

Conferences > 2006 IEEE/IFIP Network Operat... ?

Analysis of Firewall Policy Rules Using Data Mining Techniques

Publisher: IEEE

Cite This

PDF

K. Golnabi ; R.K. Min ; L. Khan ; E. Al-Shaer All Authors

38
Paper
Citations

2
Patent
Citations

1122
Full
Text Views



Alerts

Manage Content Alerts

Add to Citation Alerts

Abstract

Document Sections

I. Introduction

II. Related Work

III. Mining Firewall Log File

IV. Mining Results

V. Conclusion and Future Work

Authors

Figures

References

Citations

Keywords

Metrics


Download
PDF

Abstract:Firewall is the de facto core technology of today's network security and defense. However, the management of firewall rules has been proven to be complex, error-prone, co... **View more**

► **Metadata**

Abstract:

Firewall is the de facto core technology of today's network security and defense. However, the management of firewall rules has been proven to be complex, error-prone, costly and inefficient for many large-networked organizations. These firewall rules are mostly custom-designed and hand-written thus in constant need for tuning and validation, due to the dynamic nature of the traffic characteristics, ever-changing network environment and its market demands. One of the main problems that we address in this paper is that how much the firewall rules are useful, up-to-dated, well-organized or efficient to reflect the current characteristics of network traffics. In this paper, we present a set of techniques and algorithms to analysis and manage firewall policy rules: (1) Data Mining technique to deduce efficient firewall policy rules by mining its network traffic log based on its frequency, (2) Filtering-Rule Generalization (FRG) to reduce the number of policy rules by generalization, and (3) a technique to identify any decaying rule and a set of few dominant rules, to generate a new set of efficient firewall policy rules. The anomaly

More Like This

Authorization mechanism for MQTT-based Internet of Things

2016 IEEE International Conference on Communications Workshops (ICC)

Published: 2016

A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things

IEEE Access

Published: 2020

Show More

detection based on the mining exposes many hidden but not detectable by analyzing only the firewall policy rules, resulting in two new types of the anomalies. As a result of these mechanisms, network security administrators can automatically review and update the rules. We have developed a prototype system and demonstrated usefulness of our approaches.

Published in: 2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006

Date of Conference: 03-07 April 2006 **INSPEC Accession Number:** 9061231

Date Added to IEEE Xplore: 23 October 2006 **DOI:** 10.1109/NOMS.2006.1687561

Print ISBN:1-4244-0142-9 **Publisher:** IEEE

Conference Location: Vancouver, BC, Canada

▼ **ISSN Information:**

Print ISSN: 1542-1201

Electronic ISSN: 2374-9709

Citations are not available for this document.

 Contents

I. Introduction

In the global world of Internet, firewall is the de facto core technology of today's network security and first line of defense against external network attacks and threats. Firewall controls or governs network access by allowing or denying the incoming or outgoing network traffic according to firewall policy rules. These rules are explicitly written and managed to filter out any unwanted traffic coming into or going from the secure network. However, the management of firewall rules has been proven to be complex, error-prone, costly and inefficient for many large-networked organizations. These firewall rules are often custom-designed and hand-written by and for the human policy writer of an organization and tailored to accommodate ever-changing business and market demands of the global Internet. Therefore, these rules are in a constant need of updating, tuning and validating to optimize firewall security.

Authors	▼
Figures	▼
References	▼
Citations	▲
By Papers	By Patents

Export ▼ ? | References & Cited By

Cited in Papers - IEEE (22) | Other Publishers (16)

Cited in Papers - IEEE (22)

☐ Select All

-
- ☐ 1. Cengiz Togay, Ahmet Kasif, Cagatay Catal, Bedir Tekinerdogan, "A Firewall Policy Anomaly Detection Framework for Reliable Network Security", *IEEE Transactions on Reliability*, vol.71, no.1, pp.339-347, 2022.
Show Article  Google Scholar
-
- ☐ 2. Yizhen Sun, Xiaotao Peng, Zheng Tian, Shaoming Guo, "A Deception Defense and Active Defense Based Three-Dimensional Defense Architecture: DA-3DD Design and Implementation Plan", *2019 15th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)*, pp.422-427, 2019.
Show Article  Google Scholar
-
- ☐ 3. Erick Skorupa Parolin, Sayeed Salam, Latifur Khan, Patrick Brandt, Jennifer Holmes, "Automated Verbal-Pattern Extraction from Political News Articles using CAMEO Event Coding Ontology", *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pp.258-266, 2019.
Show Article  Google Scholar
-
- ☐ 4. Qiumei Cheng, Chunming Wu, Haifeng Zhou, Yuhang Zhang, Rui Wang, Wei Ruan, "Guarding the Perimeter of Cloud-Based Enterprise Networks: An Intelligent SDN Firewall", *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pp.897-902, 2018.
Show Article  Google Scholar
-
- ☐ 5. Fatih Ertam, Mustafa Kaya, "Classification of firewall log files with multiclass support vector machine", *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pp.1-4, 2018.
Show Article  Google Scholar
-
- ☐ 6. Cheng Jin, Abhinav Srivastava, Zhi-Li Zhang, "Understanding security group usage in a public IaaS cloud", *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, pp.1-9, 2016.
Show Article  Google Scholar
-
- ☐ 7. Hiroki Nakahara, Tsutomu Sasao, Hisashi Iwamoto, Munehiro Matsuura, "LUT Cascades Based on Edge-Valued Multi-Valued Decision Diagrams: Application to Packet Classification", *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol.6, no.1, pp.73-86, 2016.
Show Article  Google Scholar
-

- ☐ 8. Wenli Shang, Ming Wan, Peng Zeng, Quansheng Qiao, "Research on self-learning method on generation and optimization of industrial firewall rules", *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, pp.47-52, 2015.
Show Article  Google Scholar

- ☐ 9. Claas Lorenz, Bettina Schnor, "Policy anomaly detection for distributed IPv6 firewalls", *2015 12th International Joint Conference on e-Business and Telecommunications (ICETE)*, vol.04, pp.210-219, 2015.
Show Article  Google Scholar

- ☐ 10. Cheng Jin, Abhinav Srivastava, Yu Jin, Zhi-Li Zhang, "Secgras: Security Group Analysis as a Cloud Service", *2014 IEEE 22nd International Conference on Network Protocols*, pp.215-220, 2014.
Show Article  Google Scholar

- ☐ 11. Qi Xiao, Yunchuan Qin, Cheng Xu, Kenli Li, "Lightweight detecting and resolving algorithm for firewall policy conflict", *2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp.234-239, 2013.
Show Article  Google Scholar

- ☐ 12. Wei Li, Haishan Wan, Sheng Li, "An approach to the generalization of firewall rules", *2013 IEEE/ACIS 12th International Conference on Computer and Information Science (ICIS)*, pp.201-206, 2013.
Show Article  Google Scholar

- ☐ 13. Suchart Khummanee, Atipong Khumseela, Somnuk Puangpronpitag, "Towards a new design of firewall: Anomaly elimination and fast verifying of firewall rules", *The 2013 10th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, pp.93-98, 2013.
Show Article  Google Scholar

- ☐ 14. Li Zhu, Huaqing Mao, Hang Qin, "A Case Study on Access Control Rules Design and Implementation of Firewall", *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*, pp.1-4, 2012.
Show Article  Google Scholar

- ☐ 15. Yang Zan, Yang Lin, Ma Lin-Ru, Liu Xiao-Ming, "Overview of the Data Mining Applications in Network Defense in Depth", *2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control*, pp.491-494, 2011.
Show Article  Google Scholar

- ☐ 16. Hiroki Nakahara, Tsutomu Sasao, Munehiro Matsuura, "A Packet Classifier Using a Parallel Branching Program

Machine", 2010 13th Euromicro Conference on Digital System Design: Architectures, Methods and Tools, pp.745-752, 2010.

Show Article  Google Scholar

- ☐ 17. Zhang Jing-xiao, Lu Ning, Xu Fei, Su Chuan-chuan, "A New Schedule Method for the Best Delay-Supply Time", 2010 International Conference on Electrical and Control Engineering, pp.157-162, 2010.

Show Article  Google Scholar

- ☐ 18. Subana Thanasegaran, Yi Yin, Yuichiro Tateiwa, Yoshiaki Katayama, Naohisa Takahashi, "A topological approach to detect conflicts in firewall policies", 2009 IEEE International Symposium on Parallel & Distributed Processing, pp.1-7, 2009.

Show Article  Google Scholar

- ☐ 19. Gianluca Maiolini, Lorenzo Cignini, Andrea Baiocchi, "Adaptive Optimization of Packet Filtering Devices Performance Ensuring a Conflict-free Network Configuration", IEEE INFOCOM Workshops 2008, pp.1-6, 2008.

Show Article  Google Scholar

- ☐ 20. Steven Davy, Brendan Jennings, John Strassner, "Application domain independent policy conflict analysis using information models", NOMS 2008 - 2008 IEEE Network Operations and Management Symposium, pp.17-24, 2008.

Show Article  Google Scholar

- ☐ 21. Lieven Desmet, Pierre Verbaeten, Wouter Joosen, Frank Piessens, "Provable Protection against Web Application Vulnerabilities Related to Session Data Dependencies", IEEE Transactions on Software Engineering, vol.34, no.1, pp.50-64, 2008.

Show Article  Google Scholar

- ☐ 22. Tihomir Katic, Predrag Pale, "Optimization of Firewall Rules", 2007 29th International Conference on Information Technology Interfaces, pp.685-690, 2007.

Show Article  Google Scholar

Cited in Papers - Other Publishers (16)

1. Ramtin Aryan, Anis Yazidi, Øivind Kure, Paal Einar Engelstad, "A parallel approach for detecting OpenFlow rule anomalies based on a general formalism", Concurrency and Computation: Practice and Experience, vol.33, no.15, 2021.

CrossRef Google Scholar

2. Jorge Lobo, Elisa Bertino, Alessandra Russos, "On Security Policy Migrations", Proceedings of the 25th ACM Symposium on Access Control Models and Technologies, pp.179, 2020.

CrossRef Google Scholar

3. Amani Abu Jabal, Maryam Davari, Elisa Bertino, Christian Makaya, Seraphin Calo, Dinesh Verma, Alessandra Russo, Christopher Williams, "Methods and Tools for Policy Analysis", *ACM Computing Surveys*, vol.51, no.6, pp.1, 2019.
CrossRef Google Scholar

4. Christoph Haar, Erik Buchmann, "FANE: A Firewall Appliance for the Smart Home", *2019 Federated Conference on Computer Science and Information Systems (FedCSIS)*, pp.449-458, 2019.
Full Text: PDF Full Text: HTML Google Scholar

5. Hajar Esmaeil As-Suhbani, S. D. Khamitkar, *Recent Trends in Image Processing and Pattern Recognition*, vol.1037, pp.561, 2019.
CrossRef

6. Erdem Ucar, Erkan Ozhan, "The Analysis of Firewall Policy Through Machine Learning and Data Mining", *Wireless Personal Communications*, vol.96, no.2, pp.2891, 2017.
CrossRef Google Scholar

7. Haining Chen, Omar Chowdhury, Ninghui Li, Warut Khern-am-nuai, Suresh Chari, Ian Molloy, Youngja Park, "Tri-Modularization of Firewall Policies", *Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies*, pp.37, 2016.
CrossRef Google Scholar

8. Amit Kumar Bhardwaj, Maninder Singh, "Data mining-based integrated network traffic visualization framework for threat detection", *Neural Computing and Applications*, vol.26, no.1, pp.117, 2015.
CrossRef Google Scholar

9. Hanaa M. Said, Abdel-Badeeh M. Salem, "Exploiting Computational Intelligence Paradigms in e-Technologies and Activities", *Procedia Computer Science*, vol.65, pp.396, 2015.
CrossRef Google Scholar

10. Qi Xiao, Yunchuan Qin, Kenli Li, *High Performance Computing*, vol.207, pp.118, 2013.
CrossRef

11. *Data Mining Tools for Malware Detection*, pp.297, 2011.
CrossRef

12. Hiroki NAKAHARA, Tsutomu SASAO, Munehiro MATSUURA, Yoshifumi KAWAMURA, "A Parallel Branching Program Machine for Sequential Circuits: Implementation and Evaluation", *IEICE Transactions on Information and Systems*, vol.E93-D, no.8, pp.2048, 2010.
CrossRef Google Scholar

13. Kamel Karoui, Fakher Ben Ftima, Henda Ben Ghezala, *Data Mining and Multi-agent Integration*, pp.267, 2009.
CrossRef

14. S. Pozo, R. Ceballos, R.M. Gasca, "Model-Based Development of firewall rule sets: Diagnosing model inconsistencies", *Information and Software Technology*, vol.51, no.5, pp.894, 2009.
CrossRef Google Scholar

15. Steven Davy, Brendan Jennings, John Strassner, "The policy continuum—Policy authoring and conflict analysis", *Computer Communications*, vol.31, no.13, pp.2981, 2008.
CrossRef Google Scholar

16. Muhammad Abedin, Syeda Nessa, Latifur Khan, Bhavani Thuraisingham, *Data and Applications Security XX*, vol.4127, pp.15, 2006.
CrossRef

Keywords



Metrics



IEEE Personal Account

CHANGE
USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
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

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [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 2022 IEEE - All rights reserved.

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](#) | [Accessibility](#) | [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 2022 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.