a. Since the priority associated with new rule 399 is high, new rule 399 needs to be placed on top;

b. Rule 305 also matches this flow for traffic originating on host buss-fe01. If a new rule is created on top, then part of rule 305 is unnecessary, so rule 305 should be automatically revised; and

c. Rule 311 is in conflict with part of the flow required for new rule 399. Since rule 311 is a deny rule, a warning should be issued to the administrator pointing out the conflict; and

    i. If the flow-denial of rule 311 is to be maintained, rule 311 should be moved to a position with a smaller seq# than new flow 399. Alternatively, if rule 311 is to be "forgotten" due to the higher priority of new flow 399, then rule 311 should be removed.

[0073] FIG. 4 illustrates an exemplary snapshot of a security policy rule management system interface 400 in accordance with an embodiment of the present invention. The snapshot 400 illustrates an exemplary frontend/administrator interface for management of security policy

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

rules. According to one embodiment, system interface 400 can present a user/administrator with various options for managing one or more policy rules including, but not limited to, viewing policy rules, adding new policy rules, searching for policy rules, checking dependencies of one or more rules, deleting/modifying/re-ordering and optimizing policy rules. In an aspect, a user/administrator, by means of viewing policy rules, can also add new policy rules to the existing set of flow control policy rules, analyze performance of current rules, view traffic pattern/attributes/characteristics, and manage conflicts/modification of rules. In another aspect, the administrator can also check dependency in order to view automatically identified dependencies that any rule has on the other set of rules that form part of the rules repository. In yet another aspect, based on a selected optimization criteria (e.g., optimization based on priority verses optimization based on traffic statistics) dependencies, traffic related attributes, weights of different types of policy rules, organizational policies, among other parameters, the administrator can also enable optimization of the policy rules.

[0074] In yet another embodiment, as shown in FIG 4, optimization can either take place for all the flow control policy rules or can be performed automatically for a defined number interlinked/selected/related rules. In yet another embodiment, through the "optimize policy rules" option, the administrator can also select and/or define criteria to be used for optimization, define policy settings to be adopted for optimization, assign weights to different policy rules, enable usage statistics to be incorporated during optimization, define priority of one or more rules, enable traffic attributes/characteristics to be incorporated along with the defining, say the technology required for security policy implementation.

[0075] In yet another embodiment, through the "optimize policy rules" option a user/ administrator can select and define group policy rules through which the system can either through manual intervention or automatically, arrange new and/or existing policy rules into groups. Such an option can allow automatic merging of possible flow control policy rules or creating of new rules that relate to subnets and not to individual IP addresses, for instance.

[0076] In yet another embodiment, through the "optimize policy rules" option, the administrator can enable all or part of the policy rules to be re-ordered, leading to, for instance, higher priority rules or more frequently referred rules to be brought up the hierarchy for faster access when compared with lower priority rules. Any other basis such as most accessed rules

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

can also be applied for re-ordering or re-arranging one or more policy rules. In yet another embodiment, through the "optimize policy rules" option a user/ administrator can enable deletion of one or more rules based on, for instance, duplicate/redundant rules, conflicting rules (that act differently for same source-destination packet for instance). One should appreciate that the various options illustrated through security policy rule management system interface 400 are completely exemplary in nature and all other options for management of policy rules are within the scope of present disclosure.

[0077] FIGs. 5A, FIG. 5B and FIG. 5C illustrate exemplary policy rules 500 stored in a policy rule database along with dependencies and possible groupings detected in accordance with an embodiment of the present invention. FIG. 5A illustrates an exemplary representation 500 having multiple policy rules, specifying actions to be taken by a network security device for specific services between specific sources and specific destinations. For instance, as can be seen, traffic from 192.168.0.0/24 to any destination is allowed for Domain Name System (DNS), HyperText Transfer Protocol (HTTP), and HTTP Secure (HTTPS) packets and the priority of such packets is Normal. The exemplary representation 500 of FIG. 5A also shows, for instance, the number of sessions impacted by each policy rule over a given time period and the corresponding percentage of sessions of the total number of sessions during the given time period.

[0078] FIG. 5B illustrates the policy rules 500 of FIG. 5A with a "Dependencies" column annotating various automatically identified dependencies among the policy rules 500. For instance, as the policy rule at index 7 blocks any traffic from 192.168.3.2 to 192.168.0.0/16, the execution order of the policy rule at index 6 rule depends on the policy rule of index 7. Similarly, as the policy rule of index 8 applies to all traffic from 192.168.3.2 to any destination, the policy rule at index 7 shadows the policy rule at index 8.

[0079] FIG. 5C illustrates how potential policy rules that can be merged/grouped can be identified and represented. For instance, the column "Dependencies B" includes annotations indicating that the policy rule at index 1 and the policy rule at index 2 rule can be partially merged together as they have the same source-destination pairs/priority and only differ in the type of service they allow to pass, and therefore, if merged, they can allow a combined traffic for DNS, HTTP, HTTPS, and SMTP. Similarly, the policy rule at index 8 can also be partially

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

merged with the policy rule at index 2, wherein post merger, the priority of the policy rule at index 2 can either be set to High or can be kept at Normal as specified manually by the administrator or determined automatically based on one or more of the weight of each rule, traffic characteristics, among other defined set of parameters.

[0080] FIG. 5D illustrates an optimized version of the security policy that seeks to optimize performance based on traffic statistics gathered by the flow control device in accordance with an embodiment of the present disclosure. As shown, the updated policy rule set has a policy rule at index 1 resulting from a partial merger of former policy rules associated with index 1 and index 2 of FIG. 5C, with the source being 192.168.0.0/23 and allowing issuance of packets to all destinations using DNS, HTTP and/or HTTPS services. The representation of FIG. 5D further shows the former policy rule associated with index 6 having been reordered to now be associated with index 2, and the former policy rule associated with index 7 being reordered to now be associated with index 3 as the volume of hits for this policy rule 3 are relatively high (50000 sessions). Similarly, a new policy rule associated with index 4 is a partial merger of the former policy rule associated with index 2 and the former policy rule associated with index 8, and a new policy rule at index 5 represents a reordered version of the former policy rule associated with index 4. Likewise, policy rule at index 7 has been put toward the end as the number of sessions/hits for this transaction (192.168.3.1 to 192.168.1.80 over HTTP) is low.

[0081] FIG. 5E illustrates an alternative optimized version of the security policy that seeks to optimize performance based on administrator-defined traffic priority in accordance with an embodiment of the present disclosure. As shown, the optimized policy rule set reflects, among other things, movement of former policy rule associated with index 6 in FIG. 5C to index 2. As former policy rule associated with index 7 in FIG. 5C had a high number of hits/sessions, that former policy rule has been moved to index 3, and the new policy rule at index 4 represents the partial merger of former policy rules associated with index 2 and 8 in FIG. 5C.

[0082] Those skilled in the art will appreciate that the two previously described optimization scenarios are merely exemplary and are based on a defined set of administrator-defined and/or system maintained parameters. In alternative embodiments, policy rules may be selected and evaluated with respect to their hits/session/frequency of use, potential of merger to

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

reduce the overall number of rules and/or potential for making the database light and efficient, along with considering other parameters discussed above to reorder the rule database.

[0083] FIG. 6 illustrates an exemplary flow diagram 600 for optimization of policy rules in a rule database in accordance with an embodiment of the present disclosure. At step 602, a network security management device receives a request to add a new traffic flow policy rule to an existing set of policy rules. In an aspect, such a request can either be manually generated by say a user/administrator or can be automatically generated based on traffic pattern/characteristics, network usage statistics, user activities, among other like actions.

[0084] At step 604, upon receipt of the request to add the new traffic flow policy rule, the network security management device automatically determines dependencies of the new traffic flow policy rule in relation to one or more of the existing policy rules. At step 606, an updated set of policy rules based on the determined dependencies can be created/generated, and at step 608, the updated set of policy rules can be automatically optimized by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein such optimization of the updated set of policy rules can be performed based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

[0085] According to one embodiment, dependencies can be determined by means of evaluation of dependence in execution of the new traffic flow policy rule on one or more policy rules. In another aspect, grouping of the first sub-set of policy rules of the updated set of policy rules can include merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging can be conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination (IP) addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules. According to another embodiment, merging of the combinable policy rules can be conducted based on superneting of one or more of the source IP addresses and the destination IP addresses.

[0086] According to another embodiment, reordering a second sub-set of policy rules can include changing an order of policy rules of the second sub-set of policy rules based on one or

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters. According to one embodiment, order of the policy rules of the second sub-set of policy rules can be changed based on frequency of usage thereof.

[0087] According to another embodiment, deleting a third sub-set of policy rules can include deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules. In an exemplary embodiment, the one or more conflicts can include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules. One or more conflicts can also include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule.

[0088] According to one embodiment, weights assigned to types of traffic can be defined manually based on scope and attributes of policy rule or can be defined automatically. According to another embodiment, formation of the updated set of policy rules can be conducted/performed based on the one or more weights, the preference settings, the priority settings for the policy rules, network traffic characteristics, and network usage statistics.

[0088.1] FIG. 7 is an example of a computer system 700 with which embodiments of the present disclosure may be utilized. Computer system 700 may represent or form a part of a network security management device (e.g., a firewall, a gateway, an intrusion prevention device, an intrusion detection device, a server, an integrated security appliance, a switch, a unified threat management (UTM) device) or other device implementing one or more components of a network security policy management system (e.g., network security policy management system 200).

[0088.2] Embodiments of the present disclosure include various steps, which have been described in detail above. A variety of these steps may be performed by hardware components or may be tangibly embodied on a computer-readable storage medium in the form of machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor programmed with instructions to perform these steps. Alternatively, the steps may be performed by a combination of hardware, software, and/or firmware.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0088.3] As shown, computer system 700 includes a bus 730, a processor 705, communication port 710, a main memory 715, a removable storage media 740, a read only memory 720 and a mass storage 725. A person skilled in the art will appreciate that computer system 700 may include more than one processor and communication ports.

[0088.4] Examples of processor 705 include, but are not limited to, an Intel® Itanium® or Itanium 2 processor(s), or AMD® Opteron® or Athlon MP® processor(s), Motorola® lines of processors, FortiSOC™ system on a chip processors or other future processors. Processor 705 may include various modules associated with monitoring unit as described in FIGs. 2-4. Communication port 710 can be any of an RS-232 port for use with a modem based dialup connection, a 10/100 Ethernet port, a Gigabit or 10 Gigabit port using copper or fiber, a serial port, a parallel port, or other existing or future ports. Communication port 710 may be chosen depending on a network, such a Local Area Network (LAN), Wide Area Network (WAN), a WLAN or any network to which computer system 700 connects.

[0088.5] Memory 715 can be Random Access Memory (RAM), or any other dynamic storage device commonly known in the art. Read only memory 720 can be any static storage device(s) such as, but not limited to, a Programmable Read Only Memory (PROM) chips for storing static information such as start-up or BIOS instructions for processor 705.

[0088.6] Mass storage 725 may be any current or future mass storage solution, which can be used to store information and/or instructions. Exemplary mass storage solutions include, but are not limited to, Parallel Advanced Technology Attachment (PATA) or Serial Advanced Technology Attachment (SATA) hard disk drives or solid-state drives (internal or external, e.g., having Universal Serial Bus (USB) and/or Firewire interfaces), such as those available from Seagate (e.g., the Seagate Barracuda 7200 family) or Hitachi (e.g., the Hitachi Deskstar 7K1000), one or more optical discs, Redundant Array of Independent Disks (RAID) storage, such as an array of disks (e.g., SATA arrays), available from various vendors including Dot Hill Systems Corp., LaCie, Nexsan Technologies, Inc. and Enhance Technology, Inc.

[0088.7] Bus 730 communicatively couples processor(s) 705 with the other memory, storage and communication blocks. Bus 730 can be, such as a Peripheral Component Interconnect (PCI) / PCI Extended (PCI-X) bus, Small Computer System Interface (SCSI), USB or the like, for

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

connecting expansion cards, drives and other subsystems as well as other buses, such a front side bus (FSB), which connects processor 705 to system memory.

[0088.8] Optionally, operator and administrative interfaces, such as a display, keyboard, and a cursor control device, may also be coupled to bus 730 to support direct operator interaction with computer system 700. Other operator and administrative interfaces can be provided through network connections connected through communication port 710.

[0088.9] Removable storage media 740 can be any kind of external hard-drives, floppy drives, IOMEGA® Zip Drives, Compact Disc - Read Only Memory (CD-ROM), Compact Disc - Re-Writable (CD-RW), Digital Video Disk - Read Only Memory (DVD-ROM).

[0088.10] Components described above are meant only to exemplify various possibilities. In no way should the aforementioned exemplary computer system limit the scope of the present disclosure.

[0089] While embodiments of the present disclosure have been illustrated and described, it will be clear that the present disclosure is not limited to these embodiments only. Numerous modifications, changes, variations, substitutions, and equivalents will be apparent to those skilled in the art, without departing from the spirit and scope of the present disclosure, as described in the claims.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Atty. Docket No.: FORT-012500 Patent Application
Fortinet Ref. No.: 13048

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TITLE OF THE INVENTION

DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

Inventor:

Hugo Filipe Parreira Pernicha, residing at:
Av. 9 de Julho, nº 12, 3 Dto
2665-520 Venda do Pinheiro
PORTUGAL

Assignee: **FORTINET, INC.**
A Delaware Corporation

Entity: Regular Undiscounted

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

COPYRIGHT NOTICE

[0001] Contained herein is material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction of the patent disclosure by any person as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all rights to the copyright whatsoever. Copyright © 2014, Fortinet, Inc.

BACKGROUND

Field

[0002] Embodiments of the present invention generally relate to network traffic control. In particular, embodiments of the present invention relate to systems and methods for firewall and/or access control policy management and optimization of policy rules to enhance performance of policy rule processing.

Description of the Related Art

[0003] A firewall generally represents an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system. A firewall may assume the form of a flow control device or set of devices configured to permit, deny, encrypt, decrypt and/or proxy computer traffic between different security domains based upon a set of rules and other criteria. Organizations that use Internet Protocol (IP) based communication networks have firewalls or access control devices/mechanisms to control the traffic that crosses into and out of their networks, or between different network segments. Each firewall is basically a special-purpose computer that enforces the organization's traffic filtering policy. Typically, the filtering policy is implemented in a rule base, which is an ordered list of rules, wherein each rule consists of a set of field value-ranges, and an associated action that is generally either “PASS” or “DROP”.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0004] Most firewalls enforce the policy according to "first-match" semantics, wherein for each new IP connection, the firewall checks the rules one by one, according to their order in the rule-base, until it finds a rule that matches the new connection. The first rule that matches the connection determines the firewall's action, wherein if the first matching rule has an action of "PASS" then the firewall will allow the connection to continue, and if the rule's action is "DROP" then the firewall will discard all the packets belonging to the connection. If no rule matches the connection then the firewall uses a default action, which is usually DROP.

[0005] As firewall or access control policies can have numerous rules, searching for a matching rule in sequence can require considerable CPU time. In such an implementation, the computational effort to match a connection to the rule-base is proportional (linearly) to the number of rules the firewall needs to try in sequence until it reaches the first matching rule. If checking a match against one rule typically requires M computer instructions, then checking K rules in sequence requires K times M instructions. If the first-matching rule happens to be one of the first in the rule-base, the firewall will identify the corresponding action quickly and with a low computational effort. Conversely, if the first-matching rule is near the end of the rule-base, the firewall will take longer to identify the corresponding action.

[0006] Firewall rule-based policy is typically static. As such, once it is configured, it will stay the same, in the same order and not be changed unless explicitly changed by a user/administrator. In practice, large enterprises end up with a substantial set of firewall rule-based policies that are more oriented to user/operator visibility than rule processing efficiency. Furthermore, addition of each new policy rule or modification of an existing rule typically has ripple effects on other existing/stored rules and policies. For instance, a new policy rule may be configured to allow packets of a specific traffic type to a given destination, which otherwise may have been denied by an already existing policy rule in the rule database. Existing security policy management techniques require manual detection of issues, such as duplication of rules, conflicts between rules, dependency between rules, or shadowing of one rule by another and therefore are error prone. These issues are exacerbated in the context of large policy rule databases.

[0007] There is therefore a need for systems and methods that allow efficient addition or modification of one or more policy rules by enabling enhanced system performance, manageability and reduced human error. There is also a need for systems and methods that

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

allow dynamic and automatic optimization of policy rules by efficiently grouping/merging, deleting, reordering and otherwise managing policy rules based on defined and configurable optimization criteria so as to enable improved overall performance and significant reduction in session establishment/rule access/rule processing delay.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

SUMMARY

[0008] Methods and systems are described for dynamically optimizing rule-based security policies. According to one embodiment, a security policy optimization method is provided. A request is received by a network security management device to add a new traffic flow policy rule to multiple existing policy rules managed by the network security management device. Dependencies of the new traffic flow policy rule on one or more of the existing policy rules are automatically determined. An updated set of policy rules is formed by incorporating the new traffic flow policy rule within the existing policy rules based on the determined dependencies. The updated set of policy rules is then optimized by (i) grouping a first sub-set of policy rules of the updated set of policy rules; (ii) reordering a second sub-set of policy rules of the updated set of policy rules; and/or (iii) deleting a third sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules.

[0009] Other features of embodiments of the present disclosure will be apparent from accompanying drawings and from detailed description that follows.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] In the Figures, similar components and/or features may have the same reference label. Further, various components of the same type may be distinguished by following the reference label with a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

[0011] FIG. 1 illustrates exemplary security policy architecture in accordance with an embodiment of the present invention.

[0012] FIG. 2 illustrates exemplary functional units of a rule-based security policy management system in accordance with an embodiment of the present invention.

[0013] ~~FIG. 3 illustrates exemplary~~FIGs. 3A and 3B illustrate addition of a new security policy rule to a policy rule database in accordance with an embodiment of the present invention.

[0014] FIG. 4 illustrates an exemplary snapshot of a security policy rule management system in accordance with an embodiment of the present invention.

[0015] FIGs. 5A to 5E illustrate exemplary optimization of policy rules stored in a rule database based on dependencies, priorities, traffic attributes, hits, sessions, potential of merger/modification/deletion, among other attributes in accordance with an embodiment of the present invention.

[0016] ~~Fig~~FIG. 6 is a flow diagram illustrating security policy rule management in accordance with an embodiment of the present invention.

[0017] FIG. 7 is an exemplary computer system in which or with which embodiments of the present invention may be utilized.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

DETAILED DESCRIPTION

[0018] Methods and systems are described for dynamically optimizing rule-based security policies. Methods and systems are also provided for creation and modification of firewall/access control policy rules so as to allow enhanced computing performance, rule management, policy optimization, and session/network traffic packet flow management. Methods and systems are further provided for optimizing the security policy rules by performing any or a combination of reordering, grouping, updating, deleting, along with performing any other actions on one or more policy rules based on parameters, including, but not limited to, weights assigned to traffic attributes (e.g., source address, destination address, service, port information, among other such attributes), preference settings, priority settings for the policy rules, network traffic characteristics, network usage statistics, among other optimization parameters.

[0019] In the following description, numerous specific details are set forth in order to provide a thorough understanding of embodiments of the present disclosure. It will be apparent to one skilled in the art that embodiments of the present disclosure may be practiced without some of these specific details. Embodiments of the present disclosure include various steps, which will be described below. The steps may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor programmed with the instructions to perform the steps. Alternatively, steps may be performed by a combination of hardware, software, firmware and/or by human operators.

[0020] Embodiments of the present disclosure may be provided as a computer program product, which may include a machine-readable storage medium tangibly embodying thereon instructions, which may be used to program a computer (or other electronic devices) to perform a process. The machine-readable medium may include, but is not limited to, fixed (hard) drives, magnetic tape, floppy diskettes, optical disks, compact disc read-only memories (CD-ROMs), and magneto-optical disks, semiconductor memories, such as ROMs, PROMs, random access memories (RAMs), programmable read-only memories (PROMs), erasable PROMs (EPROMs), electrically erasable PROMs (EEPROMs), flash memory, magnetic or optical cards, or other type of media/machine-readable medium suitable for storing electronic instructions (e.g., computer programming code, such as software or firmware).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0021] Various methods described herein may be practiced by combining one or more machine-readable storage media containing the code according to the present disclosure with appropriate standard computer hardware to execute the code contained therein. An apparatus for practicing various embodiments of the present disclosure may involve one or more computers (or one or more processors within a single computer) and storage systems containing or having network access to computer program(s) coded in accordance with various methods described herein, and the method steps of the disclosure could be accomplished by modules, routines, subroutines, or subparts of a computer program product.

[0022] In various embodiments, the article(s) of manufacture (e.g., the computer program products) containing the computer programming code may be used by executing the code directly from the machine-readable storage medium or by copying the code from the machine-readable storage medium into another machine-readable storage medium (e.g., a hard disk, RAM, etc.) or by transmitting the code on a network for remote execution. Various methods described herein may be practiced by combining one or more machine-readable storage media containing the code according to the present disclosure with appropriate standard computer hardware to execute the code contained therein. An apparatus for practicing various embodiments of the present disclosure may involve one or more computers (or one or more processors within a single computer) and storage systems containing or having network access to computer program(s) coded in accordance with various methods described herein, and the method steps of the present disclosure could be accomplished by modules, routines, subroutines, or subparts of a computer program product.

[0023] Various embodiments are described assuming rule optimization and/or dependency detection are performed in real-time responsive to the proposed addition of a new traffic flow policy rule to an existing set of policy rules. Those skilled in the art will appreciate, however, that rule optimization and/or dependency detection may also or alternatively be performed in the background.

[0024] Notably, while embodiments of the present disclosure may be described using modular programming terminology, the code implementing various embodiments of the present disclosure is not so limited. For example, the code may reflect other programming paradigms and/or styles, including, but not limited to object-oriented programming (OOP), agent oriented

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

programming, aspect-oriented programming, attribute-oriented programming (@OP), automatic programming, dataflow programming, declarative programming, functional programming, event-driven programming, feature oriented programming, imperative programming, semantic-oriented programming, functional programming, genetic programming, logic programming, pattern matching programming and the like.

[0025] If the specification states a component or feature "may", "can", "could", or "might" be included or have a characteristic, that particular component or feature is not required to be included or have the characteristic.

[0026] Exemplary embodiments will now be described more fully hereinafter with reference to the accompanying drawings, in which exemplary embodiments are shown. This disclosure may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. These embodiments are provided so that this disclosure will be thorough and complete and will fully convey the scope of the disclosure to those of ordinary skill in the art. Moreover, all statements herein reciting embodiments of the disclosure, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future (i.e., any elements developed that perform the same function, regardless of structure).

[0027] Thus, for example, it will be appreciated by those of ordinary skill in the art that the diagrams, schematics, illustrations, and the like represent conceptual views or processes illustrating systems and methods embodying this disclosure. The functions of the various elements shown in the figures may be provided through the use of dedicated hardware as well as hardware capable of executing associated software. Similarly, any switches shown in the figures are conceptual only. Their function may be carried out through the operation of program logic, through dedicated logic, through the interaction of program control and dedicated logic, or even manually, the particular technique being selectable by the entity implementing this disclosure. Those of ordinary skill in the art further understand that the exemplary hardware, software, processes, methods, and/or operating systems described herein are for illustrative purposes and, thus, are not intended to be limited to any particular named.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0028] Aspects of the present disclosure provide a method that can be implemented in a network security management device for automatically optimizing security policy rules in real-time based on traffic conditions or when one or more traffic rules are added/edited/deleted/modified. According to one embodiment, the method includes receiving, by the network security management device, a request to add a new traffic flow policy rule to a repository of existing control rules. In an aspect, such a request can either be manually generated by say a user/administrator or can be automatically generated based on traffic pattern/characteristics, network usage statistics, user activities, among other like actions. One should also appreciate that even though part of the disclosure has been explained with reference to new rules being added, the same systems/methods is also clearly applicable to any other action that needs to be taken place on existing set of traffic flow policy rules such as modification of one or more rules stored in rule repository or even deletion of one or more rules.

[0029] In an aspect, upon receipt of the request to add the new traffic flow policy rule, network security management device can be configured to automatically determine dependencies of the new traffic flow policy rule on one or more policy rules, and form an updated set of policy rules based on the determined dependencies. Methods of the present disclosure can further be configured to automatically optimize, by means of the network security management device, the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein such optimization of the updated set of policy rules can be performed based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

[0030] According to one embodiment, dependencies can be determined by means of evaluation of dependence in execution of the new traffic flow policy rule on one or more policy rules. In another aspect, grouping of the first sub-set of policy rules of the updated set of policy rules can include merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging can be conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination (IP) addresses, services, applications, interfaces, rule

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

tags, priorities, and parameters of the combinable policy rules. According to another embodiment, merging of the combinable policy rules can be conducted based on superneting of one or more of the source IP addresses and the destination IP addresses.

[0031] According to another embodiment, reordering a second sub-set of policy rules can include changing an order of policy rules of the second sub-set of policy rules based on one or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters. According to one embodiment, order of the policy rules of the second sub-set of policy rules can be changed based on frequency of usage thereof.

[0032] According to another embodiment, deleting a third sub-set of policy rules can include deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules. In an exemplary embodiment, the one or more conflicts can include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules. One or more conflicts can also include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule. According to one embodiment, when conflicts exist between a denied traffic flow and an allowed traffic flow, in order to avoid creating a potential security issue, the denied traffic flow will be placed before the allowed traffic flow. Alternatively, if an advantage exists, the allowed traffic flow can be split to suppress the denied traffic flow.

[0033] According to one embodiment, weights assigned to types of traffic can be defined manually based on scope and attributes of policy rule or can be defined automatically. According to another embodiment, formation of the updated set of policy rules can be conducted/performed based on the one or more weights, the preference settings, the priority settings for the policy rules, network traffic characteristics, and network usage statistics.

[0034] Aspects of the present disclosure also provide for a system for automatically optimizing security policy rules in real-time based on network traffic conditions/characteristics/usage in addition to when one or more traffic rules are added/modified. According to one embodiment, system of the present disclosure can include a business traffic flow input module configured to receive a request to add a new traffic flow policy rule to a

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

repository of existing policy rules managed by the system. The system can further include a dependency detection module configured to automatically determine dependencies of the new traffic flow policy rule on one or more policy rules, and a traffic flow policy rule incorporation module configured to form an updated set of policy rules by incorporating the new traffic flow policy rule within the policy rules based on the determined dependencies. System of the present disclosure can further include a policy rule optimization module configured to automatically optimize the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

[0035] FIG. 1 illustrates an exemplary security policy implementation architecture 100 in accordance with an embodiment of the present disclosure. In the context of the present simplified example, a protected network coupled to a public network 112 (e.g., the Internet) includes a firewall/flow control device 108, a policy rule database 110, an access point 106 and a local area network (LAN) 104 containing multiple end points 102-1, 102-2 and 102-3. When a system residing outside of the protected network attempts to communicate with a device on LAN 104 or when end points 102-1, 102-2 or 102-3 attempt to access network 112 or any resource within the network 112 through access point 106, a network security management device, (e.g., firewall/flow control device 108), which is configured to, among other things, monitor and/or filter traffic flow between end points 102 and network 112, determines whether the attempted access/communication is permitted by the enterprise security policy.

[0036] According to one embodiment, the enterprise security policy is represented by a set of rules (e.g., assess control lists (ACLs), traffic flow control rules, etc.) stored within policy rule database 110 that are used for filtering traffic flow (e.g., blocking or allowing packets between LAN 104 and network 112). Those skilled in the art will appreciate that policy rule database 110 may be separate from firewall/flow control device 108 or integral to firewall/flow control device 108.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0037] Those skilled in the art will appreciate, end points 102 may represent a variety of different operating environments. For example, end points 102 may include, but are not limited to, personal computers (PCs), end user workstations, server computers, mobile computer systems (e.g., hand-held devices, tablet computers, laptop devices), multiprocessor systems, microprocessor-based systems, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments and the like.

[0038] According to one embodiment, although the firewall/flow control device 108 in the present illustration is depicted as residing between access point 106 and network 112, in other example implementations, firewall/flow control device 108 may simply be logically interposed between end points 102 and network 112, and therefore various other network architectures/configurations are possible. In an aspect, the monitored network traffic can include, but is not limited to, HyperText Transfer Protocol (HTTP) traffic, File Transfer Protocol (FTP) traffic, Domain Name System (DNS) requests/responses, unclassified (e.g., unknown) or classified (e.g., known) application traffic and/or other types of traffic (e.g., traffic using other types of known or unknown protocols).

[0039] As explained earlier, existing firewall/flow control devices or network security management device use static policy rules to filter/block/allow traffic entering or leaving a protected network and once configured, the firewall/flow control device always searches through the same set of policy rules in the same hierarchical order. This hierarchical based execution of policy rules may delay the decision to allow/block the traffic and may impact the performance of the network. In a typical enterprise set-up, a firewall/flow control device can have thousands of policy rules, some of which may be generic policy rules that are applicable to all the traffic flow from/to network 112 and others of which may be specific to a set or range of source IP addresses, destination IP addresses, applications, ports and/or services. As discussed in the Background, increased network delays are observed for existing firewall/flow control devices or network security management devices when the matching rule of a rule base for the packet at issue is found lower in hierarchy as all policy rules placed higher in the hierarchy must be evaluated before evaluating those rules at the bottom of the hierarchy.

[0040] In order to address certain deficiencies of existing firewall/flow control devices, in an aspect, a network security management device (e.g., firewall/flow control device 108) can be

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

configured to implement systems and methods of the present disclosure and can be configured to optimize security policy rules in real-time based on traffic conditions or when one or more traffic rules within policy rule database 110 are added/edited/deleted/modified. According to one embodiment, network security device 108 can receive a request to add a new traffic flow policy rule to the rules stored in policy rule database 110, based on which firewall/flow control device 108 can be configured to automatically determine dependencies of the new traffic flow policy rule on one or more of the existing policy rules within policy rule database 110 and form an updated set of policy rules based on the determined dependencies. Firewall/flow control device 108 can then automatically optimize the updated set of policy rules grouping one or more policy rules of the updated set of policy rules, reordering one or more policy rules of the updated set of policy rules and/or deleting one or more policy rules of the updated set of policy rules, wherein such optimization of the updated set of policy rules can be performed based on various predetermined or configurable parameters, including, but not limited to, weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and/or network usage statistics for the policy rules of the updated set of policy rules. For example, if redundant rules are found in policy rule database 110 or rules that contradict each other are found in policy rule database 110 the redundancy or conflict can be proactively addressed by deleting one of the redundant or conflicting rules (e.g., manually, automatically or by a combination of manual and automated means).

[0041] As discussed in further detail below, in some embodiments, when a policy rule within policy rule database 110 is modified/amended, all other rules that are impacted by the amended rule can be automatically modified or deleted to maintain consistency with the modified rule. Similarly, when two or more rules are identified as being capable of being merged with each other by virtue of having the same source IP addresses, destination IP addresses, a common intended destination/department and/or any other relevant commonality, such rules can be automatically merged in the background or in real-time so as to avoid unnecessary growth in the size and complexity of policy rule database 110. According to one embodiment, validation and optimization functionality can be performed in the background to identify duplicate entries, mergeable entries, shadowed rules and other usual security rule based errors or sub-optimal configurations.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0042] According to another embodiment, firewall/flow control device 108 provides for dynamic reordering of policy rules within policy rule database 110 based on statistical data or weights assigned to one or more policy rules. Such dynamic reordering of the evaluation sequence of policy rules can be based on the most frequently used or the most recently used policy rule(s), for example. Such reordering will facilitate faster decision making by firewall/flow control device 108 as the rules observed to be used most frequently, for example, will be found faster as a result of being placed earlier in the search sequence of policy rule database 110. Typically, the policy rules will be reordered in accordance with administrator-defined criteria; however, in the absence of such criteria embodiments of the present invention may place less specific rules on top or very specific rules on top. Statistical analysis of the application/usage of existing policy rules may be used to select an appropriate default ordering approach.

[0043] Further, as security requirements change over time, network administrator and/or security provider may want to add new policy rules, in which case, the network security device 108 or any other network security management device (e.g., a firewall, a gateway, an intrusion prevention device, an intrusion detection device, a server, an integrated security appliance, a switch, a unified threat management (UTM) device, among others, can be configured to use the systems and methods of the present disclosure for creation and modification of firewall/access control policy rules so as to facilitate enhanced computing performance, rule management, policy optimization and/or session/network traffic packet flow management. In an aspect, firewall/flow control device 108 can be configured to use the method of present disclosure so as to overcome the limitation of existing static rule based policy by incorporating dynamic addition/modification of one or more policy rules and to create and optimize the new set of policy rules.

[0044] In an aspect, methods of the present disclosure can be used by firewall/flow control device 108 for implementation, execution, and management of policy rules, including but not limited to addition of one or more policy rules, modification of one or more existing policy rules, grouping/merging of one or more existing policy rules, reordering of one or more policy rules, and/or deletion of one or more policy rules in real-time or in the background, without impacting performance of network security device 108. Those skilled in the art will recognize the various

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

purposes of the optimization of flow control policy rules include, but are not limited to, increasing the efficiency of rule scanning/evaluation during packet filtering processing, optimizing storage of policy rule database 110, facilitating management of rules within policy rule database 110 and facilitating fast processing of packets received by firewall/flow control device 108.

[0045] According to one embodiment, firewall/flow control device 108 of the present disclosure can also be operatively coupled with a security service/server/software (not show), for example, using secure communications, such as encrypted communication techniques, to store parameters and/or attributes of incoming and outgoing network traffic packets (such as signatures, heuristics, application ID related information, packet attributes, user ID related information, content ID related information, and trusted/untrusted zone information). Based on heuristic/statistical information regarding such parameters and/or attributes, new flow control policy rules may be automatically conceived/generated and added to policy rule database 110. As another example, firewall/flow control device 108 can communicate with the service (e.g., using secure communications, such as encrypted communication techniques) to provide monitored traffic information (e.g., potential malware samples, such as in the form of subsets of such monitored traffic information, such as a portion of the packet flow, monitored Universal Resource Locator (URL)/DNS information, monitored files requested for upload/download/access, and/or other information, along with possibly other information, such as content information for the client device associated with the traffic flow and possibly user identification and/or application identification information as well), and the service can perform additional real-time and or post analysis (e.g., additional heuristic analysis as described herein with respect to various embodiments for detecting malware, including new malware threats and zero-day attacks, and/or to compare to other samples received and analyzed for other customers of the security cloud service).

[0046] FIG. 2 illustrates exemplary functional modules of a network security policy management system 200 in accordance with an embodiment of the present disclosure. In the context of the present example, system 200 includes a business traffic flow input module 202, a dependency detection module 204, a traffic flow policy rule incorporation module 206 and a policy rule optimization module 208.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0047] In one embodiment, business traffic flow input module 202 can be configured to receive a request to add a new traffic flow policy rule to a repository of policy rules managed by system 200. Such a request can either be generated automatically or can be manually generated by the user/administrator of the network. In another aspect, business traffic flow input module 202 can also be configured to receive a request relating to modification of an existing stored policy rule, wherein the modification can either be suggested by the administrator or can proposed automatically based on observed traffic patterns (e.g., source/destination IP address patterns), protocols being used, rule hits, types of prevalent attacks, frequency of attacks, changes in organization policy, among other like factors. For example, responsive to observing that one or more policies of a rule base have been unused over a configurable or predetermined period of time, a warning may be provided to the network administrator along with one or more suggested changes to be made to the rule base (e.g., removal or editing of such rules). For example, rules or objects (e.g., addresses or services) that are unused for a long period of time may be recommended for removal or, for performance reasons, the traffic flows containing the unused object may be automatically reordered to place them on the bottom of the security policy. If the unused rules or objects are removed (rather than reordered), in one embodiment, a new security policy optimization is performed.

[0048] According to one embodiment, business traffic flow input module 202 can be configured to receive one or more traffic flow policy rules corresponding to a traffic policy control requirement of the business. For example, the enterprise may desire that some traffic be processed faster or given priority over other types of traffic (e.g., a Voice over Internet Protocol (VoIP) provider might choose to have voice sessions be given a higher priority than management sessions). The traffic flow policy rules received by business traffic flow input module 202 may represent new policy rules that needs to be created and added to the policy rule database and can be defined by means of a traffic policy control requirement given as input by a user/administrator. The traffic policy control requirement can be received by a user/administrator in a defined yet flexible format such that the user/administrator may not need to be aware of the already existing policy rules or about the constraints/conflicts that the addition of the new policy rule might create. Adding one or more new policy rules or editing or deleting some preexisting policy rules can have ripple effects on other existing policy rules. As a new policy rule needs to be added and incorporated with the preexisting set of policy rules, automated

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

checks for dependency and shadowing may be implemented by business traffic flow input module 202 or one or more other functional units within system 200.

[0049] In another aspect, dependency detection module 204 can be configured to automatically determine dependencies of a new traffic flow policy rule on one or more existing policy rules. In an aspect, dependency detection module 204 can be further configured to evaluate dependence in execution of the new traffic flow policy rule on one or more existing policy rules. In an example implementation, a dependency can be established between policy rules if one policy rule (R1) partially or completely shadows another policy rule (R2) such that execution of rule R1 directly or indirectly impacts the rule R2. According to one embodiment, two rules are dependent if they mutually exhibit a precedence relationship. Such a dependency may not necessarily be detrimental or contradictory to the execution of rule R1, but may overlap with and/or depend on R2. For instance, rules R1 and R2 may be dependent on each other when they are not disjoint such that R2 cannot be moved before R1 without violating semantic integrity of the rule set. Dependency detection module 204 can therefore be configured to detect whether the newly proposed policy rule (one or more traffic flow policy rules) depends, for its execution, on any preexisting policy rule, so as to understand relationships between the newly proposed policy rule and the stored policy rules.

[0050] In another instance of dependency detection, consider two rules as follows: rule 1 permits packets with characteristic A (source address, for example) and rule 2 denies packets with characteristic B (destination address, for example). A packet with a profile matching both characteristics (from A to B in this case) will match both rules. In such a case therefore, the rules are dependent. In an aspect, dependency can be determined by means of multiple methods. For example, a rule can be selected, e.g., rule 1, for determining whether other rules in a policy rule database (e.g., policy rule database 110) depend on it. In selecting the rule, match types and associated values that would be used to filter packets can be identified, wherein match types are characteristics of packets that are used for comparison to a rule. Packet characteristics can include, for example, the protocol, port, originating IP address, destination IP address, etc. For example, a match type may be "protocol" and the value is "TCP." The rule might also have a match type "port" with a value of "20." The rule might also have a match type "IP" with a value of "123.45.67.89." One of ordinary skill in the art will recognize that a match type may be any

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

characteristic associated with the profile of a packet. A second rule, e.g., rule 2, may then be selected for comparison to rule 1. In selecting the second rule, again match types and associated values that would be used to filter packets may be identified for that rule. The match types of rule 1 can then be compared to rule 2 such that if rule 1 and rule 2 have at least one of the same match types, the values of each of the match types of rule 1 and rule 2 are compared. If all of the match types have different values than their corresponding match types in rule 2, rule 1 and rule 2 may be determined to be order independent. If rule 1 and rule 2 have at least one match type that is not in common, or if at least one match type of rule 1 shares the same value as the corresponding match type in rule 2, or if at least one of the match type of rule 1 is included (e.g., IP address and subnet) on the corresponding match type in rule 2, or or if at least one of the match type of rule 2 is included (e.g., IP address and subnet) on the corresponding match type in rule 1, rule 1 and rule 2 may be determined to be order dependent. This background process can be repeated until each pair of rules has been compared.

[0051] In another aspect, traffic flow policy rule incorporation module 206 can be configured to form an updated set of policy rules by incorporating the new traffic flow policy rule within the policy rules based on the determined dependencies, if any. In an implementation, traffic flow policy rule incorporation module 206 can either be configured to simply incorporate the new traffic flow policy rule into the policy database and leave the dependencies to be evaluated and handled later, or it can be configured to handle the dependencies and accordingly add or remove one or more existing traffic flow policy rules to/from the policy rules database. For instance, the position at which a new traffic flow policy rule is added to the database and the level at which it would be executed can be based on the dependencies computed by dependency detection module 204. Furthermore, an order of the new rule in the existing repository of flow control policy rules can also be accounted for while forming the updated set of policy rules. In an exemplary implementation, when the new rule is found to be dependent on another rule stored in the repository, both the rules can be assigned the same equivalence class.

[0052] In another aspect, policy rule optimization module 208 can be configured to automatically optimize the updated set of policy rules by grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules and/or deleting a third sub-set of policy rules of the updated set of policy rules

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

based on weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and/or network usage statistics for the policy rules of the updated set of policy rules.

[0053] According to one embodiment, grouping policy rules includes identifying potentially combinable policy rules associated with similar allowed flows (e.g., only different sources, only different destinations or only different services) and merging the identified combinable policy rules into a single policy rule. The merging can also be conducted based on matching of source IP addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities and/or parameters of the policy rules. In some embodiment, identifying potentiall combinable policy rules can be based on IP supernetting of the source IP addresses and/or the destination IP addresses. For example, a first traffic flow from source 192.168.0.0/24 to destination 1.1.1.1:80 and a second flow from source 192.168.1.0/24 to destination 1.1.1.1:80 can be merged into a new flow from source 192.168.0.0/25 to destination 1.1.1.1:80. In an instance, multiple parameters of the rule space, including, but not limited to, source, destination, user, service, enterprise firewall ID, and other such parameters can be used to identify rules that may interact or be combinable.

[0054] As a specific non-limiting example for purposes of illustration, assume there are three FTP rules that are candidates for combination, including rules allowing FTP traffic from trusted sources trusted.com and reliableco.com. In various embodiments, these trusted sources would be identified by an IP address or an IP address range. In the context of the present example, rules for both trusted sources allow FTP traffic, but require a virus scan to be performed. A third rule allows FTP traffic from all other sources except for "put" functions that may be used to upload a file. This rule allows unknown sources to log on and download, but not upload, files. As such, no antivirus scan is required for the third rule. While it is evident that the first two rules can be easily combined as they are identical except for a single parameter that does not overlap or interact in identifying two different connection sources, the third rule is distinctly different. Further, the order of the third rule is important, as the rule should be processed only after the first two rules, so that the trusted sources are allowed to FTP and "put" files to the servers protected by the firewall. Adding the third rule to the other two to form a combined rule or otherwise modifying the first two rules based on the third will result in firewall

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

behavior not intended by the administrator for at least some connections. In this example, it may be acceptable to allow FTP access including upload capability for all users, requiring anti-virus scanning for uploads only. The administrator may deem this a reasonable risk to take, or may decide the change to rule set functionality is unacceptable and only allow combination of the first two rules while declining to allow the third rule to be combined with the first two. In an aspect, whether two or more rules can be grouped/merged is determined by examining whether the rules at issue differ in relation to only a single parameter (e.g., source, destination, service), in which case, they are identified as capable of being grouped/merged. In another aspect, whenever possible, rules are grouped by superneting. If two rules differ in two or more elements/parameters, they may be grouped/reordered in such a way that results in more hits in one of the generated rules. Meanwhile, if the scope of one rule is contained entirely by the scope of another rule, the narrower rule may be deleted and the broader rule may be retained.

[0055] In an example implementation, merging of policy rules can be implemented based on superneting of one or more of the source IP addresses and the destination IP addresses, i.e. applying a single policy rule for IP addresses belonging to same class of IP addresses. In an example implementation, one or more parameters can be used to determine the group-able/merge-able policy rules. For example, if two rules differ in just one element (e.g., source, destination, service), they can be grouped together. Similarly, the policy rules applied for a group of network elements can be grouped by superneting. In an example implementation, when the scope of one policy rule is "contained" in another policy rule or all the security checks of the one policy one rule are covered by a broader security rule, then both rules can be merged into the policy rule having broader scope.

[0056] Those skilled in the art will appreciate that policy rule optimization module 208 can also be configured to demerge one or more rules to make them separate in case their order, for instance, plays an important role in deciding how the traffic packets are to be processed, and therefore, although the functions of deletion, grouping, and re-ordering have been mentioned above, any other function that enables optimization of the updated set of rules is completely within the scope of the present disclosure.

[0057] According to one embodiment, reordering of policy rules can include changing an order of policy rules based on their respective source IP addresses, destination IP addresses,

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

network usage statistics, applications, interfaces, rule tags, priorities and/or parameters. In an example implementation, the order of policy rules may be changed based on frequency of past usage, a manual priority set according to the business needs and/or other predefined or dynamically determined criteria. For example, a policy rule that is observed to be used the most frequently can be reordered to be executed first. In an example implementation, a dynamic priority can be assigned to each policy rule and the order of execution can therefore be dynamically changed. In an example implementation, if one policy rules is dependent upon another, then their relative order of execution will be preserved.

[0058] According to one embodiment, deletion of a policy rule or recommendation of deletion of a policy rule to the administrator is as a result of identifying one or more conflicts among policy rules. Conflicts include, but are not limited to, existence of a duplicate policy rule and existence of a policy rule that is contrary to a new traffic flow policy rule, for example. According to one embodiment, new rules may subsume or negate previous rules, or conflicting rules may be present in the rule set. Depending upon the particular implementation, optimization module 208 can be configured to simply bring to the attention of the administration policy rules that have been identified to be in conflict so that the administrator can select which of the rules to apply, what order the rules should be applied, or whether to merge the rules into a single rule if appropriate. In an alternative embodiment, optimization module 208 may implement changes to the policy rule database and maintain a log of changes to allow an administrator to selectively undo certain optimizations and/or revert to a prior state of the policy rule database if desired. When statistical data (e.g., frequency of execution during one or more particular time frames) is tracked and maintained relating to execution of policy rules, optimization module 208 may provide a warning to the administrator regarding any unused policies, suggest changes (e.g., removal, editing or reordering of an unused policy) and/or automatically implement and log changes to the policy rule database deemed to be appropriate.

[0059] Depending upon the particular implementation, the updated set of policy rules may be defined dynamically based on the scope and attributes of policy rules and weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and/or network usage statistics based on automatic or manual criteria, at any given time, with or without administrator intervention. In an aspect, assignment of weights to types of traffic can be

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

conducted manually or automatically or a combination thereof based on scope and/or attributes of the policy rule. In an example implementation, each policy rule can be assigned a dynamic priority/weight for its hierarchical execution. While reordering policy rules, dynamic priority can be used to define the execution order of policy rules. Policy rules can be executed in hierarchical/sequential manner according to their priority such that policy rules with highest priority is executed before execution of policy rules of comparatively lower priority. The priority can be assigned by the user/administrator or can be automatically determined based on statistical and/or historical data regarding the actual use of the policy rules. In an example implementation, an updated set of policy rules can be executed in parallel or in sequence based on the one or more weights assigned, the preference settings, the priority settings for the policy rules, network traffic characteristics, and network usage statistics, among other attributes/parameters.

[0060] Depending upon the particular implementation, network security policy management system 200 may be implemented separately from or integrated within a network security device, for example, comprising one or more processors, a communication interface mechanism, one or more internal data storage devices operatively coupled to the one or more processors and storing policy rule optimization module 208 configured to retrieve a set of policy rules and optimize the retrieved set of policy rules.

[0061] According to one embodiment, policy rule optimization module 208 can also be configured to run on a periodic basis or when one or more optimization parameters are defined/modified so as to ensure that at any given moment, the policy rules are optimally ordered, grouped and managed. Policy rule optimization module 208 may also or alternatively be manually initiated by the network administrator or automatically initiated upon detection of one of a set of predefined events (e.g., a change to the policy rule database or a change to defined business flows, expressing the relative priorities of various types of traffic within the enterprise, for example).

[0062] In an example implementation, network security policy management system 200 can have a front end interface module (not shown) that can be used by user/administrator to create and/or upload one or more new security policy rules. Other modules of the present system can run in the background for validation and optimization of updated policy rules that would

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

identify duplicate entries, merge-able entries, shadowed rules and other usual security rule based errors or non-optimized configurations. Optimization module 208 can, periodically or dynamically or based on user-defined actions, create an optimized version of the policy rules that would effectively reduce the size of the actual security policy being executed by the firewall/flow control device/ network security management device. For example, the network security device may calculate whether the creation of one or more explicit denied flows might be advantageous in connection with reducing the security policy size. In an exemplary embodiment, policy rule optimization module 208 can also reorder security policies based on customer business drivers, thereby reducing the initial rule matching time for network traffic so as to increase the performance of the security system based on automatic and/or user defined criteria. Thus, flow control policy rules can be reordered and/or rebuilt/modified dynamically based on automatic and/or manual criteria at any given time, with or without user intervention.

[0063] In an exemplary implementation, proposed changes to the policy rule database may be brought to the attention of the user/administrator via the frontend interface for further modification and/or confirmation before taking affect. Alternatively, confirmation of optimized policy rules may not require to be confirmed/approved by any user/administrator prior to being implemented and taking affect.

[0064] In accordance with embodiments of the present invention, creation and/or ordering of optimized policy rules can be based on various criteria, including, but not limited to, performance (e.g., rule hits), business flows (e.g., to guarantee one or more types traffic are processed faster) and/or statistical analysis of the actual policy rules being used. The security policy can also self-adjust automatically over time in order to improve performance and further reduce delay for new session establishment.

[0065] In an exemplary implementation, network security policy management system 200 may generate a warning if a rule remains unused over a predetermined or configurable period of time. Network security policy management system 200 may alternatively or additionally suggest re-ordering of rules within the policy rule database (e.g., moving unused or infrequently used rules to the end) or removal of unused rules. Network security policy management system 200 can also be configured to simplify management of policy rules so as to allow the administrator to focus his/her attention on traffic flows that reflect particular business needs. For example,

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

because network security policy management system 200 will take care of evaluating and creating a valid, effective, efficient and optimized security policy, the administrator no longer needs to check the complete rule base before making any changes. In an aspect, higher priority rules can also be identified and re-ordered and/or categorized in order to optimize packet filtering. In another embodiment, priorities of optimization parameters (e.g., network traffic characteristics, source/destination IP addresses, frequency/time aspects of packets, type of traffic, among others) can also be configured/changed based on usage/context/organization policies/objectives. For example, some enterprises may value (and therefore prioritize) increased performance in initial session establishment (e.g., as a result of reordering of rules based on frequency of execution or based on whether they specify one or more specific IP addresses or are subnet based) over a more compact rule set (e.g., as a result of merging rules).

[0066] FIG. 3A illustrates an exemplary representation 300 showing a snapshot of a simplified security policy, and FIG. 3B shows addition of a new security policy rule 399 to the security policy in accordance with an embodiment of the present disclosure. In the present example, representation 300, includes a Host/Network column 310, identify the source host/network(s) with which the policy rule is associated, a Peer Host/Network column, identifying the destination/target peer host/network(s) with which the policy rule is associated, a Ports column 330, identifying particular ports on which the traffic is allowed, a Business Case/tag column 340, identifying a project with which the corresponding policy rule is associated, and a rule ID/seq column 350, potentially indicating an order in which the policy rules are applied. Those skilled in the art will appreciate the exemplary functional modules described herein are for purposes of illustration only and that the functionality described with reference to various of the exemplary functional modules may be combined and/or distributed differently.

[0067] FIG. 3A illustrates a simplified example of preexisting flow control security policy rules having rule identifiers (IDs) 350 ranging from 1 to 15 and representing different policy rules that are defined/configured by the user/administrator/system in order to filter incoming/outgoing traffic/packet/connection requests from/to the network. Rule IDs 350 can also indicate the sequence in which the processing of the network traffic takes place, wherein the traffic would first pass through the entries/flows associated with sequence ID 1 and then to 2 and

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

so on. As can be seen, each rule ID 1-15 can be implemented for one or more projects that correspond to respective business cases/tags 340. Each project can also be associated with multiple sessions between source host and destination/peer host.

[0068] As can be seen in the present example, entry 301a of policy rule 301 relates to all traffic/packet/connection requests sent from host 10.184.17.0/26 to peer host/network 10.135.32.0/26, which, can be sent on any of the ports, wherein the interaction between the source-destination relates to a project referred to as "Initial Project." Similarly, in accordance with entry 303a of policy rule 303, traffic can be sent from buss-server02 to 10.135.35.121 on ports 3315/TCP, 3380/TCP, 3366/UDP, and 3390/TCP. While representation 300 FIG. 3A only shows twenty-one entries representing twelve policy rules, those skilled in the art will appreciate, in practice, there can be hundreds of such entries.

[0069] FIG. 3B illustrates a new rule 399 created by user/administrator, which needs to be incorporated with the existing policy rules of FIG. 3A. New rule 399 may be used for traffic analysis and monitoring of traffic flow, for example, between buss-fe01 and 10.135.35.0/24 through port TCP-1024. Prior to incorporation of new rule 399 into the existing policy rules, various initial checks may be performed to identify policy rules within the existing policy rule database upon which new rule 303 may be dependent, identify duplicate/overlapping/dependent/shadowing rules and/or determine the relative priority of new rule 399, based on which new rule 399 can be incorporated into the policy rule database. Since the project ("Web-API-Integration") with which new rule 399 is associated is business critical, it will be given high priority which should be reflected during reordering of the policy rules.

[0070] If the flow represented by new rule 399 is expected to have many sessions and in view of its high priority, the administrator, without the benefit of performing a detailed analysis of the security policy, may manually create the following flawed security rule entry on top of the security policy represented in FIG. 3A:

Host/Network	Peer Host/Network	Ports	Business Case/tag	rule ID/seq
buss-fe01	10.135.35.0/24	TCP-1024	web_API integration	1

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0071] In existing systems, with the insertion of this new rule, the sequence numbers of subsequent rules would be incremented by one. With this change, the newly defined traffic flow would have the highest priority in relation to new session matching processing, but the security policy may effectively shadow part of rule 305, and allow traffic that should be denied by rule 311, thus creating unnecessary processing on rule 305 and allowing a traffic flow that should have been denied by rule 311. Since traffic meeting rule 311 (which should be denied) is allowed in accordance with the present example, it is unlikely anyone would complain (as end users typically only notice the denial of traffic they desire to be allowed), but a security issue has been created by the introduction of a flawed security rule.

[0072] In accordance with embodiments of the present invention, on the other hand, without analyzing the security policy, the administrator can instruct the security system to create a flow with the characteristics of new rule 399 without concern as network security policy management system 200 would automatically evaluate the existing security policy and reach the following conclusions:

a. Since the priority associated with new rule 399 is high, new rule 399 needs to be placed on top;

b. Rule 305 also matches this flow for traffic originating on host buss-fe01. If a new rule is created on top, then part of rule 305 is unnecessary, so rule 305 should be automatically revised; and

c. Rule 311 is in conflict with part of the flow required for new rule 399. Since rule 311 is a deny rule, a warning should be issued to the administrator pointing out the conflict; and

    i. If the flow-denial of rule 311 is to be maintained, rule 311 should be moved to a position with a smaller seq# than new flow 399. Alternatively, if rule 311 is to be "forgotten" due to the higher priority of new flow 399, then rule 311 should be removed.

[0073] FIG. 4 illustrates an exemplary snapshot of a security policy rule management system interface 400 in accordance with an embodiment of the present invention. The snapshot 400 illustrates an exemplary frontend/administrator interface for management of security policy

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

rules. According to one embodiment, system interface 400 can present a user/administrator with various options for managing one or more policy rules including, but not limited to, viewing policy rules, adding new policy rules, searching for policy rules, checking dependencies of one or more rules, deleting/modifying/re-ordering and optimizing policy rules. In an aspect, a user/administrator, by means of viewing policy rules, can also add new policy rules to the existing set of flow control policy rules, analyze performance of current rules, view traffic pattern/attributes/characteristics, and manage conflicts/modification of rules. In another aspect, the administrator can also check dependency in order to view automatically identified dependencies that any rule has on the other set of rules that form part of the rules repository. In yet another aspect, based on a selected optimization criteria (e.g., optimization based on priority verses optimization based on traffic statistics) dependencies, traffic related attributes, weights of different types of policy rules, organizational policies, among other parameters, the administrator can also enable optimization of the policy rules.

[0074] In yet another embodiment, as shown in FIG 4, optimization can either take place for all the flow control policy rules or can be performed automatically for a defined number interlinked/selected/related rules. In yet another embodiment, through the "optimize policy rules" option, the administrator can also select and/or define criteria to be used for optimization, define policy settings to be adopted for optimization, assign weights to different policy rules, enable usage statistics to be incorporated during optimization, define priority of one or more rules, enable traffic attributes/characteristics to be incorporated along with the defining, say the technology required for security policy implementation.

[0075] In yet another embodiment, through the "optimize policy rules" option a user/ administrator can select and define group policy rules through which the system can either through manual intervention or automatically, arrange new and/or existing policy rules into groups. Such an option can allow automatic merging of possible flow control policy rules or creating of new rules that relate to subnets and not to individual IP addresses, for instance.

[0076] In yet another embodiment, through the "optimize policy rules" option, the administrator can enable all or part of the policy rules to be re-ordered, leading to, for instance, higher priority rules or more frequently referred rules to be brought up the hierarchy for faster access when compared with lower priority rules. Any other basis such as most accessed rules

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

can also be applied for re-ordering or re-arranging one or more policy rules. In yet another embodiment, through the "optimize policy rules" option a user/ administrator can enable deletion of one or more rules based on, for instance, duplicate/redundant rules, conflicting rules (that act differently for same source-destination packet for instance). One should appreciate that the various options illustrated through security policy rule management system interface 400 are completely exemplary in nature and all other options for management of policy rules are within the scope of present disclosure.

[0077] FIGs. 5A, FIG. 5B and FIG. 5C illustrate exemplary policy rules 500 stored in a policy rule database along with dependencies and possible groupings detected in accordance with an embodiment of the present invention. FIG. 5A illustrates an exemplary representation 500 having multiple policy rules, specifying actions to be taken by a network security device for specific services between specific sources and specific destinations. For instance, as can be seen, traffic from 192.168.0.0/24 to any destination is allowed for Domain Name System (DNS), HyperText Transfer Protocol (HTTP), and HTTP Secure (HTTPS) packets and the priority of such packets is Normal. The exemplary representation 500 of FIG. 5A also shows, for instance, the number of sessions impacted by each policy rule over a given time period and the corresponding percentage of sessions of the total number of sessions during the given time period.

[0078] FIG. 5B illustrates the policy rules 500 of FIG. 5A with a "Dependencies" column annotating various automatically identified dependencies among the policy rules 500. For instance, as the policy rule at index 7 blocks any traffic from 192.168.3.2 to 192.168.0.0/16, the execution order of the policy rule at index 6 rule depends on the policy rule of index 7. Similarly, as the policy rule of index 8 applies to all traffic from 192.168.3.2 to any destination, the policy rule at index 7 shadows the policy rule at index 8.

[0079] FIG. 5C illustrates how potential policy rules that can be merged/grouped can be identified and represented. For instance, the column "Dependencies B" includes annotations indicating that the policy rule at index 1 and the policy rule at index 2 rule can be partially merged together as they have the same source-destination pairs/priority and only differ in the type of service they allow to pass, and therefore, if merged, they can allow a combined traffic for DNS, HTTP, HTTPS, and SMTP. Similarly, the policy rule at index 8 can also be partially

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

merged with the policy rule at index 2, wherein post merger, the priority of the policy rule at index 2 can either be set to High or can be kept at Normal as specified manually by the administrator or determined automatically based on one or more of the weight of each rule, traffic characteristics, among other defined set of parameters.

[0080] FIG. 5D illustrates an optimized version of the security policy that seeks to optimize performance based on traffic statistics gathered by the flow control device in accordance with an embodiment of the present disclosure. As shown, the updated policy rule set has a policy rule at index 1 resulting from a partial merger of former policy rules associated with index 1 and index 2 of FIG. 5C, with the source being 192.168.0.0/23 and allowing issuance of packets to all destinations using DNS, HTTP and/or HTTPS services. The representation of FIG. 5D further shows the former policy rule associated with index 6 having been reordered to now be associated with index 2, and the former policy rule associated with index 7 being reordered to now be associated with index 3 as the volume of hits for this policy rule 3 are relatively high (50000 sessions). Similarly, a new policy rule associated with index 4 is a partial merger of the former policy rule associated with index 2 and the former policy rule associated with index 8, and a new policy rule at index 5 represents a reordered version of the former policy rule associated with index 4. Likewise, policy rule at index 7 has been put toward the end as the number of sessions/hits for this transaction (192.168.3.1 to 192.168.1.80 over HTTP) is low.

[0081] FIG. 5E illustrates an alternative optimized version of the security policy that seeks to optimize performance based on administrator-defined traffic priority in accordance with an embodiment of the present disclosure. As shown, the optimized policy rule set reflects, among other things, movement of former policy rule associated with index 6 in FIG. 5C to index 2. As former policy rule associated with index 7 in FIG. 5C had a high number of hits/sessions, that former policy rule has been moved to index 3, and the new policy rule at index 4 represents the partial merger of former policy rules associated with index 2 and 8 in FIG. 5C.

[0082] Those skilled in the art will appreciate that the two previously described optimization scenarios are merely exemplary and are based on a defined set of administrator-defined and/or system maintained parameters. In alternative embodiments, policy rules may be selected and evaluated with respect to their hits/session/frequency of use, potential of merger to

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

reduce the overall number of rules and/or potential for making the database light and efficient, along with considering other parameters discussed above to reorder the rule database.

[0083] FIG. 6 illustrates an exemplary flow diagram 600 for optimization of policy rules in a rule database in accordance with an embodiment of the present disclosure. At step 602, a network security management device receives a request to add a new traffic flow policy rule to an existing set of policy rules. In an aspect, such a request can either be manually generated by say a user/administrator or can be automatically generated based on traffic pattern/characteristics, network usage statistics, user activities, among other like actions.

[0084] At step 604, upon receipt of the request to add the new traffic flow policy rule, the network security management device automatically determines dependencies of the new traffic flow policy rule in relation to one or more of the existing policy rules. At step 606, an updated set of policy rules based on the determined dependencies can be created/generated, and at step 608, the updated set of policy rules can be automatically optimized by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein such optimization of the updated set of policy rules can be performed based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

[0085] According to one embodiment, dependencies can be determined by means of evaluation of dependence in execution of the new traffic flow policy rule on one or more policy rules. In another aspect, grouping of the first sub-set of policy rules of the updated set of policy rules can include merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging can be conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination (IP) addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules. According to another embodiment, merging of the combinable policy rules can be conducted based on superneting of one or more of the source IP addresses and the destination IP addresses.

[0086] According to another embodiment, reordering a second sub-set of policy rules can include changing an order of policy rules of the second sub-set of policy rules based on one or

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters. According to one embodiment, order of the policy rules of the second sub-set of policy rules can be changed based on frequency of usage thereof.

[0087] According to another embodiment, deleting a third sub-set of policy rules can include deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules. In an exemplary embodiment, the one or more conflicts can include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules. One or more conflicts can also include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule.

[0088] According to one embodiment, weights assigned to types of traffic can be defined manually based on scope and attributes of policy rule or can be defined automatically. According to another embodiment, formation of the updated set of policy rules can be conducted/performed based on the one or more weights, the preference settings, the priority settings for the policy rules, network traffic characteristics, and network usage statistics.

{0088.1} FIG. 7 is an example of a computer system 700 with which embodiments of the present disclosure may be utilized. Computer system 700 may represent or form a part of a network security management device (e.g., a firewall, a gateway, an intrusion prevention device, an intrusion detection device, a server, an integrated security appliance, a switch, a unified threat management (UTM) device) or other device implementing one or more components of a network security policy management system (e.g., network security policy management system 200).

{0088.2} Embodiments of the present disclosure include various steps, which have been described in detail above. A variety of these steps may be performed by hardware components or may be tangibly embodied on a computer-readable storage medium in the form of machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor programmed with instructions to perform these steps. Alternatively, the steps may be performed by a combination of hardware, software, and/or firmware.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0088.3] As shown, computer system 700 includes a bus 730, a processor 705, communication port 710, a main memory 715, a removable storage media 740, a read only memory 720 and a mass storage 725. A person skilled in the art will appreciate that computer system 700 may include more than one processor and communication ports.

[0088.4] Examples of processor 705 include, but are not limited to, an Intel® Itanium® or Itanium 2 processor(s), or AMD® Opteron® or Athlon MP® processor(s), Motorola® lines of processors, FortiSOC™ system on a chip processors or other future processors. Processor 705 may include various modules associated with monitoring unit as described in FIGs. 2-4. Communication port 710 can be any of an RS-232 port for use with a modem based dialup connection, a 10/100 Ethernet port, a Gigabit or 10 Gigabit port using copper or fiber, a serial port, a parallel port, or other existing or future ports. Communication port 710 may be chosen depending on a network, such a Local Area Network (LAN), Wide Area Network (WAN), a WLAN or any network to which computer system 700 connects.

[0088.5] Memory 715 can be Random Access Memory (RAM), or any other dynamic storage device commonly known in the art. Read only memory 720 can be any static storage device(s) such as, but not limited to, a Programmable Read Only Memory (PROM) chips for storing static information such as start-up or BIOS instructions for processor 705.

[0088.6] Mass storage 725 may be any current or future mass storage solution, which can be used to store information and/or instructions. Exemplary mass storage solutions include, but are not limited to, Parallel Advanced Technology Attachment (PATA) or Serial Advanced Technology Attachment (SATA) hard disk drives or solid-state drives (internal or external, e.g., having Universal Serial Bus (USB) and/or Firewire interfaces), such as those available from Seagate (e.g., the Seagate Barracuda 7200 family) or Hitachi (e.g., the Hitachi Deskstar 7K1000), one or more optical discs, Redundant Array of Independent Disks (RAID) storage, such as an array of disks (e.g., SATA arrays), available from various vendors including Dot Hill Systems Corp., LaCie, Nexsan Technologies, Inc. and Enhance Technology, Inc.

[0088.7] Bus 730 communicatively couples processor(s) 705 with the other memory, storage and communication blocks. Bus 730 can be, such as a Peripheral Component Interconnect (PCI) / PCI Extended (PCI-X) bus, Small Computer System Interface (SCSI), USB or the like, for

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

connecting expansion cards, drives and other subsystems as well as other buses, such a front side bus (FSB), which connects processor 705 to system memory.

[0088.8] Optionally, operator and administrative interfaces, such as a display, keyboard, and a cursor control device, may also be coupled to bus 730 to support direct operator interaction with computer system 700. Other operator and administrative interfaces can be provided through network connections connected through communication port 710.

[0088.9] Removable storage media 740 can be any kind of external hard-drives, floppy drives, IOMEGA® Zip Drives, Compact Disc - Read Only Memory (CD-ROM), Compact Disc - Re-Writable (CD-RW), Digital Video Disk - Read Only Memory (DVD-ROM).

[0088.10] Components described above are meant only to exemplify various possibilities. In no way should the aforementioned exemplary computer system limit the scope of the present disclosure.

[0089] While embodiments of the present disclosure have been illustrated and described, it will be clear that the present disclosure is not limited to these embodiments only. Numerous modifications, changes, variations, substitutions, and equivalents will be apparent to those skilled in the art, without departing from the spirit and scope of the present disclosure, as described in the claims.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	14566403
	Filing Date	2014-12-10
	First Named Inventor	Hugo Filipe Parreira Pernicha
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	FORT-012500

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button							Add	

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14566403
	Filing Date	2014-12-10
	First Named Inventor	Hugo Filipe Parreira Pernicha
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	FORT-012500

	1	AlgoSec BusinessFlow®. "Data Center Application Connectivity Management." 2013. 2 pages.	☐
	2	AlgoSec. "Managing Security at the Speed of Business." 2014. 6 pages.	☐
	3	EMA. "FireMon's Security Manager V7.0 Release Expands Value to Enterprises and Service Providers." 2013. 4 pages.	☐
	4	Tufin. SecureTrackTM. "Firewall Operations Management, Auditing & Compliance." Feb, 2012. 10 pages.	☐
	5	Ramachandran, V. "HOW TURBO ACL'S WORK." 6 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14566403
	Filing Date	2014-12-10
	First Named Inventor	Hugo Filipe Parreira Pernicha
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	FORT-012500

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael A. DeSanctis/	Date (YYYY-MM-DD)	2014-12-26
Name/Print	Michael A. DeSanctis	Registration Number	39957

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	21079480
Application Number:	14566403
International Application Number:	
Confirmation Number:	7209
Title of Invention:	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT
First Named Inventor/Applicant Name:	Hugo Filipe Parreira Pernicha
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-012500
Receipt Date:	30-DEC-2014
Filing Date:	10-DEC-2014
Time Stamp:	16:02:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS_12500.pdf	612489 f0bbef29472ea49c6dac73104d418d434e0917a4	no	4
Warnings:					
Information:					

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Non Patent Literature	NPL_1.pdf	400467 7a40154e0094d5b36fa5075cff5a4e6daba6172d	no	2
Warnings:					
Information:					
3	Non Patent Literature	NPL_2.pdf	2081119 3f1bad7f9437d8fe00d8cdb643bde15463ba8f00	no	6
Warnings:					
Information:					
4	Non Patent Literature	NPL_3.pdf	129213 b490bffc73dc09f78568c0e4703e3a67e684131d	no	4
Warnings:					
Information:					
5	Non Patent Literature	NPL_4.pdf	319414 c28064da121dcc62ba666c09c76774a66cfda483	no	10
Warnings:					
Information:					
6	Non Patent Literature	NPL_5.pdf	149441 7022e89c167381387cefe66d3ba27fbc79bc0d77	no	6
Warnings:					
Information:					
			Total Files Size (in bytes):	3692143	

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/566,403

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	600
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	26 minus 20 =	* 6			OR	x 80 =	480
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 420 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	2080

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/566,403	12/10/2014	2431	2080	FORT-012500	26	3

CONFIRMATION NO. 7209

64128
MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

FILING RECEIPT

OC000000072559098

Date Mailed: 12/29/2014

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)
Hugo Filipe Parreira Pernicha, Venda do Pinheiro, PORTUGAL;

Applicant(s)
Fortinet, Inc., Sunnyvale, CA

Assignment For Published Patent Application
FORTINET, INC., Sunnyvale, CA

Power of Attorney: The patent practitioners associated with Customer Number 64128

Domestic Applications for which benefit is claimed - None.
A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 12/23/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/566,403**

Projected Publication Date: To Be Determined - pending completion of Corrected Papers

Non-Publication Request: No

Early Publication Request: No

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Title

DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/566,403	12/10/2014	Hugo Filipe Parreira Pernicha	FORT-012500

CONFIRMATION NO. 7209

64128
MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

FORMALITIES LETTER

OC000000072559100

Date Mailed: 12/29/2014

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Filing Date Granted

An application number and filing date have been accorded to this application. The application is informal since it does not comply with the regulations for the reason(s) indicated below. Applicant is given TWO MONTHS from the date of this Notice within which to correct the informalities indicated below. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

The required item(s) identified below must be timely submitted to avoid abandonment:

- A substitute specification in compliance with 37 CFR 1.52, 1.121(b)(3), and 1.125, is required. The substitute specification must be submitted with markings and be accompanied by a clean version (without markings) as set forth in 37 CFR 1.125(c) and a statement that the substitute specification contains no new matter (see 37 CFR 1.125(b)). The specification, claims, and/or abstract page(s) submitted is not acceptable and cannot be scanned or properly stored because:
  - The application contains drawings, but the specification does not contain a brief description of the several views of the drawings as required by 37 CFR 1.74 and 37 CFR 1.77(b)(9).

The following item(s) appear to have been **omitted** from the application:

- Figure(s) **3** described in the specification.

Applicant must reply to this notice within the time period set forth in this notice to avoid abandonment of this application. Applicant must select one of the three following options and the reply must comply with the requirements set forth in the selected option and any other requirements set forth in this notice. The reply should also indicate which option applicant has selected.

I. Petition for date of deposit: Should applicant contend that the above-noted omitted item(s) was in fact deposited in the U.S. Patent and Trademark Office (USPTO) with the nonprovisional application papers, a copy of this Notice and a petition (and the petition fee set forth in 37 CFR 1.17(f) with evidence of such deposit **must** be filed within **TWO MONTHS** of the date of this Notice. The petition fee will be refunded if it is determined that the item(s) was received by the USPTO. **THIS TWO MONTH PERIOD IS EXTENDABLE UNDER 37 CFR 1.136(a) or (b).**

II. Petition for later filing date: Should applicant desire to supply the omitted item(s) and accept the date that such omitted item(s) was filed in the USPTO as the filing date of the above-identified application, a copy of this Notice, the omitted item(s), and a petition under 37 CFR 1.182 with the petition fee set forth in 37 CFR 1.17(f) requesting the later filing date **must** be filed within **TWO MONTHS** of the date of this Notice. **THIS TWO MONTH PERIOD IS EXTENDABLE UNDER 37 CFR 1.136(a) or (b).**

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Applicant is advised that generally the filing fee required for an application is the filing fee in effect on the filing date accorded the application and that payment of the requisite basic filing fee on a date later than the filing date of the application requires payment of a surcharge (37 CFR 1.16(f)). To avoid processing delays and payment of a surcharge, applicant should submit any balance due for the requisite filing fee based on the later filing date being requested when submitting the omitted item(s) and the petition (and petition fee) requesting the later filing date.

III. Acceptance of application as deposited: Applicant may accept the application as deposited in the USPTO by filing an appropriate amendment as set forth in either (A) or (B) below within **TWO MONTHS** of the date of this Notice. **THIS TWO MONTH PERIOD IS EXTENDABLE UNDER 37 CFR 1.136(a) or (b)** . The application will maintain a filing date as of the date of deposit of the application papers in the USPTO, and original application papers (i.e., the original disclosure of the invention) will include only those application papers present in the USPTO on the date of deposit. A petition is not required for this option.

(A) If applicant wants to accept the application as deposited without adding the subject matter that was in the omitted item (e.g., a missing page or figure), applicant is required to submit one or more of the following items without adding any new matter (see 35 U.S.C. 132(a)):

1. For a missing page of the specification,
   a) a substitute specification including claims that amends the specification to renumber the pages consecutively and cancels any incomplete sentences, and
   b) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125;
2. For a missing figure of the drawings,
   a) replacement drawing sheets in compliance with 37 CFR 1.121(d) to renumber the drawing figures consecutively (if necessary),
   b) a substitute specification excluding claims that amends the specification to cancel any references to any omitted drawing(s) and corrects the references in the specification to the drawing figures to correspond with any relabeled drawing figures, and
   c) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125;
3. For a missing page of the claim listing only, a replacement claim listing with the claims renumbered consecutively or, if amendment to the claims is also necessary, then a complete claim listing in compliance with 37 CFR 1.121(c);
4. For a missing or unreadable compact disc,
   a) a substitute specification (excluding the claims) deleting the reference to the compact disc and the files contained on the compact disc, and
   b) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125; and
5. For a missing or unreadable file submitted on a compact disc,
   a) a substitute specification (excluding the claims) deleting the reference to the missing or unreadable file, and a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125; and
   b) a replacement transmittal letter listing all of the files except the missing or unreadable file in compliance with 37 CFR 1.52(e)(3)(ii).

(B) Alternatively, if applicant wants to accept the application as deposited but wishes to add the subject matter in the omitted item (e.g., a missing page or figure) by relying on an incorporation by reference under 37 CFR 1.57 or other portions of the original disclosure, applicant is required to submit one or more of the following items without adding any new matter (see 35 U.S.C. 132(a)):

1. To add the subject matter in a missing page of specification,
   a) a substitute specification excluding claims and
   b) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125;

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

2. To add a missing figure of the drawings, new and replacement drawing sheets in compliance with 37 CFR 1.121(d);
3. To add the subject matter in a missing page of the claim listing, a complete claim listing in compliance with 37 CFR 1.121(c) (e.g., a claim in the missing page should be submitted as a new claim);
4. To add the subject matter in a missing or unreadable compact disc,
   a) a replacement compact disc and a duplicate copy of the compact disc, in compliance with 37 CFR 1.52(e); and
   b) a statement that the replacement compact disc contains no new matter in compliance with 37 CFR 1.52(e)(4); and,
5. To add the subject matter in a missing or unreadable file submitted on a compact disc,
   a) a replacement compact disc that contains all of the files listed in the specification including the missing or unreadable file and a duplicate copy of the compact disc, in compliance with 37 CFR 1.52(e); and
   b) a statement that the replacement compact disc contains no new matter in compliance with 37 CFR 1.52(e)(4).

If applicant is relying on an incorporation by reference under 37 CFR 1.57 to add the omitted subject matter, then applicant must also comply with the requirements of 37 CFR 1.57.

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/kung/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PTO/AIA/80 (07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

■ Practitioners associated with Customer Number: 64128

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

■ The address associated with Customer Number: 64128

OR

☐

Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address: Fortinet, Inc.
899 Kifer Rd.
Sunnyvale, CA 94086

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be Filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of The practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record
The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	
Name	Todd A. Nelson	Telephone	(408) 486-7803
Title	Vice President Legal		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT			
First Named Inventor/Applicant Name:	Hugo Filipe Parreira Pernicha			
Filer:	Michael A. DeSanctis			
Attorney Docket Number:				
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:				
Utility application filing	1011	1	280	280
Utility Search Fee	1111	1	600	600
Utility Examination Fee	1311	1	720	720
Pages:				
Claims:				
Claims in Excess of 20	1202	6	80	480
Miscellaneous-Filing:				
Petition:				

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		2080

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Electronic Acknowledgement Receipt	
EFS ID:	20925650
Application Number:	14566403
International Application Number:	
Confirmation Number:	7209
Title of Invention:	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT
First Named Inventor/Applicant Name:	Hugo Filipe Parreira Pernicha
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	10-DEC-2014
Filing Date:	
Time Stamp:	17:41:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$2080
RAM confirmation Number	4620
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Patent_Application.pdf	291201 009ecb5e40f022b0b02e629b5943d36aa71ece80	yes	38

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	32
	Claims	33	37
	Abstract	38	38

Warnings:					
Information:					
2	Drawings-only black and white line drawings	drawings.pdf	59532 c4a38156ac8d1aeb606c26c782fb47b5b73579ee	no	9
Warnings:					
Information:					
3	Application Data Sheet	ads.pdf	1560990 9280dfbbd49ad7f5c2c908a82c80baba2b2c647b	no	7
Warnings:					
Information:					
4	Oath or Declaration filed	Executed_Declaration.pdf	1167734 4344f11526420af58eb8cb39a94e734fa852784e	no	2
Warnings:					
Information:					
5	Assignee showing of ownership per 37 CFR 3.73.	statement.pdf	117087 7c7e6c73df7358fee3b11313fc1ab3bd10ee7325	no	3
Warnings:					
Information:					
6	Assignee showing of ownership per 37 CFR 3.73.	Executed_Assignment.pdf	1057483 49cbe1ad2f857c5b1e146120cdca358e1cacdebf	no	2

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Warnings:					
Information:					
7	Power of Attorney	Executed_POA_3_73_c_2.pdf	76400 f4ad760f71d7becdc33b00b6c2c4b21776d380d1	no	1
Warnings:					
Information:					
8	Fee Worksheet (SB06)	fee-info.pdf	36635 adcaa6d5a72294393f117bc56b8a253913ee8265	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	4367062	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Atty. Docket No.: FORT-012500 Patent Application
Fortinet Ref. No.: 13048

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TITLE OF THE INVENTION

DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

Inventor:

Hugo Filipe Parreira Pernicha, residing at:
Av. 9 de Julho, nº 12, 3 Dto
2665-520 Venda do Pinheiro
PORTUGAL

Assignee: **FORTINET, INC.**
A Delaware Corporation

Entity: Regular Undiscounted

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

COPYRIGHT NOTICE

[0001] Contained herein is material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction of the patent disclosure by any person as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all rights to the copyright whatsoever. Copyright © 2014, Fortinet, Inc.

BACKGROUND

Field

[0002] Embodiments of the present invention generally relate to network traffic control. In particular, embodiments of the present invention relate to systems and methods for firewall and/or access control policy management and optimization of policy rules to enhance performance of policy rule processing.

Description of the Related Art

[0003] A firewall generally represents an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system. A firewall may assume the form of a flow control device or set of devices configured to permit, deny, encrypt, decrypt and/or proxy computer traffic between different security domains based upon a set of rules and other criteria. Organizations that use Internet Protocol (IP) based communication networks have firewalls or access control devices/mechanisms to control the traffic that crosses into and out of their networks, or between different network segments. Each firewall is basically a special-purpose computer that enforces the organization's traffic filtering policy. Typically, the filtering policy is implemented in a rule base, which is an ordered list of rules, wherein each rule consists of a set of field value-ranges, and an associated action that is generally either “PASS” or “DROP”.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0004] Most firewalls enforce the policy according to "first-match" semantics, wherein for each new IP connection, the firewall checks the rules one by one, according to their order in the rule-base, until it finds a rule that matches the new connection. The first rule that matches the connection determines the firewall's action, wherein if the first matching rule has an action of "PASS" then the firewall will allow the connection to continue, and if the rule's action is "DROP" then the firewall will discard all the packets belonging to the connection. If no rule matches the connection then the firewall uses a default action, which is usually DROP.

[0005] As firewall or access control policies can have numerous rules, searching for a matching rule in sequence can require considerable CPU time. In such an implementation, the computational effort to match a connection to the rule-base is proportional (linearly) to the number of rules the firewall needs to try in sequence until it reaches the first matching rule. If checking a match against one rule typically requires M computer instructions, then checking K rules in sequence requires K times M instructions. If the first-matching rule happens to be one of the first in the rule-base, the firewall will identify the corresponding action quickly and with a low computational effort. Conversely, if the first-matching rule is near the end of the rule-base, the firewall will take longer to identify the corresponding action.

[0006] Firewall rule-based policy is typically static. As such, once it is configured, it will stay the same, in the same order and not be changed unless explicitly changed by a user/administrator. In practice, large enterprises end up with a substantial set of firewall rule-based policies that are more oriented to user/operator visibility than rule processing efficiency. Furthermore, addition of each new policy rule or modification of an existing rule typically has ripple effects on other existing/stored rules and policies. For instance, a new policy rule may be configured to allow packets of a specific traffic type to a given destination, which otherwise may have been denied by an already existing policy rule in the rule database. Existing security policy management techniques require manual detection of issues, such as duplication of rules, conflicts between rules, dependency between rules, or shadowing of one rule by another and therefore are error prone. These issues are exacerbated in the context of large policy rule databases.

[0007] There is therefore a need for systems and methods that allow efficient addition or modification of one or more policy rules by enabling enhanced system performance, manageability and reduced human error. There is also a need for systems and methods that

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

allow dynamic and automatic optimization of policy rules by efficiently grouping/merging, deleting, reordering and otherwise managing policy rules based on defined and configurable optimization criteria so as to enable improved overall performance and significant reduction in session establishment/rule access/rule processing delay.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

SUMMARY

[0008] Methods and systems are described for dynamically optimizing rule-based security policies. According to one embodiment, a security policy optimization method is provided. A request is received by a network security management device to add a new traffic flow policy rule to multiple existing policy rules managed by the network security management device. Dependencies of the new traffic flow policy rule on one or more of the existing policy rules are automatically determined. An updated set of policy rules is formed by incorporating the new traffic flow policy rule within the existing policy rules based on the determined dependencies. The updated set of policy rules is then optimized by (i) grouping a first sub-set of policy rules of the updated set of policy rules; (ii) reordering a second sub-set of policy rules of the updated set of policy rules; and/or (iii) deleting a third sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules.

[0009] Other features of embodiments of the present disclosure will be apparent from accompanying drawings and from detailed description that follows.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] In the Figures, similar components and/or features may have the same reference label. Further, various components of the same type may be distinguished by following the reference label with a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

[0011] FIG. 1 illustrates exemplary security policy architecture in accordance with an embodiment of the present invention.

[0012] FIG. 2 illustrates exemplary functional units of a rule-based security policy management system in accordance with an embodiment of the present invention.

[0013] FIG. 3 illustrates exemplary addition of a new security policy rule to a policy rule database in accordance with an embodiment of the present invention.

[0014] FIG. 4 illustrates an exemplary snapshot of a security policy rule management system in accordance with an embodiment of the present invention.

[0015] FIGs. 5A to 5E illustrate exemplary optimization of policy rules stored in a rule database based on dependencies, priorities, traffic attributes, hits, sessions, potential of merger/modification/deletion, among other attributes in accordance with an embodiment of the present invention.

[0016] Fig. 6 is a flow diagram illustrating security policy rule management in accordance with an embodiment of the present invention.

[0017] FIG. 7 is an exemplary computer system.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

DETAILED DESCRIPTION

[0018] Methods and systems are described for dynamically optimizing rule-based security policies. Methods and systems are also provided for creation and modification of firewall/access control policy rules so as to allow enhanced computing performance, rule management, policy optimization, and session/network traffic packet flow management. Methods and systems are further provided for optimizing the security policy rules by performing any or a combination of reordering, grouping, updating, deleting, along with performing any other actions on one or more policy rules based on parameters, including, but not limited to, weights assigned to traffic attributes (e.g., source address, destination address, service, port information, among other such attributes), preference settings, priority settings for the policy rules, network traffic characteristics, network usage statistics, among other optimization parameters.

[0019] In the following description, numerous specific details are set forth in order to provide a thorough understanding of embodiments of the present disclosure. It will be apparent to one skilled in the art that embodiments of the present disclosure may be practiced without some of these specific details. Embodiments of the present disclosure include various steps, which will be described below. The steps may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor programmed with the instructions to perform the steps. Alternatively, steps may be performed by a combination of hardware, software, firmware and/or by human operators.

[0020] Embodiments of the present disclosure may be provided as a computer program product, which may include a machine-readable storage medium tangibly embodying thereon instructions, which may be used to program a computer (or other electronic devices) to perform a process. The machine-readable medium may include, but is not limited to, fixed (hard) drives, magnetic tape, floppy diskettes, optical disks, compact disc read-only memories (CD-ROMs), and magneto-optical disks, semiconductor memories, such as ROMs, PROMs, random access memories (RAMs), programmable read-only memories (PROMs), erasable PROMs (EPROMs), electrically erasable PROMs (EEPROMs), flash memory, magnetic or optical cards, or other type of media/machine-readable medium suitable for storing electronic instructions (e.g., computer programming code, such as software or firmware).

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0021] Various methods described herein may be practiced by combining one or more machine-readable storage media containing the code according to the present disclosure with appropriate standard computer hardware to execute the code contained therein. An apparatus for practicing various embodiments of the present disclosure may involve one or more computers (or one or more processors within a single computer) and storage systems containing or having network access to computer program(s) coded in accordance with various methods described herein, and the method steps of the disclosure could be accomplished by modules, routines, subroutines, or subparts of a computer program product.

[0022] In various embodiments, the article(s) of manufacture (e.g., the computer program products) containing the computer programming code may be used by executing the code directly from the machine-readable storage medium or by copying the code from the machine-readable storage medium into another machine-readable storage medium (e.g., a hard disk, RAM, etc.) or by transmitting the code on a network for remote execution. Various methods described herein may be practiced by combining one or more machine-readable storage media containing the code according to the present disclosure with appropriate standard computer hardware to execute the code contained therein. An apparatus for practicing various embodiments of the present disclosure may involve one or more computers (or one or more processors within a single computer) and storage systems containing or having network access to computer program(s) coded in accordance with various methods described herein, and the method steps of the present disclosure could be accomplished by modules, routines, subroutines, or subparts of a computer program product.

[0023] Various embodiments are described assuming rule optimization and/or dependency detection are performed in real-time responsive to the proposed addition of a new traffic flow policy rule to an existing set of policy rules. Those skilled in the art will appreciate, however, that rule optimization and/or dependency detection may also or alternatively be performed in the background.

[0024] Notably, while embodiments of the present disclosure may be described using modular programming terminology, the code implementing various embodiments of the present disclosure is not so limited. For example, the code may reflect other programming paradigms and/or styles, including, but not limited to object-oriented programming (OOP), agent oriented

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

programming, aspect-oriented programming, attribute-oriented programming (@OP), automatic programming, dataflow programming, declarative programming, functional programming, event-driven programming, feature oriented programming, imperative programming, semantic-oriented programming, functional programming, genetic programming, logic programming, pattern matching programming and the like.

[0025] If the specification states a component or feature "may", "can", "could", or "might" be included or have a characteristic, that particular component or feature is not required to be included or have the characteristic.

[0026] Exemplary embodiments will now be described more fully hereinafter with reference to the accompanying drawings, in which exemplary embodiments are shown. This disclosure may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. These embodiments are provided so that this disclosure will be thorough and complete and will fully convey the scope of the disclosure to those of ordinary skill in the art. Moreover, all statements herein reciting embodiments of the disclosure, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future (i.e., any elements developed that perform the same function, regardless of structure).

[0027] Thus, for example, it will be appreciated by those of ordinary skill in the art that the diagrams, schematics, illustrations, and the like represent conceptual views or processes illustrating systems and methods embodying this disclosure. The functions of the various elements shown in the figures may be provided through the use of dedicated hardware as well as hardware capable of executing associated software. Similarly, any switches shown in the figures are conceptual only. Their function may be carried out through the operation of program logic, through dedicated logic, through the interaction of program control and dedicated logic, or even manually, the particular technique being selectable by the entity implementing this disclosure. Those of ordinary skill in the art further understand that the exemplary hardware, software, processes, methods, and/or operating systems described herein are for illustrative purposes and, thus, are not intended to be limited to any particular named.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0028] Aspects of the present disclosure provide a method that can be implemented in a network security management device for automatically optimizing security policy rules in real-time based on traffic conditions or when one or more traffic rules are added/edited/deleted/modified. According to one embodiment, the method includes receiving, by the network security management device, a request to add a new traffic flow policy rule to a repository of existing control rules. In an aspect, such a request can either be manually generated by say a user/administrator or can be automatically generated based on traffic pattern/characteristics, network usage statistics, user activities, among other like actions. One should also appreciate that even though part of the disclosure has been explained with reference to new rules being added, the same systems/methods is also clearly applicable to any other action that needs to be taken place on existing set of traffic flow policy rules such as modification of one or more rules stored in rule repository or even deletion of one or more rules.

[0029] In an aspect, upon receipt of the request to add the new traffic flow policy rule, network security management device can be configured to automatically determine dependencies of the new traffic flow policy rule on one or more policy rules, and form an updated set of policy rules based on the determined dependencies. Methods of the present disclosure can further be configured to automatically optimize, by means of the network security management device, the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein such optimization of the updated set of policy rules can be performed based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

[0030] According to one embodiment, dependencies can be determined by means of evaluation of dependence in execution of the new traffic flow policy rule on one or more policy rules. In another aspect, grouping of the first sub-set of policy rules of the updated set of policy rules can include merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging can be conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination (IP) addresses, services, applications, interfaces, rule

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

tags, priorities, and parameters of the combinable policy rules. According to another embodiment, merging of the combinable policy rules can be conducted based on superneting of one or more of the source IP addresses and the destination IP addresses.

[0031] According to another embodiment, reordering a second sub-set of policy rules can include changing an order of policy rules of the second sub-set of policy rules based on one or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters. According to one embodiment, order of the policy rules of the second sub-set of policy rules can be changed based on frequency of usage thereof.

[0032] According to another embodiment, deleting a third sub-set of policy rules can include deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules. In an exemplary embodiment, the one or more conflicts can include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules. One or more conflicts can also include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule. According to one embodiment, when conflicts exist between a denied traffic flow and an allowed traffic flow, in order to avoid creating a potential security issue, the denied traffic flow will be placed before the allowed traffic flow. Alternatively, if an advantage exists, the allowed traffic flow can be split to suppress the denied traffic flow.

[0033] According to one embodiment, weights assigned to types of traffic can be defined manually based on scope and attributes of policy rule or can be defined automatically. According to another embodiment, formation of the updated set of policy rules can be conducted/performed based on the one or more weights, the preference settings, the priority settings for the policy rules, network traffic characteristics, and network usage statistics.

[0034] Aspects of the present disclosure also provide for a system for automatically optimizing security policy rules in real-time based on network traffic conditions/characteristics/usage in addition to when one or more traffic rules are added/modified. According to one embodiment, system of the present disclosure can include a business traffic flow input module configured to receive a request to add a new traffic flow policy rule to a

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

repository of existing policy rules managed by the system. The system can further include a dependency detection module configured to automatically determine dependencies of the new traffic flow policy rule on one or more policy rules, and a traffic flow policy rule incorporation module configured to form an updated set of policy rules by incorporating the new traffic flow policy rule within the policy rules based on the determined dependencies. System of the present disclosure can further include a policy rule optimization module configured to automatically optimize the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

[0035] FIG. 1 illustrates an exemplary security policy implementation architecture 100 in accordance with an embodiment of the present disclosure. In the context of the present simplified example, a protected network coupled to a public network 112 (e.g., the Internet) includes a firewall/flow control device 108, a policy rule database 110, an access point 106 and a local area network (LAN) 104 containing multiple end points 102-1, 102-2 and 102-3. When a system residing outside of the protected network attempts to communicate with a device on LAN 104 or when end points 102-1, 102-2 or 102-3 attempt to access network 112 or any resource within the network 112 through access point 106, a network security management device, (e.g., firewall/flow control device 108), which is configured to, among other things, monitor and/or filter traffic flow between end points 102 and network 112, determines whether the attempted access/communication is permitted by the enterprise security policy.

[0036] According to one embodiment, the enterprise security policy is represented by a set of rules (e.g., assess control lists (ACLs), traffic flow control rules, etc.) stored within policy rule database 110 that are used for filtering traffic flow (e.g., blocking or allowing packets between LAN 104 and network 112). Those skilled in the art will appreciate that policy rule database 110 may be separate from firewall/flow control device 108 or integral to firewall/flow control device 108.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0037] Those skilled in the art will appreciate, end points 102 may represent a variety of different operating environments. For example, end points 102 may include, but are not limited to, personal computers (PCs), end user workstations, server computers, mobile computer systems (e.g., hand-held devices, tablet computers, laptop devices), multiprocessor systems, microprocessor-based systems, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments and the like.

[0038] According to one embodiment, although the firewall/flow control device 108 in the present illustration is depicted as residing between access point 106 and network 112, in other example implementations, firewall/flow control device 108 may simply be logically interposed between end points 102 and network 112, and therefore various other network architectures/configurations are possible. In an aspect, the monitored network traffic can include, but is not limited to, HyperText Transfer Protocol (HTTP) traffic, File Transfer Protocol (FTP) traffic, Domain Name System (DNS) requests/responses, unclassified (e.g., unknown) or classified (e.g., known) application traffic and/or other types of traffic (e.g., traffic using other types of known or unknown protocols).

[0039] As explained earlier, existing firewall/flow control devices or network security management device use static policy rules to filter/block/allow traffic entering or leaving a protected network and once configured, the firewall/flow control device always searches through the same set of policy rules in the same hierarchical order. This hierarchical based execution of policy rules may delay the decision to allow/block the traffic and may impact the performance of the network. In a typical enterprise set-up, a firewall/flow control device can have thousands of policy rules, some of which may be generic policy rules that are applicable to all the traffic flow from/to network 112 and others of which may be specific to a set or range of source IP addresses, destination IP addresses, applications, ports and/or services. As discussed in the Background, increased network delays are observed for existing firewall/flow control devices or network security management devices when the matching rule of a rule base for the packet at issue is found lower in hierarchy as all policy rules placed higher in the hierarchy must be evaluated before evaluating those rules at the bottom of the hierarchy.

[0040] In order to address certain deficiencies of existing firewall/flow control devices, in an aspect, a network security management device (e.g., firewall/flow control device 108) can be

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

configured to implement systems and methods of the present disclosure and can be configured to optimize security policy rules in real-time based on traffic conditions or when one or more traffic rules within policy rule database 110 are added/edited/deleted/modified. According to one embodiment, network security device 108 can receive a request to add a new traffic flow policy rule to the rules stored in policy rule database 110, based on which firewall/flow control device 108 can be configured to automatically determine dependencies of the new traffic flow policy rule on one or more of the existing policy rules within policy rule database 110 and form an updated set of policy rules based on the determined dependencies. Firewall/flow control device 108 can then automatically optimize the updated set of policy rules grouping one or more policy rules of the updated set of policy rules, reordering one or more policy rules of the updated set of policy rules and/or deleting one or more policy rules of the updated set of policy rules, wherein such optimization of the updated set of policy rules can be performed based on various predetermined or configurable parameters, including, but not limited to, weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and/or network usage statistics for the policy rules of the updated set of policy rules. For example, if redundant rules are found in policy rule database 110 or rules that contradict each other are found in policy rule database 110 the redundancy or conflict can be proactively addressed by deleting one of the redundant or conflicting rules (e.g., manually, automatically or by a combination of manual and automated means).

[0041] As discussed in further detail below, in some embodiments, when a policy rule within policy rule database 110 is modified/amended, all other rules that are impacted by the amended rule can be automatically modified or deleted to maintain consistency with the modified rule. Similarly, when two or more rules are identified as being capable of being merged with each other by virtue of having the same source IP addresses, destination IP addresses, a common intended destination/department and/or any other relevant commonality, such rules can be automatically merged in the background or in real-time so as to avoid unnecessary growth in the size and complexity of policy rule database 110. According to one embodiment, validation and optimization functionality can be performed in the background to identify duplicate entries, mergeable entries, shadowed rules and other usual security rule based errors or sub-optimal configurations.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0042] According to another embodiment, firewall/flow control device 108 provides for dynamic reordering of policy rules within policy rule database 110 based on statistical data or weights assigned to one or more policy rules. Such dynamic reordering of the evaluation sequence of policy rules can be based on the most frequently used or the most recently used policy rule(s), for example. Such reordering will facilitate faster decision making by firewall/flow control device 108 as the rules observed to be used most frequently, for example, will be found faster as a result of being placed earlier in the search sequence of policy rule database 110. Typically, the policy rules will be reordered in accordance with administrator-defined criteria; however, in the absence of such criteria embodiments of the present invention may place less specific rules on top or very specific rules on top. Statistical analysis of the application/usage of existing policy rules may be used to select an appropriate default ordering approach.

[0043] Further, as security requirements change over time, network administrator and/or security provider may want to add new policy rules, in which case, the network security device 108 or any other network security management device (e.g., a firewall, a gateway, an intrusion prevention device, an intrusion detection device, a server, an integrated security appliance, a switch, a unified threat management (UTM) device, among others, can be configured to use the systems and methods of the present disclosure for creation and modification of firewall/access control policy rules so as to facilitate enhanced computing performance, rule management, policy optimization and/or session/network traffic packet flow management. In an aspect, firewall/flow control device 108 can be configured to use the method of present disclosure so as to overcome the limitation of existing static rule based policy by incorporating dynamic addition/modification of one or more policy rules and to create and optimize the new set of policy rules.

[0044] In an aspect, methods of the present disclosure can be used by firewall/flow control device 108 for implementation, execution, and management of policy rules, including but not limited to addition of one or more policy rules, modification of one or more existing policy rules, grouping/merging of one or more existing policy rules, reordering of one or more policy rules, and/or deletion of one or more policy rules in real-time or in the background, without impacting performance of network security device 108. Those skilled in the art will recognize the various

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

purposes of the optimization of flow control policy rules include, but are not limited to, increasing the efficiency of rule scanning/evaluation during packet filtering processing, optimizing storage of policy rule database 110, facilitating management of rules within policy rule database 110 and facilitating fast processing of packets received by firewall/flow control device 108.

[0045] According to one embodiment, firewall/flow control device 108 of the present disclosure can also be operatively coupled with a security service/server/software (not show), for example, using secure communications, such as encrypted communication techniques, to store parameters and/or attributes of incoming and outgoing network traffic packets (such as signatures, heuristics, application ID related information, packet attributes, user ID related information, content ID related information, and trusted/untrusted zone information). Based on heuristic/statistical information regarding such parameters and/or attributes, new flow control policy rules may be automatically conceived/generated and added to policy rule database 110. As another example, firewall/flow control device 108 can communicate with the service (e.g., using secure communications, such as encrypted communication techniques) to provide monitored traffic information (e.g., potential malware samples, such as in the form of subsets of such monitored traffic information, such as a portion of the packet flow, monitored Universal Resource Locator (URL)/DNS information, monitored files requested for upload/download/access, and/or other information, along with possibly other information, such as content information for the client device associated with the traffic flow and possibly user identification and/or application identification information as well), and the service can perform additional real-time and or post analysis (e.g., additional heuristic analysis as described herein with respect to various embodiments for detecting malware, including new malware threats and zero-day attacks, and/or to compare to other samples received and analyzed for other customers of the security cloud service).

[0046] FIG. 2 illustrates exemplary functional modules of a network security policy management system 200 in accordance with an embodiment of the present disclosure. In the context of the present example, system 200 includes a business traffic flow input module 202, a dependency detection module 204, a traffic flow policy rule incorporation module 206 and a policy rule optimization module 208.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0047] In one embodiment, business traffic flow input module 202 can be configured to receive a request to add a new traffic flow policy rule to a repository of policy rules managed by system 200. Such a request can either be generated automatically or can be manually generated by the user/administrator of the network. In another aspect, business traffic flow input module 202 can also be configured to receive a request relating to modification of an existing stored policy rule, wherein the modification can either be suggested by the administrator or can proposed automatically based on observed traffic patterns (e.g., source/destination IP address patterns), protocols being used, rule hits, types of prevalent attacks, frequency of attacks, changes in organization policy, among other like factors. For example, responsive to observing that one or more policies of a rule base have been unused over a configurable or predetermined period of time, a warning may be provided to the network administrator along with one or more suggested changes to be made to the rule base (e.g., removal or editing of such rules). For example, rules or objects (e.g., addresses or services) that are unused for a long period of time may be recommended for removal or, for performance reasons, the traffic flows containing the unused object may be automatically reordered to place them on the bottom of the security policy. If the unused rules or objects are removed (rather than reordered), in one embodiment, a new security policy optimization is performed.

[0048] According to one embodiment, business traffic flow input module 202 can be configured to receive one or more traffic flow policy rules corresponding to a traffic policy control requirement of the business. For example, the enterprise may desire that some traffic be processed faster or given priority over other types of traffic (e.g., a Voice over Internet Protocol (VoIP) provider might choose to have voice sessions be given a higher priority than management sessions). The traffic flow policy rules received by business traffic flow input module 202 may represent new policy rules that needs to be created and added to the policy rule database and can be defined by means of a traffic policy control requirement given as input by a user/administrator. The traffic policy control requirement can be received by a user/administrator in a defined yet flexible format such that the user/administrator may not need to be aware of the already existing policy rules or about the constraints/conflicts that the addition of the new policy rule might create. Adding one or more new policy rules or editing or deleting some preexisting policy rules can have ripple effects on other existing policy rules. As a new policy rule needs to be added and incorporated with the preexisting set of policy rules, automated

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

checks for dependency and shadowing may be implemented by business traffic flow input module 202 or one or more other functional units within system 200.

[0049] In another aspect, dependency detection module 204 can be configured to automatically determine dependencies of a new traffic flow policy rule on one or more existing policy rules. In an aspect, dependency detection module 204 can be further configured to evaluate dependence in execution of the new traffic flow policy rule on one or more existing policy rules. In an example implementation, a dependency can be established between policy rules if one policy rule (R1) partially or completely shadows another policy rule (R2) such that execution of rule R1 directly or indirectly impacts the rule R2. According to one embodiment, two rules are dependent if they mutually exhibit a precedence relationship. Such a dependency may not necessarily be detrimental or contradictory to the execution of rule R1, but may overlap with and/or depend on R2. For instance, rules R1 and R2 may be dependent on each other when they are not disjoint such that R2 cannot be moved before R1 without violating semantic integrity of the rule set. Dependency detection module 204 can therefore be configured to detect whether the newly proposed policy rule (one or more traffic flow policy rules) depends, for its execution, on any preexisting policy rule, so as to understand relationships between the newly proposed policy rule and the stored policy rules.

[0050] In another instance of dependency detection, consider two rules as follows: rule 1 permits packets with characteristic A (source address, for example) and rule 2 denies packets with characteristic B (destination address, for example). A packet with a profile matching both characteristics (from A to B in this case) will match both rules. In such a case therefore, the rules are dependent. In an aspect, dependency can be determined by means of multiple methods. For example, a rule can be selected, e.g., rule 1, for determining whether other rules in a policy rule database (e.g., policy rule database 110) depend on it. In selecting the rule, match types and associated values that would be used to filter packets can be identified, wherein match types are characteristics of packets that are used for comparison to a rule. Packet characteristics can include, for example, the protocol, port, originating IP address, destination IP address, etc. For example, a match type may be "protocol" and the value is "TCP." The rule might also have a match type "port" with a value of "20." The rule might also have a match type "IP" with a value of "123.45.67.89." One of ordinary skill in the art will recognize that a match type may be any

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

characteristic associated with the profile of a packet. A second rule, e.g., rule 2, may then be selected for comparison to rule 1. In selecting the second rule, again match types and associated values that would be used to filter packets may be identified for that rule. The match types of rule 1 can then be compared to rule 2 such that if rule 1 and rule 2 have at least one of the same match types, the values of each of the match types of rule 1 and rule 2 are compared. If all of the match types have different values than their corresponding match types in rule 2, rule 1 and rule 2 may be determined to be order independent. If rule 1 and rule 2 have at least one match type that is not in common, or if at least one match type of rule 1 shares the same value as the corresponding match type in rule 2, or if at least one of the match type of rule 1 is included (e.g., IP address and subnet) on the corresponding match type in rule 2, or or if at least one of the match type of rule 2 is included (e.g., IP address and subnet) on the corresponding match type in rule 1, rule 1 and rule 2 may be determined to be order dependent. This background process can be repeated until each pair of rules has been compared.

[0051] In another aspect, traffic flow policy rule incorporation module 206 can be configured to form an updated set of policy rules by incorporating the new traffic flow policy rule within the policy rules based on the determined dependencies, if any. In an implementation, traffic flow policy rule incorporation module 206 can either be configured to simply incorporate the new traffic flow policy rule into the policy database and leave the dependencies to be evaluated and handled later, or it can be configured to handle the dependencies and accordingly add or remove one or more existing traffic flow policy rules to/from the policy rules database. For instance, the position at which a new traffic flow policy rule is added to the database and the level at which it would be executed can be based on the dependencies computed by dependency detection module 204. Furthermore, an order of the new rule in the existing repository of flow control policy rules can also be accounted for while forming the updated set of policy rules. In an exemplary implementation, when the new rule is found to be dependent on another rule stored in the repository, both the rules can be assigned the same equivalence class.

[0052] In another aspect, policy rule optimization module 208 can be configured to automatically optimize the updated set of policy rules by grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules and/or deleting a third sub-set of policy rules of the updated set of policy rules

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

based on weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and/or network usage statistics for the policy rules of the updated set of policy rules.

[0053] According to one embodiment, grouping policy rules includes identifying potentially combinable policy rules associated with similar allowed flows (e.g., only different sources, only different destinations or only different services) and merging the identified combinable policy rules into a single policy rule. The merging can also be conducted based on matching of source IP addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities and/or parameters of the policy rules. In some embodiment, identifying potentiall combinable policy rules can be based on IP supernetting of the source IP addresses and/or the destination IP addresses. For example, a first traffic flow from source 192.168.0.0/24 to destination 1.1.1.1:80 and a second flow from source 192.168.1.0/24 to destination 1.1.1.1:80 can be merged into a new flow from source 192.168.0.0/25 to destination 1.1.1.1:80. In an instance, multiple parameters of the rule space, including, but not limited to, source, destination, user, service, enterprise firewall ID, and other such parameters can be used to identify rules that may interact or be combinable.

[0054] As a specific non-limiting example for purposes of illustration, assume there are three FTP rules that are candidates for combination, including rules allowing FTP traffic from trusted sources trusted.com and reliableco.com. In various embodiments, these trusted sources would be identified by an IP address or an IP address range. In the context of the present example, rules for both trusted sources allow FTP traffic, but require a virus scan to be performed. A third rule allows FTP traffic from all other sources except for "put" functions that may be used to upload a file. This rule allows unknown sources to log on and download, but not upload, files. As such, no antivirus scan is required for the third rule. While it is evident that the first two rules can be easily combined as they are identical except for a single parameter that does not overlap or interact in identifying two different connection sources, the third rule is distinctly different. Further, the order of the third rule is important, as the rule should be processed only after the first two rules, so that the trusted sources are allowed to FTP and "put" files to the servers protected by the firewall. Adding the third rule to the other two to form a combined rule or otherwise modifying the first two rules based on the third will result in firewall

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

behavior not intended by the administrator for at least some connections. In this example, it may be acceptable to allow FTP access including upload capability for all users, requiring anti-virus scanning for uploads only. The administrator may deem this a reasonable risk to take, or may decide the change to rule set functionality is unacceptable and only allow combination of the first two rules while declining to allow the third rule to be combined with the first two. In an aspect, whether two or more rules can be grouped/merged is determined by examining whether the rules at issue differ in relation to only a single parameter (e.g., source, destination, service), in which case, they are identified as capable of being grouped/merged. In another aspect, whenever possible, rules are grouped by superneting. If two rules differ in two or more elements/parameters, they may be grouped/reordered in such a way that results in more hits in one of the generated rules. Meanwhile, if the scope of one rule is contained entirely by the scope of another rule, the narrower rule may be deleted and the broader rule may be retained.

[0055] In an example implementation, merging of policy rules can be implemented based on superneting of one or more of the source IP addresses and the destination IP addresses, i.e. applying a single policy rule for IP addresses belonging to same class of IP addresses. In an example implementation, one or more parameters can be used to determine the group-able/merge-able policy rules. For example, if two rules differ in just one element (e.g., source, destination, service), they can be grouped together. Similarly, the policy rules applied for a group of network elements can be grouped by superneting. In an example implementation, when the scope of one policy rule is "contained" in another policy rule or all the security checks of the one policy one rule are covered by a broader security rule, then both rules can be merged into the policy rule having broader scope.

[0056] Those skilled in the art will appreciate that policy rule optimization module 208 can also be configured to demerge one or more rules to make them separate in case their order, for instance, plays an important role in deciding how the traffic packets are to be processed, and therefore, although the functions of deletion, grouping, and re-ordering have been mentioned above, any other function that enables optimization of the updated set of rules is completely within the scope of the present disclosure.

[0057] According to one embodiment, reordering of policy rules can include changing an order of policy rules based on their respective source IP addresses, destination IP addresses,

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

network usage statistics, applications, interfaces, rule tags, priorities and/or parameters. In an example implementation, the order of policy rules may be changed based on frequency of past usage, a manual priority set according to the business needs and/or other predefined or dynamically determined criteria. For example, a policy rule that is observed to be used the most frequently can be reordered to be executed first. In an example implementation, a dynamic priority can be assigned to each policy rule and the order of execution can therefore be dynamically changed. In an example implementation, if one policy rules is dependent upon another, then their relative order of execution will be preserved.

[0058] According to one embodiment, deletion of a policy rule or recommendation of deletion of a policy rule to the administrator is as a result of identifying one or more conflicts among policy rules. Conflicts include, but are not limited to, existence of a duplicate policy rule and existence of a policy rule that is contrary to a new traffic flow policy rule, for example. According to one embodiment, new rules may subsume or negate previous rules, or conflicting rules may be present in the rule set. Depending upon the particular implementation, optimization module 208 can be configured to simply bring to the attention of the administration policy rules that have been identified to be in conflict so that the administrator can select which of the rules to apply, what order the rules should be applied, or whether to merge the rules into a single rule if appropriate. In an alternative embodiment, optimization module 208 may implement changes to the policy rule database and maintain a log of changes to allow an administrator to selectively undo certain optimizations and/or revert to a prior state of the policy rule database if desired. When statistical data (e.g., frequency of execution during one or more particular time frames) is tracked and maintained relating to execution of policy rules, optimization module 208 may provide a warning to the administrator regarding any unused policies, suggest changes (e.g., removal, editing or reordering of an unused policy) and/or automatically implement and log changes to the policy rule database deemed to be appropriate.

[0059] Depending upon the particular implementation, the updated set of policy rules may be defined dynamically based on the scope and attributes of policy rules and weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and/or network usage statistics based on automatic or manual criteria, at any given time, with or without administrator intervention. In an aspect, assignment of weights to types of traffic can be

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

conducted manually or automatically or a combination thereof based on scope and/or attributes of the policy rule. In an example implementation, each policy rule can be assigned a dynamic priority/weight for its hierarchical execution. While reordering policy rules, dynamic priority can be used to define the execution order of policy rules. Policy rules can be executed in hierarchical/sequential manner according to their priority such that policy rules with highest priority is executed before execution of policy rules of comparatively lower priority. The priority can be assigned by the user/administrator or can be automatically determined based on statistical and/or historical data regarding the actual use of the policy rules. In an example implementation, an updated set of policy rules can be executed in parallel or in sequence based on the one or more weights assigned, the preference settings, the priority settings for the policy rules, network traffic characteristics, and network usage statistics, among other attributes/parameters.

[0060] Depending upon the particular implementation, network security policy management system 200 may be implemented separately from or integrated within a network security device, for example, comprising one or more processors, a communication interface mechanism, one or more internal data storage devices operatively coupled to the one or more processors and storing policy rule optimization module 208 configured to retrieve a set of policy rules and optimize the retrieved set of policy rules.

[0061] According to one embodiment, policy rule optimization module 208 can also be configured to run on a periodic basis or when one or more optimization parameters are defined/modified so as to ensure that at any given moment, the policy rules are optimally ordered, grouped and managed. Policy rule optimization module 208 may also or alternatively be manually initiated by the network administrator or automatically initiated upon detection of one of a set of predefined events (e.g., a change to the policy rule database or a change to defined business flows, expressing the relative priorities of various types of traffic within the enterprise, for example).

[0062] In an example implementation, network security policy management system 200 can have a front end interface module (not shown) that can be used by user/administrator to create and/or upload one or more new security policy rules. Other modules of the present system can run in the background for validation and optimization of updated policy rules that would

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

identify duplicate entries, merge-able entries, shadowed rules and other usual security rule based errors or non-optimized configurations. Optimization module 208 can, periodically or dynamically or based on user-defined actions, create an optimized version of the policy rules that would effectively reduce the size of the actual security policy being executed by the firewall/flow control device/ network security management device. For example, the network security device may calculate whether the creation of one or more explicit denied flows might be advantageous in connection with reducing the security policy size. In an exemplary embodiment, policy rule optimization module 208 can also reorder security policies based on customer business drivers, thereby reducing the initial rule matching time for network traffic so as to increase the performance of the security system based on automatic and/or user defined criteria. Thus, flow control policy rules can be reordered and/or rebuilt/modified dynamically based on automatic and/or manual criteria at any given time, with or without user intervention.

[0063] In an exemplary implementation, proposed changes to the policy rule database may be brought to the attention of the user/administrator via the frontend interface for further modification and/or confirmation before taking affect. Alternatively, confirmation of optimized policy rules may not require to be confirmed/approved by any user/administrator prior to being implemented and taking affect.

[0064] In accordance with embodiments of the present invention, creation and/or ordering of optimized policy rules can be based on various criteria, including, but not limited to, performance (e.g., rule hits), business flows (e.g., to guarantee one or more types traffic are processed faster) and/or statistical analysis of the actual policy rules being used. The security policy can also self-adjust automatically over time in order to improve performance and further reduce delay for new session establishment.

[0065] In an exemplary implementation, network security policy management system 200 may generate a warning if a rule remains unused over a predetermined or configurable period of time. Network security policy management system 200 may alternatively or additionally suggest re-ordering of rules within the policy rule database (e.g., moving unused or infrequently used rules to the end) or removal of unused rules. Network security policy management system 200 can also be configured to simplify management of policy rules so as to allow the administrator to focus his/her attention on traffic flows that reflect particular business needs. For example,

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

because network security policy management system 200 will take care of evaluating and creating a valid, effective, efficient and optimized security policy, the administrator no longer needs to check the complete rule base before making any changes. In an aspect, higher priority rules can also be identified and re-ordered and/or categorized in order to optimize packet filtering. In another embodiment, priorities of optimization parameters (e.g., network traffic characteristics, source/destination IP addresses, frequency/time aspects of packets, type of traffic, among others) can also be configured/changed based on usage/context/organization policies/objectives. For example, some enterprises may value (and therefore prioritize) increased performance in initial session establishment (e.g., as a result of reordering of rules based on frequency of execution or based on whether they specify one or more specific IP addresses or are subnet based) over a more compact rule set (e.g., as a result of merging rules).

[0066] FIG. 3A illustrates an exemplary representation 300 showing a snapshot of a simplified security policy, and FIG. 3B shows addition of a new security policy rule 399 to the security policy in accordance with an embodiment of the present disclosure. In the present example, representation 300, includes a Host/Network column 310, identify the source host/network(s) with which the policy rule is associated, a Peer Host/Network column, identifying the destination/target peer host/network(s) with which the policy rule is associated, a Ports column 330, identifying particular ports on which the traffic is allowed, a Business Case/tag column 340, identifying a project with which the corresponding policy rule is associated, and a rule ID/seq column 350, potentially indicating an order in which the policy rules are applied. Those skilled in the art will appreciate the exemplary functional modules described herein are for purposes of illustration only and that the functionality described with reference to various of the exemplary functional modules may be combined and/or distributed differently.

[0067] FIG. 3A illustrates a simplified example of preexisting flow control security policy rules having rule identifiers (IDs) 350 ranging from 1 to 15 and representing different policy rules that are defined/configured by the user/administrator/system in order to filter incoming/outgoing traffic/packet/connection requests from/to the network. Rule IDs 350 can also indicate the sequence in which the processing of the network traffic takes place, wherein the traffic would first pass through the entries/flows associated with sequence ID 1 and then to 2 and

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

so on. As can be seen, each rule ID 1-15 can be implemented for one or more projects that correspond to respective business cases/tags 340. Each project can also be associated with multiple sessions between source host and destination/peer host.

[0068] As can be seen in the present example, entry 301a of policy rule 301 relates to all traffic/packet/connection requests sent from host 10.184.17.0/26 to peer host/network 10.135.32.0/26, which, can be sent on any of the ports, wherein the interaction between the source-destination relates to a project referred to as "Initial Project." Similarly, in accordance with entry 303a of policy rule 303, traffic can be sent from buss-server02 to 10.135.35.121 on ports 3315/TCP, 3380/TCP, 3366/UDP, and 3390/TCP. While representation 300 FIG. 3A only shows twenty-one entries representing twelve policy rules, those skilled in the art will appreciate, in practice, there can be hundreds of such entries.

[0069] FIG. 3B illustrates a new rule 399 created by user/administrator, which needs to be incorporated with the existing policy rules of FIG. 3A. New rule 399 may be used for traffic analysis and monitoring of traffic flow, for example, between buss-fe01 and 10.135.35.0/24 through port TCP-1024. Prior to incorporation of new rule 399 into the existing policy rules, various initial checks may be performed to identify policy rules within the existing policy rule database upon which new rule 303 may be dependent, identify duplicate/overlapping/dependent/shadowing rules and/or determine the relative priority of new rule 399, based on which new rule 399 can be incorporated into the policy rule database. Since the project ("Web-API-Integration") with which new rule 399 is associated is business critical, it will be given high priority which should be reflected during reordering of the policy rules.

[0070] If the flow represented by new rule 399 is expected to have many sessions and in view of its high priority, the administrator, without the benefit of performing a detailed analysis of the security policy, may manually create the following flawed security rule entry on top of the security policy represented in FIG. 3A:

Host/Network	Peer Host/Network	Ports	Business Case/tag	rule ID/seq
buss-fe01	10.135.35.0/24	TCP-1024	web_API integration	1

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

[0071] In existing systems, with the insertion of this new rule, the sequence numbers of subsequent rules would be incremented by one. With this change, the newly defined traffic flow would have the highest priority in relation to new session matching processing, but the security policy may effectively shadow part of rule 305, and allow traffic that should be denied by rule 311, thus creating unnecessary processing on rule 305 and allowing a traffic flow that should have been denied by rule 311. Since traffic meeting rule 311 (which should be denied) is allowed in accordance with the present example, it is unlikely anyone would complain (as end users typically only notice the denial of traffic they desire to be allowed), but a security issue has been created by the introduction of a flawed security rule.

[0072] In accordance with embodiments of the present invention, on the other hand, without analyzing the security policy, the administrator can instruct the security system to create a flow with the characteristics of new rule 399 without concern as network security policy management system 200 would automatically evaluate the existing security policy and reach the following conclusions:

a. Since the priority associated with new rule 399 is high, new rule 399 needs to be placed on top;

b. Rule 305 also matches this flow for traffic originating on host buss-fe01. If a new rule is created on top, then part of rule 305 is unnecessary, so rule 305 should be automatically revised; and

c. Rule 311 is in conflict with part of the flow required for new rule 399. Since rule 311 is a deny rule, a warning should be issued to the administrator pointing out the conflict; and

    i. If the flow-denial of rule 311 is to be maintained, rule 311 should be moved to a position with a smaller seq# than new flow 399. Alternatively, if rule 311 is to be "forgotten" due to the higher priority of new flow 399, then rule 311 should be removed.

[0073] FIG. 4 illustrates an exemplary snapshot of a security policy rule management system interface 400 in accordance with an embodiment of the present invention. The snapshot 400 illustrates an exemplary frontend/administrator interface for management of security policy

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

rules. According to one embodiment, system interface 400 can present a user/administrator with various options for managing one or more policy rules including, but not limited to, viewing policy rules, adding new policy rules, searching for policy rules, checking dependencies of one or more rules, deleting/modifying/re-ordering and optimizing policy rules. In an aspect, a user/administrator, by means of viewing policy rules, can also add new policy rules to the existing set of flow control policy rules, analyze performance of current rules, view traffic pattern/attributes/characteristics, and manage conflicts/modification of rules. In another aspect, the administrator can also check dependency in order to view automatically identified dependencies that any rule has on the other set of rules that form part of the rules repository. In yet another aspect, based on a selected optimization criteria (e.g., optimization based on priority verses optimization based on traffic statistics) dependencies, traffic related attributes, weights of different types of policy rules, organizational policies, among other parameters, the administrator can also enable optimization of the policy rules.

[0074] In yet another embodiment, as shown in FIG 4, optimization can either take place for all the flow control policy rules or can be performed automatically for a defined number interlinked/selected/related rules. In yet another embodiment, through the "optimize policy rules" option, the administrator can also select and/or define criteria to be used for optimization, define policy settings to be adopted for optimization, assign weights to different policy rules, enable usage statistics to be incorporated during optimization, define priority of one or more rules, enable traffic attributes/characteristics to be incorporated along with the defining, say the technology required for security policy implementation.

[0075] In yet another embodiment, through the "optimize policy rules" option a user/ administrator can select and define group policy rules through which the system can either through manual intervention or automatically, arrange new and/or existing policy rules into groups. Such an option can allow automatic merging of possible flow control policy rules or creating of new rules that relate to subnets and not to individual IP addresses, for instance.

[0076] In yet another embodiment, through the "optimize policy rules" option, the administrator can enable all or part of the policy rules to be re-ordered, leading to, for instance, higher priority rules or more frequently referred rules to be brought up the hierarchy for faster access when compared with lower priority rules. Any other basis such as most accessed rules

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

can also be applied for re-ordering or re-arranging one or more policy rules. In yet another embodiment, through the "optimize policy rules" option a user/ administrator can enable deletion of one or more rules based on, for instance, duplicate/redundant rules, conflicting rules (that act differently for same source-destination packet for instance). One should appreciate that the various options illustrated through security policy rule management system interface 400 are completely exemplary in nature and all other options for management of policy rules are within the scope of present disclosure.

[0077] FIGs. 5A, FIG. 5B and FIG. 5C illustrate exemplary policy rules 500 stored in a policy rule database along with dependencies and possible groupings detected in accordance with an embodiment of the present invention. FIG. 5A illustrates an exemplary representation 500 having multiple policy rules, specifying actions to be taken by a network security device for specific services between specific sources and specific destinations. For instance, as can be seen, traffic from 192.168.0.0/24 to any destination is allowed for Domain Name System (DNS), HyperText Transfer Protocol (HTTP), and HTTP Secure (HTTPS) packets and the priority of such packets is Normal. The exemplary representation 500 of FIG. 5A also shows, for instance, the number of sessions impacted by each policy rule over a given time period and the corresponding percentage of sessions of the total number of sessions during the given time period.

[0078] FIG. 5B illustrates the policy rules 500 of FIG. 5A with a "Dependencies" column annotating various automatically identified dependencies among the policy rules 500. For instance, as the policy rule at index 7 blocks any traffic from 192.168.3.2 to 192.168.0.0/16, the execution order of the policy rule at index 6 rule depends on the policy rule of index 7. Similarly, as the policy rule of index 8 applies to all traffic from 192.168.3.2 to any destination, the policy rule at index 7 shadows the policy rule at index 8.

[0079] FIG. 5C illustrates how potential policy rules that can be merged/grouped can be identified and represented. For instance, the column "Dependencies B" includes annotations indicating that the policy rule at index 1 and the policy rule at index 2 rule can be partially merged together as they have the same source-destination pairs/priority and only differ in the type of service they allow to pass, and therefore, if merged, they can allow a combined traffic for DNS, HTTP, HTTPS, and SMTP. Similarly, the policy rule at index 8 can also be partially

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

merged with the policy rule at index 2, wherein post merger, the priority of the policy rule at index 2 can either be set to High or can be kept at Normal as specified manually by the administrator or determined automatically based on one or more of the weight of each rule, traffic characteristics, among other defined set of parameters.

[0080] FIG. 5D illustrates an optimized version of the security policy that seeks to optimize performance based on traffic statistics gathered by the flow control device in accordance with an embodiment of the present disclosure. As shown, the updated policy rule set has a policy rule at index 1 resulting from a partial merger of former policy rules associated with index 1 and index 2 of FIG. 5C, with the source being 192.168.0.0/23 and allowing issuance of packets to all destinations using DNS, HTTP and/or HTTPS services. The representation of FIG. 5D further shows the former policy rule associated with index 6 having been reordered to now be associated with index 2, and the former policy rule associated with index 7 being reordered to now be associated with index 3 as the volume of hits for this policy rule 3 are relatively high (50000 sessions). Similarly, a new policy rule associated with index 4 is a partial merger of the former policy rule associated with index 2 and the former policy rule associated with index 8, and a new policy rule at index 5 represents a reordered version of the former policy rule associated with index 4. Likewise, policy rule at index 7 has been put toward the end as the number of sessions/hits for this transaction (192.168.3.1 to 192.168.1.80 over HTTP) is low.

[0081] FIG. 5E illustrates an alternative optimized version of the security policy that seeks to optimize performance based on administrator-defined traffic priority in accordance with an embodiment of the present disclosure. As shown, the optimized policy rule set reflects, among other things, movement of former policy rule associated with index 6 in FIG. 5C to index 2. As former policy rule associated with index 7 in FIG. 5C had a high number of hits/sessions, that former policy rule has been moved to index 3, and the new policy rule at index 4 represents the partial merger of former policy rules associated with index 2 and 8 in FIG. 5C.

[0082] Those skilled in the art will appreciate that the two previously described optimization scenarios are merely exemplary and are based on a defined set of administrator-defined and/or system maintained parameters. In alternative embodiments, policy rules may be selected and evaluated with respect to their hits/session/frequency of use, potential of merger to

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

reduce the overall number of rules and/or potential for making the database light and efficient, along with considering other parameters discussed above to reorder the rule database.

[0083] FIG. 6 illustrates an exemplary flow diagram 600 for optimization of policy rules in a rule database in accordance with an embodiment of the present disclosure. At step 602, a network security management device receives a request to add a new traffic flow policy rule to an existing set of policy rules. In an aspect, such a request can either be manually generated by say a user/administrator or can be automatically generated based on traffic pattern/characteristics, network usage statistics, user activities, among other like actions.

[0084] At step 604, upon receipt of the request to add the new traffic flow policy rule, the network security management device automatically determines dependencies of the new traffic flow policy rule in relation to one or more of the existing policy rules. At step 606, an updated set of policy rules based on the determined dependencies can be created/generated, and at step 608, the updated set of policy rules can be automatically optimized by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules, wherein such optimization of the updated set of policy rules can be performed based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

[0085] According to one embodiment, dependencies can be determined by means of evaluation of dependence in execution of the new traffic flow policy rule on one or more policy rules. In another aspect, grouping of the first sub-set of policy rules of the updated set of policy rules can include merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging can be conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination (IP) addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules. According to another embodiment, merging of the combinable policy rules can be conducted based on superneting of one or more of the source IP addresses and the destination IP addresses.

[0086] According to another embodiment, reordering a second sub-set of policy rules can include changing an order of policy rules of the second sub-set of policy rules based on one or

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters. According to one embodiment, order of the policy rules of the second sub-set of policy rules can be changed based on frequency of usage thereof.

[0087] According to another embodiment, deleting a third sub-set of policy rules can include deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules. In an exemplary embodiment, the one or more conflicts can include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules. One or more conflicts can also include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule.

[0088] According to one embodiment, weights assigned to types of traffic can be defined manually based on scope and attributes of policy rule or can be defined automatically. According to another embodiment, formation of the updated set of policy rules can be conducted/performed based on the one or more weights, the preference settings, the priority settings for the policy rules, network traffic characteristics, and network usage statistics.

[0089] While embodiments of the present disclosure have been illustrated and described, it will be clear that the present disclosure is not limited to these embodiments only. Numerous modifications, changes, variations, substitutions, and equivalents will be apparent to those skilled in the art, without departing from the spirit and scope of the present disclosure, as described in the claims.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

CLAIMS

What is claimed is:

1. A method comprising:

receiving, by a network security management device, a request to add a new traffic flow policy rule to a plurality of policy rules managed by the network security management device;

automatically determining, by the network security management device, dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules;

forming, by the network security management device, an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules based on the determined dependencies;

automatically optimizing, by the network security management device, the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules.

2. The method of claim 1, wherein said determining dependencies comprises evaluating dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules.

3. The method of claim 1, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging is conducted based on matching of one or more of source Internet Protocol (IP) addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

4. The method of claim 3, wherein the merging of combinable policy rules is conducted based on superneting of one or more of the source IP addresses and the destination IP addresses.

5. The method of claim 1, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of policy rules based on one or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters.

6. The method of claim 5, wherein the order of the policy rules of the second sub-set of policy rules is changed based on frequency of usage thereof.

7. The method of claim 1, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules.

8. The method of claim 7, wherein the one or more conflicts include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules.

9. The method of claim 7, wherein the one or more conflicts include one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule.

10. The method of claim 1, wherein the one or more weights are defined manually based on scope and attributes of policy rule.

11. The method of claim 1, wherein the one or more weights are defined automatically.

12. The method of claim 1, wherein said forming an updated set of policy rules is conducted based on the one or more weights, the preference settings, the priority settings for the policy rules, network traffic characteristics, and network usage statistics.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

13. A network security policy management system comprising:

one or more processors; and

one or more internal data storage devices operatively coupled to the one or more processors and storing:

a business traffic flow input module configured to receive a request to add a new traffic flow policy rule to a plurality of policy rules managed by the system;

a dependency detection module configured to automatically determine dependencies of the new traffic flow policy rule on one or more of the plurality of policy rules;

a traffic flow policy rule incorporation module configured to form an updated set of policy rules by incorporating the new traffic flow policy rule within the plurality of policy rules based on the determined dependencies; and

a policy rule optimization module configured to automatically optimize the updated set of policy rules by one or more of grouping a first sub-set of policy rules of the updated set of policy rules, reordering a second sub-set of policy rules of the updated set of policy rules, and deleting a third sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and network usage statistics for the policy rules of the updated set of policy rules.

14. The system of claim 13, wherein the dependency detection module is further configured to evaluate dependence in execution of the new traffic flow policy rule on one or more of the plurality of policy rules.

15. The system of claim 13, wherein said grouping the first sub-set of policy rules of the updated set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging is conducted based on matching of one or more of source IP addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

16. The system of claim 15, wherein the merging of combinable policy rules is conducted based on superneting of one or more of the source Internet Protocol (IP) addresses and the destination IP addresses.

17. The system of claim 13, wherein said reordering the second sub-set of policy rules comprises changing an order of policy rules of the second sub-set of policy rules based on one or more of their source IP addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters.

18. The system of claim 13, wherein said deleting the third sub-set of policy rules comprises deleting the policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the updated set of policy rules.

19. The system of claim 18, wherein the one or more conflicts include existence of a duplicate policy rule in the policy rules of the third sub-set of policy rules and the updated set of policy rules.

20. The system of claim 18, wherein the one or more conflicts comprise one or more policy rules of the updated set of policy rules that are contrary to the new traffic flow policy rule.

21. The system of claim 13, wherein the one or more weights are defined manually based on scope and attributes of the policy rule.

22. The system of claim 13, wherein the one or more weights are defined automatically.

23. A network security policy management system comprising:

one or more processors; and

one or more internal data storage devices operatively coupled to the one or more processors and storing a policy rule optimization module configured to retrieve information regarding a current set of policy rules and optimize the current set of policy rules by one or more of grouping a first sub-set of policy rules of the current set of policy rules, reordering a second sub-set of policy rules of the current set of policy rules, and

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

deleting a third sub-set of policy rules of the current set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics, and usage statistics for each policy rule of the current set of policy rules.

24. The system of claim 23, wherein said grouping the first sub-set of policy rules comprises merging combinable policy rules of the first sub-set of policy rules into a single policy rule, wherein the merging is conducted based on matching of one or more of source IP addresses, destination IP addresses, services, applications, interfaces, rule tags, priorities, and parameters of the combinable policy rules.

25. The system of claim 23, wherein said reordering the second sub-set of policy rules comprises changing an order of the policy rules of the second sub-set of policy rules based on one or more of their source Internet Protocol (IP) addresses, destination IP addresses, network usage statistics, applications, interfaces, rule tags, priorities, and parameters.

26. The system of claim 23, wherein said deleting the third sub-set of policy rules comprises deleting policy rules of the third sub-set of policy rules based on one or more conflicts between policy rules of the third sub-set of policy rules and the retrieved set of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

ABSTRACT

[0090] Methods and systems for dynamically optimized rule-based security policy management are provided. A request is received by a network security management device to add a new traffic flow policy rule to multiple existing policy rules managed by the network security management device. Dependencies of the new traffic flow policy rule on the existing policy rules are automatically determined. An updated set of policy rules is formed by incorporating the new traffic flow policy rule within the existing policy rules based on the dependencies. The updated set of policy rules is then optimized by grouping, reordering and/or deleting a sub-set of policy rules of the updated set of policy rules based on one or more of weights assigned to particular types of traffic, preference settings, priority settings, network traffic characteristics and usage statistics for each policy rule of the updated set of policy rules.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

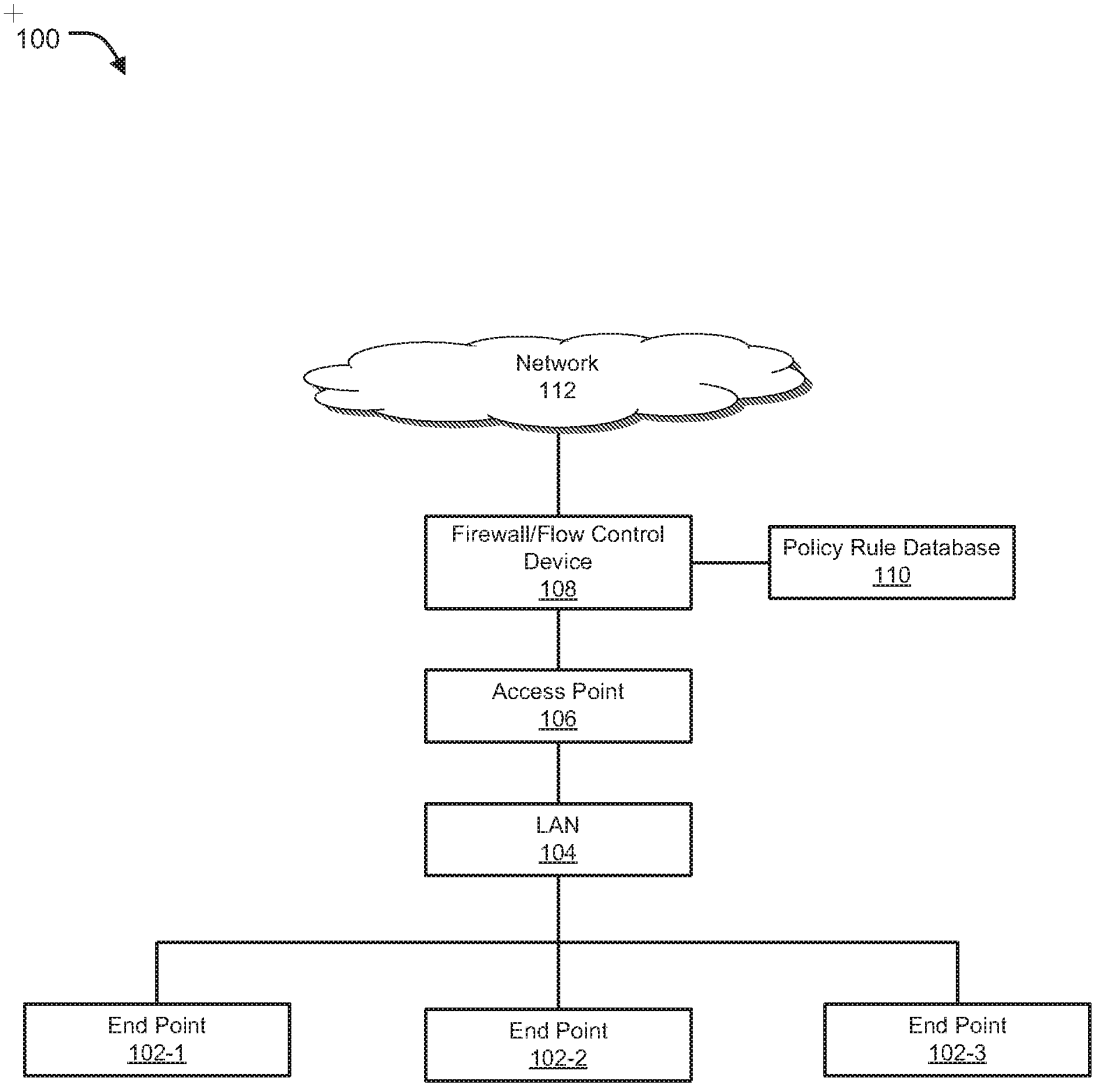


FIG. 1

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

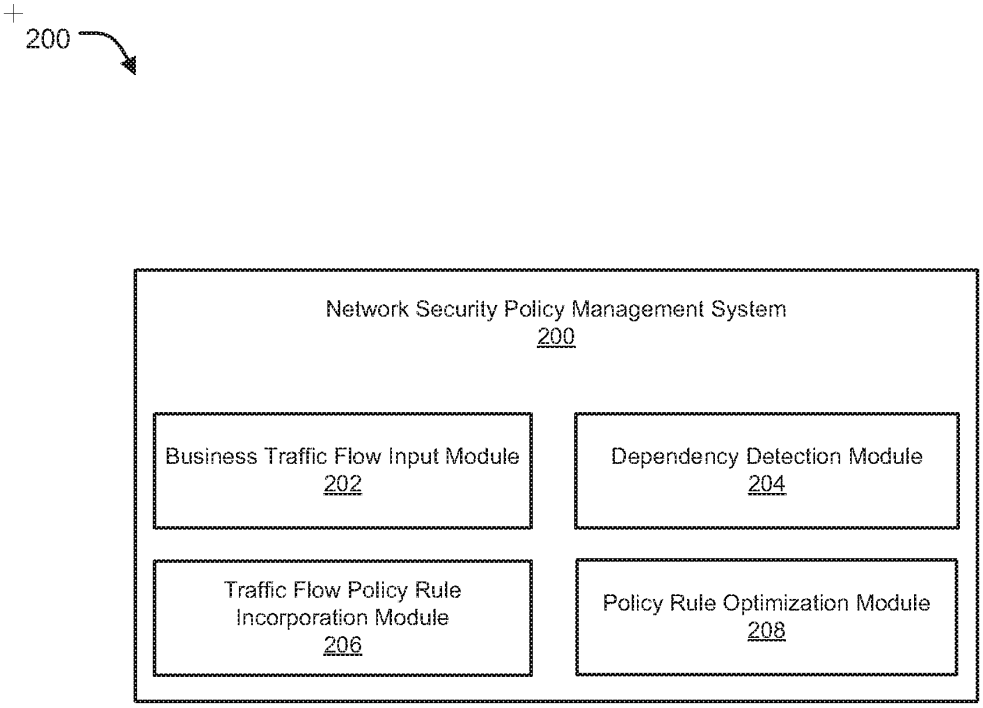


FIG. 2

301

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

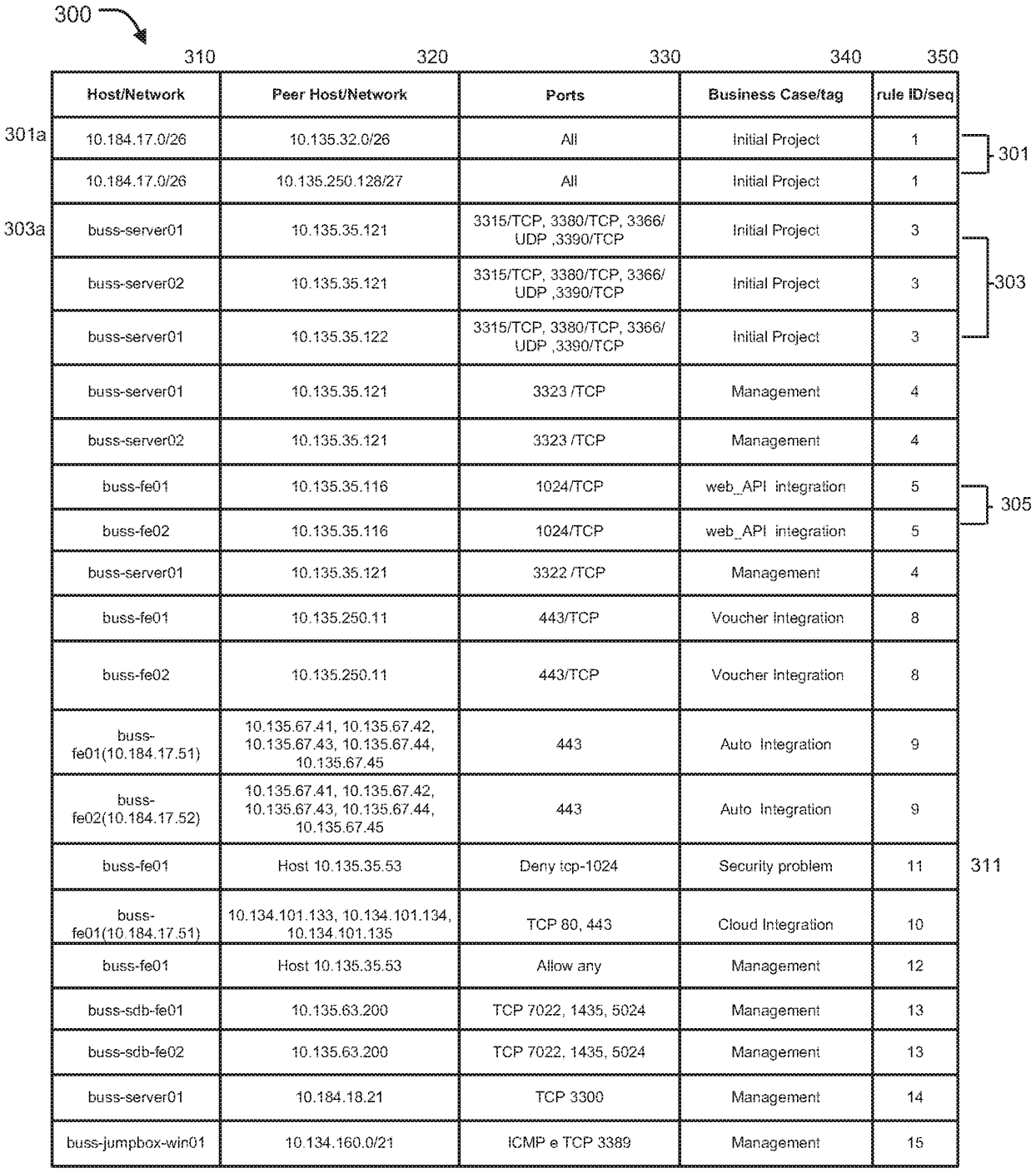


FIG. 3A

Host/Network	Peer Host/Network	Ports	Business Case/tag	Priority
buss-fe01	10.135.35.0/24	TCP-1024	web_API integration	HIGH

399

FIG. 3B

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

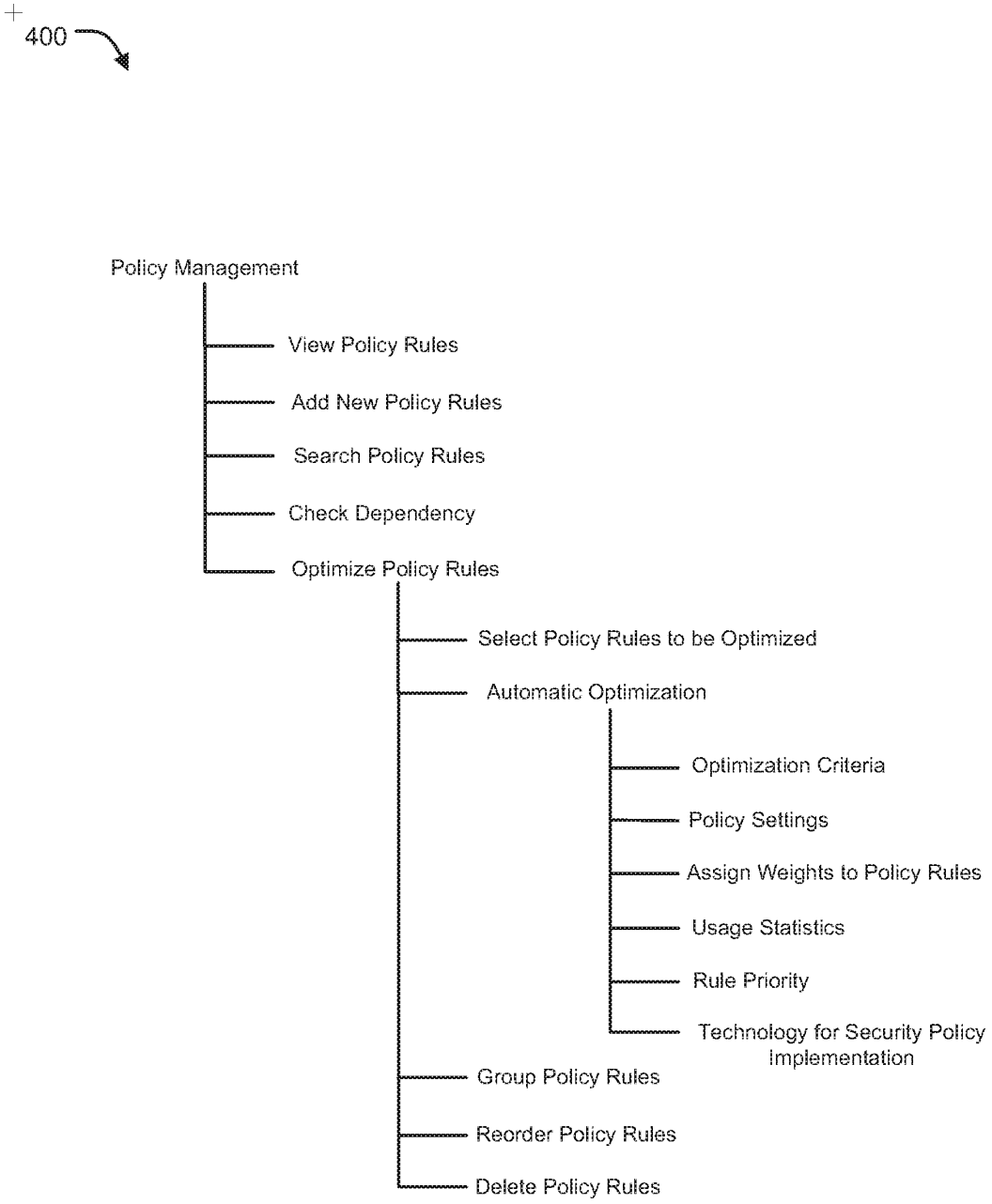


FIG. 4

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

500

Administrator Inserted Information						System Statistics	
Index	Source	Destination	Service	Action	Priority	Sessions	% Sessions
1	192.168.0.0/24	ALL	DNS, HTTP, HTTPS	Allow	Normal	50000	25.00%
2	192.168.1.0/24	ALL	DNS, HTTP, HTTPS, SMTP	Allow	Normal	40000	20.00%
3	ALL	192.168.3.1	HTTP	Allow	HIGH	10000	5.00%
4	ALL	192.168.3.2	SMTP	Allow	HIGH	15000	7.50%
5	192.168.3.1	192.168.1.80	HTTP	Allow	HIGH	5000	2.50%
6	192.168.3.2	192.168.1.25	SMTP	Allow	HIGH	15000	7.50%
7	192.168.3.2	192.168.0.0/16	ANY	Block		50000	25.00%
8	192.168.3.2	ALL	DNS, SMTP	Allow	HIGH	15000	7.50%
9	ALL	ALL	ANY	Block			

FIG. 5A

Administrator Inserted Information							System Statistics	
Index	Source	Destination	Service	Action	Priority	Dependencies	Sessions	% Sessions
1	192.168.0.0/24	ALL	DNS, HTTP, HTTPS	Allow	Normal		50000	25.00%
2	192.168.1.0/24	ALL	DNS, HTTP, HTTPS, SMTP	Allow	Normal		40000	20.00%
3	ALL	192.168.3.1	HTTP	Allow	HIGH		10000	5.00%
4	ALL	192.168.3.2	SMTP	Allow	HIGH		15000	7.50%
5	192.168.3.1	192.168.1.80	HTTP	Allow	HIGH		5000	2.50%
6	192.168.3.2	192.168.1.25	SMTP	Allow	HIGH	Execution Order Locked with Rule 7	15000	7.50%
7	192.168.3.2	192.168.0.0/16	ANY	Block		Partialy Shadows Rule 8	50000	25.00%
8	192.168.3.2	ALL	DNS, SMTP	Allow	HIGH	Partialy Shadowed by Rule 7	15000	7.50%
9	ALL	ALL	ANY	Block				

FIG. 5B

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Administrator Inserted Information								System Statistics	
Index	Source	Destination	Service	Action	Priority	Dependencies A	Dependencies B	Sessions	% Sessions
1	192.168.0.0/24	ALL	DNS, HTTP, HTTPS	Allow	Normal		Partialy Groupable with Rule 2	50000	25.00%
2	192.168.1.0/24	ALL	DNS, HTTP, HTTPS, SMTP	Allow	Normal		Partialy Groupable with Rule 1	40000	20.00%
3	ALL	192.168.3.1	HTTP	Allow	HIGH			10000	5.00%
4	ALL	192.168.3.2	SMTP	Allow	HIGH			15000	7.50%
5	192.168.3.1	192.168.1.80	HTTP	Allow	HIGH			5000	2.50%
6	192.168.3.2	192.168.1.25	SMTP	Allow	HIGH	Execution Order Locked With Rule 7		15000	7.50%
7	192.168.3.2	192.168.0.0/16	ANY	Block		Partialy Shadows Rule 8		50000	25.00%
8	192.168.3.2	ALL	DNS, SMTP	Allow	HIGH	Partialy Shadowed by Rule 7	Partialy Groupable with Rule 2	15000	7.50%
9	ALL	ALL	ANY	Block					

FIG. 5C

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Optimization Criteria: Performance Based on Statistics								
Administrator Inserted Information							System Statistics	
Index	Source	Destination	Service	Action	Priority	Optimization Notes	Sessions	% Sessions
1	192.168.0.0/23	ALL	DNS, HTTP, HTTPS	Allow	Normal	Partial Merge of Rules 1 and 2	50000	25.00%
2	192.168.3.2	192.168.1.25	SMTP	Allow	HIGH	Reorder of Rule 6	15000	7.50%
3	192.168.3.2	192.168.0.0/16	ANY	Block		Reorder of Rule 7 due to High Volume of Hits	50000	25.00%
4	192.168.1.0/24 192.168.3.2	ALL	DNS, SMTP	Allow	Normal/ HIGH	Partial Merge of Rules 2 and 8	55000	27.50%
5	ALL	192.168.3.2	SMTP	Allow	HIGH	Reorder of Rule 4	15000	7.50%
6	ALL	192.168.3.1	HTTP	Allow	HIGH	Reorder of Rule 3	10000	5.00%
7	192.168.3.1	192.168.1.80	HTTP	Allow	HIGH	Left in the End due to Lowest Number of Hits	5000	2.50%
9	ALL	ALL	ANY	Block				

FIG. 5D

Optimization Criteria: Performance Based on Priority								
Administrator Inserted Information							System statistics	
Index	Source	Destination	Service	Action	Priority	Optimization Notes	Sessions	% sessions
2	192.168.3.2	192.168.1.25	SMTP	Allow	HIGH	Reorder of Rule 6	15000	10.00%
3	192.168.3.2	192.168.0.0/16	ANY	Block		Reorder of Rule 7 due to High Volume of Hits	50000	33.33%
4	192.168.1.0/24 192.168.3.2	ALL	DNS,SMTP	Allow	Normal/ HIGH	Partial Merge of Rules 2 and 8	55000	36.67%
5	ALL	192.168.3.2	SMTP	Allow	HIGH	Reorder of Rule 4	15000	10.00%
6	ALL	192.168.3.1	HTTP	Allow	HIGH	Reorder of Rule 3	10000	6.67%
7	192.168.3.1	192.168.1.80	HTTP	Allow	HIGH	Left in the End due to Lowest Number of Hits	5000	3.33%
1	192.168.0.0/23	ALL	DNS,HTTP,HTTPS	Allow	Normal	Partial Merge of Rules 1 and 2 and Reorder	50000	33.33%
9	ALL	ALL	ANY	Block				

FIG. 5E

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

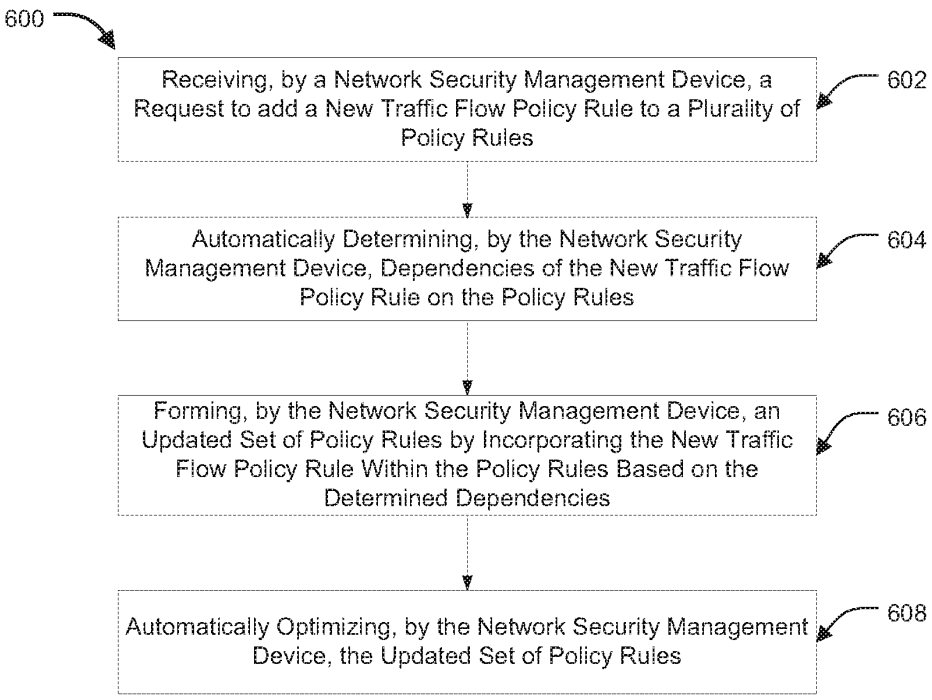


FIG. 6

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

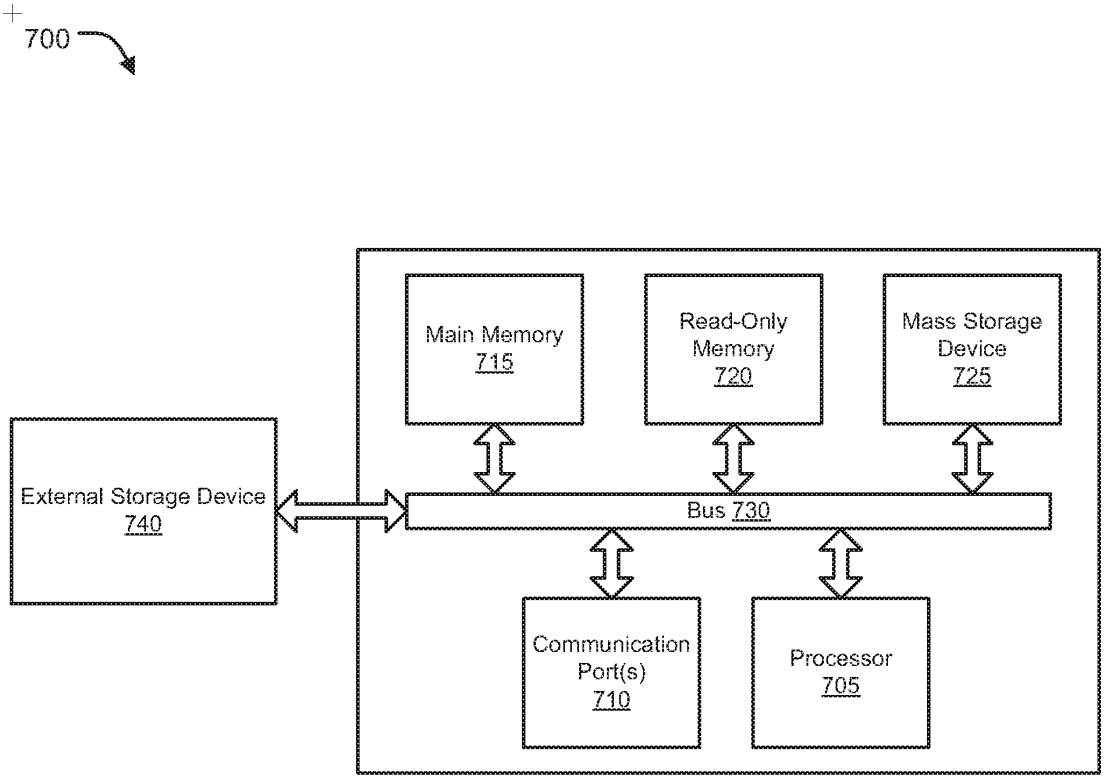


FIG. 7

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FORT-012500
	Application Number	
Title of Invention	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Hugo	Filipe Parreira	Pernicha	

Residence Information (Select One) ◯ US Residency ◉ Non US Residency ◯ Active US Military Service

City	Venda do Pinheiro	Country of Residence i	PT

Mailing Address of Inventor:

Address 1	Av. 9 de Julho, nº 12, 3 Dto		
Address 2			
City	Venda do Pinheiro	**State/Province**	
Postal Code	2665-520	**Country** i	PT

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	64128		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT		
Attorney Docket Number	FORT-012500	**Small Entity Status Claimed** ☐	
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	9	**Suggested Figure for Publication (if any)**	6

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FORT-012500
	Application Number	
Title of Invention	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT	

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	64128		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FORT-012500
	Application Number	
Title of Invention	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT	

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i]the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FORT-012500
	Application Number	
Title of Invention	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT	

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :	
If the Applicant is an Organization check here. ☒	
Organization Name	Fortinet, Inc.

Mailing Address Information:

Address 1	1090 Kifer Rd.		
Address 2			
City	Sunnyvale	**State/Province**	CA
Country [i]	US	Postal Code	94086
Phone Number		Fax Number	

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FORT-012500
	Application Number	
Title of Invention	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT	

Email Address	

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

Organization Name	Fortinet, Inc.

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	1090 Kifer Rd.		
Address 2			
City	Sunnyvale	**State/Province**	CA
Country i	US	Postal Code	94086
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/Michael A DeSanctis/			Date (YYYY-MM-DD)	2014-12-10
First Name	Michael A.	Last Name	DeSanctis	Registration Number	39957

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FORT-012500
	Application Number	
Title of Invention	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Hugo Filipe Parreira Pernicha Date (Optional): December 10th 2014

Signature: Hugo Filipe Parreira Pernicha

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office;U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of1995, no persons arerequired to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Fortinet, Inc.

Application No./Patent No.: _____ Filed/Issue Date: December 10, 2014

Titled: DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT

Fortinet, Inc., a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by37 CFR3.73(b). The information is required toobtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentialityis governed by35 U.S.C. 122and 37 CFR1.11 and1.14. Thiscollection is estimated to take 12 minutes to complete, including gathering, preparing, and submittingthe completed application form to the USPTO.Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent tothe Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.**SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Michael A DeSanctis/	December 10, 2014
Signature	Date
Michael A. DeSanctis	39957
Printed or Typed Name	Title or Registration Number

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that yoube given certain informationin connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, pleasebe advised that: (1) the general authority forthe collection of thisinformation is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and(3) the principal purpose forwhich the information isused by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent applicationor patent. If you do not furnish the requested information,the U.S. Patent and Trademark Office may not be able to process and/or examineyour submission,which may result in termination of proceedings or abandonment of the applicationor expiration of the patent.

The informationprovided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the informationin order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an InternationalApplication filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, arecord may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from thissystem of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

ASSIGNMENT

WHEREAS, I, **Hugo Filipe Parreira Pernicha** have invented certain new and useful improvements for which an application entitled

"**DYNAMICALLY OPTIMIZED SECURITY POLICY MANAGEMENT**"

is about to be made for Letters Patent of the United States, the application having been executed on even date herewith, and which may be identified in the United States Patent and Trademark Office by Application No. _____, filed on _____ and further identified as Atty. Docket No. FORT-012500.

WHEREAS, **Fortinet, Inc.**, a Corporation of the State of Delaware, and having its principal offices at 1090 Kifer Rd., Sunnyvale, CA 94086 (hereafter "Assignee"), is desirous of acquiring the entire right, title and interest in and to the application, any inventions or discoveries described therein and in, to and under any and all Letters Patents to be obtained therefor;

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, I have sold, assigned and transferred, and by these presents do hereby sell, assign and transfer unto the Assignee, its successors and assigns:

1. the entire right, title and interest in and to the application, any inventions or discoveries described therein and the Letters Patent(s), both foreign and domestic, that may or shall issue, including all rights under the International Convention, and

2. all proceeds of the application, any inventions or discoveries described therein and the Letters Patent(s) (including but not limited to, damages for pre-patent grant infringement, all license royalties and proceeds of infringement suits); and in and to any and all causes of action (excepting claims upon the United States of America) for past, present, and future infringement of any of the Letters Patent(s), or relating to any inventions or discoveries described therein, including the right to collect royalties and seek injunctive relief, for all such infringements and the right to sue on all such causes of action for their own use and benefit and the use and benefit of their successors, assigns and legal representatives.

I do hereby authorize and request the Commissioner of Patents to issue the Letters Patent(s) to the Assignee in accordance herewith.

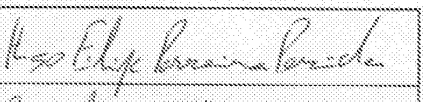
I hereby authorize the Assignee, its successors and assigns or anyone it may properly designate, to insert in this instrument the filing date and Application No. of the application when ascertained.

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041

I further authorize the Assignee, its successors and assigns, or anyone it may properly designate, to apply for Letters Patent, in its own name, if desired, in any and all foreign countries, and additionally to claim the filing date of the United States application and/or otherwise take advantage of the provisions of the International Convention.

I do hereby covenant and agree with the Assignee, its successors and assigns, that I will not execute any writing or do any act whatsoever conflicting with these presents, and that I or my executors or administrators will, at any time upon request, without further or additional consideration, but at the expense of the Assignee, its successors and assigns, execute such additional writings and do such additional acts as the Assignee, its successors and assigns, may deem necessary or desirable to perfect the Assignee's enjoyment of this grant, and render all necessary assistance in making application for and obtaining original, continuation, divisional, reissued, reexamined, substitute or extended Letters Patent(s) of the United States, or of any and all foreign countries on the invention, and in enforcing any rights, occurring as a result of such applications or patents, by giving testimony in any proceedings or transactions involving such applications or patents.

In Witness Whereof, I have hereunto set my hand and affixed my seal on the date written below.

Signature:	
Date:	December 10th, 2014
Full Name:	**Hugo Filipe Parreira Pernicha**
Address:	Av. 9 de Julho, nº 12, 3 Dto
	2665-520 Venda do Pinheiro
	PORTUGAL

Netskope, Ex. 2009
Fortinet v. Netskope, IPR2026-00041