IN THE UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

OPTIMORPHIX, INC., ***Plaintiff,*** v. **FORTINET, INC.,** ***Defendant.***	**Civil Action No._________** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

OptiMorphix, Inc. ("OptiMorphix" or "Plaintiff") brings this action and makes the following allegations of patent infringement relating to U.S. Patent Nos.: 7,099,273 (the "'273 Patent"); 8,521,901 (the "'901 Patent"); 7,616,559 (the "'559 Patent"); 10,412,388 (the "'388 Patent"); 9,894,361 (the "'361 Patent"); 8,429,169 (the "'169 Patent"); (collectively, the "Patents-in-Suit"). Defendant Fortinet, Inc. ("Fortinet" or "Defendant") infringes the Patents-in-Suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

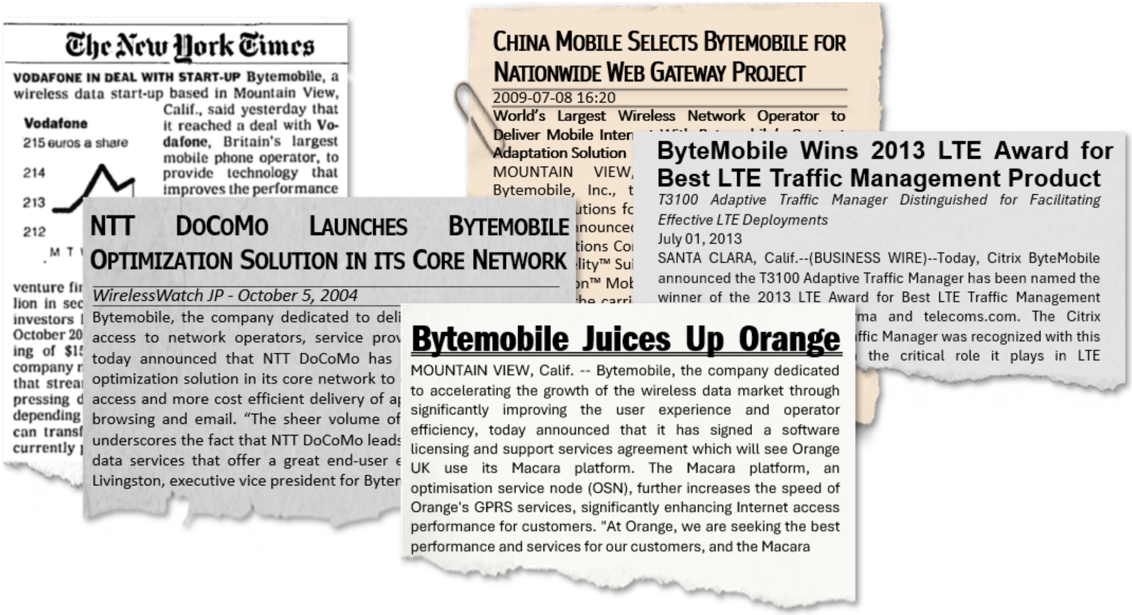
THE PARTIES

1. Plaintiff OptiMorphix, Inc. is a Delaware corporation that holds a portfolio of over 250 patent assets that were developed at Citrix Systems, Inc. ("Citrix") and Bytemobile, Inc.

2. Bytemobile, Inc. ("Bytemobile") was a global leader in mobile internet solutions for network operators. The company was founded in 2000. Bytemobile's mission was to optimize video and web content services for mobile network operators to improve users' experiences while maximizing the efficiency of network infrastructure.

3. Bytemobile was established during a time when the mobile landscape was evolving rapidly. The advent of 3G technology, coupled with increasingly sophisticated smartphones, led to a surge in demand for data services. However, mobile networks at the time were not optimized

to handle this influx, particularly for data-rich services like video streaming. Recognizing this opportunity, Bytemobile sought to create solutions that would enable network operators to deliver high-quality, consistent mobile data services. By 2011, Bytemobile was a "market leader in video and web optimization, with more than 125 cumulative operator deployments in 60 countries.[1]



The New York Times

VODAFONE IN DEAL WITH START-UP Bytemobile, a wireless data start-up based in Mountain View, Calif., said yesterday that it reached a deal with Vodafone, Britain's largest mobile phone operator, to provide technology that improves the performance

Vodafone
215 euros a share
214
213
212
M T

venture fir
lion in sec
investors
October 20
ing of $15
company r
that strea
pressing d
depending
can transf
currently

CHINA MOBILE SELECTS BYTEMOBILE FOR NATIONWIDE WEB GATEWAY PROJECT

2009-07-08 16:20

World's Largest Wireless Network Operator to Deliver Mobile Inter
Adaptation Solution

MOUNTAIN VIEW,
Bytemobile, Inc., t
utions fo
nnounced
tions Co
lity™ Su
on™ Mob
the carri

NTT DOCOMO LAUNCHES BYTEMOBILE OPTIMIZATION SOLUTION IN ITS CORE NETWORK

WirelessWatch JP - October 5, 2004

Bytemobile, the company dedicated to deli
access to network operators, service prov
today announced that NTT DoCoMo has
optimization solution in its core network to
access and more cost efficient delivery of ap
browsing and email. "The sheer volume of
underscores the fact that NTT DoCoMo leads
data services that offer a great end-user e
Livingston, executive vice president for Byten

ByteMobile Wins 2013 LTE Award for Best LTE Traffic Management Product

T3100 Adaptive Traffic Manager Distinguished for Facilitating Effective LTE Deployments

July 01, 2013

SANTA CLARA, Calif.--(BUSINESS WIRE)--Today, Citrix ByteMobile announced the T3100 Adaptive Traffic Manager has been named the winner of the 2013 LTE Award for Best LTE Traffic Management
rma and telecoms.com. The Citrix
ffic Manager was recognized with this
the critical role it plays in LTE

Bytemobile Juices Up Orange

MOUNTAIN VIEW, Calif. -- Bytemobile, the company dedicated to accelerating the growth of the wireless data market through significantly improving the user experience and operator efficiency, today announced that it has signed a software licensing and support services agreement which will see Orange UK use its Macara platform. The Macara platform, an optimisation service node (OSN), further increases the speed of Orange's GPRS services, significantly enhancing Internet access performance for customers. "At Orange, we are seeking the best performance and services for our customers, and the Macara

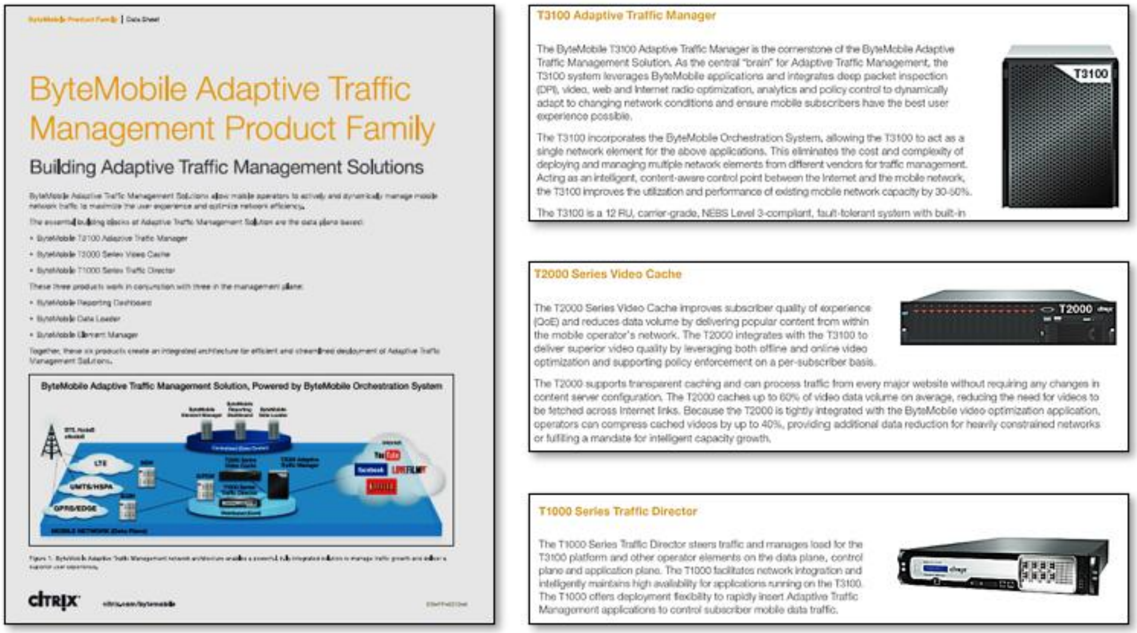
Andrew Zipern, *Vodafone in Deal with Start-Up Bytemobile*, NYTimes at C4 (January 29, 2002) ("Bytemobile, a wireless data start-up . . . reached a deal with Vodafone, Britain's largest mobile phone operator"); *NTT DoCoMo Launches Bytemobile Optimization Solution in its Core Network*, WIRELESSWATCH IP (October 5, 2004) ("NTT DoCoMo has deployed Bytemobile's optimization solution in its core network"); *China Mobile Selects Bytemobile for Nationwide Web Gateway Project*, BUSINESS WIRE (July 8, 2009) ("A Bytemobile customer since 2004, CMCC has deployed its web optimization solutions"); *Bytemobile Juices Up Orange*, ESPICOM TELECOMMUNICATION NEWS (October 10, 2002) ("Orange customers will experience faster application performance and Web page downloads"); *ByteMobile Wins 2013 LTE Award for Best LTE Traffic Management Product*, MARKETSCREENER (July 1, 2013) ("ByteMobile technology has been deployed . . . in networks serving nearly two billion subscribers.").

4. Bytemobile products, such as the Unison platform and the T3100 Adaptive Traffic Manager, were designed to optimize mobile data traffic in real-time, ensuring a high-quality

[1] *Bytemobile: Importance of Video and Web Optimizations*, TELECOM REVIEW at 58 (2011); *see also Bytemobile Secures Its 36th Video Optimisation Win for MNO Deployment*, TOTAL TELECOM & TOTAL TELECOM MAGAZINE (March 21, 2011).

mobile internet experience for end-users. This approach was groundbreaking at the time and set the stage for many of the mobile data optimization techniques used today.

5. Bytemobile's innovative technologies and customer-centric approach led to rapid growth and success. Bytemobile's innovative product portfolio included: the T3100 Adaptive Traffic Manager which was designed to handle high volumes of traffic efficiently and provide real-time optimization, compression, and management of mobile data; Bytemobile's T2000 Series Video Cache, which supported transparent caching of content; and Bytemobile's T1000 Series Traffic Director, which enabled traffic steering and load balancing for high availability of applications.



ByteMobile Product Family | Data Sheet

ByteMobile Adaptive Traffic Management Product Family

Building Adaptive Traffic Management Solutions

ByteMobile Adaptive Traffic Management Solutions allow mobile operators to actively and dynamically manage mobile network traffic to maximize the user experience and optimize network efficiency.

The essential building blocks of Adaptive Traffic Management Solution are the data plane based:

- ByteMobile T3100 Adaptive Traffic Manager
- ByteMobile T2000 Series Video Cache
- ByteMobile T1000 Series Traffic Director

These three products work in conjunction with three in the management plane:

- ByteMobile Reporting Dashboard
- ByteMobile Data Loader
- ByteMobile Element Manager

Together, these six products create an integrated architecture for efficient and streamlined deployment of Adaptive Traffic Management Solutions.

ByteMobile Adaptive Traffic Management Solution, Powered by ByteMobile Orchestration System

Figure 1: ByteMobile Adaptive Traffic Management network architecture enables a powerful, fully integrated solution to manage traffic growth and deliver a superior user experience.

citrix.com/bytemobile

T3100 Adaptive Traffic Manager

The ByteMobile T3100 Adaptive Traffic Manager is the cornerstone of the ByteMobile Adaptive Traffic Management Solution. As the central "brain" for Adaptive Traffic Management, the T3100 system leverages ByteMobile applications and integrates deep packet inspection (DPI), video, web and Internet radio optimization, analytics and policy control to dynamically adapt to changing network conditions and ensure mobile subscribers have the best user experience possible.

The T3100 incorporates the ByteMobile Orchestration System, allowing the T3100 to act as a single network element for the above applications. This eliminates the cost and complexity of deploying and managing multiple network elements from different vendors for traffic management. Acting as an intelligent, content-aware control point between the Internet and the mobile network, the T3100 improves the utilization and performance of existing mobile network capacity by 30-50%.

The T3100 is a 12 RU, carrier-grade, NEBS Level 3-compliant, fault-tolerant system with built-in

T2000 Series Video Cache

The T2000 Series Video Cache improves subscriber quality of experience (QoE) and reduces data volume by delivering popular content from within the mobile operator's network. The T2000 integrates with the T3100 to deliver superior video quality by leveraging both offline and online video optimization and supporting policy enforcement on a per-subscriber basis.

The T2000 supports transparent caching and can process traffic from every major website without requiring any changes in content server configuration. The T2000 caches up to 60% of video data volume on average, reducing the need for videos to be fetched across Internet links. Because the T2000 is tightly integrated with the ByteMobile video optimization application, operators can compress cached videos by up to 40%, providing additional data reduction for heavily constrained networks or fulfilling a mandate for intelligent capacity growth.

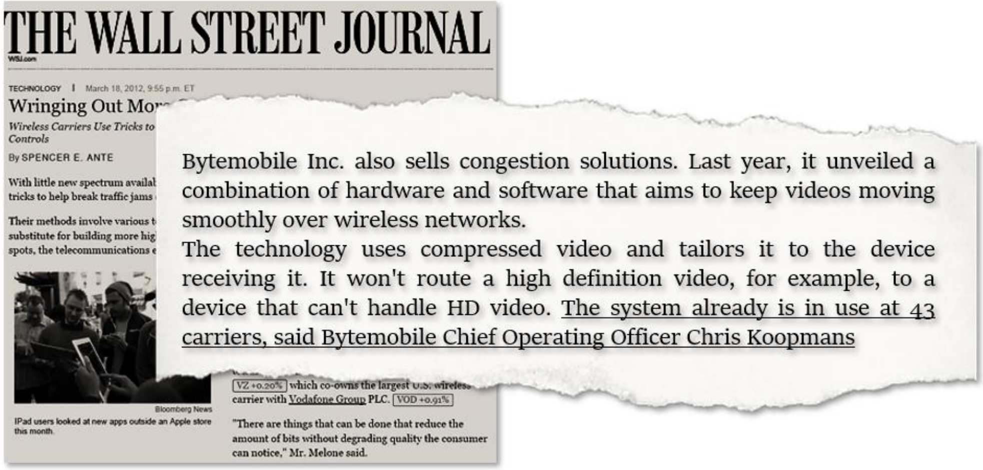
T1000 Series Traffic Director

The T1000 Series Traffic Director steers traffic and manages load for the T3100 platform and other operator elements on the data plane, control plane and application plane. The T1000 facilitates network integration and intelligently maintains high availability for applications running on the T3100. The T1000 offers deployment flexibility to rapidly insert Adaptive Traffic Management applications to control subscriber mobile data traffic.

Bytemobile Adaptive Traffic Management Product Family, BYTEMOBILE DATA SHEET at 1-2 (2014).

6. Bytemobile's groundbreaking technologies also included products for data optimization. Bytemobile's data optimization solutions were designed to compress and accelerate data transfer. By reducing the size of data packets without compromising quality, these technologies allowed faster data transmission and minimized network congestion. Bytemobile

also offered solutions to analyze and manage network traffic, allowing network operators to identify patterns, allocate bandwidth intelligently, and prioritize different types of content.



THE WALL STREET JOURNAL

WSJ.com

TECHNOLOGY | March 18, 2012, 9:55 p.m. ET

Wringing Out Mor

Wireless Carriers Use Tricks to
Controls

By SPENCER E. ANTE

With little new spectrum availab
tricks to help break traffic jams

Their methods involve various t
substitute for building more hig
spots, the telecommunications e

Bytemobile Inc. also sells congestion solutions. Last year, it unveiled a combination of hardware and software that aims to keep videos moving smoothly over wireless networks.

The technology uses compressed video and tailors it to the device receiving it. It won't route a high definition video, for example, to a device that can't handle HD video. The system already is in use at 43 carriers, said Bytemobile Chief Operating Officer Chris Koopmans

Bloomberg News

IPad users looked at new apps outside an Apple store this month.

VZ +0.20% which co-owns the largest U.S. wireless carrier with Vodafone Group PLC. VOD +0.91%

"There are things that can be done that reduce the amount of bits without degrading quality the consumer can notice," Mr. Melone said.

Spencer E. Ante, *Wringing Out More Capacity*, WALL STREET JOURNAL at B3 (March 19, 2012) (emphasis added).

7. In July 2012, Bytemobile was acquired by Citrix Systems, Inc. ("Citrix") for $435 million. Bytemobile "became part of [Citrix's] Enterprise division and extend[ed] [Citrix's] industry reach into the mobile and cloud markets."[2]

8. OptiMorphix owns a portfolio of patents developed at Bytemobile and later Citrix. Highlighting the importance of the patents-in-suit is the fact that the OptiMorphix's patent portfolio has been cited by over 4,800 U.S. and international patents and patent applications assigned to a wide variety of the largest companies operating in the networking, content delivery, and cloud computing fields. OptiMorphix's patents have been cited by companies such as:

- Amazon.com, Inc. (263 citing patents and applications)[3]
- Oracle (59 citing patents and applications)[4]
- Alphabet, Inc. (103 citing patents and applications)[5]
- Broadcom Ltd. (93 citing patents and applications)[6]

[2] CITRIX SYSTEMS, INC. 2012 ANNUAL REPORT at 33 (2013).

[3] *See e.g.*, U.S. Patent Nos. 7,817,563; 9,384,204; 9,462,019; 11,343,551; and 11,394,620.

[4] *See e.g.*, U.S. Patent Nos. 7,475,402; 7,574,710; 8,589,610; 8,635,185; and 11,200,240.

[5] *See e.g.*, U.S. Patent Nos. 7,743,003; 8,458,327; 9,166,864; 9,665,617; and 10,733,376.

[6] *See e.g.*, U.S. Patent Nos. 7,636,323; 8,448,214; 9,083,986; 9,357,269; and 10,091,528.

- Cisco Systems, Inc. (277 citing patents and applications)[7]
- Lumen Technologies, Inc. (77 citing patents and applications)[8]
- Intel Corporation (45 citing patents and applications)[9]
- Microsoft Corporation (150 citing patents and applications)[10]
- AT&T, Inc. (93 citing patents and applications)[11]
- Verizon Communications, Inc. (31 citing patents and applications)[12]
- Juniper Networks, Inc. (29 citing patents and applications)[13]

9. Defendant Fortinet, Inc. is a Delaware corporation with its principal place of business at 909 Kifer Road, Sunnyvale, CA 94086. Fortinet may be served through its registered agent Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

JURISDICTION AND VENUE

10. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

11. Venue is proper in this District under 28 U.S.C. §§ 1391(b)-(d) and 1400(b).

12. This Court has personal jurisdiction over Fortinet because it is organized under the laws of the State of Delaware and it maintains a registered agent in Delaware.

THE ASSERTED PATENTS

U.S. PATENT NO. 7,099,273

13. U.S. Patent No. 7,099,273 entitled, *Data Transport Acceleration and Management Within a Network Communication System*, was filed on January 29, 2002. The ‘273 Patent is subject to a 35 U.S.C. § 154(b) term extension of 1,021 days. The ‘273 Patent claims priority to

[7] *See e.g.*, U.S. Patent Nos. 7,656,800; 7,930,734; 8,339,954; 9,350,822; and 10,284,484.

[8] *See e.g.*, U.S. Patent Nos. 7,519,353; 8,315,179; 8,989,002; 10,511,533; and 11,233,740.

[9] *See e.g.*, U.S. Patent Nos. 7,394,809; 7,408,932; 9,515,942; 9,923,821; and 10,644,961.

[10] *See e.g.*, U.S. Patent Nos. 8,248,944; 9,071,841; 9,852,118; 10,452,748; and 11,055,47.

[11] *See e.g.*, U.S. Patent Nos. 8,065,374; 8,429,302; 9,558,293; 9,800,638; and 10,491,645.

[12] *See e.g.*, U.S. Patent Nos. 8,149,706; 8,930,559; 9,253,231; 10,003,697; and 10,193,942.

[13] *See e.g.*, U.S. Patent Nos. 8,112,800; 8,509,071; 8,948,174; 9,407,726; and 11,228,631.

U.S. Provisional Patent Application No. 60/309,212 filed on July 31, 2001, and U.S. Provisional Patent Application No. 60/283,542 filed on April 12, 2001. A true and correct copy of the ‘273 Patent is attached hereto as Exhibit 1.

14. The ‘273 Patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the ‘273 Patent.

15. The technologies disclosed in the ‘273 Patent improve the efficiency and speed of data transmission within network communication systems. The ‘273 Patent introduces methods and apparatuses that enhance data transport, especially in environments where network conditions are variable or unpredictable and “provide systems and method for data transport acceleration and management within a network communication system.” ‘273 Patent, col. 3:31-33.

16. The ‘273 Patent is directed to solving the problem of inefficient data transport within network communication systems. This inefficiency can lead to poor utilization of network resources, increased latency, and reduced overall performance.

17. The ‘273 Patent identifies the shortcomings of the prior art. Specifically, the specification describes that traditional methods of data transport in network communication systems often fail to efficiently manage and accelerate data transport, especially in environments with variable or unpredictable network conditions. These methods may not adequately handle network congestion, leading to poor utilization of network resources, increased latency, and reduced overall performance. “This bursty nature of data transmission may under-utilize the available bandwidth on the downlink channel, and may cause some applications requiring a steady flow of data, such as audio or video, to experience unusually poor performance.” ‘273 Patent, col. 2:1-6.

18. The ‘273 Patent points out that conventional congestion control mechanisms tend to exhibit sub-optimal performance during initialization of data connections over reduced-bandwidth channels, such as wireless links. When a connection is initiated, the congestion control mechanism aggressively increases the size of the congestion window until it senses a data packet loss. This process may adversely impact other connections that share the same reduced-bandwidth channel as the connection being initialized attempts to maximize its data throughput without regard of the other pre-existing connections. This can lead to inefficient use of resources with decreased overall throughput.

19. The ‘273 Patent teaches the use of various techniques to accelerate and manage data transport in network communication systems. These techniques include the use of congestion control mechanisms, timers, and other methods to optimize data transmission. By implementing these techniques, the patent aims to improve the efficiency of data transport, particularly in environments with variable or unpredictable network conditions. This can lead to better utilization of network resources, reduced latency, and improved overall performance. The inventions disclosed in the ‘273 Patent provide significant benefits and improvements to the function of the hardware in a computer network.

20. On March 8, 2024, Unified Patents, LLC filed a Request for *Ex Parte* Reexamination of the ‘273 Patent with the United States Patent and Trademark Office. The Patent Office entered an Order Granting *Ex Parte* Reexamination of the ‘273 Patent on April 29, 2024. On September 11, 2024, the Primary Examiner assigned to the Reexamination of the ‘273 Patent issued an Order confirming the patentability of all claims of the ‘273 Patent. On November 14, 2024, the United States Patent and Trademark Office issued *Ex Parte* Reexamination Certificate

No. 12770 confirming the patentability of Claims 1-15 of the '273 Patent. A true and correct copy of that Certificate is attached hereto as Exhibit 2.

21. The '273 Patent family has been cited by 1,466 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies and research institutions have cited the '273 Patent family as relevant prior art:

- Cisco Technology, Inc.
- Qualcomm Incorporated
- International Business Machines Corporation
- Intel Corporation
- Microsoft Corporation
- Broadcom Corporation
- Google Inc.
- F5 Networks, Inc.
- Adobe Systems Incorporated
- Apple Inc.
- Lumen Technologies, Inc
- Oracle Corporation
- Amazon.com, Inc.

U.S. PATENT NO. 8,521,901

22. U.S. Patent No. 8,521,901 entitled, *TCP Burst Avoidance*, was filed on December 22, 2008. The '901 Patent claims priority to Provisional Patent Application No. 61/017,275, filed on December 28, 2007. The '901 Patent is subject to a 35 U.S.C. § 154(b) term extension of 525 days. A true and correct copy of the '901 Patent is attached hereto as Exhibit 3.

23. The '901 Patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the '901 Patent.

24. The '901 Patent generally relates to methods and systems for minimizing packet bursts. The '901 Patent teaches implementing a packet scheduler layer between the network layer and the transport layer of a device, which smooths the delivery of TCP packets by delaying their

delivery, thus addressing the challenges posed by the rapid and bursty transmission of data packets in network communications.

25. The ‘901 Patent is directed to solving the problem of TCP packet bursts in high-speed data networks, which can result from the buffering of TCP acknowledgment packets. These bursts can cause packet loss and inefficient use network bandwidth.

26. The ‘901 Patent identifies the shortcomings of the prior art. Specifically, the specification describes that the prior art does not adequately address the issues of packet loss and inefficient bandwidth utilization resulting from the bursty nature of TCP packet transmission in data networks. The prior technologies do not effectively manage the sudden bursts of TCP acknowledgment packets, which can be caused by buffering, leading to suboptimal utilization of available bandwidth and undesirable packet loss.

27. The ‘901 Patent teaches the use of a packet scheduler layer, which is positioned between the network and transport layers of a device. This layer receives, smoothens (by delaying), and sends TCP packets to ensure that the delivery of these packets is managed in a manner that mitigates the issues of packet bursts. The packet scheduler layer manages both incoming and outgoing packets, ensuring that the transmission of these packets is smoothed out, thereby minimizing packet loss and ensuring more efficient use of available bandwidth. This approach provides benefits that differ from conventional methods by ensuring that TCP packet transmission is managed in a way that minimizes packet loss and ensures efficient bandwidth utilization, thereby addressing the specific challenges posed by TCP packet bursts in high-speed data networks.

28. The invention taught by the ‘901 Patent solves discrete, technological problems associated with computer systems; specifically, it addresses the issues of packet loss and inefficient

bandwidth utilization in high-speed data networks by managing the transmission of TCP packets in a manner that smoothens their delivery, thereby ensuring that the available bandwidth is utilized efficiently, and that packet loss is minimized.

29. The ‘901 Patent family has been cited by 21 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘901 Patent family as relevant prior art:

- Lenovo Group Limited
- Telefonaktiebolaget Lm Ericsson
- Qualcomm, Inc.
- Nippon Telegraph & Telephone Corp.
- Hitachi, Ltd.
- Cisco Systems, Inc.
- Akamai Technologies, Inc.
- Huawei Technologies Co., Ltd.

U.S. PATENT NO. 7,616,559

30. U.S. Patent No. 7,616,559 entitled, *Multi-Link Network Architecture, Including Security, In Seamless Roaming Communications Systems And Methods*, was filed on September 2, 2004. The ‘559 Patent claims priority to Provisional Application No. 60/499,648, which was filed on September 3, 2003. The ‘559 Patent is subject to a 35 U.S.C. § 154(b) term extension of 638 days. A true and correct copy of the ‘559 Patent is attached hereto as Exhibit 4.

31. The ‘559 Patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the ‘559 Patent.

32. The ‘559 Patent generally relates to a communications system that provides secure communications of information over multiple communication links. This system includes a client device, a server device, and at least one communication channels, elements, modes, and links for connecting the devices for communication of information between them. The system includes a link detector for determining the existence and usability of the communication links for

communication of the information, a pathfinder for selecting one or more of the communication links for communication of at least some of the information, a link handover for switching to the selected one or more communication links for communication of the information or portion thereof, and an auto reconnector for re-connecting to detected and selected one or more communication links for communication of the information or portions of it in the event that any communication is hindered, terminated, or upset.

33. The ‘559 Patent is directed to solving the problem of ensuring secure and reliable communication over multiple communication links, especially in environments that include mobile or other roaming devices capable of communicating over multiple channels and with channel switching characteristics.

34. The ‘559 Patent identifies the shortcomings of the prior art. Specifically, the specification describes that when multiple links, both physical elements and the bands or channels within each such element, are employed for communications in data networks, substantial coordination of communicated information, as well as security of the information, is exponentially complicated. In wireless communications, concurrent or sequential operations can occur over cellular or wireless LAN technologies. Each of these wireless communications methods experiences substantially greater complexity in timing, security, packet sequencing, data loss, and connectivity, over wired communications conditions.

35. The ‘559 Patent teaches the use of a system that includes a link detector for determining the existence and usability of the communication links for communication of the information, a pathfinder for selecting one or more of the communication links for communication of at least some of the information, a link handover for switching to the selected one or more communication links for communication of the information or portion thereof, and an auto

reconnector for re-connecting to detected and selected one or more communication links for communication of the information or portions of it in the event that any communication is hindered, terminated, or upset.

36. The inventions disclosed in the ‘559 Patent provide significant benefits and improvements to the function of the hardware in a computer network by ensuring secure and reliable communication over multiple communication links. This is particularly beneficial in environments that include mobile or other roaming devices capable of communicating over multiple channels and with channel switching characteristics. The system’s ability to detect usable communication links, select the most suitable ones, switch between them as needed, and reconnect in the event of communication disruption greatly enhances the reliability and efficiency of data transmission in a computer network.

37. The ‘559 Patent family has been cited by 17 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies and research institutions have cited the ‘559 Patent family as relevant prior art:

- International Business Machines Corporation
- Samsung Electronics Co., Ltd
- Alphabet Inc.
- Research In Motion Limited
- BT Group plc

U.S. PATENT NO. 10,412,388

38. U.S. Patent No. 10,412,388 entitled, *Framework for Quality-Aware Video Optimization*, was filed on January 8, 2018. The ‘388 Patent claims priority to U.S. Patent Application No. 12/751,951, which was filed on March 31, 2010, and which claims priority to U.S. Provisional Patent Application No. 61/165,224, which was filed on March 31, 2009. A true and correct copy of the ‘388 Patent is attached hereto as Exhibit 5.

39. The ‘388 Patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the ‘388 Patent.

40. The ‘388 Patent generally relates to a method and system for quality-aware video optimization. It teaches receiving an encoded video frame, decompressing it, extracting a first quantization parameter (QP), and acquiring a delta QP based on the first QP. The method also includes acquiring a second QP based on the delta QP and the first QP, compressing the decompressed video frame based on the second QP, and providing the compressed video frame. The process allows for fine control of quality degradation in byte-reduced content and can be applied to transcoding scenarios where the input and output compression formats are different.

41. The ‘388 Patent identifies the shortcomings of the prior art. Specifically, existing single-pass rate control techniques had a problem in that the relationship between the compressed byte size of a video frame and its quantization parameter were only known after the frame is encoded. This made it challenging to achieve byte reduction and controllable quality degradation in a single pass.

42. The ‘388 Patent teaches the use of a quality-aware video optimization technique that modifies a video frame sequence to reduce the byte size while limiting perceptual quality degradation to a controllable level.

43. The inventions disclosed in the ‘388 Patent provide significant benefits and improvements to the function of hardware in a computer network by enabling efficient video optimization. The method allows for single-pass, on-the-fly quality-aware optimization, making it well-suited for various environments, including live video feeds and storage arrays.

44. The ‘388 Patent family has been cited by 30 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies and research institutions have cited the ‘388 Patent family as relevant prior art:

- Interdigital, Inc.
- Tencent Holdings Ltd
- Microsoft Corporation
- Qualcomm, Inc.
- Lattice Semiconductor
- Openwave Mobility, Inc.
- Samsung Electronics Co., Ltd.
- Beijing Dajia Interconnection Information Technology Co., Ltd.

U.S. PATENT NO. 9,894,361

45. U.S. Patent No. 9,894,361 entitled, *Framework for Quality-Aware Video Optimization*, was filed on March 31, 2010. The ‘361 Patent claims priority to U.S. Provisional Application No. 61/165,224, which was filed on March 31, 2009. The ‘361 Patent is subject to a 35 U.S.C. § 154(b) term extension of 1,038 days. A true and correct copy of the ‘361 Patent is attached hereto as Exhibit 6.

46. The ‘361 Patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the ‘361 Patent.

47. The ‘361 Patent relates to a method and system for quality-aware video optimization. Specifically, it teaches receiving an encoded video frame, decompressing it, extracting a first quantization parameter (QP), and acquiring a delta QP based on the first QP. The method further includes acquiring a second QP based on the delta QP and the first QP, compressing the decompressed video frame based on the second QP, and providing the compressed video frame. The process is designed to reduce the byte size of the video stream as much as possible while limiting perceptual quality degradation to a controllable level.

48. The ‘361 Patent is directed to solving the problem of optimizing video quality in a way that balances the reduction of byte size with the preservation of perceptual quality. This involves a nuanced understanding of how quantization parameters (QPs) affect both the perceptual quality and the bitrate of a video frame, and how to manipulate these QPs to achieve the desired balance.

49. The ‘361 Patent identifies the shortcomings of the prior art. Specifically, existing single-pass rate control techniques had a problem in that the relationship between the compressed byte size of a video frame and its quantization parameter was only known after the frame was encoded. This made it challenging to achieve byte reduction and controllable quality degradation in a single pass.

50. The ‘361 Patent teaches the use of a quality-aware video optimization technique that requires only a single pass over the previously encoded video frame sequence to optimize the video frame sequence. It introduces a novel function that defines ΔQP according to the value of QPInput, allowing fine control of quality degradation in the byte-reduced content. It also considers differences between input and output compression formats (codecs) and computes codec adjustment that accounts for these differences.

51. The inventions disclosed in the ‘361 Patent provide significant benefits and improvements to the function of hardware in a computer network by enabling efficient video optimization. By allowing for single-pass, on-the-fly, quality-aware optimization, the patent’s methods can be applied in various environments, including optimizing live video feeds before they traverse a low-capacity network segment, or optimizing surveillance video before archiving, thus saving storage space and network bandwidth.

52. The ‘361 Patent family has been cited by 30 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies and research institutions have cited the ‘361 Patent family as relevant prior art:

- Interdigital, Inc.
- Tencent Holdings Ltd
- Microsoft Corporation
- Qualcomm, Inc.
- Lattice Semiconductor
- Openwave Mobility, Inc.
- Samsung Electronics Co., Ltd.
- Beijing Dajia Interconnection Information Technology Co., Ltd.

U.S. Patent No. 8,429,169

53. U.S. Patent No. 8,429,169 entitled, *Systems and Methods For Video Cache Indexing*, was filed on July 29, 2011. The ‘169 Patent claims priority to U.S. Provisional Patent Application No. 61/369,513, which was filed on July 30, 2010. A true and correct copy of the ‘169 Patent is attached hereto as Exhibit 7.

54. The ‘169 Patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the ‘169 Patent.

55. The ‘169 Patent is directed to solving the problem of inefficient caching of content, particularly when dynamic URLs are used to refer to the content. Traditional caching methods that index content based on URLs can lead to multiple cache entries for the same content or entries with expired references, reducing the efficiency and capacity of the cache. The technologies taught in the ‘169 Patent overcomes these inefficiencies by indexing the content cache based on a characterization of the content rather than the URL.

56. The ‘169 Patent identifies the shortcomings of the prior art. Specifically, that conventional content caching methods, especially those employing dynamic URLs, lead to two

main inefficiencies: (a) multiple cache entries corresponding to the same video content, thereby reducing the cache's capacity to serve unique content, and (b) content cache entries with expired references to content, reducing the useful capacity of the content cache. These inefficiencies hinder the performance of middleware services and website performance.

57. The '169 Patent teaches the use of a novel approach to cache video content by indexing the content cache based on a characterization of the video content rather than the URL. This method involves identifying characterization data related to the content request and using a hash function to generate an index. This index is then used to identify the corresponding entry in the cache data structure. By avoiding the use of dynamic URLs in the indexing process, the patent's method allows for more efficient caching, eliminating redundancies and invalid entries, and improving the overall efficiency of content delivery.

58. The inventions disclosed in the '169 Patent provide significant benefits and improvements to the function of the hardware in a computer network by enabling more efficient caching of video content. By indexing the content cache based on the characterization of the content rather than the URL, the patented method avoids the problems of redundant and invalid cache entries. This leads to better utilization of cache capacity, reduced burden on network infrastructure and web servers, and faster content delivery to users. The invention also allows for distinguishing between similar but non-identical videos, avoiding content aliasing, and ensuring that the correct content is delivered to the user.

59. The '169 Patent family has been cited by 92 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies and research institutions have cited the '169 Patent family as relevant prior art:

- Akamai Technologies, Inc.
- AMC Networks Inc.

- AT&T Inc.
- Atlassian Pty Ltd
- Canon Inc.
- Charter Communications, Inc.
- China Mobile Communications Corporation
- EchoStar Corporation
- Huawei Investment & Holding Co., Ltd.
- Interdigital, Inc.
- Juniper Networks, Inc.
- Koninklijke Philips Nv
- Microsoft Corporation
- Open Text Corporation
- SK Telecom Co., Ltd.
- Skyfire Labs, Inc., California
- ZTE Corporation

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 7,099,273

60. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

61. Fortinet designs, makes, uses, sells, and/or offers for sale in the United States products comprising systems and methods for data transport acceleration and management within a network communication system.

62. Fortinet designs, makes, sells, offers to sell, imports, and/or uses Fortinet products and services supporting FortiOS 7.4.0 and later, which include at least the following: FortiGate Models FG-40F, FG-40F-3G4G, FG-60F, FG-61F, FG-70F, FG-71F, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81F, FG-81F-POE, FG-90G, FG-91G, FG-100F, FG-101F, FG-120G, FG-121G, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-

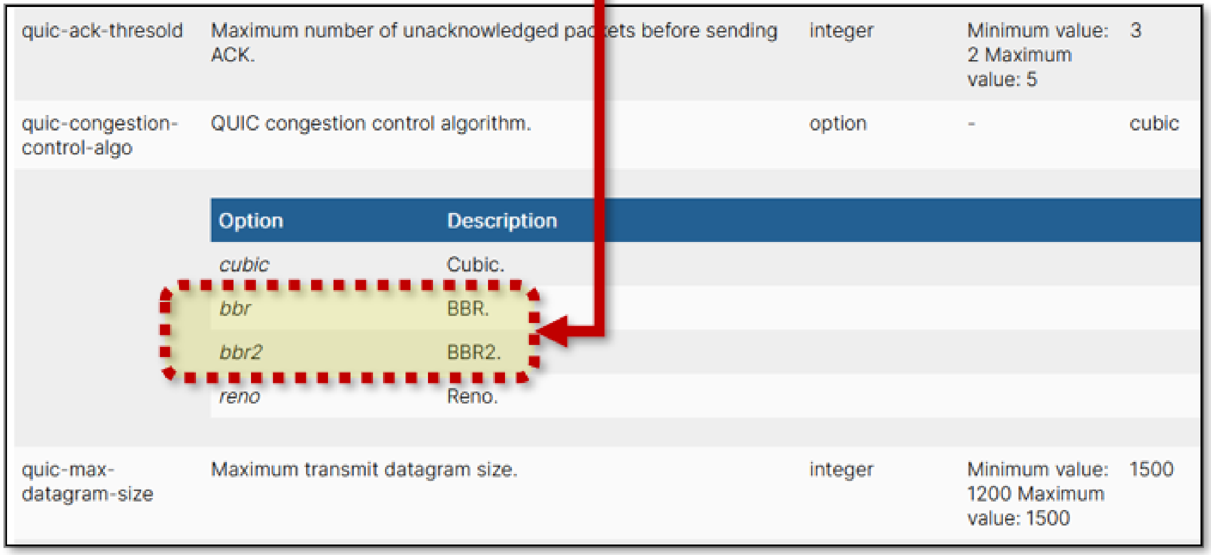
3000F, FG-3001F, FG-3100D, FG-3200D, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, and FG-7000F; FortiWiFi Models FWF-40F, FWF-40F-3G4G, FWF-60F, FWF-61F, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-POE, and FWF-81F-2R-3G4G-POE; FortiGate Rugged Models FGR-60F, FGR-60F-3G4G, FGR-70F, and FGR-70F-3G4G; FortiFirewall Models FFW-1801F, FFW-2600F, FFW-3001F, FFW-3501F, FFW-3980E, FFW-4200F, FFW-4400F, FFW-4401F, FFW-4801F, FFW-VM64, and FFW-VM64-KVM; FortiGate VM Models FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, and FG-VM64-XEN; FortiGate 6000 Models FG-6001F, FG-6300F, FG-6301F, FG-6500F, and FG-6501F; and FortiGate 7000 Models FG-7030E, FG-7040E, FG-7060E, FG-7081F, and FG-7121F (collectively, the "Fortinet '273 Product(s)").

63. One or more Fortinet subsidiaries and/or affiliates use the Fortinet '273 Products in regular business operations.

64. One or more of the Fortinet '273 Products include technology that performs the step of establishing a data connection between a sender and receiver using a handshake process.

65. The Fortinet '273 Products utilize QUIC BBR. Specifically, the Fortinet '273 Products perform congestion control through the "quic-congestion-control-algo" which allows a choice between "bbr" and "bbr2." The parameters in the Fortinet '273 Products that set this congestion control selection are identified in the below excerpts from Fortinet documentation.

The Fortinet '273 Products Use The Infringing Congestion Control



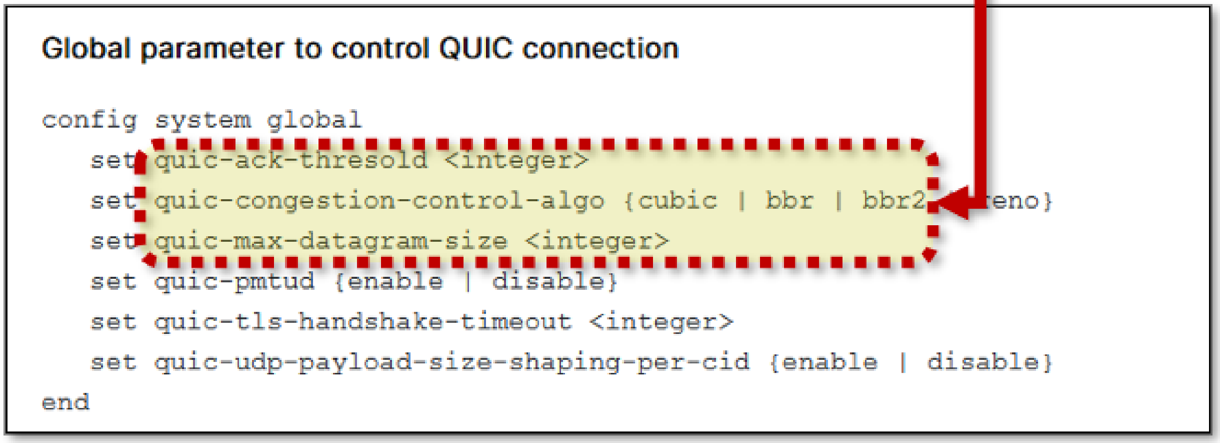
quic-ack-thresold	Maximum number of unacknowledged packets before sending ACK.	integer	Minimum value: 2 Maximum value: 5	3
quic-congestion-control-algo	QUIC congestion control algorithm.	option	-	cubic

Option	Description
cubic	Cubic.
bbr	BBR.
bbr2	BBR2.
reno	Reno.

quic-max-datagram-size	Maximum transmit datagram size.	integer	Minimum value: 1200 Maximum value: 1500	1500

FortiGate CLI Reference, FORTINET DOCUMENT LIBRARY, *available at*: https://docs.fortinet.com/document/fortigate/7.4.1/cli -reference/1620/config-system-global (last visited December 2024) (annotation added).

The Fortinet '273 Products Use Infringing Congestion Control Such As BBR2 QUIC Congestion Control



Global parameter to control QUIC connection

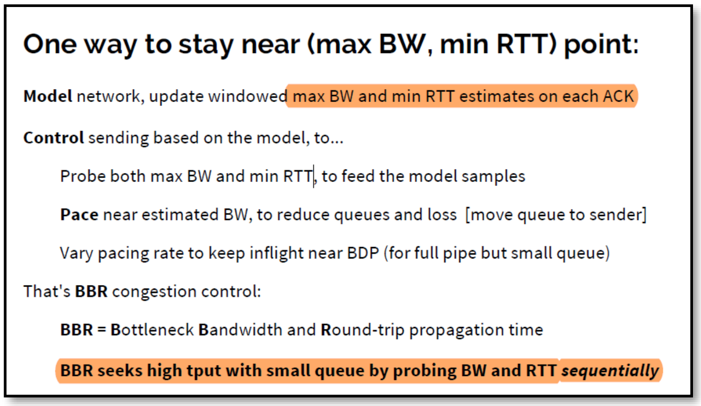
```
config system global
    set quic-ack-thresold <integer>
    set quic-congestion-control-algo {cubic | bbr | bbr2 | reno}
    set quic-max-datagram-size <integer>
    set quic-pmtud {enable | disable}
    set quic-tls-handshake-timeout <integer>
    set quic-udp-payload-size-shaping-per-cid {enable | disable}
end
```

FortiGate – FortiOS 7.4.0 New Features, FORTINET DOCUMENT LIBRARY, *available at*: https://docs.fortinet.com/document/fortigate/7.4.0/new-features/777101/enhancement-to-quic-and-http3-inspection-7-4-1 (last visited December 2024) (annotation added).

66. The Fortinet ‘273 Products measure round trip times (RTT) of packets sent between a client and server over a network. Specifically, the Fortinet ‘273 Products measure the round-trip propagation time (RTprop) using the minimum round-trip time (RTT) for the connection by keeping track of the lowest observed RTT in the recent past. This value represents the round-trip propagation time (RTprop) of the connection.

67. The Fortinet ‘273 Products perform timestamping. Specifically, when a Fortinet ‘273 Product transmits a data packet, it records the current time as a timestamp.

68. The Fortinet ‘273 Products perform a round-trip time (RTT) calculation. Specifically, the Fortinet ‘273 Products calculate the RTT for a specific packet by subtracting the original timestamp from the current time when the ACK is received. This gives an individual RTT sample for that packet as explained in the below excerpt.



One way to stay near (max BW, min RTT) point:

Model network, update windowed max BW and min RTT estimates on each ACK

Control sending based on the model, to...

Probe both max BW and min RTT, to feed the model samples

Pace near estimated BW, to reduce queues and loss [move queue to sender]

Vary pacing rate to keep inflight near BDP (for full pipe but small queue)

That's **BBR** congestion control:

BBR = **B**ottleneck **B**andwidth and **R**ound-trip propagation time

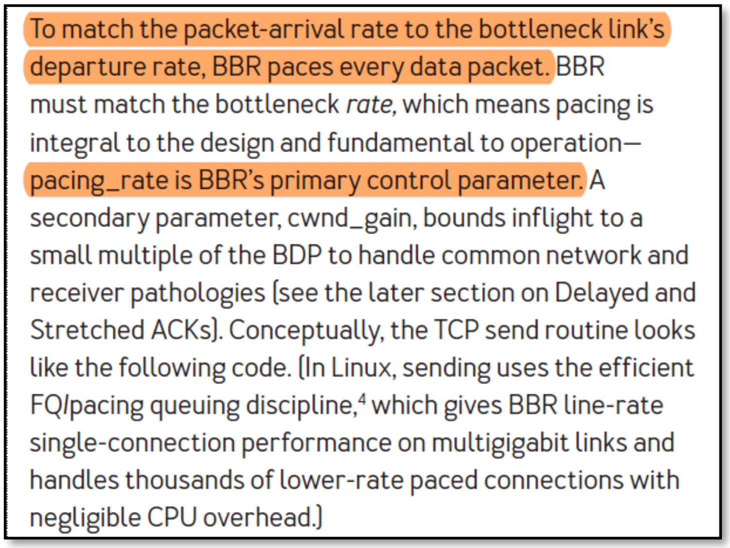
BBR seeks high tput with small queue by probing BW and RTT *sequentially*

Neal Cardwell, Yunchung Cheng, et al,, *BBR Congestion Control*, Google IETF 97: Seoul Presentation at 9 (November 2016) (emphasis added) (describing RTT_sample = ACK_receive_time - original_timestamp).

69. The Fortinet ‘273 Products perform the step of MinRTT estimation. Specifically, the Fortinet ‘273 Products maintain a running estimate of the minimum RTT observed (MinRTT) over a specified time window. The MinRTT is used by the Fortinet ‘273 Products to estimate the base round-trip propagation time without queuing delay. When a new RTT sample is calculated,

the Fortinet '273 Products compare it with the current MinRTT value. If the new sample is lower than the existing MinRTT, the Fortinet '273 Products update MinRTT with a new value.

70. The Fortinet '273 Products perform round-trip time-based pacing. Specifically, the Fortinet products use the MinRTT estimate in performing pacing rate and congestion window calculations to ensure the sending rate is adapted based on the observed network conditions. BBR's pacing rate and congestion window calculations factor in the MinRTT value to maintain a balance between efficient data transfer and minimal congestion.



To match the packet-arrival rate to the bottleneck link's departure rate, BBR paces every data packet. BBR must match the bottleneck *rate,* which means pacing is integral to the design and fundamental to operation—pacing_rate is BBR's primary control parameter. A secondary parameter, cwnd_gain, bounds inflight to a small multiple of the BDP to handle common network and receiver pathologies (see the later section on Delayed and Stretched ACKs). Conceptually, the TCP send routine looks like the following code. (In Linux, sending uses the efficient FQ/pacing queuing discipline,[4] which gives BBR line-rate single-connection performance on multigigabit links and handles thousands of lower-rate paced connections with negligible CPU overhead.)

Neal Cardwell, Yuchung Cheng, C. Stephen Gunn, Soheil Hassas Yeganeh, Van Jacobson, *BBR: Congestion-Based Congestion Control*, ACM Queue, Sep/Oct 2016 and CACM, Feb 2017 (emphasis added).

71. The Fortinet '273 Products calculate a congestion window parameter, which defines the maximum quantity of unacknowledged data packets permitted to be transmitted to the recipient.

72. The Fortinet '273 Products calculate a pacing rate based on these estimates to determine how quickly it should transmit data.

73. The Fortinet ‘273 Products calculate a congestion window. Specifically, the Fortinet ‘273 Products calculate a cwnd value based on the estimated bottleneck bandwidth (BtlBw) and RTT to ensure the congestion window is large enough not to limit the sending rate derived from the BtlBw and RTT estimates. This is done by setting the cwnd to the product of the estimated BtlBw and RTT: cwnd = BtlBw * RTT. The calculation done by the Fortinet ‘273 Products ensures that the cwnd value is large enough to accommodate the in-flight data based on the BtlBw and RTT estimates, while also accounting for potential variations in network conditions.

74. The Fortinet ‘273 Products calculate a congestion window (cwnd) based on the bottleneck bandwidth (BtlBw) and round-trip time (RTT) estimates to ensure the sending rate is not constrained by the window size. The cwnd effectively sets a limit on the number of unacknowledged data packets in transit, but it is not set by a specific parameter for the maximum number of unacknowledged packets.

75. The Fortinet ‘273 Products transmit additional data packets to the receiver in response a transmit timer expiration. The period of the transmit timer is based on the round-trip time measurements and the congestion window parameter.

76. Fortinet has directly infringed and continues to directly infringe the ‘273 Patent by, among other things, making, using, offering for sale, and/or selling technology for transferring data from a sender to a receiver in a communication network, including but not limited to the Fortinet ‘273 Products.

77. The Fortinet ‘273 Products are available to businesses and individuals throughout the United States.

78. By making, using, testing, offering for sale, and/or selling products and services for transferring data from a sender to a receiver in a communication network, including but not limited

to the Fortinet ‘273 Products, Fortinet has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘273 Patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

79. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘273 Patent.

80. As a result of Fortinet’s infringement of the ‘273 Patent, Plaintiff has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Fortinet’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Fortinet together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 8,521,901

81. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

82. Fortinet designs, makes, uses, sells, and/or offers for sale in the United States products comprising technology for a data packet scheduler that reduces packet bursts.

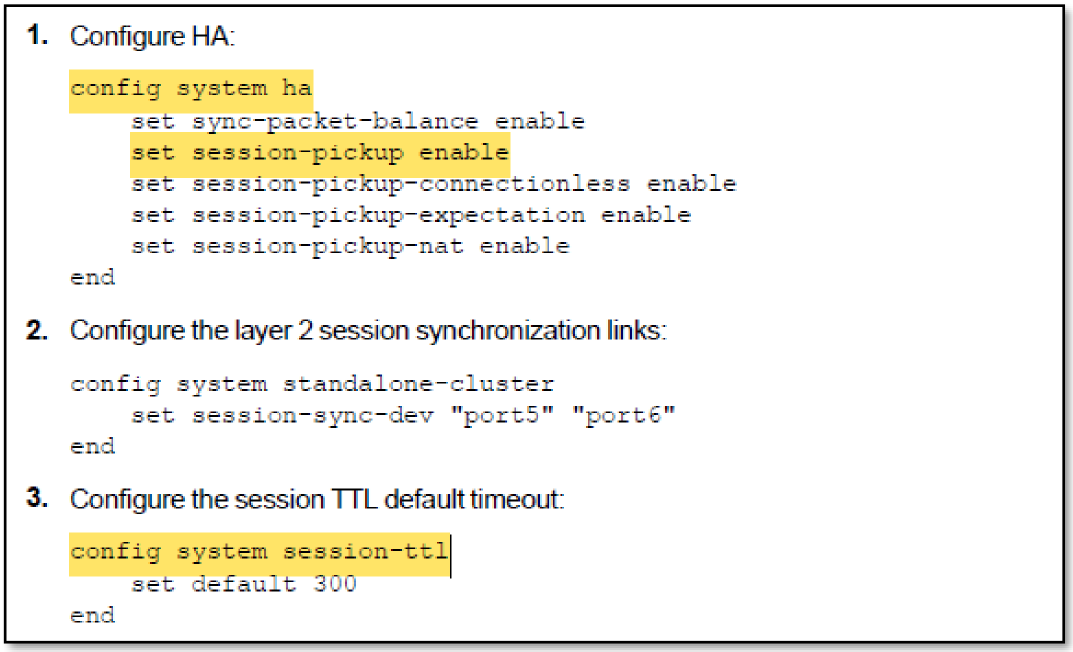
83. Fortinet designs, makes, sells, offers to sell, imports, and/or uses FortiGate products supporting FortiOS 7.4.0 and later, which include at least the following models: FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100F, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-

3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F, FG-7030E, FG-7040E, FG-7060E, FG-7081F, and FG-7121F (collectively, the "Fortinet '901 Product(s)").

84. One or more Fortinet subsidiaries and/or affiliates use the Fortinet '901 Products in regular business operations.

85. The Fortinet '901 Products receive a transmission control protocol (TCP) packet from a transport layer (*i.e.*, a sending layer) that was sent over a connection between a fist device and a second device.

86. The Fortinet '901 Products receive all incoming TCP packets by monitoring interfaces at the network boundary and processing transport-level data within their integrated session handling architecture. Specifically, the Fortinet '901 Products utilize dedicated hardware components, such as "NP6" network processors, to capture and parse each TCP packet as it arrives on "physical" interfaces configured via "config system interface" parameters. For example, when "set session-pickup enable" is applied in the device configuration, the Fortinet '901 Products leverage hardware acceleration to consistently accept, buffer, and classify incoming TCP segments based on "session-ttl" timers. In addition, the Fortinet '901 Products reference "pps" (packets-per-second) metrics collected at the port level to ensure that traffic is accurately identified and consistently directed through the appropriate policy chain.



1. Configure HA:

```
config system ha
    set sync-packet-balance enable
    set session-pickup enable
    set session-pickup-connectionless enable
    set session-pickup-expectation enable
    set session-pickup-nat enable
end
```

2. Configure the layer 2 session synchronization links:

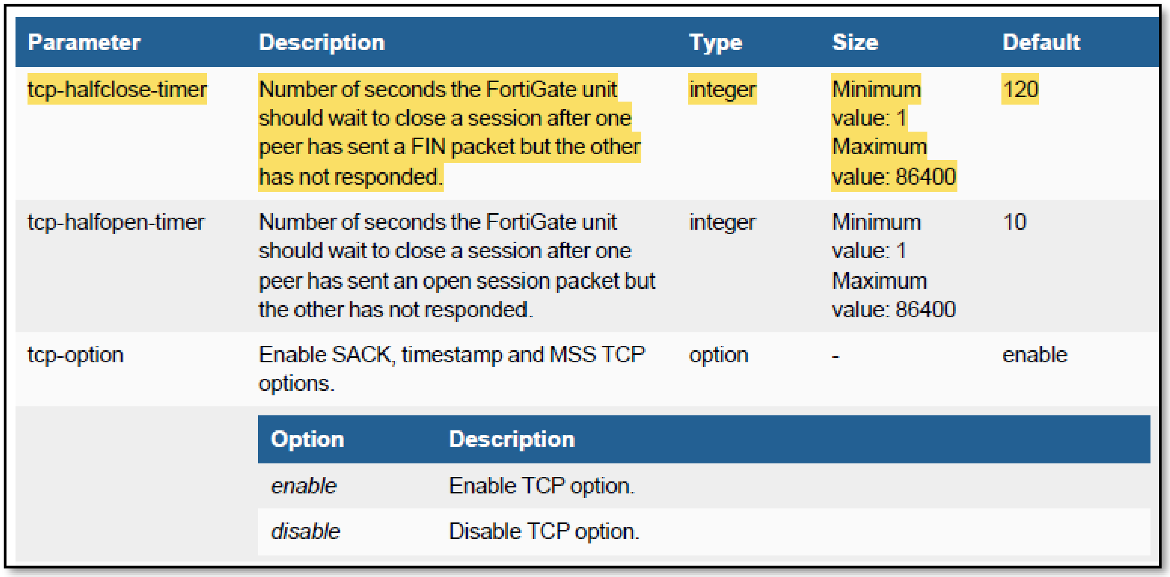
```
config system standalone-cluster
    set session-sync-dev "port5" "port6"
end
```

3. Configure the session TTL default timeout:

```
config system session-ttl
    set default 300
end
```

FORTIOS 7.6.1 ADMINISTRATION GUIDE at 3155 (December 19, 2024) (emphasis added).

87. The Fortinet ‘901 Products receive TCP packets that originate internally from their transport layer components, ensuring that data processed through features like SSL inspection or proxy-based services are re-injected into the session pipeline. Specifically, when “set internal-switch-mode interface” is enabled, the Fortinet ‘901 Products treat each virtual interface as a unique source for incoming TCP data, preserving segmentation and applying consistent firewall session logic. In addition, the Fortinet ‘901 Products utilize “tcp-halfclose-timer” values to gracefully handle sessions transitioning between external and internal sources, guaranteeing that each packet, regardless of origin, is received into the unified packet processing infrastructure.



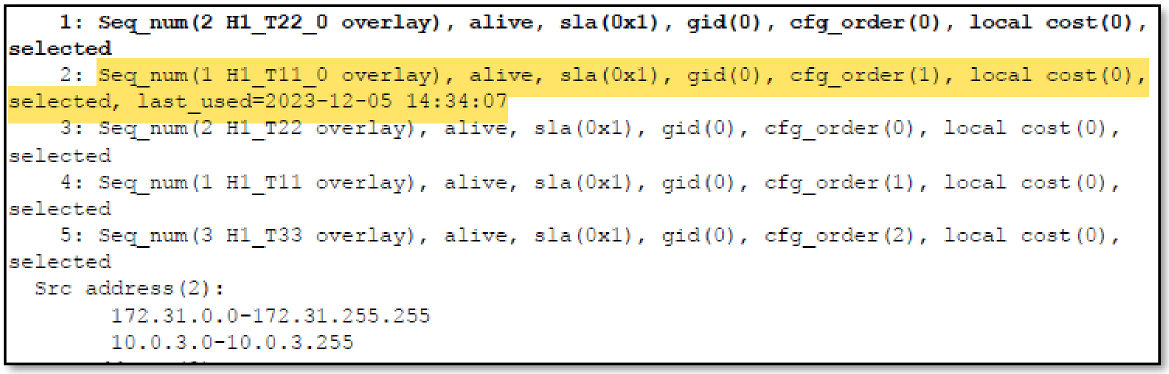
Parameter	Description	Type	Size	Default
tcp-halfclose-timer	Number of seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded.	integer	Minimum value: 1 Maximum value: 86400	120
tcp-halfopen-timer	Number of seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded.	integer	Minimum value: 1 Maximum value: 86400	10
tcp-option	Enable SACK, timestamp and MSS TCP options.	option	-	enable

Option	Description
enable	Enable TCP option.
disable	Disable TCP option.

FORTIOS 7.6.1 CLI REFERENCE at 1702 (November 28, 2024) (emphasis added).

88. The Fortinet '901 Products store, at the first device, information about the connection between the first device and the second device. The stored information includes a last packet delivery time for the connection.

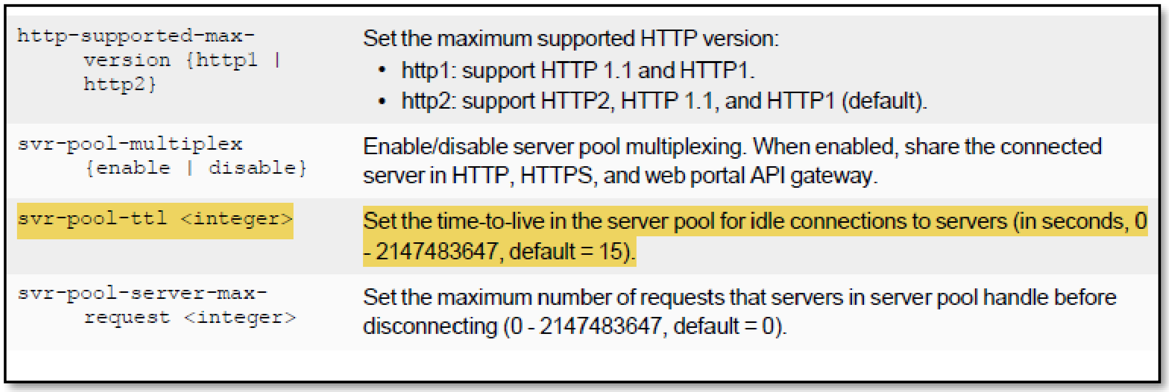
89. The Fortinet '901 Products maintain detailed connection histories by actively tracking and storing information about communication sessions. Specifically, the Fortinet '901 Products utilize session tables as a primary mechanism for managing and monitoring active connections, evidenced by the "diagnose sys session list" command, which outputs time-related metrics such as "duration," "expire," and "timeout" for each session. For example, executing this command reveals "sentpkt" and "rcvdpkt" counters within the session information, corroborating the tracking of packet flow within each connection. In addition, the "diagnose sys session list" output includes a "last_used" field for SD-WAN service entries, indicating the last time a particular SD-WAN rule was applied, providing a precise timestamp like "last_used=2023-12-05 14:34:07," while the "duration" field reflects the elapsed time since session establishment, indirectly showing time since last activity.



```
    1: Seq_num(2 H1_T22_0 overlay), alive, sla(0x1), gid(0), cfg_order(0), local cost(0),
selected
    2: Seq_num(1 H1_T11_0 overlay), alive, sla(0x1), gid(0), cfg_order(1), local cost(0),
selected, last_used=2023-12-05 14:34:07
    3: Seq_num(2 H1_T22 overlay), alive, sla(0x1), gid(0), cfg_order(0), local cost(0),
selected
    4: Seq_num(1 H1_T11 overlay), alive, sla(0x1), gid(0), cfg_order(1), local cost(0),
selected
    5: Seq_num(3 H1_T33 overlay), alive, sla(0x1), gid(0), cfg_order(2), local cost(0),
selected
  Src address(2):
        172.31.0.0-172.31.255.255
        10.0.3.0-10.0.3.255
```

FORTIOS 7.6.1 ADMINISTRATION GUIDE at 3155 (December 19, 2024) (emphasis added).

90. The Fortinet '901 Products store connection history, including the last packet activity time, by enabling actions based on time intervals and logging various session events. Specifically, configuration options like "session-ttl," which defines the "time-to-live (TTL) in seconds for session accepted by this policy," and "set pba-interim-log <log-interval>" for CGN IP pools, illustrate the Fortinet '901 Products time-awareness in session management. For example, the "svr-pool-ttl" allows setting the "time-to-live in the server pool for idle connections to servers," and "max-idle-timeout" in QUIC configuration demonstrates time storage for specific protocols.

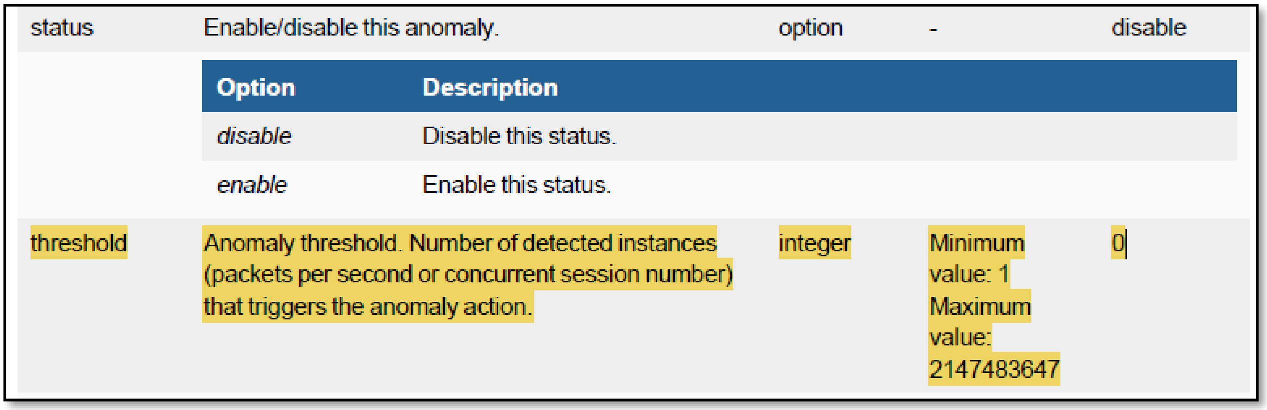


`http-supported-max-version {http1 | http2}`	Set the maximum supported HTTP version: • http1: support HTTP 1.1 and HTTP1. • http2: support HTTP2, HTTP 1.1, and HTTP1 (default).
`svr-pool-multiplex {enable | disable}`	Enable/disable server pool multiplexing. When enabled, share the connected server in HTTP, HTTPS, and web portal API gateway.
`svr-pool-ttl <integer>`	Set the time-to-live in the server pool for idle connections to servers (in seconds, 0 - 2147483647, default = 15).
`svr-pool-server-max-request <integer>`	Set the maximum number of requests that servers in server pool handle before disconnecting (0 - 2147483647, default = 0).

FORTIOS 7.6.1 ADMINISTRATION GUIDE at 1315 (December 19, 2024) (emphasis added).

91. The Fortinet '901 Products determine whether the TCP packet is part of a bursty transmission on the connection by ascertaining that a burst count of the connection is greater than a burst-count threshold. The Fortinet '901 Products identify bursty traffic by actively monitoring the rate of incoming and outgoing packets, along with session establishment. Specifically, the

Fortinet '901 Products utilize DoS policies, which include configurable parameters such as "threshold," representing the maximum rate of "packets per second or concurrent session number," to quantify and detect unusual traffic spikes. For example, the config anomaly settings within the config firewall DoS-policy of the Fortinet '901 Products specify a "threshold" which, when exceeded by incoming traffic, is identified as a burst, triggering configured actions, and the "log" setting within the config anomaly sub-section log the anomaly. In addition, the Fortinet '901 Products identify bursty traffic through its traffic shaping functionality, which monitors the rate at which traffic is processed through its configured interfaces, employing parameters like "guaranteed-bandwidth" and "maximum-bandwidth," and the "per-ip-shaper" parameter.

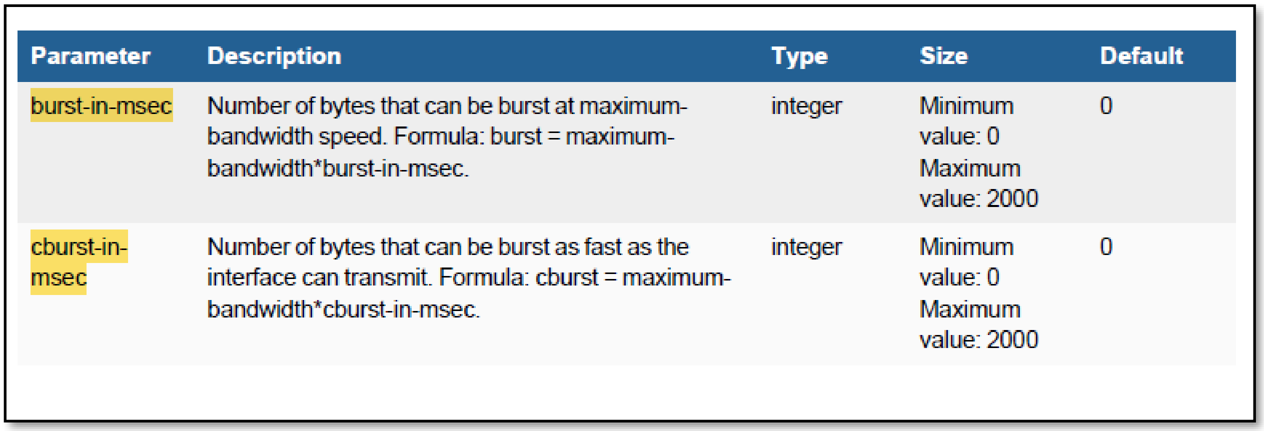


status	Enable/disable this anomaly.	option	-	disable
	Option	**Description**		
	disable	Disable this status.		
	enable	Enable this status.		
threshold	Anomaly threshold. Number of detected instances (packets per second or concurrent session number) that triggers the anomaly action.	integer	Minimum value: 1 Maximum value: 2147483647	0

FORTIOS 7.6.1 CLI REFERENCE at 235 (November 28, 2024) (emphasis added).

92. The traffic shaping feature in the Fortinet '901 Products provides parameters such as "burst-in-msec" and "cburst-in-msec" within shaping profiles to determine if an incoming packet is part of a rapid sequence. For example, the configuration command set burst-in-msec 100 under config shaping-entries defines a burst threshold based on the amount of data (in milliseconds) that can be transmitted at the maximum bandwidth before traffic shaping policies are enforced. In addition, the "diagnose netlink interface list" command output displays real-time counters for packets and bytes, allowing the Fortinet '901 Product to observe traffic patterns and identify bursts, and the "diagnose sys session list" command output, which includes "duration"

and “expire” fields, indicates that the Fortinet ‘901 Products track session information over time to assess recent traffic patterns. In addition to traffic shaping and session monitoring, the Fortinet ‘901 Products identify bursty traffic by monitoring connection rates using settings such as “svr-pool-server-max-concurrent-request,” “svr-pool-server-max-request,” and “svr-pool-ttl.”

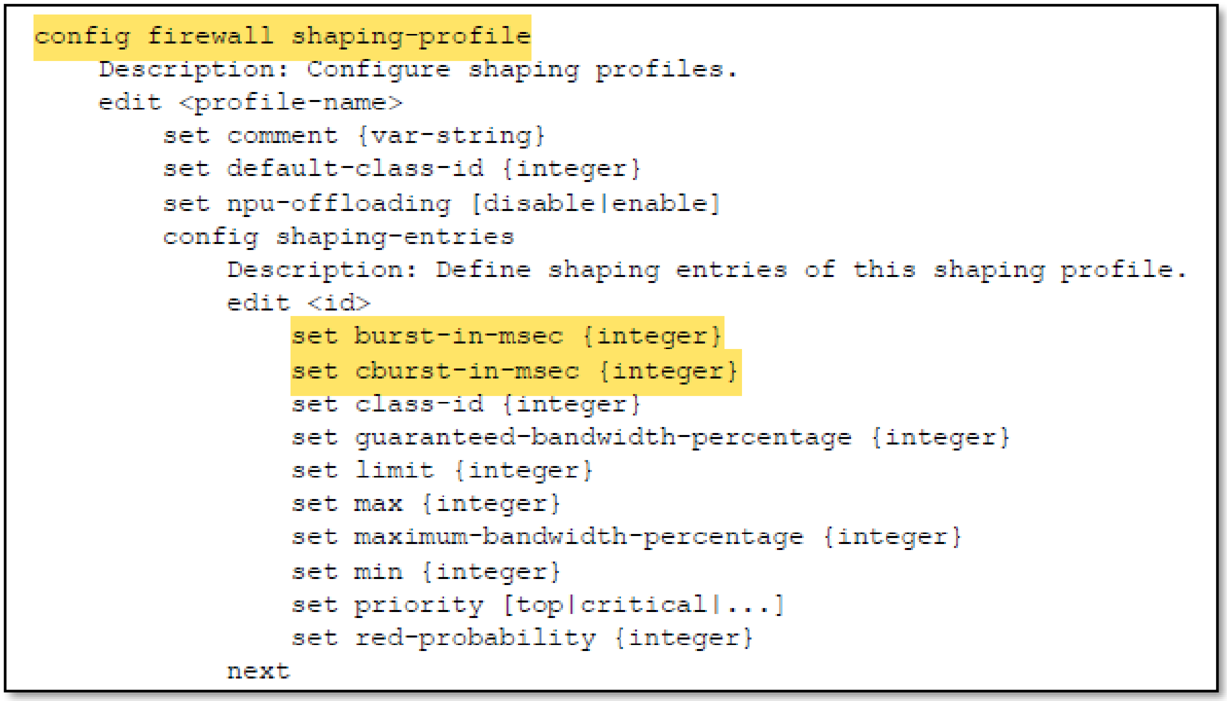


Parameter	Description	Type	Size	Default
burst-in-msec	Number of bytes that can be burst at maximum-bandwidth speed. Formula: burst = maximum-bandwidth*burst-in-msec.	integer	Minimum value: 0 Maximum value: 2000	0
cburst-in-msec	Number of bytes that can be burst as fast as the interface can transmit. Formula: cburst = maximum-bandwidth*cburst-in-msec.	integer	Minimum value: 0 Maximum value: 2000	0

FORTIOS 7.6.1 CLI REFERENCE at 472 (November 28, 2024) (emphasis added).

93. The Fortinet ‘901 Products calculate a delay time for the connection using the last packet delivery time after determining that the TCP packet is part of a bursty transmission. The Fortinet ‘901 Products calculate delay times for connections identified as part of bursty traffic by employing traffic shaping with queuing. Specifically, parameters like “burst-in-msec” and “cburst-in-msec,” in conjunction with “guaranteed-bandwidth” and “maximum-bandwidth,” define burst thresholds, as shown by the formulas “burst = maximum-bandwidthburst-in-msec” and “cburst=maximum-bandwidthcburst-in-msec.” These calculations determine the byte limit sent at the maximum rate before traffic shaping, including queuing and delays, is applied; real-time data on “guaranteed-bandwidth” and “maximum-bandwidth” from the “diagnose netlink interface list <interface_name>“ command confirms the active use of these parameters in shaping calculations. In addition, the Fortinet ‘901 Products dynamically adjust delay using the “Action” setting within “config firewall shaping-profile” to implement “static” or “dynamic” delay based on parameters like “guaranteed-bandwidth-percentage,” “maximum-bandwidth-percentage,”

"min," and "max," where setting "guaranteed-bandwidth-percentage" to 10 and "maximum-bandwidth-percentage" to 50 ensures at least 10% bandwidth availability while not exceeding 50%; the "cburst-in-msec" parameter further allows controlled bursts above "maximum-bandwidth" for a calculated duration before enforcing delay, and the "diagnose sys session list" command can verify the active shaping and introduction of delays.

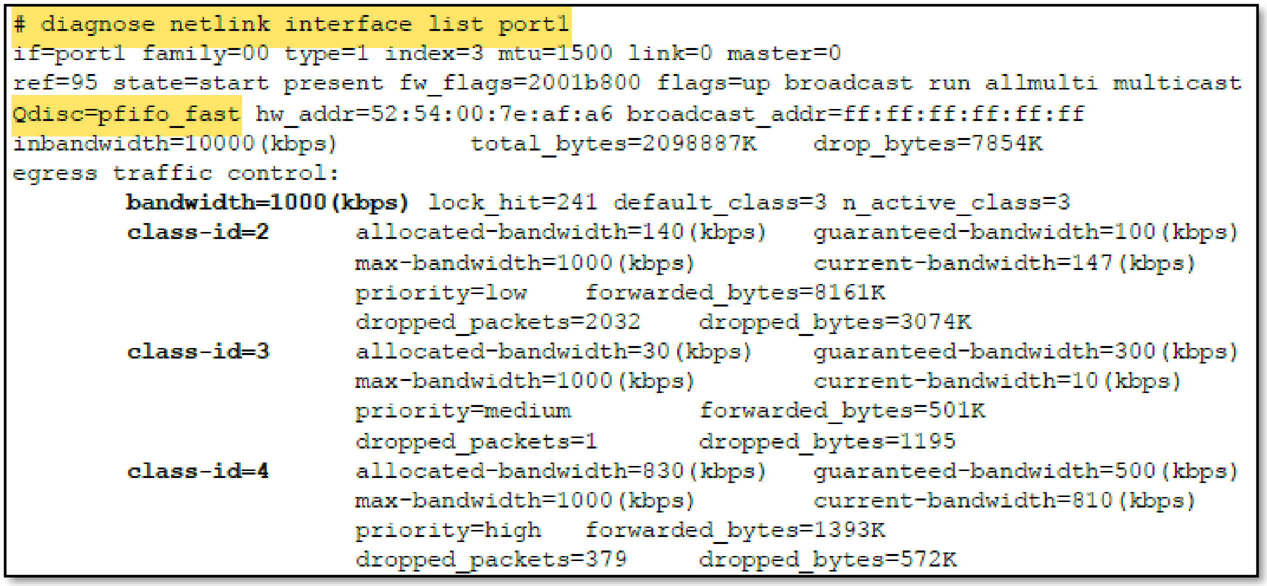


```
config firewall shaping-profile
    Description: Configure shaping profiles.
    edit <profile-name>
        set comment {var-string}
        set default-class-id {integer}
        set npu-offloading [disable|enable]
        config shaping-entries
            Description: Define shaping entries of this shaping profile.
            edit <id>
                set burst-in-msec {integer}
                set cburst-in-msec {integer}
                set class-id {integer}
                set guaranteed-bandwidth-percentage {integer}
                set limit {integer}
                set max {integer}
                set maximum-bandwidth-percentage {integer}
                set min {integer}
                set priority [top|critical|...]
                set red-probability {integer}
            next
```

FORTIOS 7.6.1 CLI REFERENCE at 471 (November 28, 2024) (emphasis added).

94. The Fortinet '901 Products delay delivering the TCP packet to a receiving layer based on the calculated delay time. The receiving layer is one of the network interface layer or the transport layer that is not the sending layer. The Fortinet '901 Products use queuing mechanisms like Random Early Detection (RED) or First-In, First-Out (FIFO) to manage traffic bursts and introduce necessary delay. Specifically, the "config firewall shaping-profile" allows setting "type queuing," activating queuing for traffic shaping, and when a profile is set to "type queuing" with a configured "burst-in-msec" parameter, the Fortinet '901 Products queue packets exceeding the burst limits; the "diagnose netlink interface list" command output includes "qdisc"

information, confirming the use of algorithms like “pfifo_fast.” For example, the Fortinet ‘901 Products calculate delay times after detecting bursty traffic by using stored session information, including the last packet delivery time, and configurable thresholds defined in DoS policy configurations for “packets per second or concurrent session number” to trigger calculations; when an anomaly is detected, the Fortinet ‘901 Products use the stored last packet delivery time and current time, alongside the “quarantine-expiry” setting, to determine the delay before dropping or forwarding traffic, and the “max-ack-delay” parameter in QUIC settings allows for delaying ACKs, resulting in a calculated delay time.

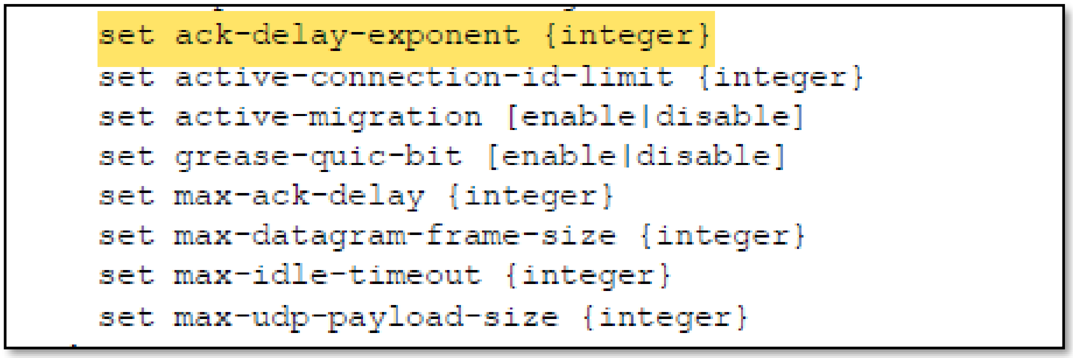


```
# diagnose netlink interface list port1
if=port1 family=00 type=1 index=3 mtu=1500 link=0 master=0
ref=95 state=start present fw_flags=2001b800 flags=up broadcast run allmulti multicast
Qdisc=pfifo_fast hw_addr=52:54:00:7e:af:a6 broadcast_addr=ff:ff:ff:ff:ff:ff
inbandwidth=10000(kbps)          total_bytes=2098887K    drop_bytes=7854K
egress traffic control:
        bandwidth=1000(kbps) lock_hit=241 default_class=3 n_active_class=3
        class-id=2      allocated-bandwidth=140(kbps)    guaranteed-bandwidth=100(kbps)
                        max-bandwidth=1000(kbps)         current-bandwidth=147(kbps)
                        priority=low     forwarded_bytes=8161K
                        dropped_packets=2032     dropped_bytes=3074K
        class-id=3      allocated-bandwidth=30(kbps)     guaranteed-bandwidth=300(kbps)
                        max-bandwidth=1000(kbps)         current-bandwidth=10(kbps)
                        priority=medium          forwarded_bytes=501K
                        dropped_packets=1        dropped_bytes=1195
        class-id=4      allocated-bandwidth=830(kbps)    guaranteed-bandwidth=500(kbps)
                        max-bandwidth=1000(kbps)         current-bandwidth=810(kbps)
                        priority=high    forwarded_bytes=1393K
                        dropped_packets=379      dropped_bytes=572K
```

FORTIOS 7.6.1 ADMINISTRATION GUIDE at 1656 (December 19, 2024) (emphasis added).

95. The Fortinet ‘901 Products calculate delay times based on burst detection, such that when traffic exceeds pre-configured “bandwidth limits” within a shaping profile, the “max-idle-timeout” along with “max-datagram-frame-size” parameters of protocols like QUIC are utilized to calculate when and how to reintroduce packets; the “holddown-interval” in access-proxy configurations allows for delaying server availability assessment, and the “ack-delay-exponent” calculates necessary acknowledgement delays, while parameters like “svr-pool-ttl,” “svr-pool-

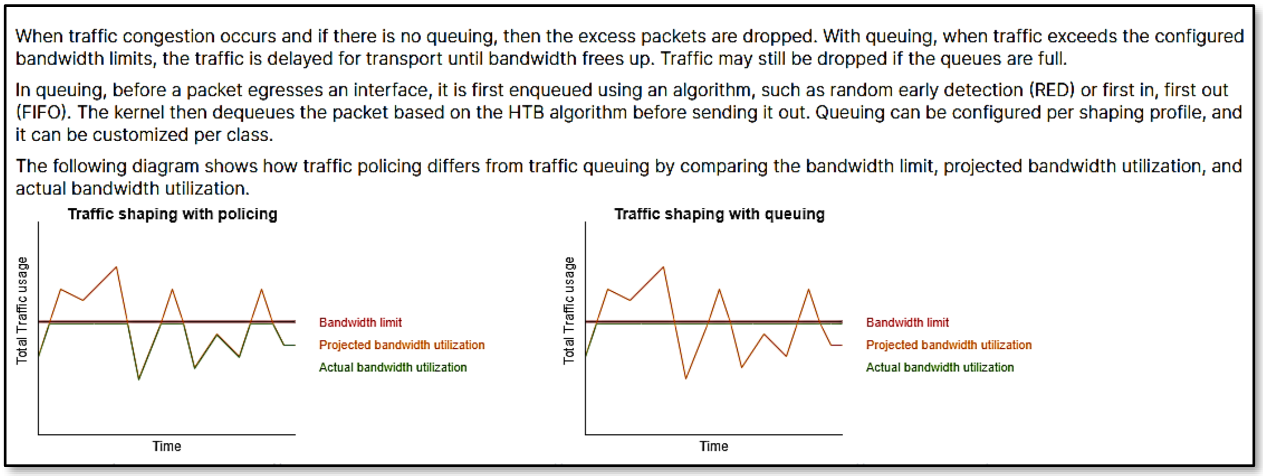
server-max-concurrent-request," and "svr-pool-server-max-request" help understand the state of load-balanced traffic for delay calculations.



```
set ack-delay-exponent {integer}
set active-connection-id-limit {integer}
set active-migration [enable|disable]
set grease-quic-bit [enable|disable]
set max-ack-delay {integer}
set max-datagram-frame-size {integer}
set max-idle-timeout {integer}
set max-udp-payload-size {integer}
```

FORTIOS 7.6.1 CLI REFERENCE at 555 (November 28, 2024) (emphasis added).

96. The Fortinet '901 Products implement mechanisms to intentionally hold back packets based on calculated delay times. Specifically, the Fortinet '901 Products utilize queuing to introduce delays for packets matching defined policies. For example, Fortinet documentation states, "[i]n queuing, before a packet egresses an interface, it is first enqueued using an algorithm, such as random early detection (RED) or first in, first out (FIFO)," indicating that packets are not immediately forwarded but experience delays within queues.



When traffic congestion occurs and if there is no queuing, then the excess packets are dropped. With queuing, when traffic exceeds the configured bandwidth limits, the traffic is delayed for transport until bandwidth frees up. Traffic may still be dropped if the queues are full.

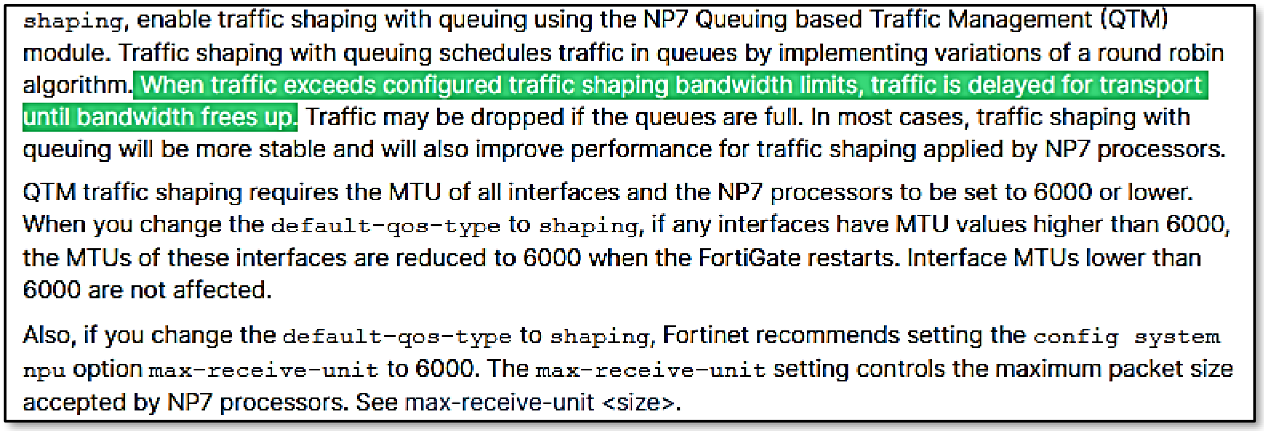
In queuing, before a packet egresses an interface, it is first enqueued using an algorithm, such as random early detection (RED) or first in, first out (FIFO). The kernel then dequeues the packet based on the HTB algorithm before sending it out. Queuing can be configured per shaping profile, and it can be customized per class.

The following diagram shows how traffic policing differs from traffic queuing by comparing the bandwidth limit, projected bandwidth utilization, and actual bandwidth utilization.

Traffic shaping with policing
Total Traffic usage
Time
Bandwidth limit
Projected bandwidth utilization
Actual bandwidth utilization
Traffic shaping with queuing
Total Traffic usage
Time
Bandwidth limit
Projected bandwidth utilization
Actual bandwidth utilization

Traffic Shaping Profiles, FORTIGATE/FORTIOS 7.6.1 ADMINISTRATIVE GUIDE, *available at*: https://docs.fortinet.com/document/fortigate/7.6.1/administration-guide/626246/traffic-shaping-profiles (last visited December 2024).

97. The Fortinet '901 Products use "burst-in-msec" and "cburst-in-msec" parameters to set burst thresholds that, when exceeded, activate queuing mechanisms, consequently introducing delays. Furthermore, the "guaranteed-bandwidth" and "maximum-bandwidth" settings in the Fortinet '901 Products, along with the "priority" level in traffic shaping profiles, determine bandwidth allocation and contribute to delay calculations based on traffic load, as confirmed by documentation stating that "when traffic exceeds configured traffic shaping bandwidth limits, traffic is delayed for transport until bandwidth frees up."



`shaping`, enable traffic shaping with queuing using the NP7 Queuing based Traffic Management (QTM) module. Traffic shaping with queuing schedules traffic in queues by implementing variations of a round robin algorithm. When traffic exceeds configured traffic shaping bandwidth limits, traffic is delayed for transport until bandwidth frees up. Traffic may be dropped if the queues are full. In most cases, traffic shaping with queuing will be more stable and will also improve performance for traffic shaping applied by NP7 processors.

QTM traffic shaping requires the MTU of all interfaces and the NP7 processors to be set to 6000 or lower. When you change the `default-qos-type` to `shaping`, if any interfaces have MTU values higher than 6000, the MTUs of these interfaces are reduced to 6000 when the FortiGate restarts. Interface MTUs lower than 6000 are not affected.

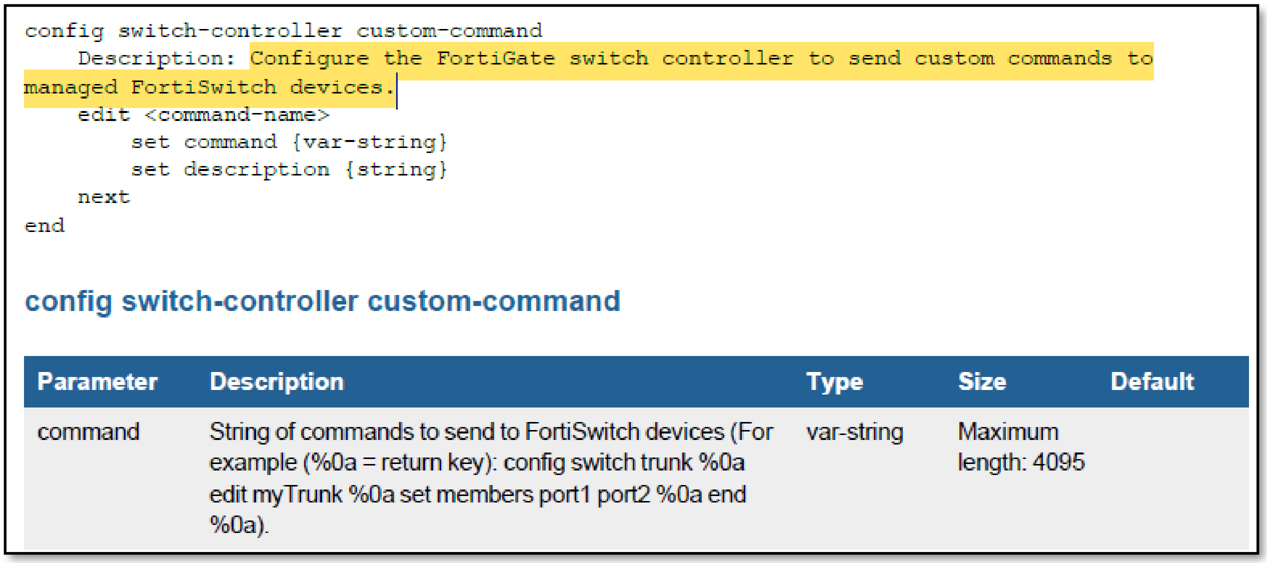
Also, if you change the `default-qos-type` to `shaping`, Fortinet recommends setting the `config system npu` option `max-receive-unit` to 6000. The `max-receive-unit` setting controls the maximum packet size accepted by NP7 processors. See max-receive-unit <size>.

NP7 Traffic Shaping, FORTIGATE/FORTIOS 7.6.1 HARDWARE ACCELERATION, *available at*: https://docs.fortinet.com/document/fortigate/7.6.1/hardware-acceleration/194588/np7-traffic-shaping (last visited December 2024) (emphasis added).

98. The Fortinet '901 Products hold back packets through configuration settings and congestion management techniques. Specifically, Fortinet '901 Products' documentation describes using "health-check" settings to pause traffic distribution to non-responsive servers, with the "timeout" and "retry" parameters dictating the delay duration. For example, the "holddown-interval" can delay when a server is used in load balancing, and the "pba-timeout" configuration determines the timing of port allocation within IP pools, both resulting in delayed packet processing. In addition, during congestion, the Fortinet '901 Products utilize a "queue limit" within traffic shaping to manage how many packets are held, as implemented by algorithms like the High Throughput Buffer (HTB), where the "backlog" parameter tracks queued traffic, allowing

for time-based release. Furthermore, protocol-specific settings, such as the QUIC protocol's "max-ack-delay," which defines the maximum delay for acknowledgement packets, and the TCP protocol's "timeout-send-rst" parameter, which manages connection release timing, further demonstrate the Fortinet '901 Products' granular control over intentionally pausing packet delivery.

99. The Fortinet '901 Products send the TCP packet to the receiving layer. Specifically, the Fortinet '901 Products route packets, as indicated by Fortinet '901 Product documentation stating the capability to "send custom commands to managed FortiSwitch devices," demonstrating network flow management. For example, when a shaping policy with queuing is active and traffic surpasses thresholds, excess packets are queued and delayed, a process explicitly enabled via the "set type queuing" configuration under "config firewall shaping-profile," as the documentation details. In addition, the "guaranteed-bandwidth" setting in the Fortinet '901 Products sets a bandwidth reservation for eventual packet delivery, and diagnostic commands like "diagnose sys session list," displaying "tx speed" and "rx speed," are used by the Fortinet '901 Products for traffic flow.



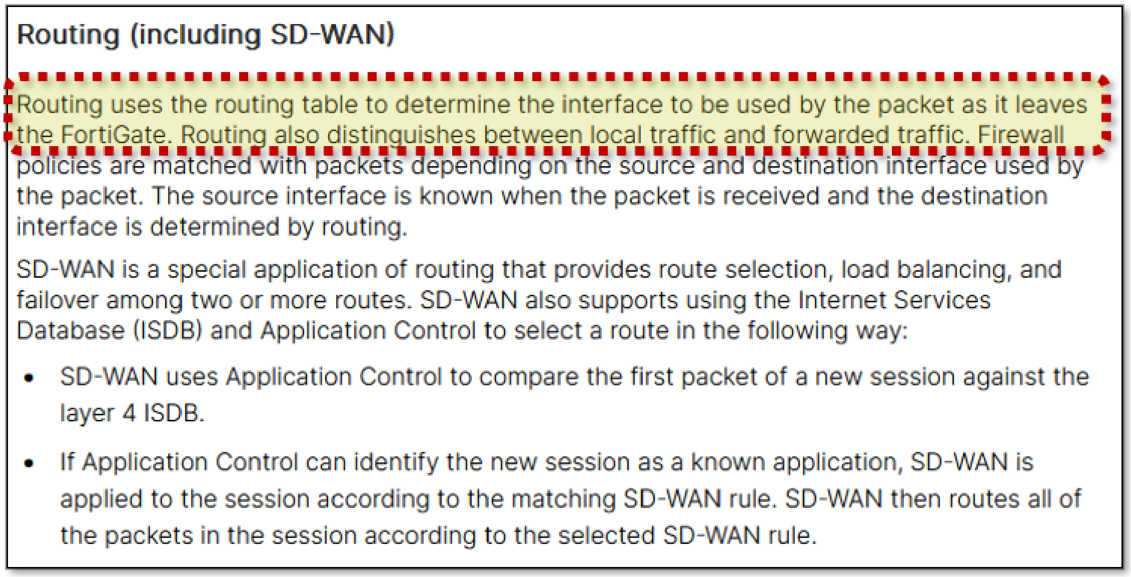
```
config switch-controller custom-command
    Description: Configure the FortiGate switch controller to send custom commands to
managed FortiSwitch devices.
    edit <command-name>
        set command {var-string}
        set description {string}
    next
end
```

config switch-controller custom-command

Parameter	Description	Type	Size	Default
command	String of commands to send to FortiSwitch devices (For example (%0a = return key): config switch trunk %0a edit myTrunk %0a set members port1 port2 %0a end %0a).	var-string	Maximum length: 4095	

FortiOS 7.6.1 CLI Reference at 1028 (November 28, 2024) (emphasis added).

100. The Fortinet '901 Products ensure TCP packet forwarding after any calculated delay by utilizing internal routing, source network address translation (SNAT), and traffic shaping policies. Specifically, the FortiGate kernel consults routing tables to determine the correct egress interface, as the documentation states it "uses the routing table to forward the packet out the correct exit interface," and employs the HTB algorithm for dequeuing shaped packets before sending them to the next layer. For example, the FortiGate uses configured IP pools for SNAT, and with "port-preserve" enabled, reuses the original source port. In addition, traffic shaping policies, controlled by allocating a "class-id," "per-ip-shaper," and "traffic-shaper" within "firewall shaping-policy," dictate the rate of traffic egress, and for traffic exiting through a Virtual Wire Pair or VPN tunnel, a defined "tunnel-encryption," as seen in access-proxy configurations, may be applied before forwarding.



Routing (including SD-WAN)

Routing uses the routing table to determine the interface to be used by the packet as it leaves the FortiGate. Routing also distinguishes between local traffic and forwarded traffic. Firewall policies are matched with packets depending on the source and destination interface used by the packet. The source interface is known when the packet is received and the destination interface is determined by routing.

SD-WAN is a special application of routing that provides route selection, load balancing, and failover among two or more routes. SD-WAN also supports using the Internet Services Database (ISDB) and Application Control to select a route in the following way:

- SD-WAN uses Application Control to compare the first packet of a new session against the layer 4 ISDB.
- If Application Control can identify the new session as a known application, SD-WAN is applied to the session according to the matching SD-WAN rule. SD-WAN then routes all of the packets in the session according to the selected SD-WAN rule.

Packet Flow Ingress and Egress: FortiGates Without Network Processor Offloading, FORTIGATE / FORTIOS 6.4.0 PARALLEL PATH PROCESSING, *available at*: https://docs.fortinet.com/document/fortigate/6.4.0/parallel-path-processing-life-of-a-packet/86811/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading (last visited December 2024) (emphasis added).

101. Fortinet has directly infringed and continues to directly infringe the ‘901 Patent by, among other things, making, using, offering for sale, and/or selling technology for a data packet scheduler that reduces packet bursts, including but not limited to the Fortinet ‘901 Products.

102. The Fortinet ‘901 Products are available to businesses and individuals throughout the United States.

103. The Fortinet ‘901 Products are provided to businesses and individuals located in this District.

104. By making, using, testing, offering for sale, and/or selling products and services comprising technology for a data packet scheduler that reduced packet bursts, including but not limited to the Fortinet ‘901 Products, Fortinet has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘901 Patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

105. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘901 Patent.

106. As a result of Fortinet’s infringement of the ‘901 Patent, Plaintiff has suffered monetary damages, and seek recovery in an amount adequate to compensate for Fortinet’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Fortinet together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 7,616,559

107. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

108. Fortinet designs, makes, uses, sells, and/or offers for sale in the United States products that communicate information over multiple communications links.

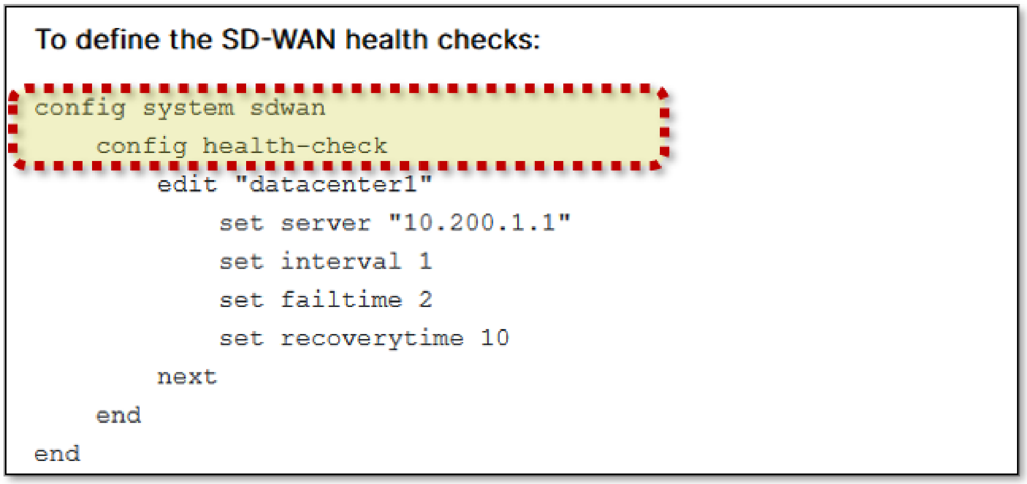
109. Fortinet designs, makes, sells, offers to sell, imports, and/or uses FortiGate Products supporting FortiOS 7.4.0 and later, which include at least the following models FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100F, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F, FG-7030E, FG-7040E, FG-7060E, FG-7081F, and FG-7121F; and FortiManager Products supporting FortiOS 7.4.0 and later, which include at least the following models FMG-200F, FMG-200G, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3000G, FMG-3700F, and FMG-3700G (collectively, the "Fortinet '559 Product(s)").

110. One or more Fortinet subsidiaries and/or affiliates use the Fortinet '559 Products in regular business operations.

111. The Fortinet '559 Products identify an initial communication path with a specific security protocol for the transmission of data between a client system and a server system.

112. The Fortinet '559 Products detect a first communications link having a first security for the communication of information between a client device and a server device. Specifically, the Fortinet '559 Products perform detailed configuration of network interfaces, including

physical, VLAN, and VPN interfaces, which can be designated as SD-WAN members. The Fortinet '559 Products detect a first communications link based on SD-WAN rules and health-check parameters. SD-WAN rules in the Fortinet '559 Products are used to determine performance SLAs (Service Level Agreements), which include security as a criterion. For example, the command "config system sdwan config health-check" sets up a health check against a specified server, using latency as a metric for link quality assessment.

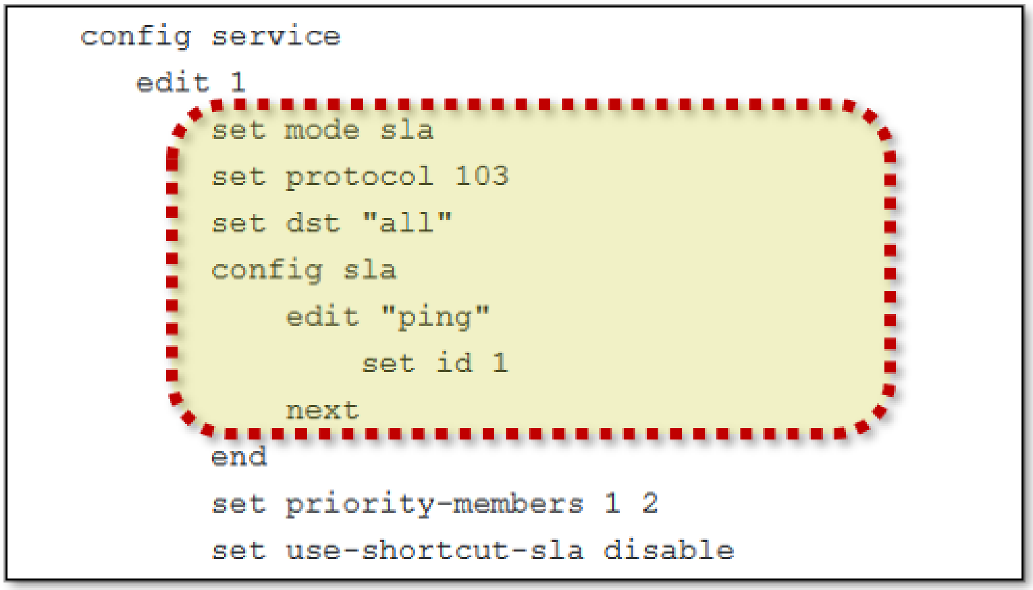


To define the SD-WAN health checks:

```
config system sdwan
    config health-check
        edit "datacenter1"
            set server "10.200.1.1"
            set interval 1
            set failtime 2
            set recoverytime 10
        next
    end
end
```

Configure SD-WAN, FORTIGATE / FORTIOS 7.0.16 ADMINISTRATION GUIDE, *available at*: https://docs.fortinet.com/document/fortigate/7.0.16/administration-guide/441466/configure-sd-wan (last visited December 2024) (emphasis added).

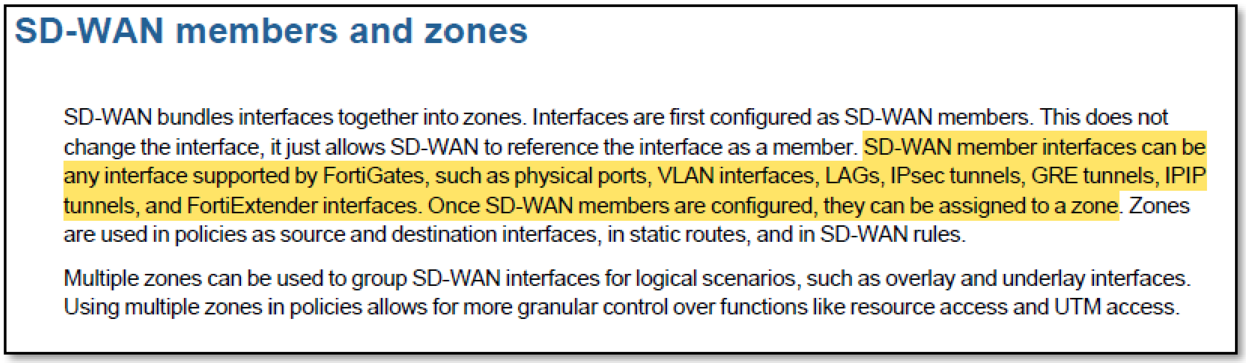
113. The subsequent application of this health check within SD-WAN service rules, as illustrated by config service edit 1 set name "1" set mode sla set dst "all" config sla edit "ping" set id 1, allows the Fortinet '559 Products to dynamically select the best-performing link based on real-time analysis, including security and performance metrics.



```
config service
    edit 1
        set mode sla
        set protocol 103
        set dst "all"
        config sla
            edit "ping"
                set id 1
            next
        end
        set priority-members 1 2
        set use-shortcut-sla disable
```

Allow Multicast Traffic To Be Steered By SD-WAN, FORTIGATE / FORTIOS 7.4.0 SD-WAN NEW FEATURES, *available at*: https://docs.fortinet.com/document/fortigate/7.4.0/sd-wan-new-features/243964/allow-multicast-traffic-to-be-steered-by-sd-wan (last visited December 2024) (emphasis added).

114. The Fortinet ‘559 Products determine a secure first communications link by integrating SD-WAN and IPsec VPN capabilities. The Fortinet ‘559 Products define multiple WAN connections as SD-WAN members, including physical interfaces, VLANs, and IPsec VPN tunnels. In addition, the Fortinet documentation states, “SD-WAN member interfaces can be any interface supported by FortiGates, such as physical ports, VLAN interfaces, LAGs, IPsec tunnels, GRE tunnels, IPIP tunnels, and FortiExtender interfaces. Once SD-WAN members are configured, they can be assigned to a zone.” This shows the ability of the Fortinet ‘559 Products to detect and recognize different communication links, such as “port1” and “port2” as shown in the topology diagrams, which can be configured with different security parameters. In addition, the configuration of “Network” > “Interfaces” includes, in this example, a “Specify” option, and “Address” and “Netmask” fields.



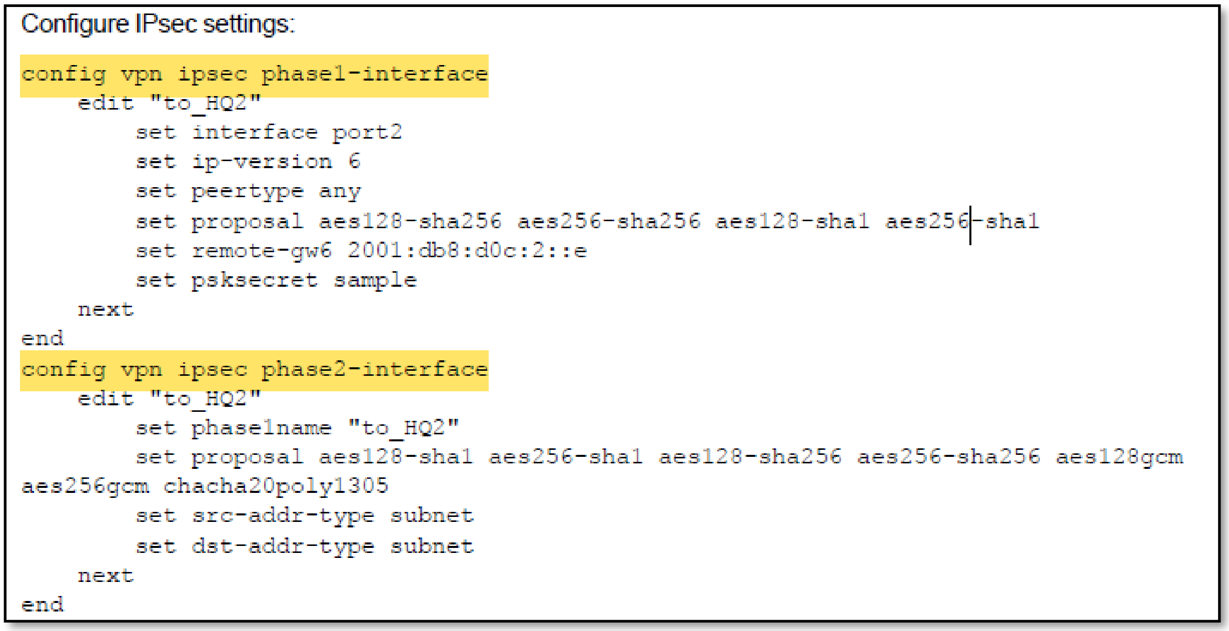
SD-WAN members and zones

SD-WAN bundles interfaces together into zones. Interfaces are first configured as SD-WAN members. This does not change the interface, it just allows SD-WAN to reference the interface as a member. SD-WAN member interfaces can be any interface supported by FortiGates, such as physical ports, VLAN interfaces, LAGs, IPsec tunnels, GRE tunnels, IPIP tunnels, and FortiExtender interfaces. Once SD-WAN members are configured, they can be assigned to a zone. Zones are used in policies as source and destination interfaces, in static routes, and in SD-WAN rules.

Multiple zones can be used to group SD-WAN interfaces for logical scenarios, such as overlay and underlay interfaces. Using multiple zones in policies allows for more granular control over functions like resource access and UTM access.

FORTIOS 7.6.1 ADMINISTRATION GUIDE at 844 (December 19, 2024) (emphasis added).

115. The Fortinet '559 Products detect a second communications link having second security, for communications of information between the client device and the server device. Specifically, the Fortinet '559 Products establish a second communications link with distinct "second security" parameters by leveraging integrated SD-WAN functionalities and IPsec VPN capabilities to create multiple secure paths. The Fortinet '559 Products define a set of WAN interfaces, including physical, logical, or IPsec tunnel interfaces, as members under config system sdwan. Each member is then assigned by the Fortinet '559 Products to different zones and associated with different health checks. For example, a secondary IPsec tunnel is provisioned using the "config vpn ipsec phase1-interface" and "config vpn ipsec phase2-interface" commands, defining unique keys, certificates, and other security parameters for encryption and authentication. This creates a secure connection distinct from the first communications link. In addition, the Fortinet '559 Products perform continuous health checks ("config health-check"), which monitor interface-level parameters such as "latency," "jitter," and "packet loss" to confirm that a second link remains available and meets defined performance thresholds. These metrics are used by the Fortinet '559 Products to actively detect and maintain awareness of a second secure communications link as an alternative path.

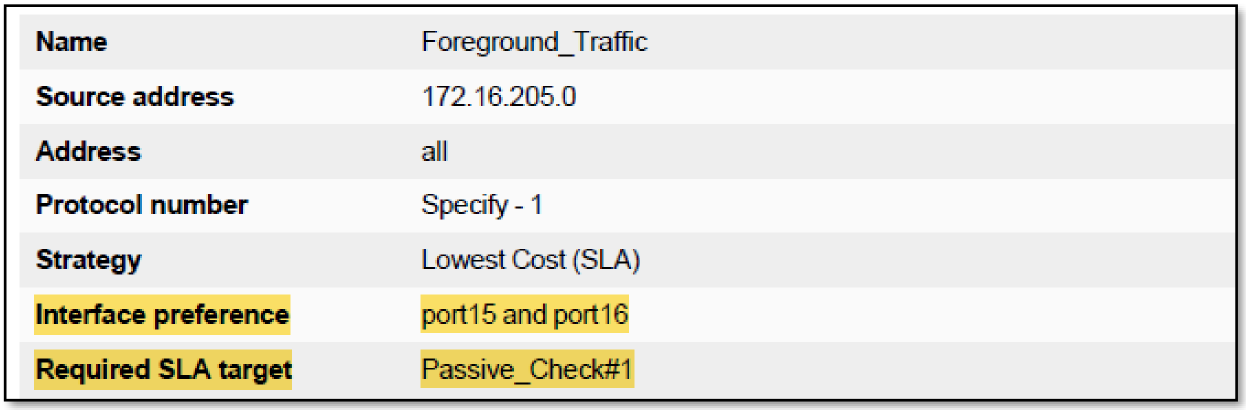


Configure IPsec settings:

```
config vpn ipsec phase1-interface
    edit "to_HQ2"
        set interface port2
        set ip-version 6
        set peertype any
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set remote-gw6 2001:db8:d0c:2::e
        set psksecret sample
    next
end
config vpn ipsec phase2-interface
    edit "to_HQ2"
        set phase1name "to_HQ2"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
        set src-addr-type subnet
        set dst-addr-type subnet
    next
end
```

FORTIOS 7.6.1 ADMINISTRATION GUIDE at 844 (December 19, 2024) (emphasis added).

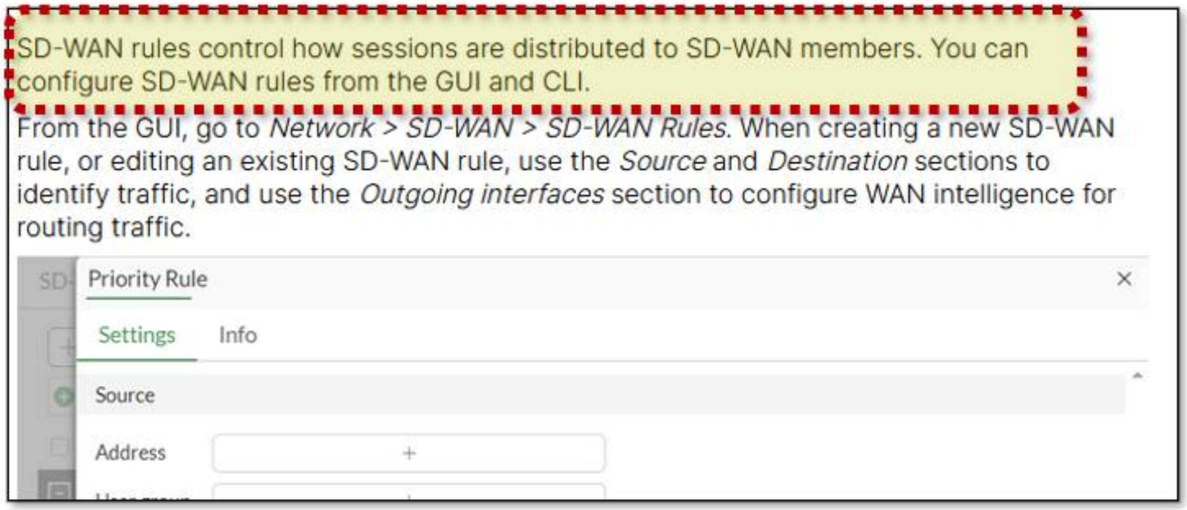
116. The Fortinet ‘559 Products select a first communications link, having a first security, for communicating between the client device and the server device if available. Specifically, the Fortinet ‘559 Products maintain a dynamic status log of each communication link’s status, including its security and performance, through configurable SD-WAN service rules and health checks. The SD-WAN rules allow the Fortinet ‘559 Products to define a preferred path based on various criteria, including manual selection, best quality, lowest cost (SLA), or maximize bandwidth. In addition, the Fortinet ‘559 Products can select an “Interface preference” and “Required SLA target” to perform the selection process, ensuring that higher security links are prioritized when they meet specified performance thresholds.



Name	Foreground_Traffic
Source address	172.16.205.0
Address	all
Protocol number	Specify - 1
Strategy	Lowest Cost (SLA)
Interface preference	port15 and port16
Required SLA target	Passive_Check#1

FORTIOS 7.6.1 ADMINISTRATION GUIDE at 844 (December 19, 2024) (emphasis added).

117. The Fortinet '559 Products implement link selection decisions via the SD-WAN rules, which are processed in a prioritized order. Specifically, the Fortinet '559 documentation states, "SD-WAN rules control how sessions are distributed to SD-WAN members," and these rules are processed in a top-down order, and the first rule that matches the traffic is applied. For example, an administrator can configure a rule to prioritize traffic matching specific criteria, such as "Source address," "Destination address," and "Protocol," to be routed through a designated SD-WAN member representing the first communications link with desired security. Furthermore, the "Interface preference" setting within SD-WAN rules allows explicit ordering of member interfaces, ensuring that the highest priority link with the first security parameter is selected if it is available and meets the defined performance SLAs.

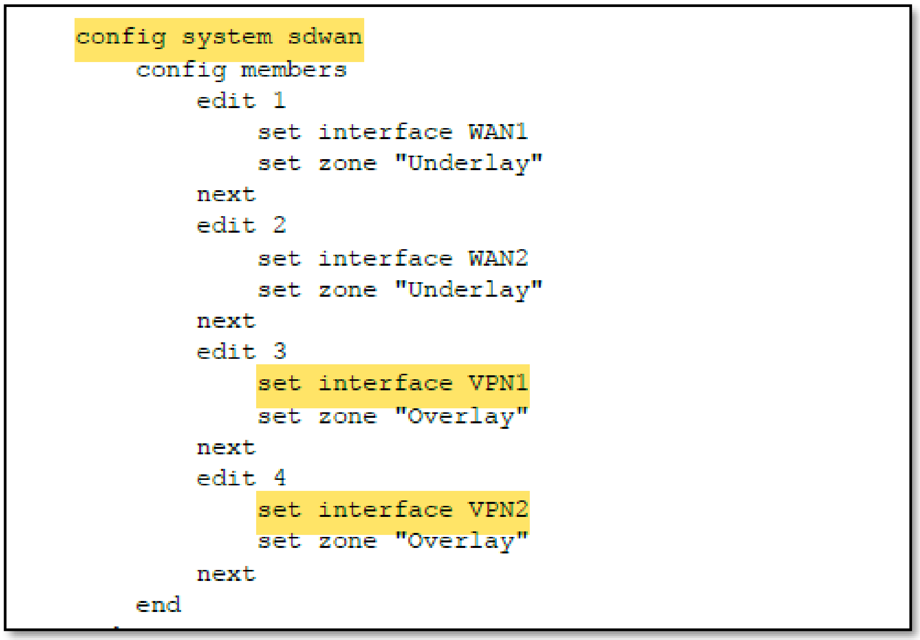


SD-WAN rules control how sessions are distributed to SD-WAN members. You can configure SD-WAN rules from the GUI and CLI.

From the GUI, go to *Network > SD-WAN > SD-WAN Rules*. When creating a new SD-WAN rule, or editing an existing SD-WAN rule, use the *Source* and *Destination* sections to identify traffic, and use the *Outgoing interfaces* section to configure WAN intelligence for routing traffic.

SD-WAN Rules Overview, FORTIGATE / FORTIOS 7.6.1 ADMINISTRATION GUIDE, *available at*: https://docs.fortinet.com/document/fortigate/7.6.1/administration-guide/413288/sd-wan-rules-overview (last visited December 2024) (emphasis added).

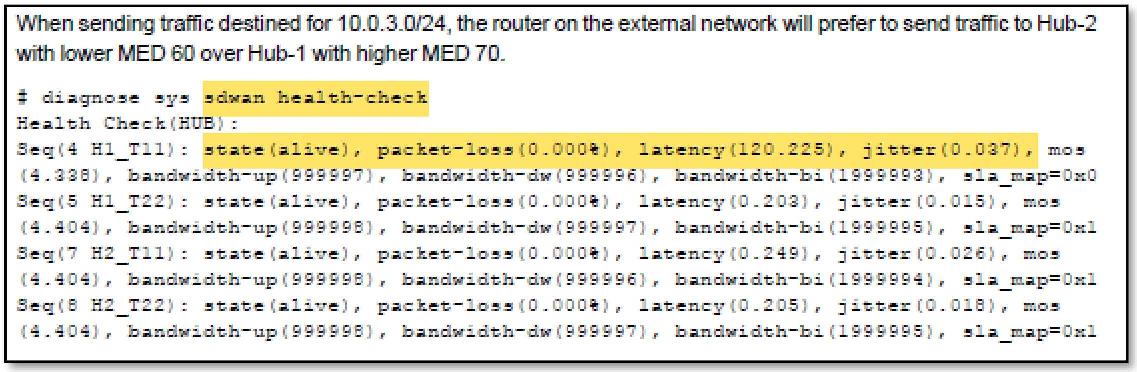
118. The Fortinet ‘559 Products select the second communications link, having second security, for communicating between the client device and the server device if the first communications link is not available. Specifically, the Fortinet ‘559 Products enable dynamic link selection and failover management for continuous connectivity between primary and secondary communication paths. The Fortinet ‘559 Products utilize SD-WAN rules in conjunction with performance SLAs to facilitate automated failover between defined interfaces and overlay tunnels. For example, within the “config system sdwan” configuration, administrators define “config members” with specific “interface” assignments, such as “set interface VPN1” or “set interface VPN2”, and associate these with distinct “gateway” IP addresses to establish secure traffic paths. In addition, the “set priority-members” parameter within the “config service” section establishes a defined order of preference among available interfaces, ensuring systematic failover when the primary link fails to meet configured thresholds.



```
config system sdwan
    config members
        edit 1
            set interface WAN1
            set zone "Underlay"
        next
        edit 2
            set interface WAN2
            set zone "Underlay"
        next
        edit 3
            set interface VPN1
            set zone "Overlay"
        next
        edit 4
            set interface VPN2
            set zone "Overlay"
        next
    end
```

FORTIOS 7.6.1 ADMINISTRATION GUIDE at 848 (December 19, 2024) (emphasis added).

119. The Fortinet '559 Products select the second communications link, having second security, for communicating between the client device and the server device, if the first communications link is not available. Specifically, the Fortinet '559 Products apply defined "priority-members" sequences to enable secondary communication links to assume traffic responsibilities without manual intervention when primary links fail to meet performance criteria. For example, when "edit <health-check>" parameters such as "set server" and "config sla" indicate primary link degradation, as shown by metrics like "state(alive), packet-loss(0.000%) latency(120.225), jitter(0.037)," the FortiGate devices immediately divert sessions to the alternate path configured with appropriate "set gateway" and "set sdwan-zone" parameters. In addition, the Fortinet '559 Products select a second communications link based on a dynamic failover process that leverages the "set sla-id-redistribute" and "set minimum-sla-meet-members" settings to ensure that failover occurs based on a comprehensive evaluation of link quality and availability.

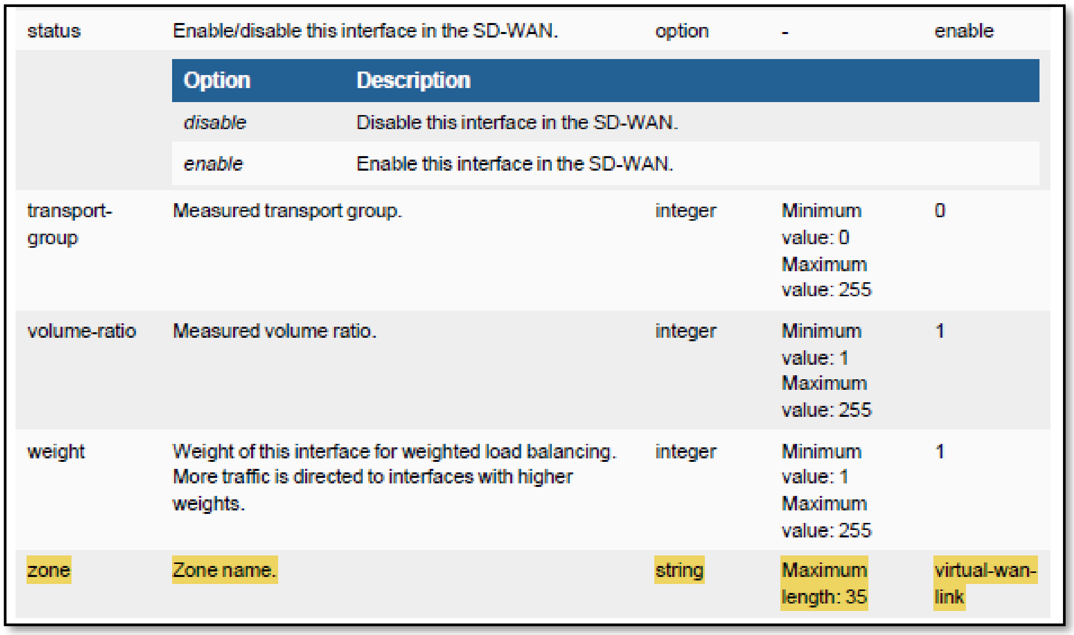


When sending traffic destined for 10.0.3.0/24, the router on the external network will prefer to send traffic to Hub-2 with lower MED 60 over Hub-1 with higher MED 70.

```
# diagnose sys sdwan health-check
Health Check(HUB):
Seq(4 H1_T11): state(alive), packet-loss(0.000%), latency(120.225), jitter(0.037), mos
(4.338), bandwidth-up(999997), bandwidth-dw(999996), bandwidth-bi(1999993), sla_map=0x0
Seq(5 H1_T22): state(alive), packet-loss(0.000%), latency(0.203), jitter(0.015), mos
(4.404), bandwidth-up(999998), bandwidth-dw(999997), bandwidth-bi(1999995), sla_map=0x1
Seq(7 H2_T11): state(alive), packet-loss(0.000%), latency(0.249), jitter(0.026), mos
(4.404), bandwidth-up(999998), bandwidth-dw(999996), bandwidth-bi(1999994), sla_map=0x1
Seq(8 H2_T22): state(alive), packet-loss(0.000%), latency(0.205), jitter(0.018), mos
(4.404), bandwidth-up(999998), bandwidth-dw(999997), bandwidth-bi(1999995), sla_map=0x1
```

SD-WAN WITH FORTIOS, FORTIMANAGER, AND FORTIANALYZER 7.6.X NEW FEATURES GUIDE at 89 (December 12, 2024) (emphasis added).

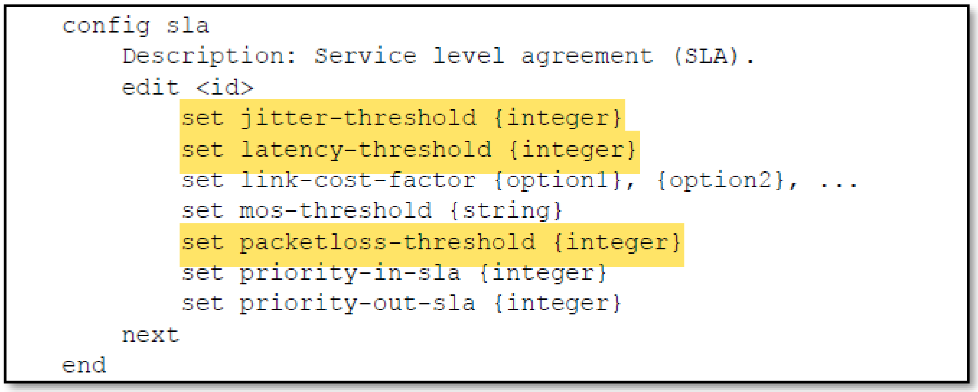
120. The Fortinet '559 Products link to one of either the first communications link and the second communications link at each instant, to maintain communicative connectivity during communications between the client device and the server device. Specifically, the Fortinet '559 Products implement multiple member interfaces, both physical and virtual, within defined zones using the "config members" configuration structure. For example, interfaces "port1" and "port2" are configured as members within a "virtual-wan-link" zone, enabling dynamic traffic routing based on SD-WAN rules and immediate failover capabilities. In addition, Fortinet '559 Products utilize gateway assignments for each member, establishing distinct communication paths and enabling instantaneous link transitions when performance degradation occurs.



status	Enable/disable this interface in the SD-WAN.	option	-	enable
	Option	**Description**		
	disable	Disable this interface in the SD-WAN.		
	enable	Enable this interface in the SD-WAN.		
transport-group	Measured transport group.	integer	Minimum value: 0 Maximum value: 255	0
volume-ratio	Measured volume ratio.	integer	Minimum value: 1 Maximum value: 255	1
weight	Weight of this interface for weighted load balancing. More traffic is directed to interfaces with higher weights.	integer	Minimum value: 1 Maximum value: 255	1
zone	Zone name.	string	Maximum length: 35	virtual-wan-link

FORTIOS 7.6.1 CLI REFERENCE at 1713 (November 28, 2024) (emphasis added).

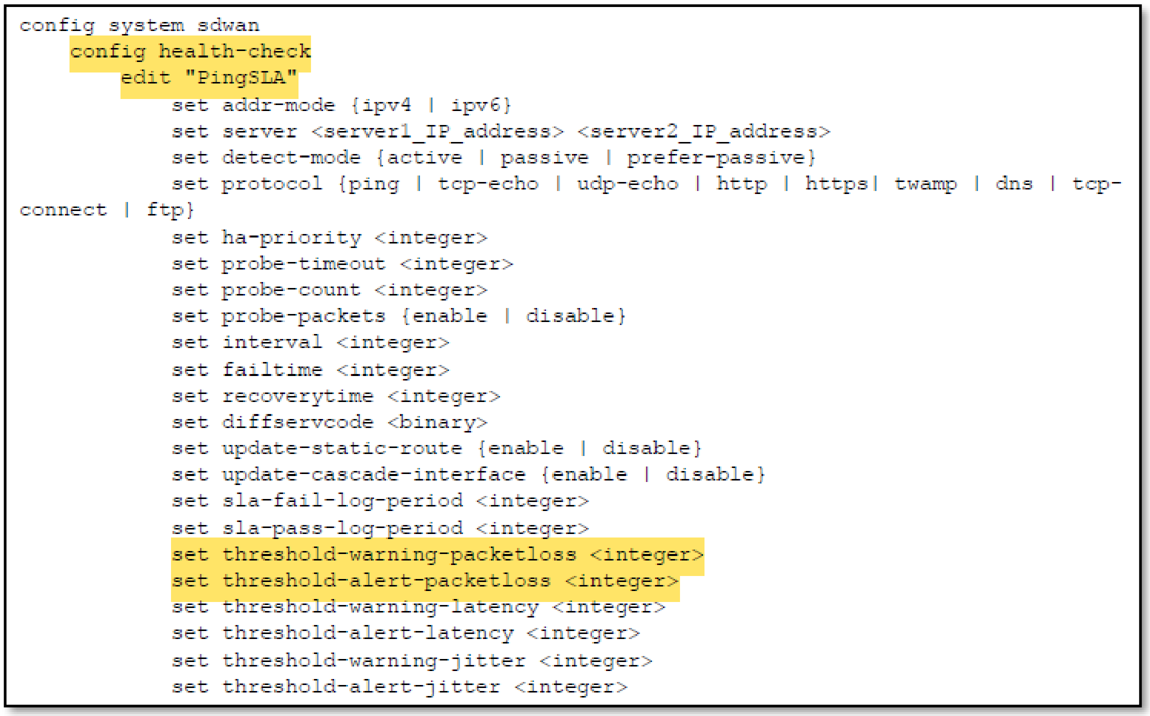
121. The Fortinet '559 Products establish a connection with either the first communications link or the second communications link at any given time to ensure continuous communication between the client device and the server device. Specifically, the Fortinet '559 Products maintain optimal connectivity through SD-WAN rule implementation and performance-based link selection strategies. The Fortinet '559 Products evaluate link performance using "mode sla" settings that incorporate "latency-threshold," "jitter-threshold," and "packetloss-threshold" metrics within the health-check configuration. For example, when configured with "priority-members 1 2 3," the Fortinet '559 Products establish a link hierarchy, ensuring traffic flows through the highest-priority functioning link that meets defined performance criteria. In addition, Fortinet '559 Products continuously monitor link status through the diagnose sys sdwan service command, marking members as "alive" or "dead" and maintaining an "sla_map" to guide real-time routing decisions.



```
config sla
    Description: Service level agreement (SLA).
    edit <id>
        set jitter-threshold {integer}
        set latency-threshold {integer}
        set link-cost-factor {option1}, {option2}, ...
        set mos-threshold {string}
        set packetloss-threshold {integer}
        set priority-in-sla {integer}
        set priority-out-sla {integer}
    next
end
```

FortiOS 7.6.1 CLI Reference at 1700 (November 28, 2024) (emphasis added).

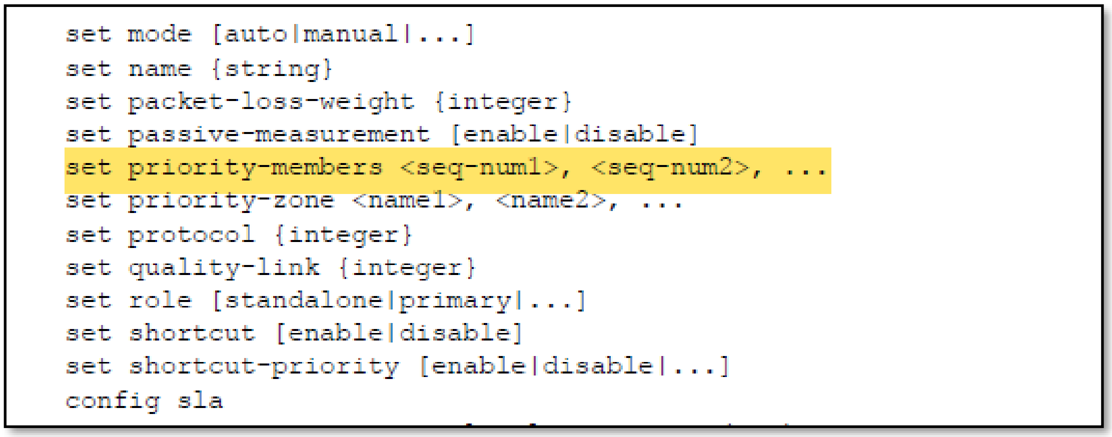
122. The Fortinet '559 Products execute link transitions through automated health monitoring and instantaneous failover mechanisms. Specifically, the Fortinet '559 Products utilize integrated SD-WAN rules and "health-check" configurations to detect performance anomalies and initiate immediate link switches. For example, when the "PingSLA" health check identifies a link failing to meet its "packetloss-threshold," the Fortinet '559 Products redirect traffic to an alternative link configured with appropriate "set gateway" parameters. In addition, the Fortinet '559 Products maintain connectivity by evaluating SLA parameters and performing routing adjustments.



```
config system sdwan
    config health-check
        edit "PingSLA"
            set addr-mode {ipv4 | ipv6}
            set server <server1_IP_address> <server2_IP_address>
            set detect-mode {active | passive | prefer-passive}
            set protocol {ping | tcp-echo | udp-echo | http | https| twamp | dns | tcp-
connect | ftp}
            set ha-priority <integer>
            set probe-timeout <integer>
            set probe-count <integer>
            set probe-packets {enable | disable}
            set interval <integer>
            set failtime <integer>
            set recoverytime <integer>
            set diffservcode <binary>
            set update-static-route {enable | disable}
            set update-cascade-interface {enable | disable}
            set sla-fail-log-period <integer>
            set sla-pass-log-period <integer>
            set threshold-warning-packetloss <integer>
            set threshold-alert-packetloss <integer>
            set threshold-warning-latency <integer>
            set threshold-alert-latency <integer>
            set threshold-warning-jitter <integer>
            set threshold-alert-jitter <integer>
```

FORTIOS 7.6.1 ADMINISTRATION GUIDE at 866 (December 19, 2024) (emphasis added).

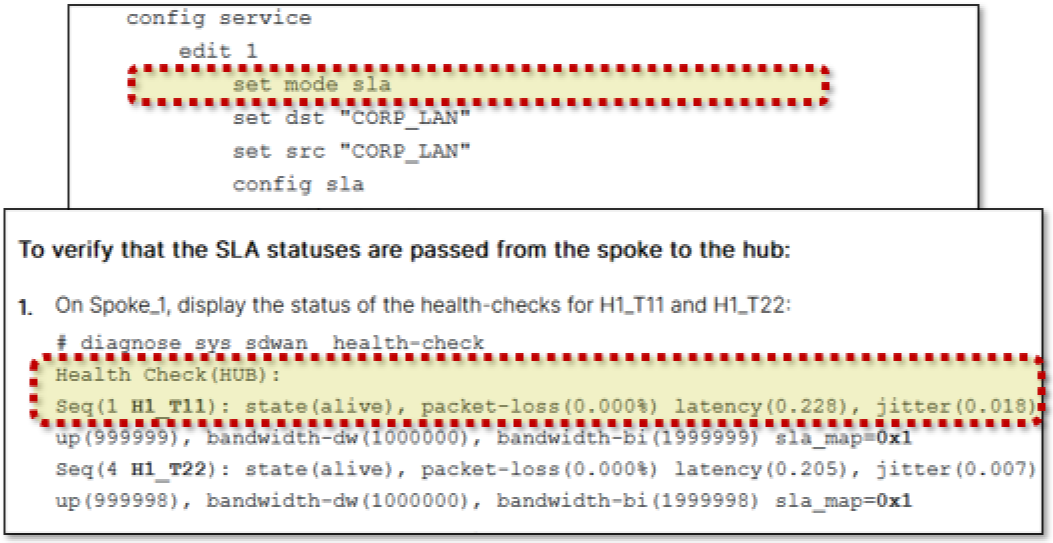
123. The Fortinet '559 Products reconnect to the first communications link for communicating information between the client device and the server device, if communication is hindered over the second communications link. Specifically, the Fortinet '559 Products revert to a primary communication link after a failover to a secondary link if the primary link meets the configured health-check criteria. This functionality is performed by the Fortinet '559 Products' SD-WAN rules and "priority-members," "health-check," and "hold-down-time" parameters.



```
set mode [auto|manual|...]
set name {string}
set packet-loss-weight {integer}
set passive-measurement [enable|disable]
set priority-members <seq-num1>, <seq-num2>, ...
set priority-zone <name1>, <name2>, ...
set protocol {integer}
set quality-link {integer}
set role [standalone|primary|...]
set shortcut [enable|disable]
set shortcut-priority [enable|disable|...]
config sla
```

FORTIOS 7.6.1 CLI REFERENCE at 1702 (November 28, 2024) (emphasis added).

124. The Fortinet '559 Products evaluate link performance using "mode sla" settings that incorporate "latency-threshold," and "packetloss-threshold" metrics within the health-check configuration. For example, when configured with "priority-members 1 2 3," the Fortinet '559 Products establish a clear link hierarchy, ensuring traffic flows through the highest-priority functioning link that meets defined performance criteria. In addition, the Fortinet '559 Products monitor link status through the "diagnose sys sdwan health-check" command.



```
config service
    edit 1
        set mode sla
        set dst "CORP_LAN"
        set src "CORP_LAN"
        config sla
```

To verify that the SLA statuses are passed from the spoke to the hub:

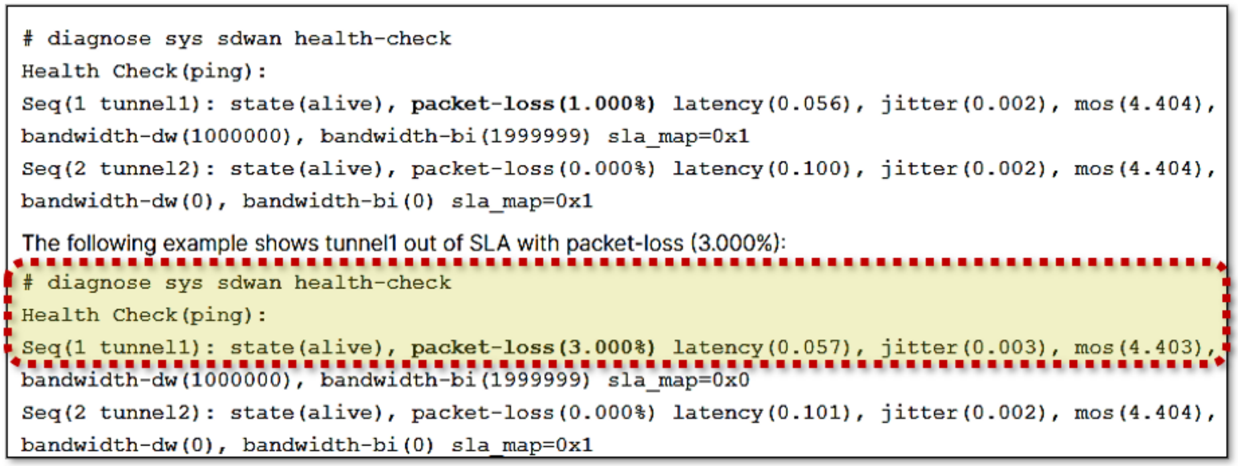
1. On Spoke_1, display the status of the health-checks for H1_T11 and H1_T22:

```
# diagnose sys sdwan  health-check
Health Check(HUB):
Seq(1 H1_T11): state(alive), packet-loss(0.000%) latency(0.228), jitter(0.018)
up(999999), bandwidth-dw(1000000), bandwidth-bi(1999999) sla_map=0x1
Seq(4 H1_T22): state(alive), packet-loss(0.000%) latency(0.205), jitter(0.007)
up(999998), bandwidth-dw(1000000), bandwidth-bi(1999998) sla_map=0x1
```

Embedded SD-WAN-SLA Information In ICMP Probes, FORTIGATE FORTIOS 7.2.0, *available at*: https://docs.fortinet.com/document/fortigate/7.2.0/new-features/848259 (last visited December 2024) (emphasis added).

125. The Fortinet '559 Products execute rapid link transitions through automated health monitoring and failover mechanisms. Specifically, the Fortinet '559 Products utilize "health-check" configurations to detect performance anomalies. For example, when the health-check status of a member becomes degraded, such as returning "state(alive), packet-loss(3.000%) latency(0.057), jitter(0.003), mos(4.403)", traffic will be rerouted through the next preferred member. When an interface has recovered, the "hold-down-time" setting introduces a delay before traffic resumes on that interface. In addition, the Fortinet '559 Products leverage the "set link-cost-factor remote" setting to prioritize the selection of a member based on the health of the

associated link. The “set priority-members” setting defines the order in which members will be selected when the “set link-cost-factor remote” setting has the same value on the preferred members.



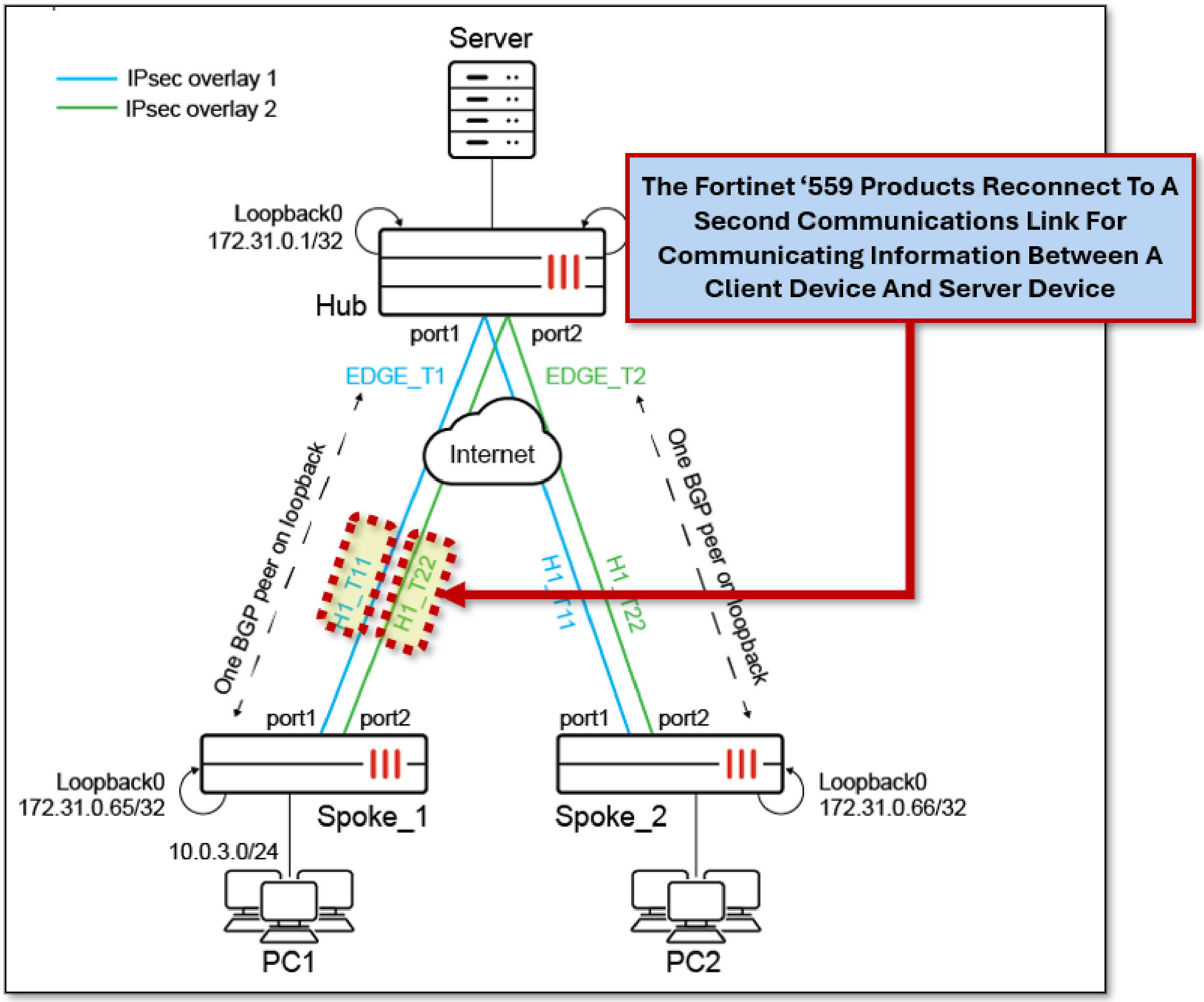
```
# diagnose sys sdwan health-check
Health Check(ping):
Seq(1 tunnel1): state(alive), packet-loss(1.000%) latency(0.056), jitter(0.002), mos(4.404),
bandwidth-dw(1000000), bandwidth-bi(1999999) sla_map=0x1
Seq(2 tunnel2): state(alive), packet-loss(0.000%) latency(0.100), jitter(0.002), mos(4.404),
bandwidth-dw(0), bandwidth-bi(0) sla_map=0x1
```

The following example shows tunnel1 out of SLA with packet-loss (3.000%):

```
# diagnose sys sdwan health-check
Health Check(ping):
Seq(1 tunnel1): state(alive), packet-loss(3.000%) latency(0.057), jitter(0.003), mos(4.403),
bandwidth-dw(1000000), bandwidth-bi(1999999) sla_map=0x0
Seq(2 tunnel2): state(alive), packet-loss(0.000%) latency(0.101), jitter(0.002), mos(4.404),
bandwidth-dw(0), bandwidth-bi(0) sla_map=0x1
```

Use SD-WAN Rules To Steer Multicast Traffic, FortiGate FortiOS 7.4.0 Administrative Guide, *available at*: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243964/use-sd-wan-rules-to-steer-multicast-traffic-new (last visited December 2024) (emphasis added).

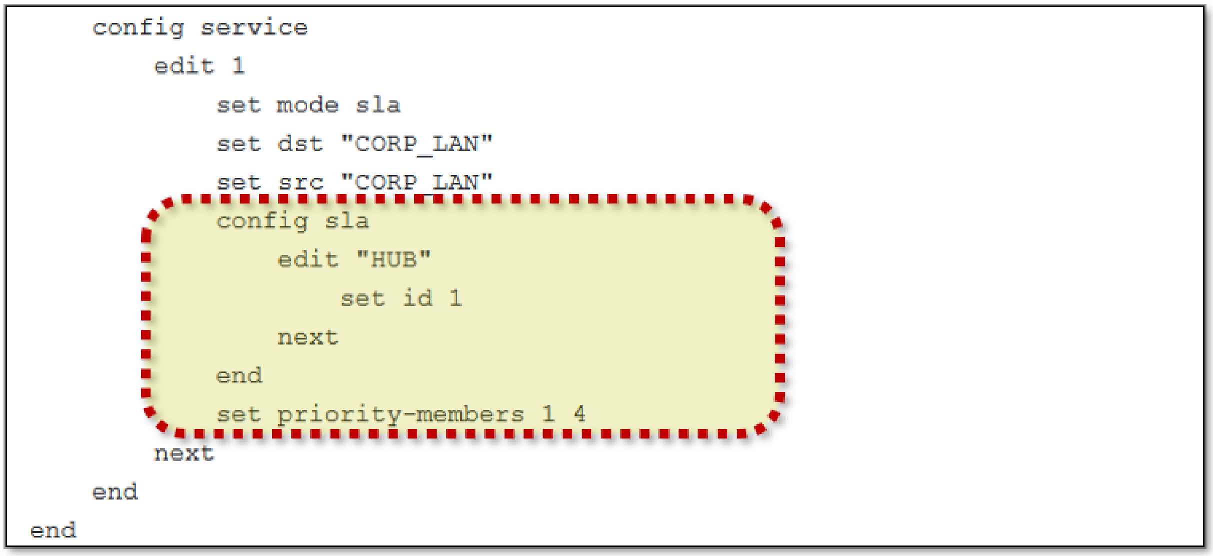
126. The Fortinet ‘559 Products reconnect to a second communications link for communicating information between a client device and server device, if communications are hindered over the first communications link. Specifically, the Fortinet ‘559 Products perform dynamic communication link management through SD-WAN. For example, when a failover occurs from “H1_T11” to “H1_T22” due to SLA violations on “H1_T11,” the Fortinet ‘559 Products continuously assess link performance through the “diagnose sys sdwan health-check” command, monitoring critical metrics including “state,” “packet-loss,” “latency,” and “jitter” for each member interface.



Embedded SD-WAN-SLA Information In ICMP Probes, FORTIGATE FORTIOS 7.4.0, *available at*: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/848259/embedded-sd-wan-sla-information-in-icmp-probes (last visited December 2024) (annotation added).

127. The Fortinet '559 Products perform failover control through prioritized member management within the Fortinet '559 Products SD-WAN service rules. Specifically, the Fortinet '559 Products implement "priority-members" assignments to establish a hierarchical failover sequence, ensuring traffic routes through the highest-priority member meeting SLA criteria. For example, when "H1_T11" holds priority 1 and experiences degradation, traffic transitions to "H1_T22" based on the configured priority in the "priority-members" list and the satisfaction of SLA requirements. In addition, the Fortinet '559 Products employ "sla-stickiness" settings to

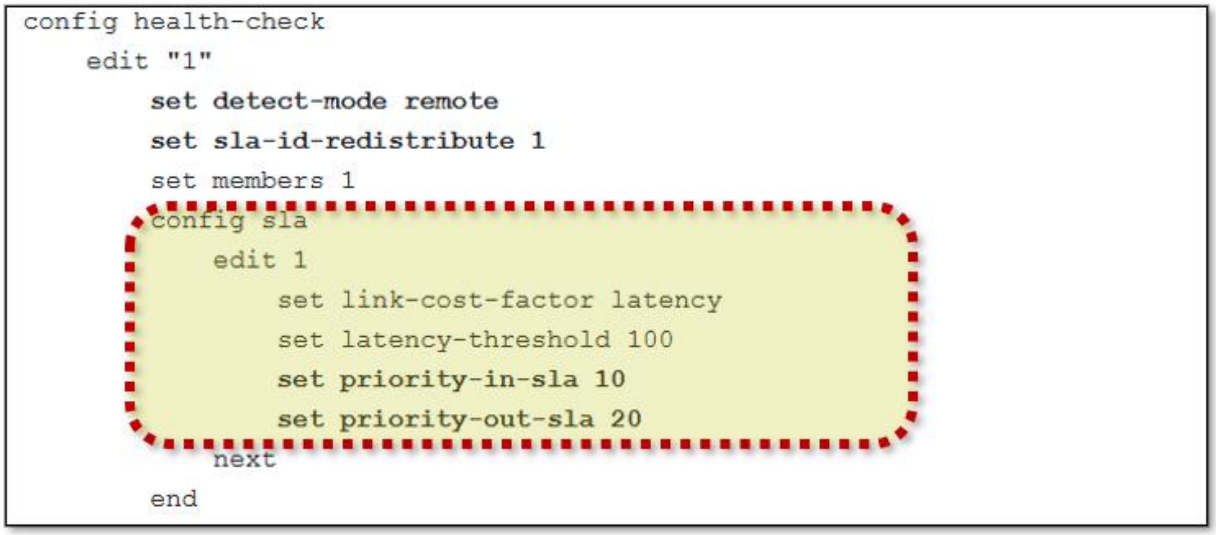
maintain session continuity, preserving existing connections on their current path while SLA requirements remain satisfied.



```
    config service
        edit 1
            set mode sla
            set dst "CORP_LAN"
            set src "CORP_LAN"
            config sla
                edit "HUB"
                    set id 1
                next
            end
            set priority-members 1 4
        next
    end
end
```

Embedded SD-WAN-SLA Information In ICMP Probes, FORTIGATE FORTIOS 7.4.0, *available at*: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/848259/embedded-sd-wan-sla-information-in-icmp-probes (last visited December 2024) (emphasis added).

128. The Fortinet ‘559 Products set link quality thresholds using dynamic routing. Specifically, the Fortinet ‘559 Products use “config system sdwan” and “health-check” parameters to evaluate “latency-threshold,” “jitter-threshold,” and “packetloss-threshold” metrics against real-time link performance. For example, when the primary link exceeds defined performance thresholds such as “packetloss-threshold 1” or “latency-threshold 100,” the devices initiate an immediate transition to the secondary link as defined by the “set priority-members” directive within the relevant SD-WAN service rule.



```
config health-check
    edit "1"
        set detect-mode remote
        set sla-id-redistribute 1
        set members 1
        config sla
            edit 1
                set link-cost-factor latency
                set latency-threshold 100
                set priority-in-sla 10
                set priority-out-sla 20
            next
        end
```

Embedded SD-WAN-SLA Information In ICMP Probes, FORTIGATE FORTIOS 7.4.0, *available at*: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/848259/embedded-sd-wan-sla-information-in-icmp-probes (last visited December 2024) (emphasis added).

129. Fortinet has directly infringed and continues to directly infringe the ‘559 Patent by, among other things, making, using, offering for sale, and/or selling technology comprising a method of communicating information over multiple communications links, including but not limited to the Fortinet ‘559 Products.

130. The Fortinet ‘559 Products are available to businesses and individuals throughout the United States.

131. The Fortinet ‘559 Products are provided to businesses and individuals located in this District.

132. By making, using, testing, offering for sale, and/or selling products and services comprising a method of communicating information over multiple communications links, including but not limited to the Fortinet ‘559 Products, Fortinet has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘559 Patent, including at least claim 5 pursuant to 35 U.S.C. § 271(a).

133. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘559 Patent.

134. As a result of Fortinet’s infringement of the ‘559 Patent, Plaintiff has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Fortinet’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Fortinet together with interest and costs as fixed by the Court.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 10,412,388

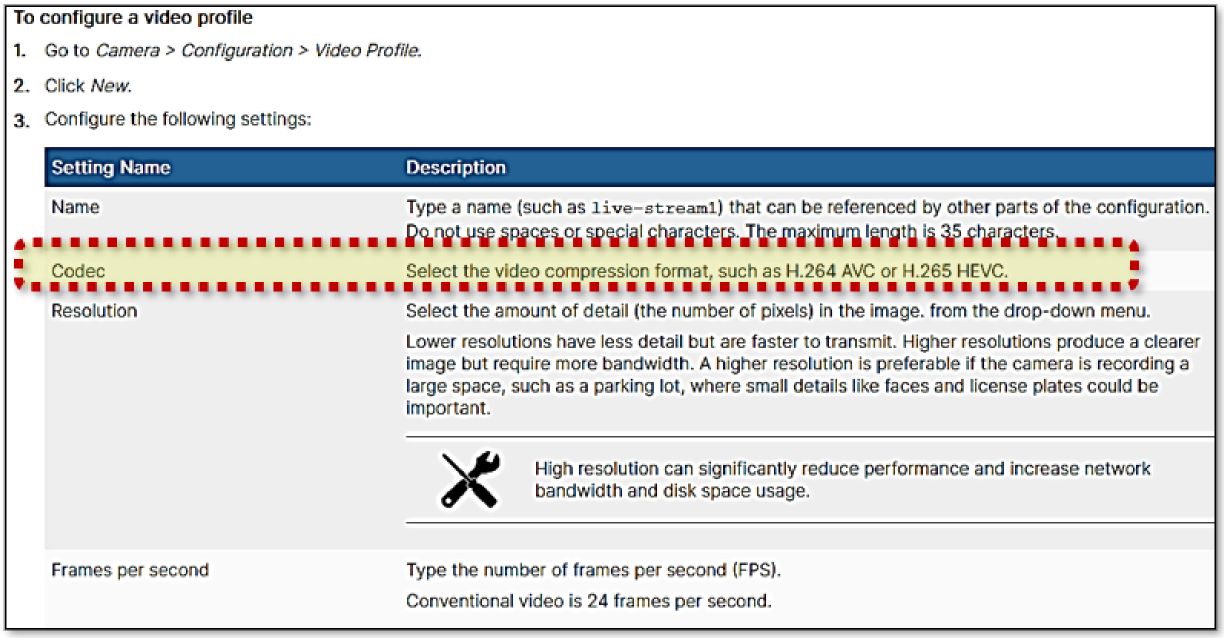
135. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

136. Fortinet designs, makes, uses, sells, and/or offers for sale in the United States products comprising technology for video compression using adaptive re-quantization using extracted and derived quantization parameters.

137. Fortinet designs, makes, sells, offers to sell, imports, and/or uses products that perform encoding of media data in compliance with the H.265 High Efficiency Video Coding (HEVC) compression standard, including but not limited to FortiCamera (including at least models: FB50, FE120, FE120B, FD20B, FD50, FD55-CA, CB50, CD51, CD51-C, CD55, CD55-C, MC51, MC51-C, MD40, MD50B, SD20B, and PD50) and FortiRecorder (including at least models: FortiRecorder-400F, FortiRecorder-400D, FortiRecorder-200D, FortiRecorder-100D, FortiRecorder-100G, and FortiRecorder-VM) (collectively, the “Fortinet ‘388 Product(s)”).

138. Fortinet designs, makes, sells, offers to sell, imports, and/or uses Fortinet ‘388 products that comply with the H.265 video encoding standard.

139. The Fortinet '388 Products perform video processing compliant with the High Efficiency Video Coding (HEVC) standard, which is also often referred to as the H.265 standard. Specifically, the Fortinet '388 products perform HEVC encoding.

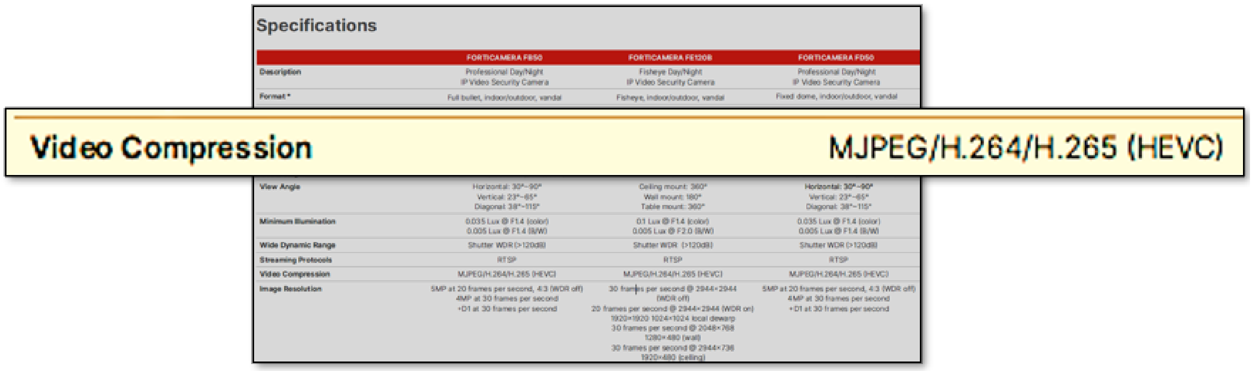


To configure a video profile

1. Go to *Camera > Configuration > Video Profile.*
2. Click *New.*
3. Configure the following settings:

Setting Name	Description
Name	Type a name (such as `live-stream1`) that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
Codec	Select the video compression format, such as H.264 AVC or H.265 HEVC.
Resolution	Select the amount of detail (the number of pixels) in the image. from the drop-down menu. Lower resolutions have less detail but are faster to transmit. Higher resolutions produce a clearer image but require more bandwidth. A higher resolution is preferable if the camera is recording a large space, such as a parking lot, where small details like faces and license plates could be important. High resolution can significantly reduce performance and increase network bandwidth and disk space usage.
Frames per second	Type the number of frames per second (FPS). Conventional video is 24 frames per second.

Video Profiles, FORTIRECORDER 7.2.2 ADMINISTRATION GUIDE, *available at*: https://docs.fortinet.com/document/fortirecorder/7.2.2/administration-guide/167853/configuring-video-profiles (last visited December 2024) (emphasis added).



Specifications

	FORTICAMERA FB50	FORTICAMERA FE120B	FORTICAMERA FD50
Description	Professional Day/Night IP Video Security Camera	Fisheye Day/Night IP Video Security Camera	Professional Day/Night IP Video Security Camera
Format *	Full bullet, indoor/outdoor, vandal	Fisheye, indoor/outdoor, vandal	Fixed dome, indoor/outdoor, vandal
View Angle	Horizontal: 30°~90° Vertical: 23°~65° Diagonal: 38°~115°	Ceiling mount: 360° Wall mount: 180° Table mount: 360°	Horizontal: 30°~90° Vertical: 23°~65° Diagonal: 38°~115°
Minimum Illumination	0.035 Lux @ F1.4 (color) 0.005 Lux @ F1.4 (B/W)	0.1 Lux @ F1.4 (color) 0.005 Lux @ F2.0 (B/W)	0.035 Lux @ F1.4 (color) 0.005 Lux @ F1.4 (B/W)
Wide Dynamic Range	Shutter WDR (>120dB)	Shutter WDR (>120dB)	Shutter WDR (>120dB)
Streaming Protocols	RTSP	RTSP	RTSP
Video Compression	MJPEG/H.264/H.265 (HEVC)	MJPEG/H.264/H.265 (HEVC)	MJPEG/H.264/H.265 (HEVC)
Image Resolution	5MP at 20 frames per second, 4:3 (WDR off) 4MP at 30 frames per second +D1 at 30 frames per second	30 frames per second @ 2944×2944 (WDR off) 20 frames per second @ 2944×2944 (WDR on) 1920×1920 1024×1024 local dewarp 30 frames per second @ 2048×768 1280×480 (wall) 30 frames per second @ 2944×736 1920×480 (ceiling)	5MP at 20 frames per second, 4:3 (WDR off) 4MP at 30 frames per second +D1 at 30 frames per second

Video Compression MJPEG/H.264/H.265 (HEVC)

FortiCamera Series Data Sheet, FORTINET DOCUMENTATION at 4 (January 17, 2024) (emphasis added).

140. One or more Fortinet subsidiaries and/or affiliates use the Fortinet '388 Products in regular business operations.

141. The Fortinet '388 Products identify an initial quantization parameter employed to compress a previously decoded frame.

142. The Fortinet '388 Products, as part of the encoding process use an initial quantization parameter (QP) for encoding each frame or coding unit (CU). In conforming to the HEVC standard, the Fortinet '388 Products must set an initial QP value that serves as the baseline for encoding the decoded frame.

143. The Fortinet '388 Products calculate a delta quantization parameter as influenced by the initial quantization parameter, where the function is designed to yield this delta parameter at least in part to achieve a bitrate reduction while sustaining a given quality threshold.

144. The Fortinet '388 Products calculate a delta QP based on the initial quantization parameter. This function aims to minimize bitrate while retaining the required video quality.

145. The Fortinet '388 Products ascertain a subsequent quantization parameter for the purpose of compressing the decoded frame, based on both the initial and delta quantization parameters.

146. The Fortinet '388 Products determine a second quantization parameter using the initial QP and the delta QP. The Fortinet '388 Products calculate the second quantization parameter as QP1 + Delta QP. This second quantization parameter is the one used for encoding either the entire frame or specific coding units within the frame.

147. The Fortinet '388 Products compress the decoded frame utilizing the second quantization parameter.

148. The Fortinet '388 Products encode the video frames using the newly derived second quantization parameter.

149. By complying with the HEVC standard, the Fortinet ‘388 Products necessarily infringe the ‘388 Patent. Mandatory sections of the HEVC standard require the elements required by certain claims of the ‘388 Patent, including but not limited to claim 1. High Efficiency Video Coding, Series H: Audiovisual And Multimedia Systems: Infrastructure Of Audiovisual Services – Coding Of Moving Video Rec. ITU-T H.265 (August 2021). The following sections of the HEVC Standard are relevant to Fortinet's infringement of the ‘388 Patent: "7.3.2.2.3 Sequence parameter set screen content coding extension syntax;" "7.3.8.4 Coding quadtree syntax;" "7.3.8.14 Delta QP syntax;" "7.4.3.3.1 General picture parameter set RBSP semantics;" "7.4.7.1 General slice segment header semantics;" "7.4.9.14 Delta QP semantics;" "8.6.1 Derivation process for quantization parameters;" and "9.3.3.10 Binarization process for cu_qp_delta_abs."

150. All implementations of the HEVC standard necessarily infringe the ‘388 Patent as every implementation of the standard requires compliant devices to carry out the following: Each frame or coding unit (CU) is encoded using a pre-defined initial Quantization Parameter (QP) which serves as a baseline for various optimizations. The standard mandates that a first QP (QP1) be identified before any encoding can occur. The Fortinet ‘388 Products are, therefore, required to have mechanisms to set this initial QP1 for the to-be-encoded (or re-encoded) frame. Further, the HEVC standard sets out a structured way to adjust this initial QP based on a delta value. The objective of introducing a delta QP is generally to adapt to the complexity variations within a video sequence and to optimize rate-distortion performance. The HEVC encoding standard sets forth calculating a new QP (QP2) after determining the delta QP. This is done by adding the initial QP (QP1) and the delta QP. This step is essential for maintaining granular control over the rate-distortion tradeoff during encoding. Finally, the final encoding of the frame or CU takes place using QP2. The HEVC standard specifies that this is a requisite step for the encoding process to

be considered compliant. The Fortinet ‘388 Products must, therefore, encode frames using this newly computed QP2 to meet the standard’s rate and quality stipulations.

151. Fortinet has directly infringed and continues to directly infringe the ‘388 Patent by, among other things, making, using, offering for sale, and/or selling technology for video compression using adaptive re-quantization using extracted and derived quantization parameters, including but not limited to the Fortinet ‘388 Products.

152. The Fortinet ‘388 Products are available to businesses and individuals throughout the United States.

153. The Fortinet ‘388 Products are provided to businesses and individuals located in this District.

154. By making, using, testing, offering for sale, and/or selling products and services comprising technology for video compression using adaptive re-quantization using extracted and derived quantization parameters, including but not limited to the Fortinet ‘388 Products, Fortinet has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘388 Patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

155. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘388 Patent.

156. As a result of Fortinet’s infringement of the ‘388 Patent, Plaintiff has suffered monetary damages, and seek recovery in an amount adequate to compensate for Fortinet’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Fortinet together with interest and costs as fixed by the Court.

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 9,894,361

157. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

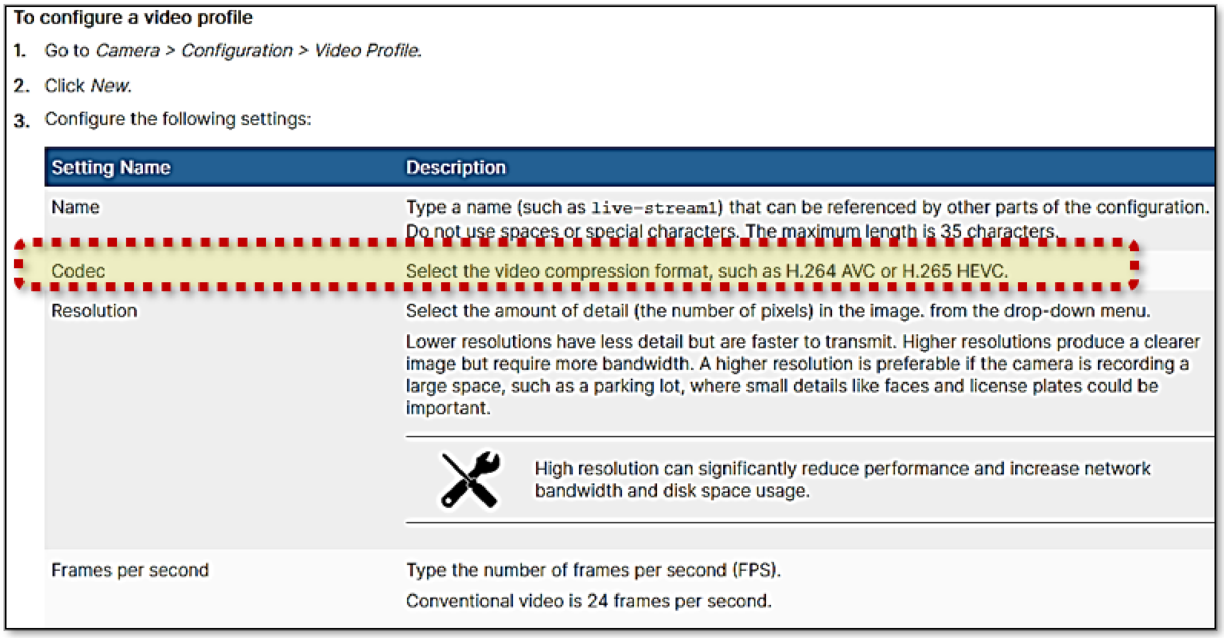
158. Fortinet designs, makes, uses, sells, and/or offers for sale in the United States products containing technology for quality-aware video optimization.

159. Fortinet designs, makes, sells, offers to sell, imports, and/or uses products that perform encoding of media data in compliance with the H.265 High Efficiency Video Coding (HEVC) compression standard, including but not limited to FortiCamera (including at least models: FB50, FE120, FE120B, FD20B, FD50, FD55-CA, CB50, CD51, CD51-C, CD55, CD55-C, MC51, MC51-C, MD40, MD50B, SD20B, and PD50) and FortiRecorder (including at least models: FortiRecorder-400F, FortiRecorder-400D, FortiRecorder-200D, FortiRecorder-100D, FortiRecorder-100G, and FortiRecorder-VM) (collectively, the "Fortinet '361 Product(s)").

160. One or more Fortinet subsidiaries and/or affiliates use the Fortinet '361 Products in regular business operations.

161. Fortinet designs, makes, sells, offers to sell, imports, and/or uses Fortinet '361 products that comply with the H.265 video encoding standard.

162. The Fortinet '361 Products perform video processing compliant with the High Efficiency Video Coding (HEVC) standard, which is also often referred to as the H.265 standard. Specifically, the Fortinet '361 products perform HEVC encoding.

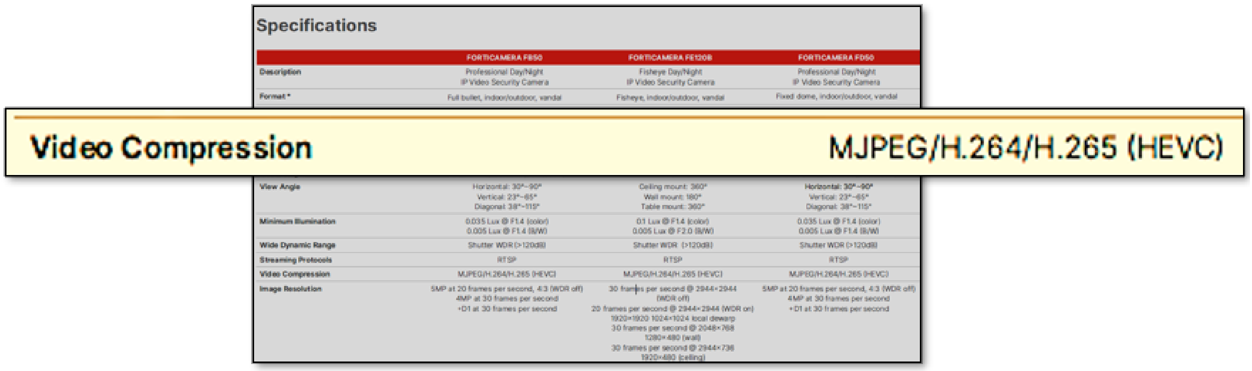


To configure a video profile

1. Go to *Camera > Configuration > Video Profile*.
2. Click *New*.
3. Configure the following settings:

Setting Name	Description
Name	Type a name (such as `live-stream1`) that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
Codec	Select the video compression format, such as H.264 AVC or H.265 HEVC.
Resolution	Select the amount of detail (the number of pixels) in the image. from the drop-down menu. Lower resolutions have less detail but are faster to transmit. Higher resolutions produce a clearer image but require more bandwidth. A higher resolution is preferable if the camera is recording a large space, such as a parking lot, where small details like faces and license plates could be important. High resolution can significantly reduce performance and increase network bandwidth and disk space usage.
Frames per second	Type the number of frames per second (FPS). Conventional video is 24 frames per second.

Video Profiles, FORTIRECORDER 7.2.2 ADMINISTRATION GUIDE, *available at*: https://docs.fortinet.com/document/fortirecorder/7.2.2/administration-guide/167853/configuring-video-profiles (last visited December 2024) (emphasis added).



Specifications

	FORTICAMERA FB50	FORTICAMERA FE120B	FORTICAMERA FD50
Description	Professional Day/Night IP Video Security Camera	Fisheye Day/Night IP Video Security Camera	Professional Day/Night IP Video Security Camera
Format *	Full bullet, indoor/outdoor, vandal	Fisheye, indoor/outdoor, vandal	Fixed dome, indoor/outdoor, vandal
View Angle	Horizontal: 30°~90° Vertical: 23°~65° Diagonal: 38°~115°	Ceiling mount: 360° Wall mount: 180° Table mount: 360°	Horizontal: 30°~90° Vertical: 23°~65° Diagonal: 38°~115°
Minimum Illumination	0.035 Lux @ F1.4 (color) 0.005 Lux @ F1.4 (B/W)	0.1 Lux @ F1.4 (color) 0.005 Lux @ F2.0 (B/W)	0.035 Lux @ F1.4 (color) 0.005 Lux @ F1.4 (B/W)
Wide Dynamic Range	Shutter WDR (>120dB)	Shutter WDR (>120dB)	Shutter WDR (>120dB)
Streaming Protocols	RTSP	RTSP	RTSP
Video Compression	MJPEG/H.264/H.265 (HEVC)	MJPEG/H.264/H.265 (HEVC)	MJPEG/H.264/H.265 (HEVC)
Image Resolution	5MP at 20 frames per second, 4:3 (WDR off) 4MP at 30 frames per second +D1 at 30 frames per second	30 frames per second @ 2944×2944 (WDR off) 20 frames per second @ 2944×2944 (WDR on) 1920×1920 1024×1024 local dewarp 30 frames per second @ 2048×768 1280×480 (wall) 30 frames per second @ 2944×736 1920×480 (ceiling)	5MP at 20 frames per second, 4:3 (WDR off) 4MP at 30 frames per second +D1 at 30 frames per second

Video Compression MJPEG/H.264/H.265 (HEVC)

FortiCamera Series Data Sheet, FORTINET DOCUMENTATION at 4 (January 17, 2024) (emphasis added).

163. The Fortinet '361 Products unpack a compressed video frame from a series containing multiple video frames.

164. The Fortinet '361 Products take an encoded video frame as input. This frame is one in a series that consists of multiple frames. The encoded frame is then passed through a decoding pipeline by the Fortinet '361 Products. The Fortinet '361 Products use inverse

quantization and inverse DCT (Discrete Cosine Transform) functions, to revert the video data to a decompressed state suitable for further manipulation.

165. The Fortinet ‘361 Products obtain an initial Quantization Parameter (QP) from the unpacked video frame, where this initial QP is indicative of the quantization configurations initially applied to compress the video frame.

166. The Fortinet ‘361 Products extract a first Quantization Parameter (QP) from the video frame metadata or from the bitstream itself. This first QP reflects the quantization settings initially applied during the original encoding. This first QP is read from the slice header or similar control structures and used to modulate the quantization matrices in the decoding process.

167. The Fortinet ‘361 Products calculate a delta QP influenced by the initial QP.

168. Upon acquiring the first QP, a delta QP is calculated by the Fortinet ‘361 Products. This delta QP value is computed through a set of heuristic functions to optimize for certain objectives like bitrate reduction, video quality, or computational efficiency. The delta QP acquired by the Fortinet ‘361 Products is a function of the first QP and other parameters, such as frame type (I-frame, P-frame, etc.).

169. The Fortinet ‘361 Products derive an inflation factor through comparing the total byte size of video frames after and before decompression, where both the newly received compressed frame and those previously decompressed belong to the same series of multiple video frames.

170. The Fortinet ‘361 Products compute an inflation adjustment factor based on the total byte size of previously decompressed frames and those frames post-compression. This comparison aids in estimating the compression efficiency.

171. The Fortinet ‘361 Products acquire a subsequent QP influenced by both the delta QP and the inflation factor, wherein this subsequent QP is indicative of the quantization configurations to be applied for recompressing the unpacked frame.

172. The second QP is then acquired by the Fortinet ‘361 Products by combining the calculated delta QP and the inflation adjustment. This second quantization parameter acquired by the Fortinet ‘361 Products aims to balance the trade-offs between quality and bitrate, taking into account the information gleaned from previous frames as indicated by the inflation adjustment.

173. The Fortinet ‘361 Products compress the unpacked video frame utilizing the subsequent QP.

174. The decompressed video frame is re-encoded based on the second QP by the Fortinet ‘361 Products. The frame is then serialized into a bitstream and packaged with appropriate headers and metadata for transmission or storage.

175. Fortinet has directly infringed and continues to directly infringe the ‘361 Patent by, among other things, making, using, offering for sale, and/or selling technology for quality-aware video optimization, including but not limited to the Fortinet ‘361 Products.

176. The Fortinet ‘361 Products are available to businesses and individuals throughout the United States.

177. The Fortinet ‘361 Products are provided to businesses and individuals located in this District.

178. By making, using, testing, offering for sale, and/or selling products and services comprising technology for quality-aware video optimization, including but not limited to the Fortinet ‘361 Products, Fortinet has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘361 Patent, including at least claim 10 pursuant to 35 U.S.C. § 271(a).

179. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '361 Patent.

180. As a result of Fortinet's infringement of the '361 Patent, Plaintiff has suffered monetary damages, and seek recovery in an amount adequate to compensate for Fortinet's infringement, but in no event less than a reasonable royalty for the use made of the invention by Fortinet together with interest and costs as fixed by the Court.

COUNT VI
INFRINGEMENT OF U.S. PATENT NO. 8,429,169

181. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

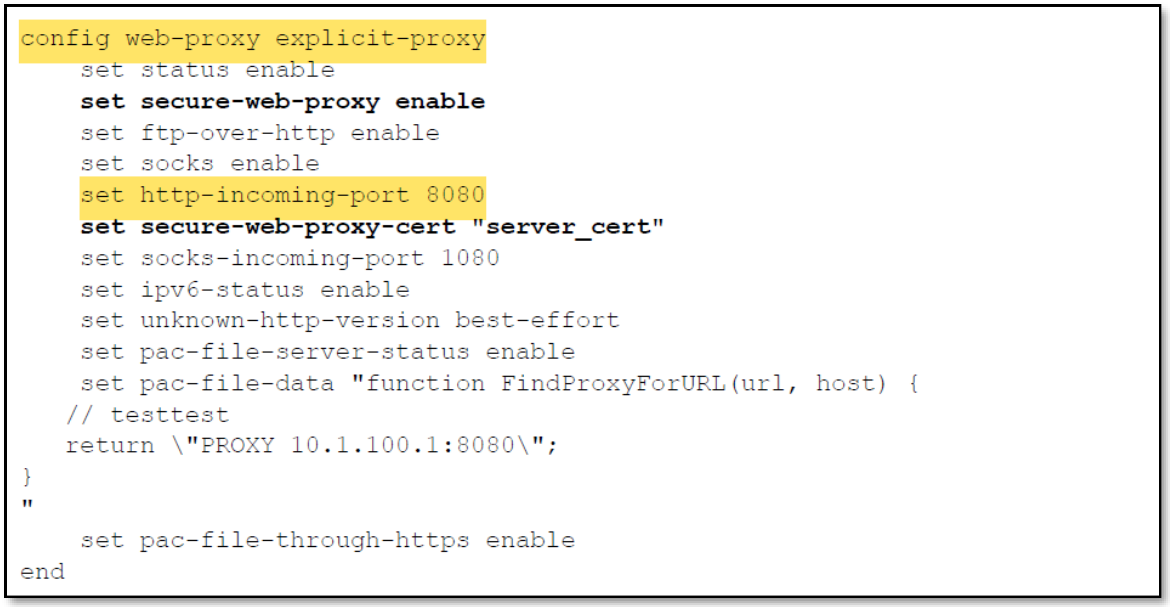
182. Fortinet designs, makes, uses, sells, and/or offers for sale in the United States products comprising technology for video cache indexing.

183. Fortinet designs, makes, sells, offers to sell, imports, and/or uses FortiGate Products supporting FortiOS 7.4.0 and later, which include at least the following models: FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100F, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F,

FG-7030E, FG-7040E, FG-7060E, FG-7081F, and FG-7121F; and FortiProxy 7.4.0 and later, which include at least the following models: FPX-400E, FPX-2000E, FPX-4000E, FPX-400G, FPX-2000G, and FPX-4000G (collectively, the "Fortinet '169 Product(s)").

184. One or more Fortinet subsidiaries and/or affiliates use the Fortinet '169 Products in regular business operations.

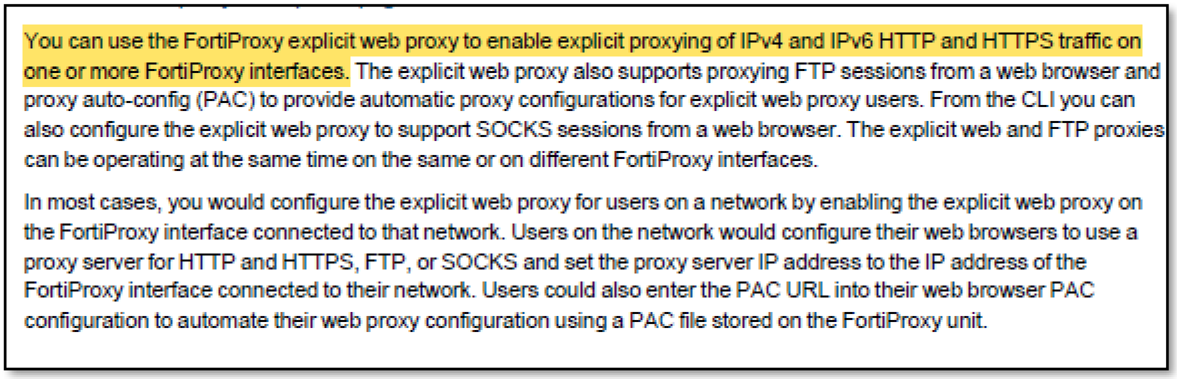
185. The Fortinet '169 Products receive and process content requests from internet-connected devices, acting as an intermediary between the user and the web server. For example, the "config web-proxy explicit-proxy" command is used by the Fortinet '169 Products to define settings such as "set http-incoming-port {user}", where the Fortinet '169 Products explicitly listen for HTTP requests on a designated port, typically the 8080 port by default. In addition, the Fortinet '169 Products' transparent web proxy capability intercepts traffic without requiring reconfiguration of user devices. The Fortinet '169 Products further perform the reception of content requests using the "config authentication rule" and "set web-auth-cookie enable" parameters which enable the Fortinet '169 Products to manage user sessions through cookies.



```
config web-proxy explicit-proxy
    set status enable
    set secure-web-proxy enable
    set ftp-over-http enable
    set socks enable
    set http-incoming-port 8080
    set secure-web-proxy-cert "server_cert"
    set socks-incoming-port 1080
    set ipv6-status enable
    set unknown-http-version best-effort
    set pac-file-server-status enable
    set pac-file-data "function FindProxyForURL(url, host) {
   // testtest
   return \"PROXY 10.1.100.1:8080\";
}
"
    set pac-file-through-https enable
end
```

FORTIPROXY 7.4.0 RELEASE NOTES at 51 (September 24, 2024) (emphasis added).

186. The Fortinet ‘169 Products operate as a forward or reverse proxy which performs the reception of incoming requests. For example, the explicit web proxy feature in the Fortinet ‘169 Products "enable[s] explicit proxying of IPv4 and IPv6 HTTP and HTTPS traffic on one or more . . . interfaces." This allows the Fortinet ‘169 Product to receive requests without specific client configurations, as "it is transparent to the end user," which requires the proxy to initially receive client requests to then direct it through defined policies.

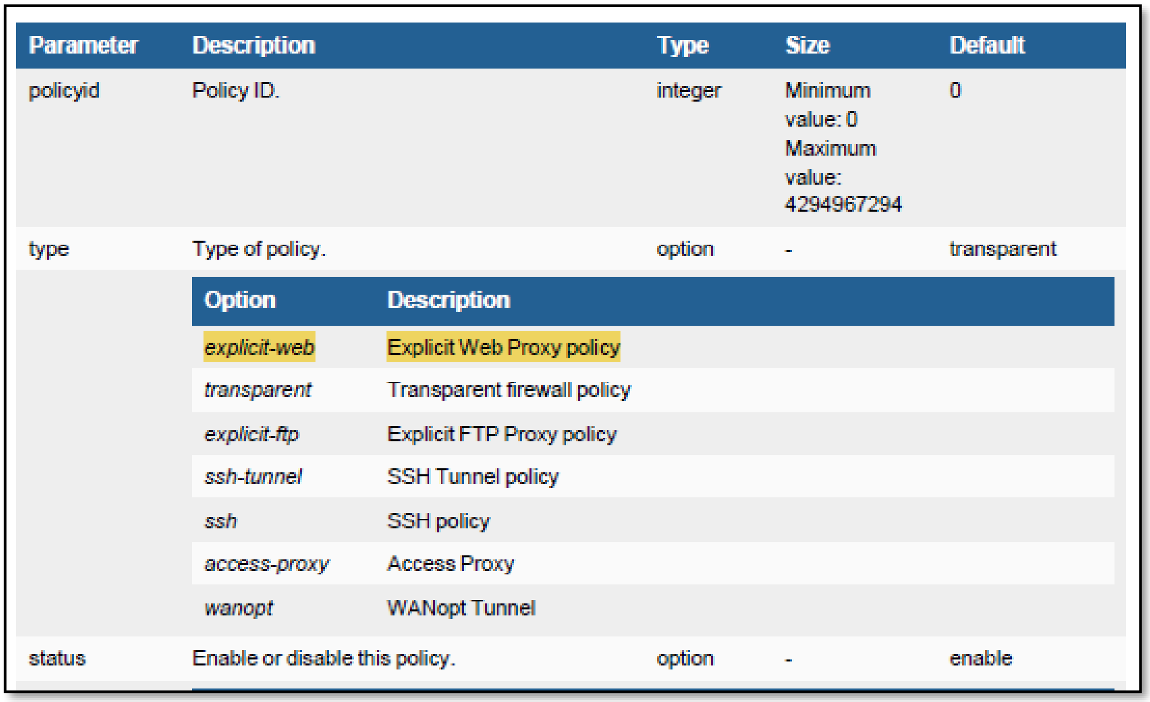


You can use the FortiProxy explicit web proxy to enable explicit proxying of IPv4 and IPv6 HTTP and HTTPS traffic on one or more FortiProxy interfaces. The explicit web proxy also supports proxying FTP sessions from a web browser and proxy auto-config (PAC) to provide automatic proxy configurations for explicit web proxy users. From the CLI you can also configure the explicit web proxy to support SOCKS sessions from a web browser. The explicit web and FTP proxies can be operating at the same time on the same or on different FortiProxy interfaces.

In most cases, you would configure the explicit web proxy for users on a network by enabling the explicit web proxy on the FortiProxy interface connected to that network. Users on the network would configure their web browsers to use a proxy server for HTTP and HTTPS, FTP, or SOCKS and set the proxy server IP address to the IP address of the FortiProxy interface connected to their network. Users could also enter the PAC URL into their web browser PAC configuration to automate their web proxy configuration using a PAC file stored on the FortiProxy unit.

FortiProxy 7.4.0 Administration Guide at 20 (November 19, 2024) (emphasis added).

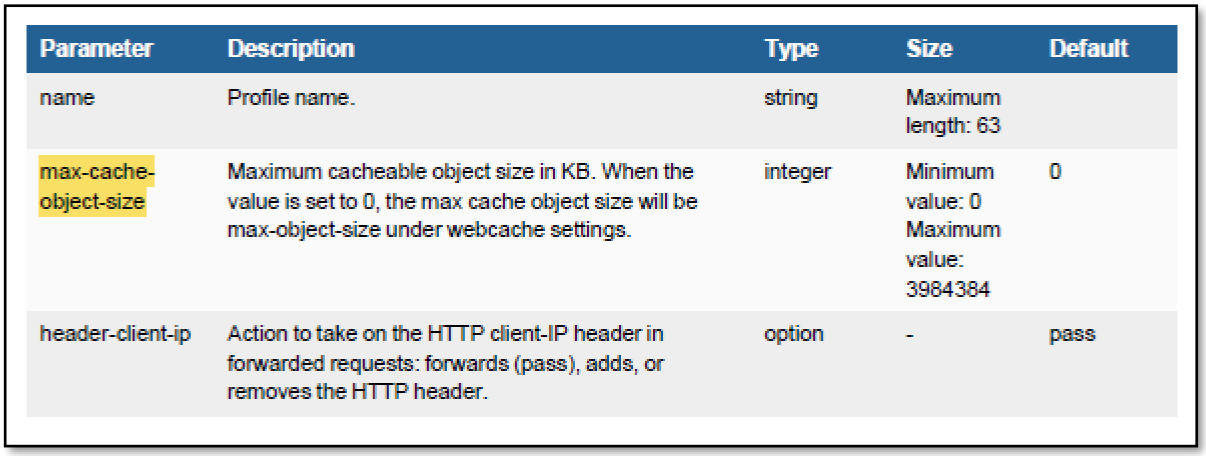
187. The Fortinet ‘169 Products perform the task of requesting a portion of content from a web server based on received content requests, acting as an intermediary between the client and the server. Specifically, the Fortinet ‘169 Products perform forward proxying wherein the Fortinet ‘169 Products receive requests from clients and forward those requests to the appropriate web server. For example, when a user attempts to access a website, the request is sent to the Fortinet ‘169 Products, which then establish a connection with the destination server using the "config web-proxy forward-server" command, further directing the request to the configured forwarding server based on the "set ldb-method" setting. In addition, the Fortinet ‘169 Products use the "set type explicit-web" to handle web proxy traffic, including making requests to web servers on behalf of a client.



<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>policyid</td><td>Policy ID.</td><td>integer</td><td>Minimum value: 0 Maximum value: 4294967294</td><td>0</td></tr>
<tr><td>type</td><td>Type of policy.</td><td>option</td><td>-</td><td>transparent</td></tr>
<tr><td></td><td colspan="4">
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><em>explicit-web</em></td><td>Explicit Web Proxy policy</td></tr>
<tr><td><em>transparent</em></td><td>Transparent firewall policy</td></tr>
<tr><td><em>explicit-ftp</em></td><td>Explicit FTP Proxy policy</td></tr>
<tr><td><em>ssh-tunnel</em></td><td>SSH Tunnel policy</td></tr>
<tr><td><em>ssh</em></td><td>SSH policy</td></tr>
<tr><td><em>access-proxy</em></td><td>Access Proxy</td></tr>
<tr><td><em>wanopt</em></td><td>WANopt Tunnel</td></tr>
</table>
</td></tr>
<tr><td>status</td><td>Enable or disable this policy.</td><td>option</td><td>-</td><td>enable</td></tr>
</table>

FORTIPROXY 7.4.7 CLI REFERENCE at 241 (December 13, 2024) (emphasis added).

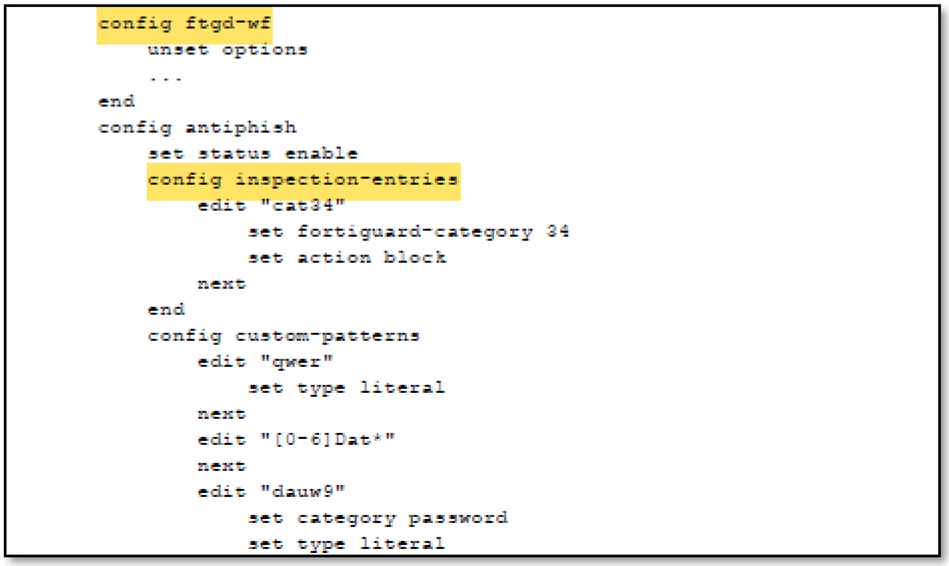
188. Furthermore, the Fortinet '169 Products use parameters such as "max-object-size" and "neg-resp-time," to determine how the Fortinet '169 Products cache content retrieved from web servers. For example, when web caching is enabled, and a user requests a webpage, the Fortinet '169 Products will first check its cache, and if the content is not found, the Fortinet '169 Products will send a request to the origin web server to retrieve the content.



Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 63	
max-cache-object-size	Maximum cacheable object size in KB. When the value is set to 0, the max cache object size will be max-object-size under webcache settings.	integer	Minimum value: 0 Maximum value: 3984384	0
header-client-ip	Action to take on the HTTP client-IP header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass

FORTIPROXY 7.4.7 CLI REFERENCE at 1180 (December 13, 2024) (emphasis added).

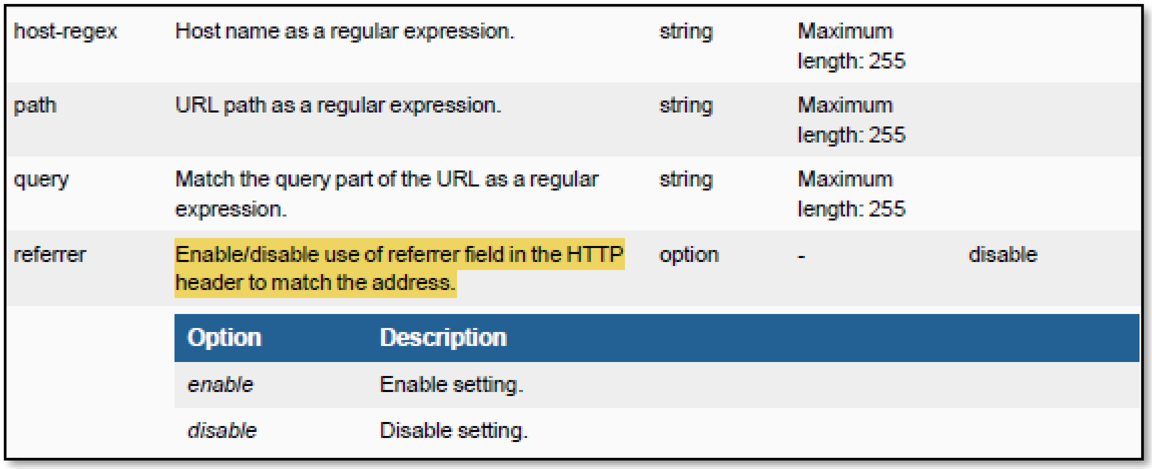
189. The Fortinet '169 Products identify characterization data for content associated with the received content request. The characterization data comprises the portion of content associated with the received content request. Specifically, the Fortinet '169 Products employ a range of security profiles and filtering mechanisms to extract and analyze various aspects of web traffic. For example, the "config webfilter profile" command enables the Fortinet '169 Products to define actions based on FortiGuard categories, URL filters, and web content filters. This is further supported by the "config ftgd-wf" settings within the web filter profile, which provide options such as "set options {block | urlfilter | activex-java-cookie | ...}" allowing granular control over various content elements. In addition, Fortinet '169 Products can leverage deep SSL inspection using "set ssl-ssh-profile" in firewall policies, enabling the examination of encrypted traffic content for characterization data.



```
config ftgd-wf
    unset options
    ...
end
config antiphish
    set status enable
    config inspection-entries
        edit "cat34"
            set fortiguard-category 34
            set action block
        next
    end
    config custom-patterns
        edit "qwer"
            set type literal
        next
        edit "[0-6]Dat*"
        next
        edit "dauw9"
            set category password
            set type literal
```

FORTIPROXY 7.4.0 ADMINISTRATION GUIDE at 315 (November 19, 2024) (emphasis added).

190. The Fortinet '169 Products utilize HTTP headers and file metadata as sources for identifying characterization data. Specifically, the Fortinet '169 Products "use of referrer field in the HTTP header to match the address" while also providing the ability to examine the "HTTP request body" for matching.

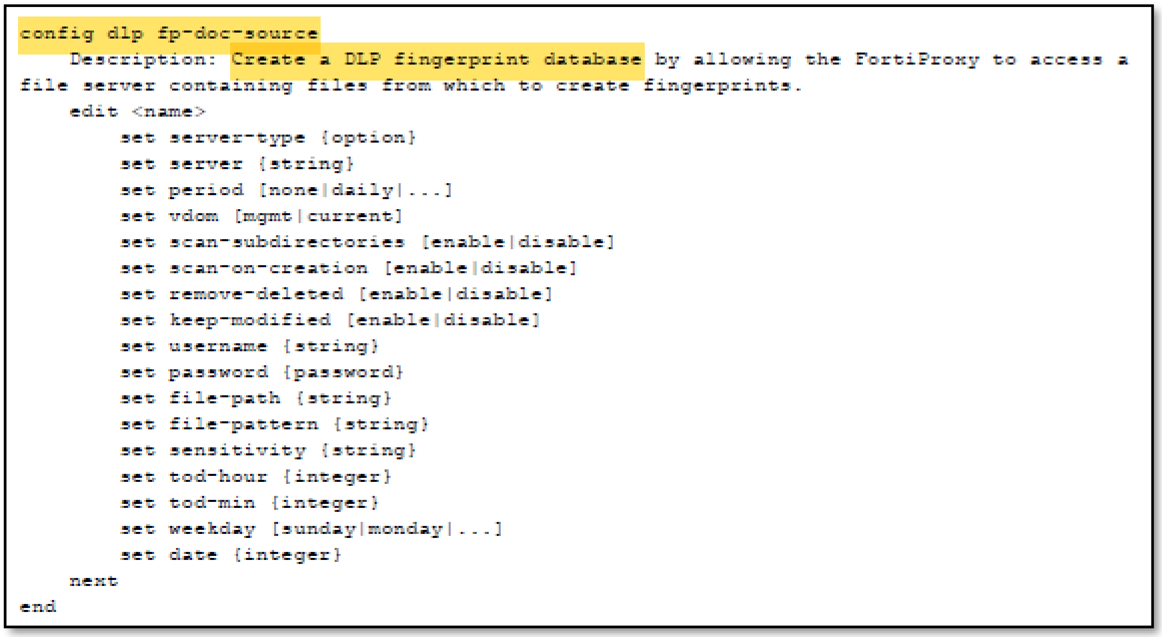


host-regex	Host name as a regular expression.	string	Maximum length: 255	
path	URL path as a regular expression.	string	Maximum length: 255	
query	Match the query part of the URL as a regular expression.	string	Maximum length: 255	
referrer	Enable/disable use of referrer field in the HTTP header to match the address.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

FORTIPROXY 7.4.7 CLI REFERENCE at 279 (December 13, 2024) (emphasis added).

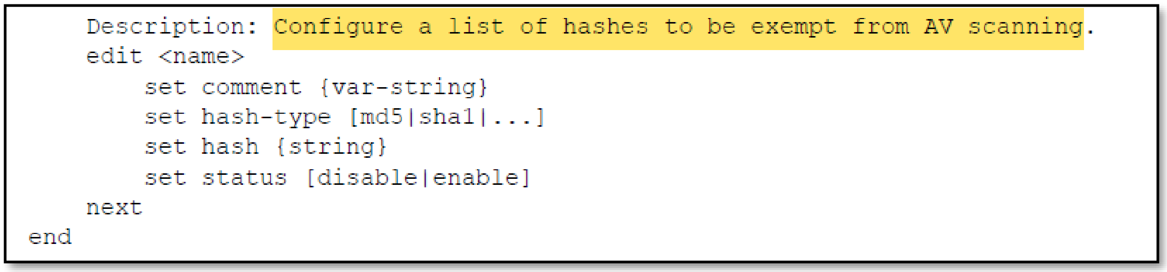
191. The Fortinet '169 Products generate an index corresponding to content associated with the received content request by inputting the at least one identified characterization data into a hash function. The generated index is used for identifying, in the cache data structure, an entry associated with the content by comparing the generated index to one or more index fields associated with one or more entries within the cache data structure. Specifically, the Fortinet '169 Products generate hash values as part of Data Loss Prevention (DLP) fingerprinting and content caching. For example, when configuring DLP fingerprinting with the "config dlp fp-doc-source" command, the Fortinet '169 Product generates checksum fingerprints for files, which can then be compared against a database of known fingerprints. This process, involves creating a "DLP fingerprint database" where the Fortinet '169 Product can access a file server containing files from which to create fingerprints.



```
config dlp fp-doc-source
    Description: Create a DLP fingerprint database by allowing the FortiProxy to access a
file server containing files from which to create fingerprints.
    edit <name>
        set server-type {option}
        set server {string}
        set period [none|daily|...]
        set vdom [mgmt|current]
        set scan-subdirectories [enable|disable]
        set scan-on-creation [enable|disable]
        set remove-deleted [enable|disable]
        set keep-modified [enable|disable]
        set username {string}
        set password {password}
        set file-path {string}
        set file-pattern {string}
        set sensitivity {string}
        set tod-hour {integer}
        set tod-min {integer}
        set weekday [sunday|monday|...]
        set date {integer}
    next
end
```

FORTIPROXY 7.4.7 CLI REFERENCE at 123 (December 13, 2024) (emphasis added).

192. The Fortinet '169 Products employ hash functions to generate indices from identified characterization data for efficient data retrieval and matching. Specifically, the "antivirus exempt-list" feature uses configured "hash" values of type "md5," "sha1," or "sha256" which act as indices. For example, by storing "a list of hashes to be exempt from AV scanning," the Fortinet '169 Products generate a hash of the file and compares the generated hash to entries in a hash-based lookup table to determine if the file should be exempted from scanning.



```
    Description: Configure a list of hashes to be exempt from AV scanning.
    edit <name>
        set comment {var-string}
        set hash-type [md5|sha1|...]
        set hash {string}
        set status [disable|enable]
    next
end
```

FORTIPROXY 7.4.7 CLI REFERENCE at 34 (December 13, 2024) (emphasis added).

193. Fortinet has directly infringed and continues to directly infringe the ‘169 Patent by, among other things, making, using, offering for sale, and/or selling technology comprising video cache indexing, including but not limited to the Fortinet ‘169 Products.

194. The Fortinet ‘169 Products are available to businesses and individuals throughout the United States.

195. The Fortinet ‘169 Products are provided to businesses and individuals located in this District.

196. By making, using, testing, offering for sale, and/or selling products and services comprising technology for video cache indexing, including but not limited to the Fortinet ‘169 Products, Fortinet has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘169 Patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

197. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘169 Patent.

198. As a result of Fortinet’s infringement of the ‘169 Patent, Plaintiff has suffered monetary damages, and seek recovery in an amount adequate to compensate for Fortinet’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Fortinet together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff OptiMorphix, Inc. respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff that Fortinet has infringed, either literally and/or under the doctrine of equivalents, the ‘273, ‘901, ‘559, ‘388, ‘361, and ‘169 Patents;

B. An award of damages resulting from Fortinet’s acts of infringement in accordance with 35 U.S.C. § 284;

C. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff reasonable attorneys' fees against Fortinet.

D. Any and all other relief to which Plaintiff may show themselves to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff OptiMorphix, Inc. requests a trial by jury of any issues so triable by right.

Dated: December 27, 2024

OF COUNSEL:

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
Erin E. McCracken (CA SB No. 244523)
BERGER & HIPSKIND LLP
9538 Brighton Way, Ste. 320
Beverly Hills, CA 90210
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com
E-Mail: eem@bergerhipskind.com

BAYARD, P.A.

/s/ Stephen B. Brauerman
Stephen B. Brauerman (No. 4952)
Ronald P. Golden, III (No. 6254)
600 N. King Street, Suite 400
P.O. Box 25130
Wilmington, Delaware 19801
(302) 655-5000
sbrauerman@bayardlaw.com
rgolden@bayardlaw.com

Attorneys for Plaintiff
OptiMorphix, Inc.