

EXHIBIT 5

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

UMBRA Technologies Ltd. (“UMBRA”) provides evidence of infringement of claims 1 and 6-9 of U.S. Patent No. 10,574,482 (hereinafter “the ’482 patent”) by Cisco Systems, Inc. (“Cisco”). In support thereof, UMBRA provides the following claim charts.

“Accused Instrumentalities” as used herein refers to at least Cisco systems and methods, including one or more hardware and software products for network virtualization and related services, which by way of example include but are not limited to Cisco Secure Access Service Edge (SASE) (*see, e.g.*, Cisco SASE, <https://www.cisco.com/site/us/en/solutions/secure-access-service-edge-sase/index.html#tabs-9cfa4a460b-item-b8ba101fed-tab>), Cisco Software Defined-WAN (*see, e.g.*, Cisco SD-WAN, https://www.cisco.com/c/en_ph/solutions/enterprise-networks/sd-wan/index.html), Cisco Security Service Edge (SSE) (*see, e.g.*, Cisco SSE, <https://www.cisco.com/site/us/en/solutions/security-service-edge-sse/index.html#tabs-9e2187ae1d-item-8d800bd1e7-tab>), and Cisco HyperFlex Systems (Hyper Converged Infrastructure or “HCI”) (*see, e.g.*, Cisco HCI, <https://www.cisco.com/site/us/en/products/computing/hyperconverged-infrastructure/index.html#tabs-9cfa4a460b-item-b8ba101fed-tab>) and related earlier versions (the “Accused Instrumentalities”). These claim charts demonstrate Cisco’s infringement, and provide notice of such infringement, by comparing each element of the asserted claims to corresponding components, aspects, and/or features of the Accused Instrumentalities. These claim charts are not intended to constitute an expert report on infringement. These claim charts include information provided by way of example, and not by way of limitation.

The analysis set forth below is based only upon information from publicly available resources regarding the Accused Instrumentalities, as Cisco has not yet provided any non-public information. An analysis of Cisco’s (or other third parties’) technical documentation and/or software source code may assist in fully identifying all infringing features and functionality. Accordingly, UMBRA reserves the right to supplement this infringement analysis once such information is made available to UMBRA. Furthermore, UMBRA reserves the right to revise this infringement analysis, as appropriate, upon issuance of a court order construing any terms recited in the asserted claims. UMBRA provides this evidence of infringement and related analysis without the benefit of claim construction or expert reports or discovery. UMBRA reserves the right to supplement, amend or otherwise modify this analysis and/or evidence based on any such claim construction or expert reports or discovery.

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

Unless otherwise noted, UMBRA contends that Cisco directly infringes the ’482 patent in violation of 35 U.S.C. § 271(a) by selling, offering to sell, making, using, and/or importing the Accused Instrumentalities. The following exemplary analysis demonstrates that infringement. Unless otherwise noted, UMBRA further contends that the evidence below supports a finding of indirect infringement under 35 U.S.C. §§ 271(b) and/or (c), in conjunction with other evidence of liability under one or more of those subsections. Cisco makes, uses, sells, imports, or offers for sale in the United States, or has made, used, sold, imported, or offered for sale in the past, without authority, or induces others to make, use, sell, import, or offer for sale in the United States, or has induced others to make, use, sell, import, or offer for sale in the past, without authority products, equipment, or services that infringe claims 1 and 6-9 of the ’482 patent, including without limitation, the Accused Instrumentalities.

Unless otherwise noted, UMBRA believes and contends that each element of each claim asserted herein is literally met through Cisco’s provision of the Accused Instrumentalities. However, to the extent that Cisco attempts to allege that any asserted claim element is not literally met, UMBRA believes and contends that such elements are met under the doctrine of equivalents. More specifically, in its investigation and analysis of the Accused Instrumentalities, UMBRA did not identify any substantial differences between the elements of the patent claims and the corresponding features of the Accused Instrumentalities, as set forth herein. In each instance, the identified feature of the Accused Instrumentalities performs at least substantially the same function in substantially the same way to achieve substantially the same result as the corresponding claim element.

To the extent the chart of an asserted claim relies on evidence about certain specifically identified Accused Instrumentalities, UMBRA asserts that, on information and belief, any similarly functioning instrumentalities also infringes the charted claim. UMBRA reserves the right to amend this infringement analysis based on other products made, used, sold, imported, or offered for sale by Cisco. UMBRA also reserves the right to amend this infringement analysis by citing other claims of the ’482 patent, not listed in the claim chart, that are infringed by the Accused Instrumentalities. UMBRA further reserves the right to amend this infringement analysis by adding, subtracting, or otherwise modifying content in the “Accused Instrumentalities” column of each chart.

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

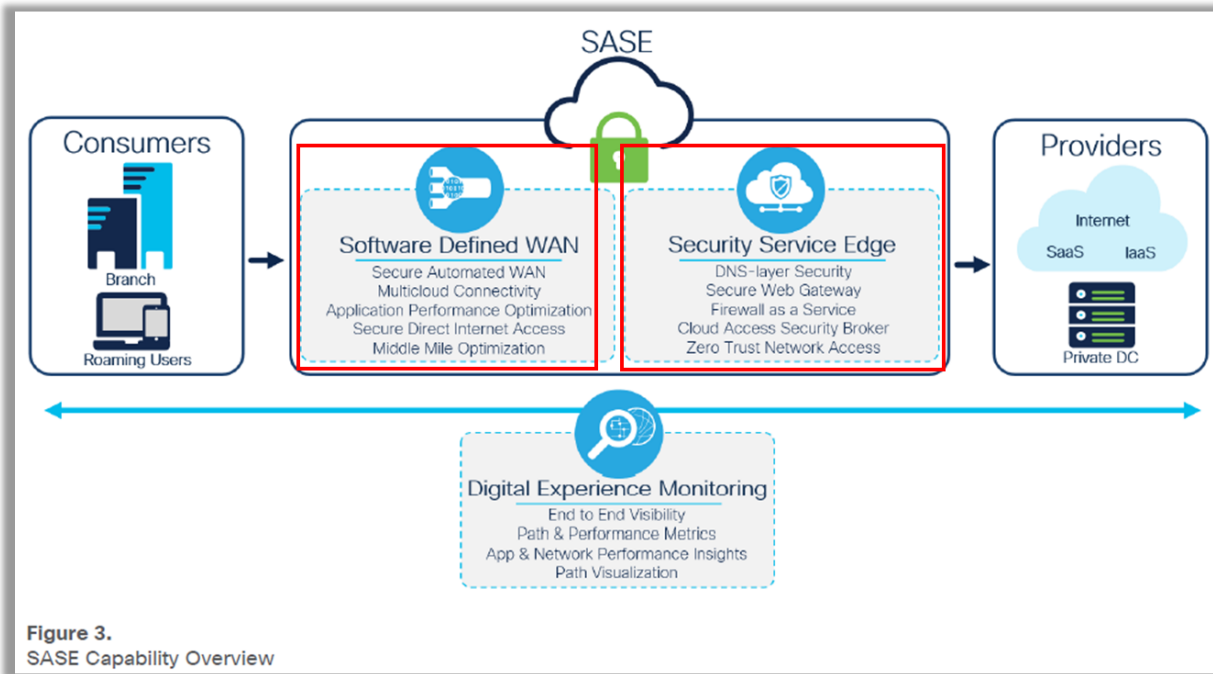
Claim #1	Accused Instrumentalities
Indep.Cl. 1 1-p A multi-perimeter firewall system located in a cloud and forming part of a global virtual network, comprising:	Cisco’s Secure Access Service Edge (SASE) concept goes beyond the capabilities found within the older cloud based Secure Internet Gateway (SIG) and includes the convergence of networking functionality as well. The Software Defined WAN (SD-WAN) and Security Service Edge (SSE) components of SASE are primarily delivered as Networking-as-a-Service (NaaS) and Security-as-a-Service (SECaaS) models. This refers to the ability to offer these services as SaaS. By delivering security and networking services together from the cloud, organizations will be able to securely connect any user or device to any application without having to install and maintain the network management and security infrastructure., i.e., a multi-perimeter firewall system located in a cloud and forming part of a global virtual network <u>In 2019, Gartner published a report called The Future of Network Security Is in the Cloud. In this report, Gartner introduced the SASE concept. Back in 2017, several vendors and analysts in the industry defined a new concept - the secure Internet gateway (SIG). This cloud native solution offers multiple functions including domain name system (DNS) security, secure web gateway (SWG), firewall as a service (FWaaS), and cloud access security broker (CASB) to improve security and performance while reducing costs and maintenance tasks. The SASE concept goes beyond the capabilities found within SIG and includes the convergence of networking functionality as well.</u> Source: Cisco Secure Access Service Edge (SASE) and Security Service Edge (SSE), p.5 https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/sase-sse-ag.pdf (annotations added) Service edge refers to global point of presence (PoP), IaaS, or colocation facilities where local traffic from branches and endpoints is secured and forwarded to the appropriate destination without first traveling to data center focal points. <u>The Software Defined WAN (SD-WAN) and Security Service Edge (SSE) components of SASE are primarily delivered as Networking-as-a-Service (NaaS) and Security-as-a-Service (SECaaS) models. This refers to the ability to offer these services as SaaS. By delivering security and networking services together from the cloud, organizations will be able to securely connect any user or device to any application without having to install and maintain the network management and security infrastructure.</u> <i>Id.</i> at 6.

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

1-p
Cont.



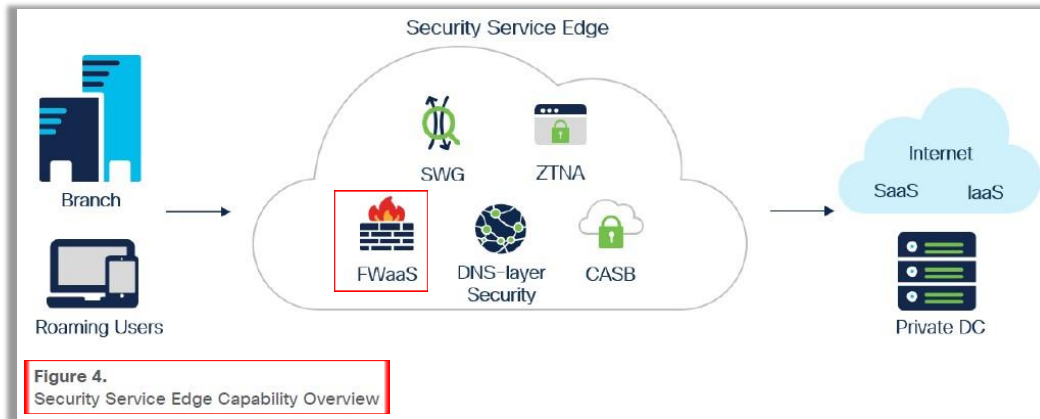
Id. at 5.

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

1-p
Cont.



Id. at 6.

Firewall As a Service

Firewall as a Service (FWaaS) is the cloud-based delivery of firewall functionality to protect non-web Internet traffic. In addition to layer 3-4 filtering, FWaaS typically includes features for intrusion prevention and application-level visibility and control.

Some of the benefits provided by FWaaS when compared to on-premises firewalls include:

- Scalable due to the pool of resources available to cloud-delivered firewalls allowing easy growth or contraction based on an organization's need
- Centralized policy management for multiple remote locations
- Easier to deploy and maintain

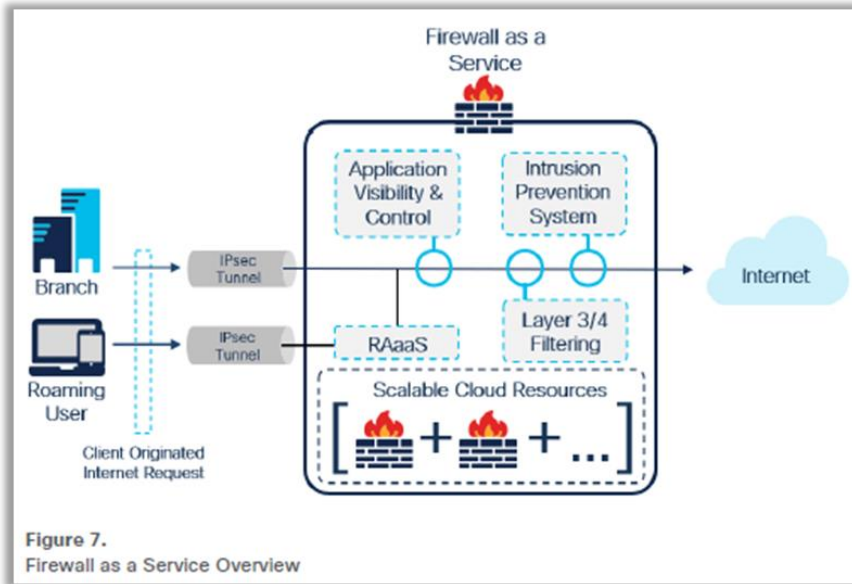
Id. at 8-9.

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

1-p
Cont.

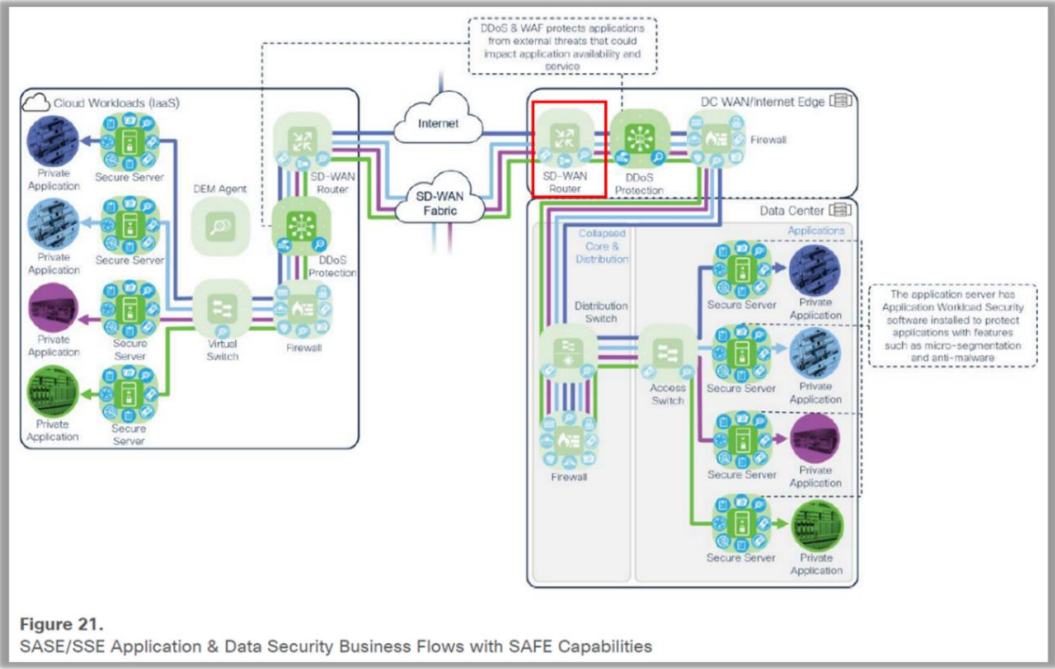


Id. at 9.

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

1-a an egress ingress point device;	The diagram below is an exemplary application of the Cisco SASE/SSE capabilities. In this example, “the Internet bound traffic is forwarded to the SASE/SSE cloud by the SD-WAN router.”, i.e., an egress ingress point device. initial step. After DNS security verifies the domain is safe, a DNS reply is sent, and the Internet bound traffic is forwarded to the SASE/SSE cloud by the SD-WAN router. The SASE/SSE service provides security and <i>Id.</i> at 32.  Figure 21. SASE/SSE Application & Data Security Business Flows with SAFE Capabilities <i>Id.</i> at 34.
---	---

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

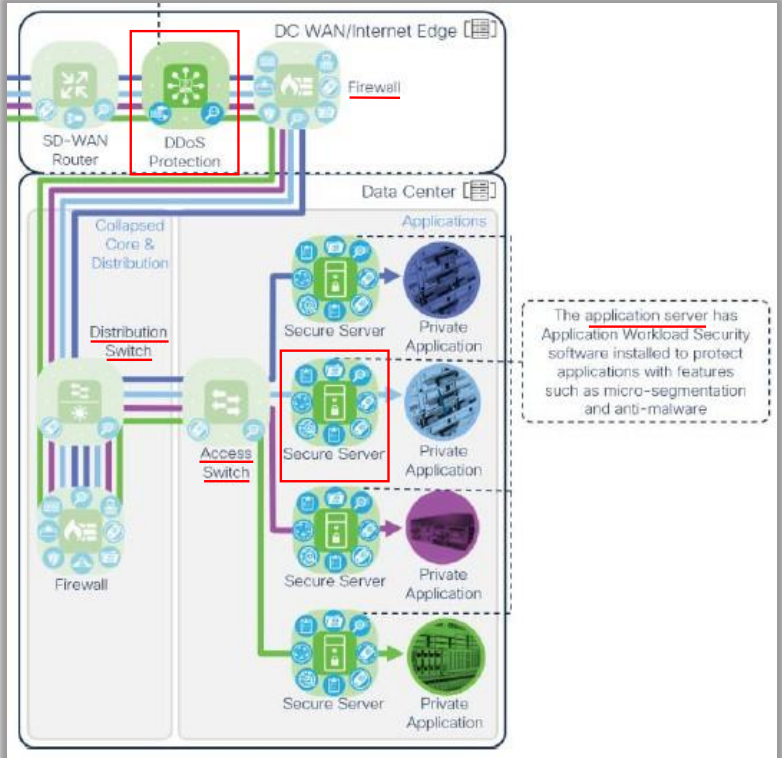
Claims 1 & 6-9

1-b a first access point server in communication with the egress ingress point device;	The “SD-WAN Router”, i.e., egress ingress point device, is in communication with a “DDoS Protector” server which “blocks attempts to overwhelm the application server and disrupt service availability.” traffic for exploits and malicious connection attempts. <u>DDoS protection blocks attempts to overwhelm the application server and disrupt service availability.</u> Successful DDoS attacks can cause productivity loss as well <i>Id.</i> at 33. Figure 21. SASE/SSE Application & Data Security Business Flows with SAFE Capabilities <i>Id.</i> at 34.
--	---

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

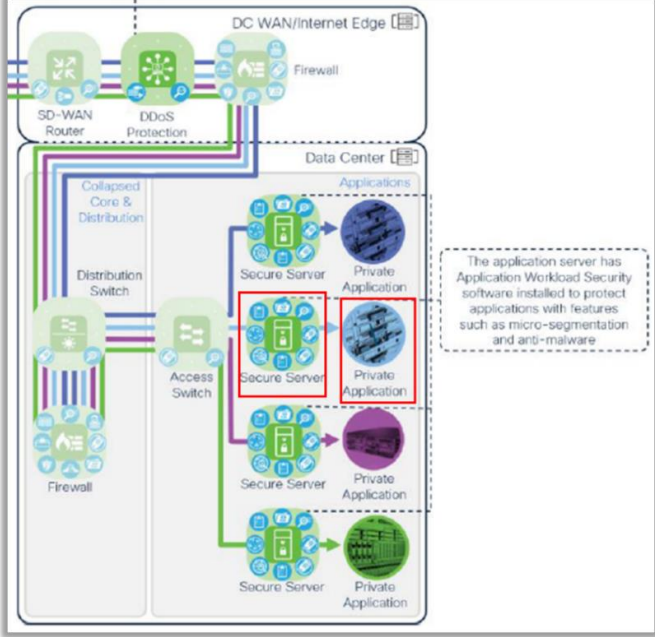
Claims 1 & 6-9

1-c a second access point server in communication with the first access point sever;	An “application server”, i.e., second server, is in communication with the “DDoS Protection” server, i.e., first access point server, through a “Firewall”, a “Distribution Switch” and an “Access Switch.”  <i>Id.</i> at 34.
--	---

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

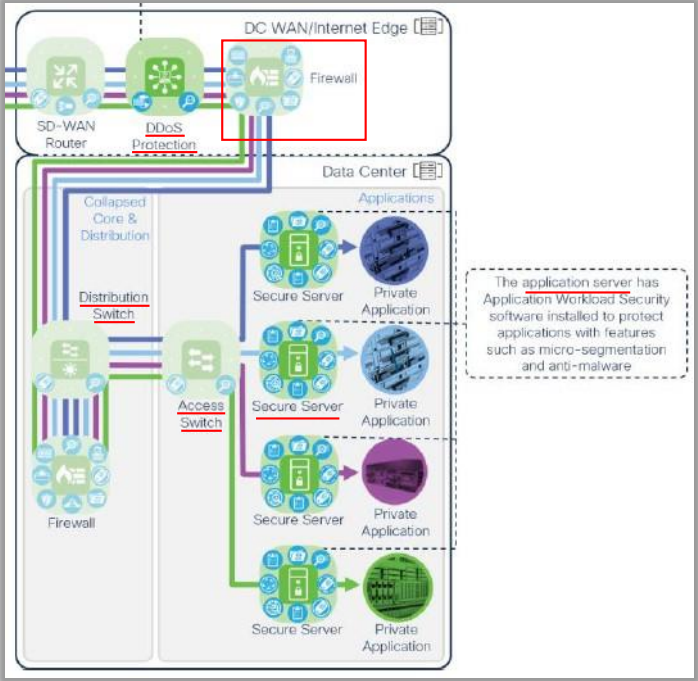
Claims 1 & 6-9

1-d an endpoint device in communication with the second access point server;	A “Private Application”, i.e., end point device, is in communication with the “application server.”  <i>Id.</i> at 34. NOTE: The “Firewall” under the Distribution Switch may also be construed as a second access point server. First is “Secure Server” then the Firewall before traffic goes “north” towards the egress to the internet. If flowing from the Private Application Server, then the Private Application server is an endpoint.
--	---

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

1-e a first perimeter firewall in communication with the first access point server,	A “Firewall,” i.e., first perimeter firewall, is in communication with the “DDoS Protection” server.  <i>Id.</i> at 34. NOTE: The first perimeter firewall may include the DDoS protection that is doing SPI. The Access Point Server may include the SD-WAN router and/or the Distribution Switch. The second perimeter firewall may be either the Firewall in DC WAN / Internet Edge or could also be the Firewall in the Data Center.
---	--

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

1-e Cont. wherein the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and	The “Firewall as a Service (FWaaS) is the cloud-based delivery of firewall functionality to protect non-web Internet traffic.” It performs “layer 3-4 filtering.” “stateful inspection in the firewall occurs at layers 3 and 4 of the OSI model and is an advanced technology in firewall filtering. In order to achieve this objective, the firewall maintains a state table of the internal structure of the firewall. Whenever a packet is to be sent across the firewall, the information of state stored in the state table is used to either allow or deny passage of that packet.”, i.e., the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server Firewall as a Service (FWaaS) is the cloud-based delivery of firewall functionality to protect non-web Internet traffic. In addition to layer 3-4 filtering, FWaaS typically includes features for intrusion prevention and application-level visibility and control. Figure 7. Firewall as a Service Overview <i>Id.</i> at 8-9.
--	--

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

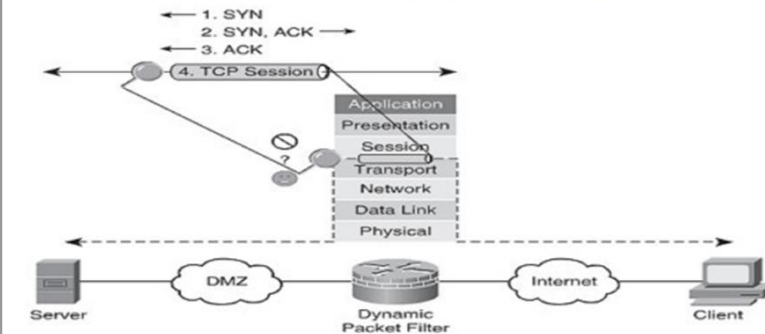
Claims 1 & 6-9

1-e
Cont.

A stateful firewall refers to that firewall which keeps a track of the state of the network connections traveling across it, hence the nomenclature. The programming of the firewall is configured in such a manner that only legible packets are allowed to be transmitted across it, whilst the others are not allowed.

This stateful inspection in the firewall occurs at layers 3 and 4 of the OSI model and is an advanced technology in firewall filtering. In order to achieve this objective, the firewall maintains a state table of the internal structure of the firewall. Whenever a packet is to be sent across the firewall, the information of state stored in the state table is used to either allow or deny passage of that packet.

Take a look at the figure below to see and understand the working of a stateful firewall.

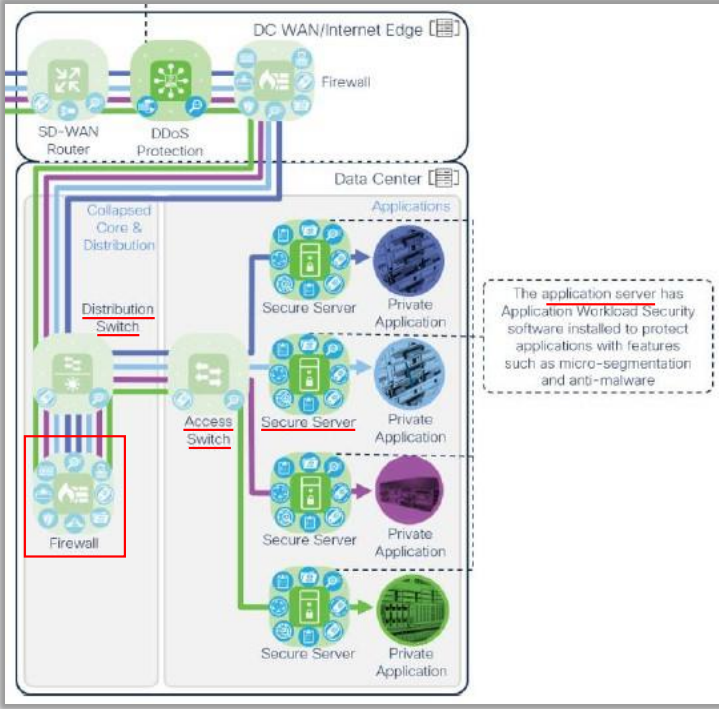


Source: Stateful Firewall Overview,
<https://learningnetwork.cisco.com/s/question/0D53i00000Ksup8CAB/stateful-firewall-overview>
(annotations added)

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

1-f a second perimeter firewall in communication with the second access point server,	Another “Firewall,” i.e., second perimeter firewall, is in communication with the “application server” server through a “Distribution Switch” and an “Access Switch.”  Source: Cisco Secure Access Service Edge (SASE) and Security Service Edge (SSE), p.34 https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/sase-sse-ag.pdf (annotations added)
---	---

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

1-f Cont. wherein the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device,	The “Firewall as a Service (FWaaS)”, i.e. second perimeter firewall, “is the cloud-based delivery of firewall functionality to protect non-web Internet traffic.” NOTE: In this context there may be two starting points. 1) Internet or SD-Wan fabric to the left of the SD-WAN router through to Private Applications, or 2) Private Application Server to a secure server to Access Switch to FW to FW to Ddos to SD-WAN router (EIP). Considering the traffic flow, SIP from the internet to protect against threats which can be identified by URL and/or IP address resolution and/or headers of individual packets using SPI - stateful packet inspection. More time consuming and resource intensive/expensive DPI - deep packet inspection can be done at the Firewall.
--	---

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

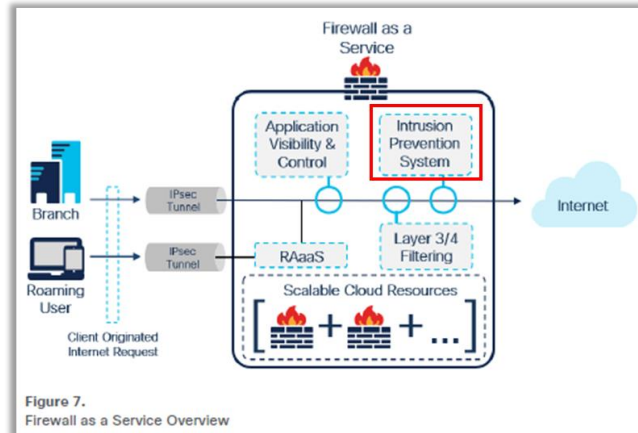
Claims 1 & 6-9

1-f
Cont.

“In addition to layer 3-4 filtering, FWaaS typically includes features for intrusion prevention and application-level visibility and control.”, i.e., performs deep packet inspection.

“An intrusion prevention system (IPS) provides network visibility, security intelligence, automation, and advanced threat protection.” “You can place a sensor in the network to analyze network traffic in one of two ways. The first option is to put a sensor inline with the traffic, which just means that any traffic going through your network is forced to go in one physical or logical port on the sensor. At the sensor, the traffic is analyzed. That is the concept behind intrusion prevention systems (IPS).”, i.e., to prevent at least some traffic from passing from the second access point server to the end point device.

Firewall as a Service (FWaaS) is the cloud-based delivery of firewall functionality to protect non-web Internet traffic. In addition to layer 3-4 filtering, FWaaS typically includes features for intrusion prevention and application-level visibility and control.



Id. at 8-9.

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

1-f Cont. wherein at least one of the egress ingress point device, the first access point server, the second access point server, the endpoint device, the first perimeter firewall, or the second perimeter firewall comprises hardware,	<u>An intrusion prevention system (IPS) provides network visibility, security intelligence, automation, and advanced threat protection.</u> <i>Id.</i> at 21. <u>You can place a sensor in the network to analyze network traffic in one of two ways. The first option is to put a sensor inline with the traffic, which just means that any traffic going through your network is forced to go in one physical or logical port on the sensor. At the sensor, the traffic is analyzed. That is the concept behind intrusion prevention systems (IPS).</u> IDS is detecting the attack (hence the term intrusion detection system) but is not preventing the attack. Source: Cisco IDS/IPS Fundamentals https://learningnetwork.cisco.com/s/question/0D53i00000KsuxDCAR/cisco-idsips-fundamentals (annotations added)
---	---

17 of 27

July 31, 2023

Note: All internet sources last accessed and downloaded July 31, 2023.

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

1-f Cont. wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the second perimeter firewall.	The “SD-WAN Router”, i.e., egress ingress point device, comprises hardware. Furthermore, the server and the firewall components comprises hardware to perform their respective functionalities, i.e., at least one of the egress ingress point device, the first access point server, the second access point server, the endpoint device, the first perimeter firewall, or the second perimeter firewall comprises hardware. “IDS is detecting the attack (hence the term intrusion detection system) but is not preventing the attack.” Intrusion detection is arguably performed to detected unknow threats and it is not performed in real time, i.e., the deep packet inspection is performed on a cloned copy of traffic that flows through the second perimeter firewall. You can place a sensor in the network to analyze network traffic in one of two ways. The first option is to put a sensor inline with the traffic, which just means that any traffic going through your network is forced to go in one physical or logical port on the sensor. At the sensor, the traffic is analyzed. That is the concept behind intrusion prevention systems (IPS). <u>IDS is detecting the attack (hence the term intrusion detection system) but is not preventing the attack.</u> Source: Cisco IDS/IPS Fundamentals https://learningnetwork.cisco.com/s/question/0D53i00000KsuxDCAR/cisco-idsips-fundamentals (annotations added)
---	--

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

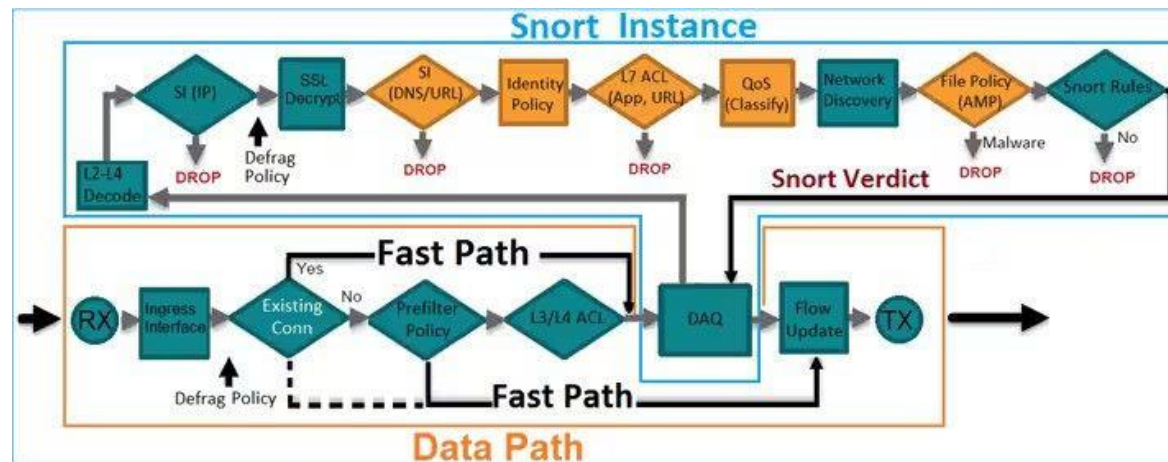
U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

1-f
Cont.

Also see: Verification 3. Firewall Engine Debug For Allowed Traffic

Firewall engine debug runs against specific components of the FTD Snort Engine like the Access Control Policy as shown in the image:



Source: <https://www.cisco.com/c/dam/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int-11.png>

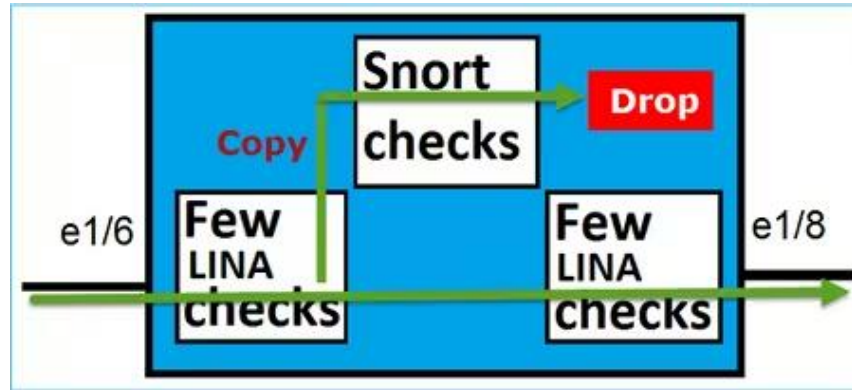
UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

1-f
Cont.

Also see:

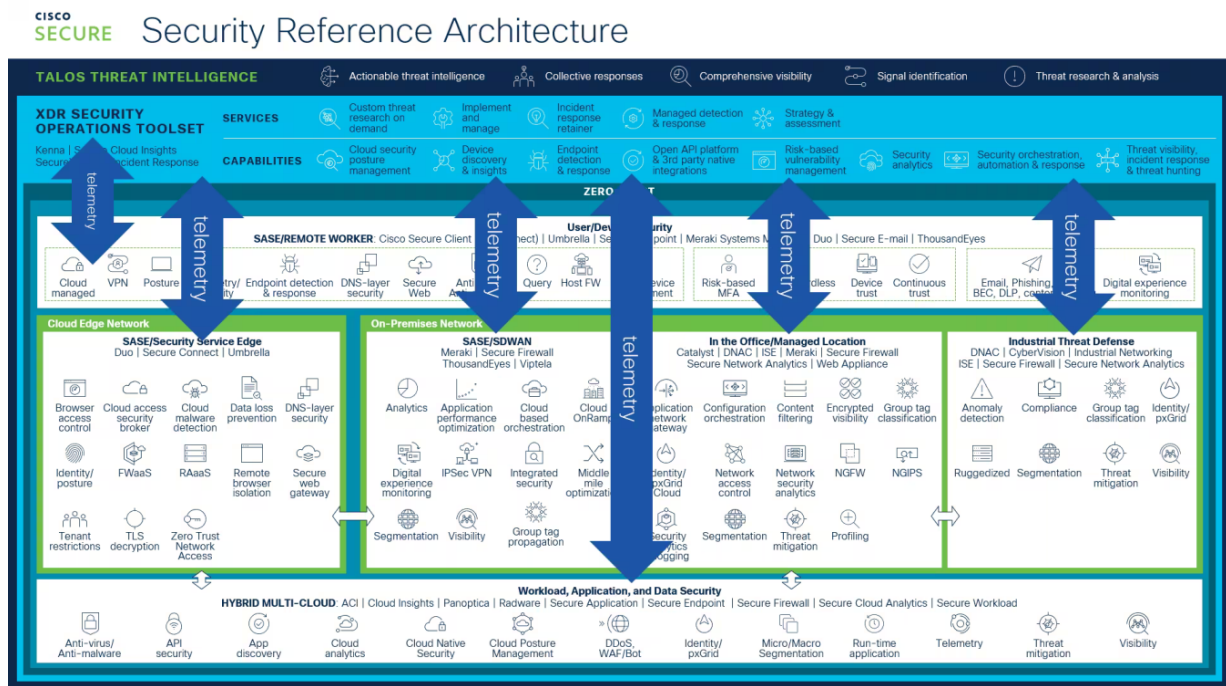


Source: <https://www.cisco.com/c/dam/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int-15.png>

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

Claim #6	Accused Instrumentalities
6. The multi-perimeter firewall system according to claim 3, wherein the first perimeter firewall and the second perimeter firewall share threat information including at least one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors.	See: https://www.cisco.com/c/en/us/products/security/cisco-security-reference-architecture.html  The diagram illustrates the Cisco Security Reference Architecture, organized into several layers and components. At the top is the 'TALOS THREAT INTELLIGENCE' layer, followed by 'XDR SECURITY OPERATIONS TOOLSET' and 'SERVICES'. Below these are 'CAPABILITIES' and 'ZERO TRUST' sections. The architecture is divided into three main network segments: 'Cloud Edge Network', 'On-Premises Network', and 'In the Office/Managed Location'. Each segment contains various security and management tools, such as firewalls, intrusion detection systems, and endpoint protection. A 'HYBRID MULTI-CLOUD' section at the bottom integrates cloud and on-premises security. Vertical double-headed arrows labeled 'telemetry' connect the different layers, indicating bidirectional data flow. The diagram also shows 'Workload, Application, and Data Security' components at the bottom. Use case: SecureX telemetry and orchestration Source: https://www.cisco.com/c/en/us/products/security/cisco-security-reference-architecture/jcr:content/Grid/category_atl/layout-category-atl/blade_copy_copy_389441412/bladeContents/image_copy/image.img.png/1672931612669.png

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

Claim #7	Accused Instrumentalities
7. The multi-perimeter firewall system according to claim 6, wherein the first perimeter firewall and the second perimeter firewall share threat information with a central control server.	See: https://blogs.cisco.com/security/a-bridge-to-the-future-of-the-firewall Introducing Cisco Security Analytics and Logging Available soon through Cisco Defense Orchestrator, the Security Analytics and Logging service helps you make better security policy management decisions by providing greater visibility and threat detection capabilities across your firewall and network. It allows you to correlate the static events on a firewall with behavioral analytics and private network monitoring enabled by Stealthwatch Cloud. First, it aggregates and centralizes intelligence from NGFW logs and network logs securely in the cloud, accessible and searchable from Cisco Defense Orchestrator. Then, it enriches and correlates threat intelligence in the context of specific events and alerts within an organization’s systems to baseline normal behavior. Lastly, it uses this intelligence to speed investigations and provide insights for corrective security policy actions.

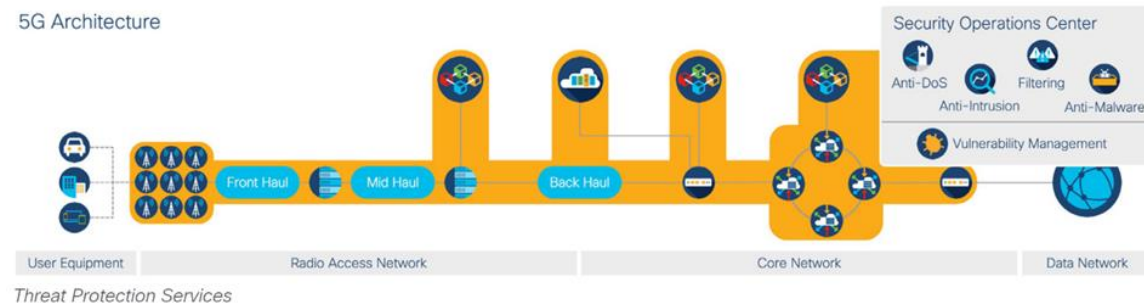
UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

Clm. 7
(cont.)

Also see:



Source: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-5g-cybersecurity-guidance.pdf

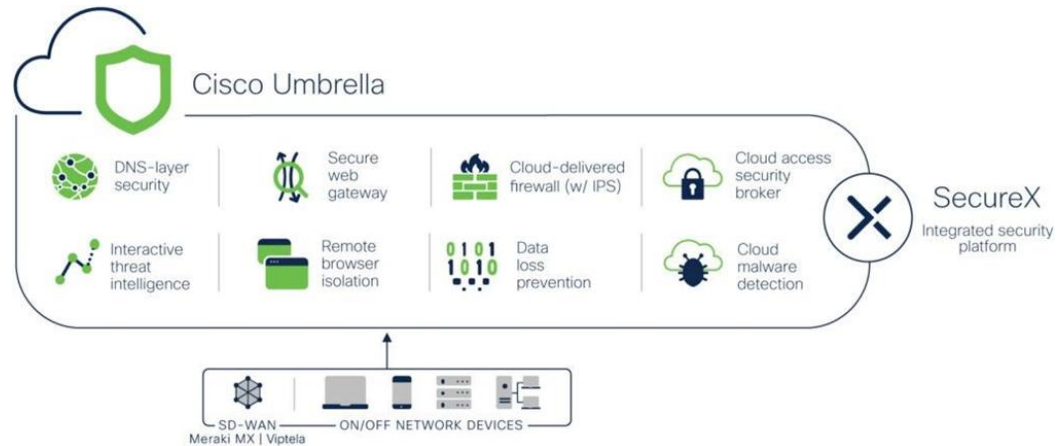
UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

Clm. 7
(cont.)

Also see:



Source: https://cdn.umbrella.marketops.umbrella.com/wp-content/uploads/2022/02/07092830/Cisco-Umbrella-SASE-Offering_full-view-1024x434.jpg

Cisco-Umbrella-SASE-Offering_full-view-1024x434.jpg

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

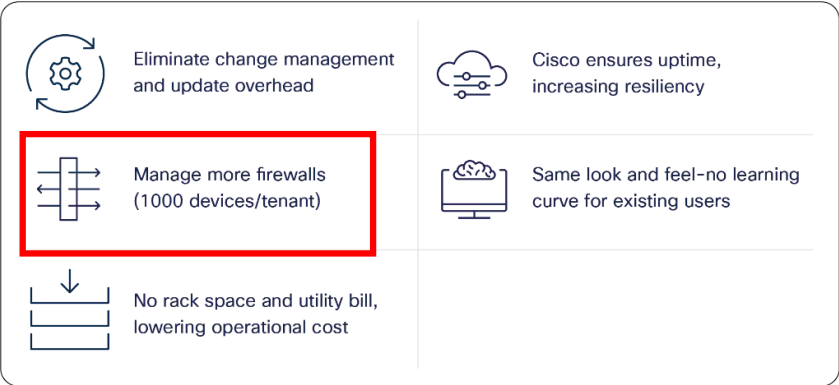
Claims 1 & 6-9

Claim #8	Accused Instrumentalities
8. The multi-perimeter firewall system according to claim 1, wherein the deep packet inspection is performed on flow through traffic.	NOTE: DPI can be configured to check in real time on flow through traffic and not on cloned copies. See, e.g., https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/m-config-deep-packet-inspection.pdf

UMBRA TECHNOLOGIES LTD.’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

Claim #9	Accused Instrumentalities
9. The multi-perimeter firewall system according to claim 1, wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand.	See: https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.html  Figure 3. Benefits of cloud-delivered Firewall Management Center via CDO Source: https://www.cisco.com/c/dam/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.docx/_jcr_content/renditions/datasheet-c78-736847_2.png

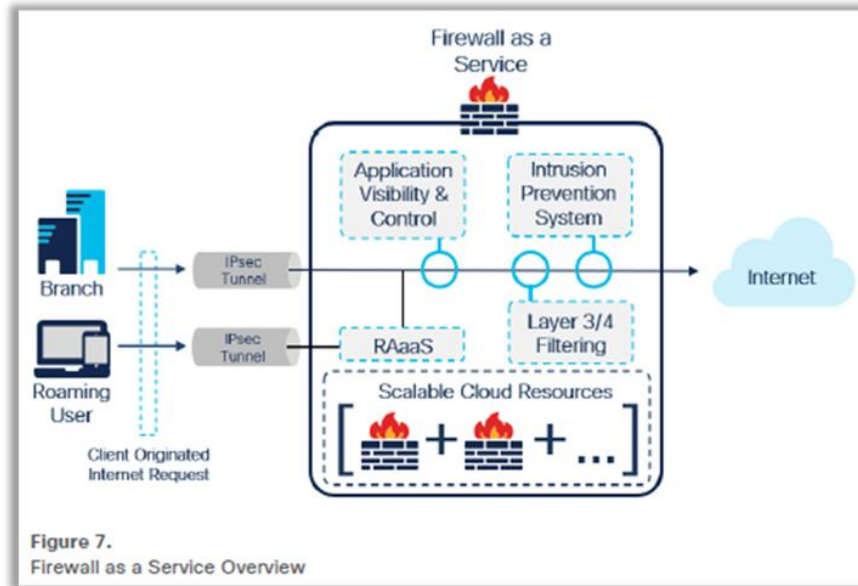
UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482 – Defendant Cisco Systems, Inc. - UMBRA Technologies Ltd. (“UMBRA”)

Claims 1 & 6-9

Clm. 9
(cont.)

Also see:



NOTE: “Scalable Cloud Resources” implies allocating more cloud firewall resources on demand.

Caveat: The notes and/or cited excerpts utilized herein are set forth for purposes only and are not meant to be limiting in any manner. For example, the notes and/or cited excerpts, may or may not be supplemented or substituted with different excerpt(s) of the relevant reference(s), as appropriate. Further, to the extent any error(s) and/or omission(s) exist herein, all rights are reserved to correct the same.