

# Firewall Test Report -YR- 2024-2025

## SUMMARY



**100 Mbps**  
Goodput



**2.479ms**  
Latency



**12%**  
Error Percentage

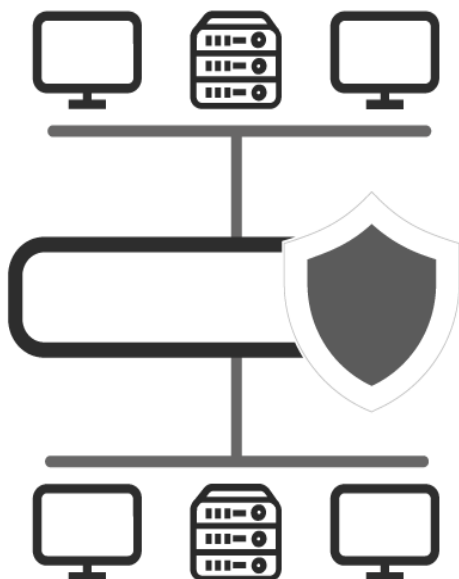


**0%**  
Malware Block Rate



**450**  
Number of Users

## NETWORK TOPOLOGY



Enterprise Internal Segmentation

## FIREWALL FUNCTIONS ENABLED

Firewall Model:

FG-101FT

Application Control

Logging and Reporting

**Date:** 2025-01-20  
**Time Start:** 2025-01-20 (09:04:56)  
**Time Stop:** 2025-01-20 (09:32:53)  
**Duration:** 00:27:57  
**Ver:** v0.9.2

## Contents

1. Introduction.....	3
2. Test Information .....	4
3. Network Topology .....	5
3.1. Enterprise Internal Segmentation .....	5
3.2. Enterprise Security Perimeter .....	5
3.3. Data Center Internal Segmentation .....	6
3.4. Data Center Security Perimeter .....	6
4. Traffic Profile .....	7
5. Test Result.....	9
5.1. Goodput .....	10
5.2. Concurrent Sessions .....	12
5.3. Latency .....	14
5.4. Error Percentage.....	16
5.5. Malware Block Rate.....	18
6. Contact Information .....	20

### **(Classification and Handling -Safeguarding Sensitive and Confidential Information)**

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in Material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

## 1. Introduction

Enterprises are investing in enterprise-grade firewalls to counteract the threats posted by the increasing network and data security breach every year. Firewalls are typically deployed at the edge of or inside enterprises to protect clients and servers from malwares, virus affection, data breach, target attacks, etc. Many security experts such as IT and security managers, and CSOs believe that they are improving their network security posture by implementing a new security solution.

However, verifying the performance of firewall and any network security device is essential to the success of the enterprise network it defends. With various advanced protection features such as application identification, intrusion prevention, threat detection, logging, etc., your firewall can easily become the performance bottleneck of the network, degrading the overall performance and user experience. Because of this trade-off, it is vital to test the performance of your firewall with specific features enabled on the firewall appliance.

Either out-of-box or firmware upgrade, firewall appliances should always be tested and evaluated before deployment in order to guarantee that new security protections do not adversely impact performance and that security shortcuts are not taken to maintain or improve the performance. The testbed should attempt to replicate the production network as close as possible, which includes network topology, network traffic that traverses through the firewall, features and policies enabled on the firewall, etc. Firewall appliances should deliver the expected performance under all circumstances.

This test report is generated by BPO Convergence Pvt Ltd Network team. We automatically measure and characterizes the performance of a firewall under realistic traffic conditions, with the results and key conclusions automatically being represented in a readable report format. Thus, the IT and network managers can easily assess the negative performance impact for the multiple firewall security features.

## 2. Test Information

Test Name:	PGT101 Example
Test Date Time:	2024-01-20
Test Start:	2024-01-20 (09:04:56)
Test Stop:	2024-01-20 (09:32:53)
Test Duration:	00:27:57

Network Topology:	Enterprise Internal Segmentation
Firewall Model:	Fortinet 101F
Firewall Interface Addresses:	Segment A: LAN, Segment B: WAN
Firewall Interface Speed:	10G
Firewall Functions Enabled:	

Application Control

Logging and Reporting

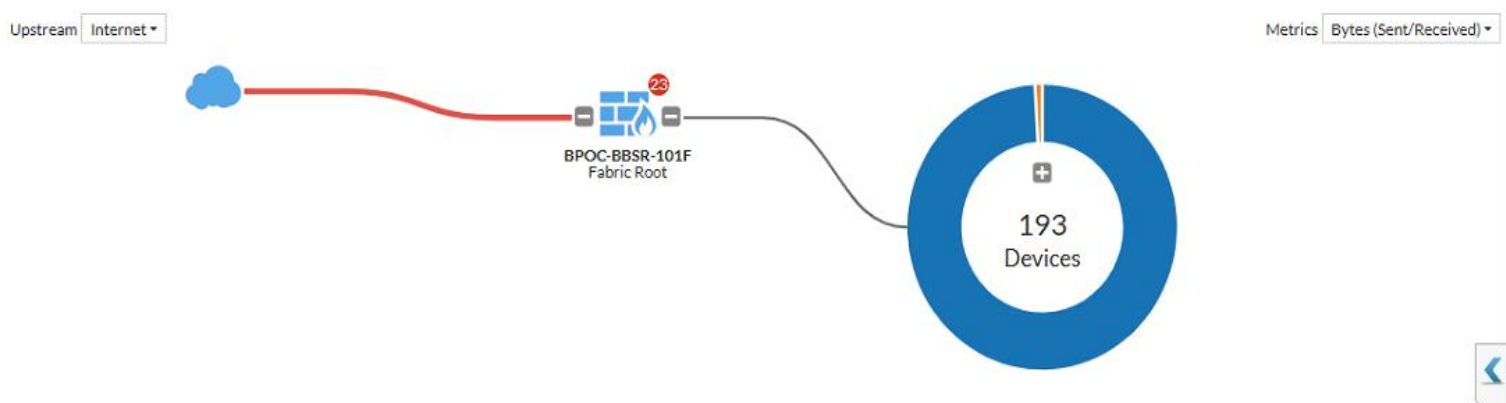
Comment:

This is an example.

Application	Category	Risk	Bytes ▾	Sessions ▾	Bandwidth ▾
Google.Chat.Video.Call	Collaboration	■ ■ ■ ■	522.91 MB <div></div>	5   <div></div>	5.26 Mbps <div></div>
Salesforce	Business	■ ■ ■ ■	154.63 MB <div></div>	139   <div></div>	1.17 Mbps <div></div>
HTTPS.BROWSER	Web.Client	■ ■ ■ ■	125.56 MB <div></div>	1,192   <div></div>	1.47 Mbps <div></div>
Google.Services	General.Interest	■ ■ ■ ■	98.22 MB <div></div>	934   <div></div>	1.12 Mbps <div></div>
Google.Play	General.Interest	■ ■ ■ ■	15.78 MB <div></div>	123   <div></div>	201.81 kbps   <div></div>
Windows.Push.Notification	General.Interest	■ ■ ■ ■	14.59 MB <div></div>	147   <div></div>	1.86 kbps   <div></div>
New.Relic	Business	■ ■ ■ ■	7.82 MB   <div></div>	134   <div></div>	296.26 kbps   <div></div>
SSL.TLSv1.3	Network.Service	■ ■ ■ ■	6.18 MB   <div></div>	22   <div></div>	17.25 kbps   <div></div>
Google.Push.Notification	General.Interest	■ ■ ■ ■	3.90 MB   <div></div>	223   <div></div>	10.34 kbps   <div></div>
SSL.TLSv1.3.PQC	Network.Service	■ ■ ■ ■	1.28 MB   <div></div>	26   <div></div>	39.32 kbps   <div></div>
Microsoft.Outlook	Email	■ ■ ■ ■	1.20 MB   <div></div>	9   <div></div>	17.68 kbps   <div></div>
Google.Accounts	General.Interest	■ ■ ■ ■	853.77 kB   <div></div>	39   <div></div>	31.34 kbps   <div></div>
SSL.TLSv1.2	Network.Service	■ ■ ■ ■	528.06 kB   <div></div>	2   <div></div>	4.43 kbps   <div></div>
Gmail	Email	■ ■ ■ ■	387.33 kB   <div></div>	9   <div></div>	4.79 kbps   <div></div>
Microsoft.Portail	Collaboration	■ ■ ■ ■	366.04 kB   <div></div>	46   <div></div>	30.27 kbps   <div></div>
Amazon.AWS_S3	Cloud.IT	■ ■ ■ ■	314.43 kB   <div></div>	6   <div></div>	30.90 kbps   <div></div>
Microsoft.Authentication	Collaboration	■ ■ ■ ■	251.08 kB   <div></div>	8   <div></div>	9.06 kbps   <div></div>
Microsoft.Windows.Update	Update	■ ■ ■ ■	153.35 kB   <div></div>	13   <div></div>	36.78 kbps   <div></div>
Google.Keep	General.Interest	■ ■ ■ ■	112.10 kB   <div></div>	10   <div></div>	4.17 kbps   <div></div>
Microsoft.365.Portail	Collaboration	■ ■ ■ ■	58.04 kB   <div></div>	6   <div></div>	3.27 kbps   <div></div>
HTTP.BROWSER_Chrome	Web.Client	■ ■ ■ ■	21.39 kB   <div></div>	1   <div></div>	152 bps   <div></div>
QUIC	Network.Service	■ ■ ■ ■	19.43 kB   <div></div>	5   <div></div>	1.32 kbps   <div></div>
LDAP	Network.Service	■ ■ ■ ■	13.02 kB   <div></div>	2   <div></div>	0 bps <div></div>

0% 81

### 3. Network Topology



In this test case, the network topology is configured as:

#### Enterprise Internal Segmentation

Firewalls are deployed in different network locations, i.e. inside the network or at the perimeter, and they are used to protect different devices, i.e. clients or servers. Depending on where the firewall is deployed and what the firewall protects, the traffic profile seen by the firewall varies. This section lists four main network topologies that you usually see in firewall deployment scenarios:

- Enterprise Internal Segmentation
- Enterprise Security Perimeter
- Data Center Internal Segmentation
- Data Center Security Perimeter

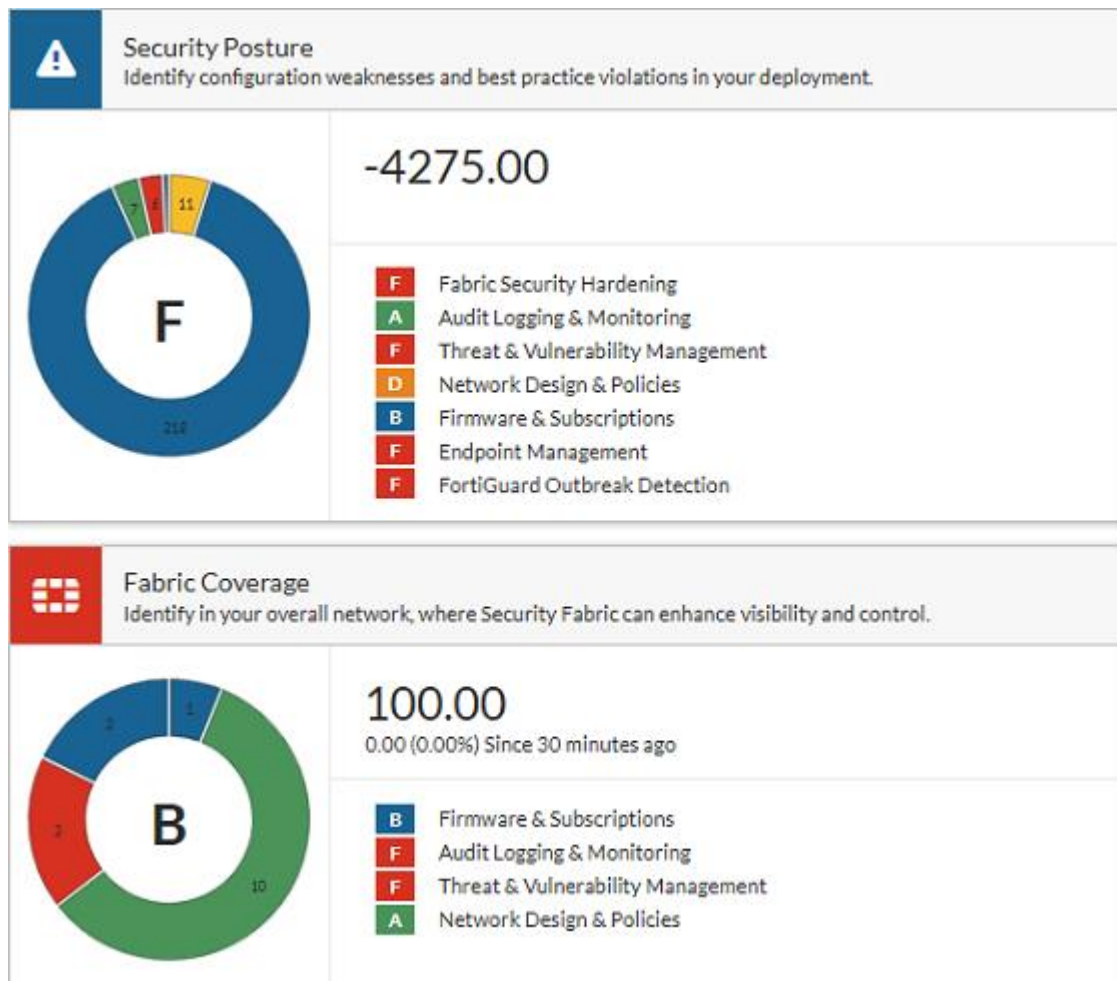


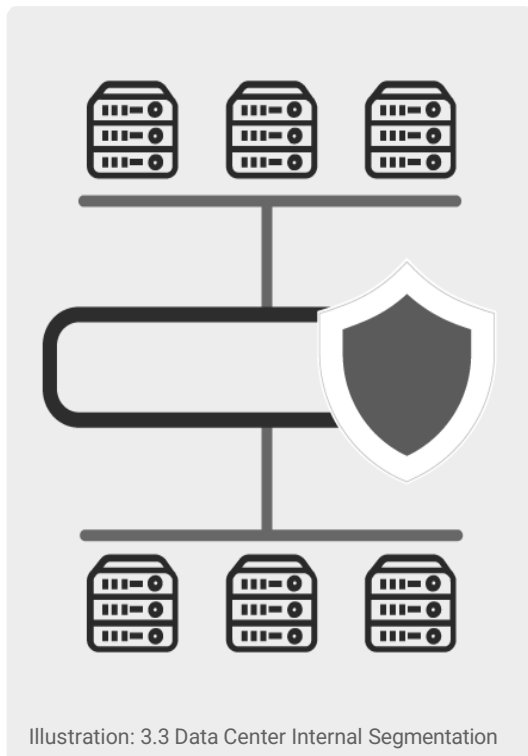
#### 3.1 Enterprise Internal Segmentation

Firewall is placed inside the enterprise network to secure enterprise network by segmenting the corporate LAN and protecting each segment from others against malware and virus usually by means of application control, antivirus, web filtering, DNS filtering, and SSL deep inspection. It is usually referred to as "Zero Trust". Traffic characteristics are symmetric and west-east. Throughput demand is high since enterprise LAN capacities and speeds are orders of magnitudes higher than at the edge.

### 3.2 Enterprise Security Perimeter

Firewall is placed at the edge of the enterprise network to protect enterprise users from internet malware and virus usually by means of application control, antivirus, web filtering, DNS filtering, and SSL deep inspection. Traffic characteristics are asymmetric and north-south. Throughput is limited by the WAN interface provisioned by the ISP.



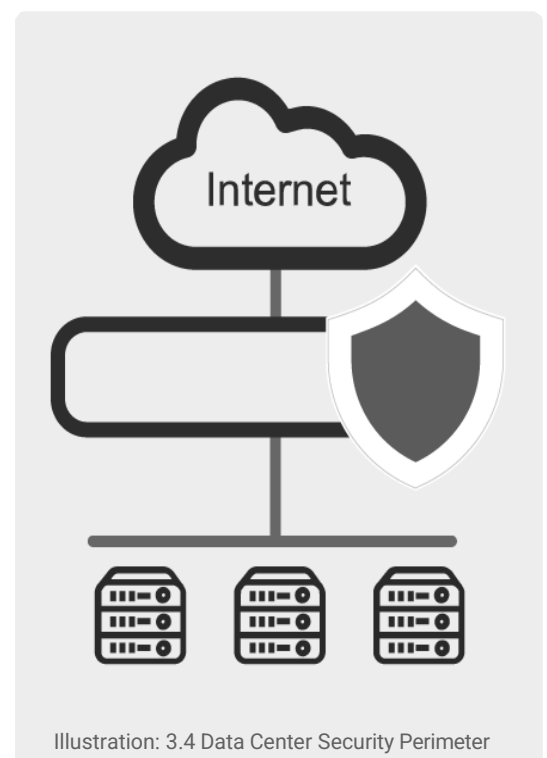


### 3.3 Data Center Internal Segmentation

Firewall is placed inside the data center network. It controls traffic flowing between servers and application tiers inside the data center usually by means of IPS, antivirus, and web filtering. Traffic characteristics are symmetric and west-east. Throughput demand is very high because intra-data center communication, such as data backup, demands bandwidth capacity of hundreds of gigabits per second.

### 3.4 Data Center Security Perimeter

Firewall is placed at the edge of the data center network. It controls traffic flowing from the internet to the data center and flowing from data center to the internet usually by means of IPS. Traffic characteristics are asymmetric and north-south. Throughput demand is high because SaaS applications demand high bandwidth and low latency in order to services SaaS users.

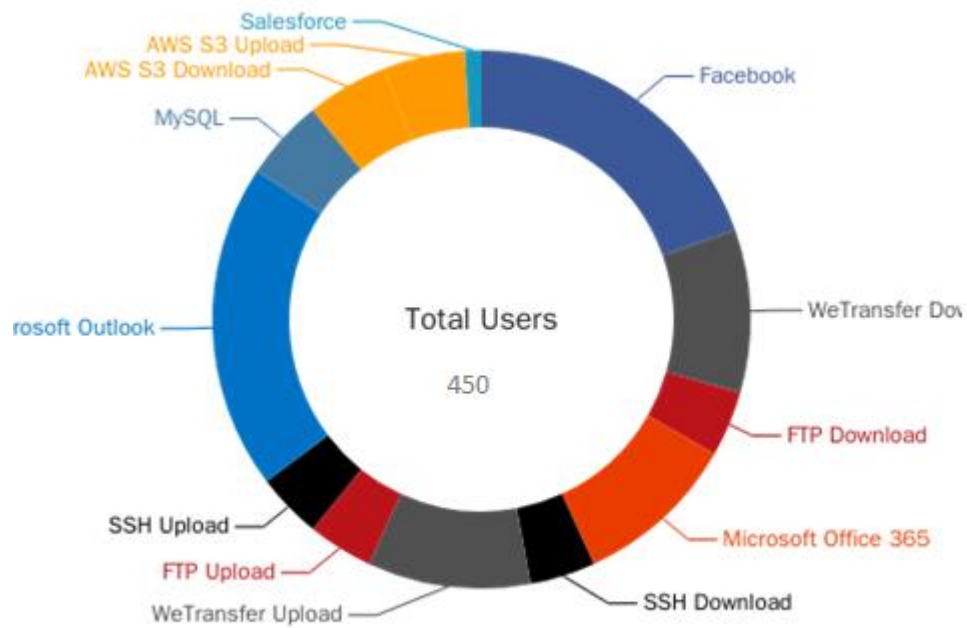


#### 4. Traffic Profile

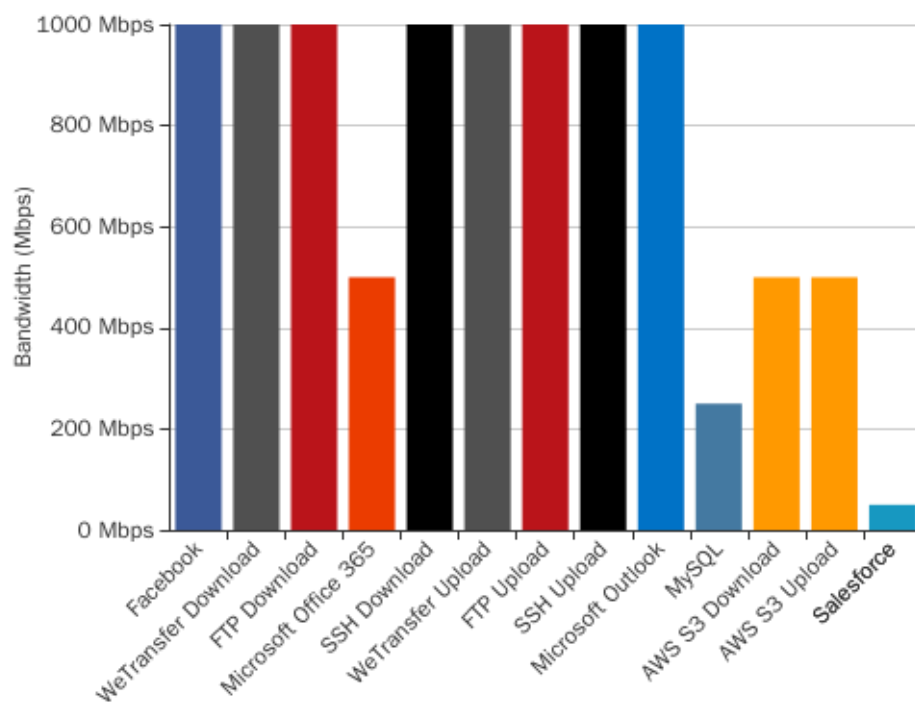
In this test report, the traffic profile is configured as follows:

Traffic Profile: **Internal Segmentation - 10G**

**Users Allocation Per Application**



**Bandwidth Allocation Per Application**





Application	Bandwidth Per User	Number of Users	Bandwidth
● Facebook	5 Mbps	200	100 Mbps
● WeTransfer Download	10 Mbps	100	100 Mbps
● FTP Download	25 Mbps	40	100 Mbps
● Microsoft Office 365	5 Mbps	100	100 Mbps
● SSH Download	25 Mbps	40	100 Mbps
● WeTransfer Upload	10 Mbps	100	100 Mbps
● FTP Upload	25 Mbps	40	100 Mbps
● SSH Upload	25 Mbps	40	100 Mbps
● Microsoft Outlook	5 Mbps	200	100 Mbps
● MySQL	5 Mbps	50	100 Mbps
● AWS S3 Download	10 Mbps	50	100 Mbps
● AWS S3 Upload	10 Mbps	50	100 Mbps
● Salesforce	5 Mbps	10	100 Mbps
Total:			100 Mbps

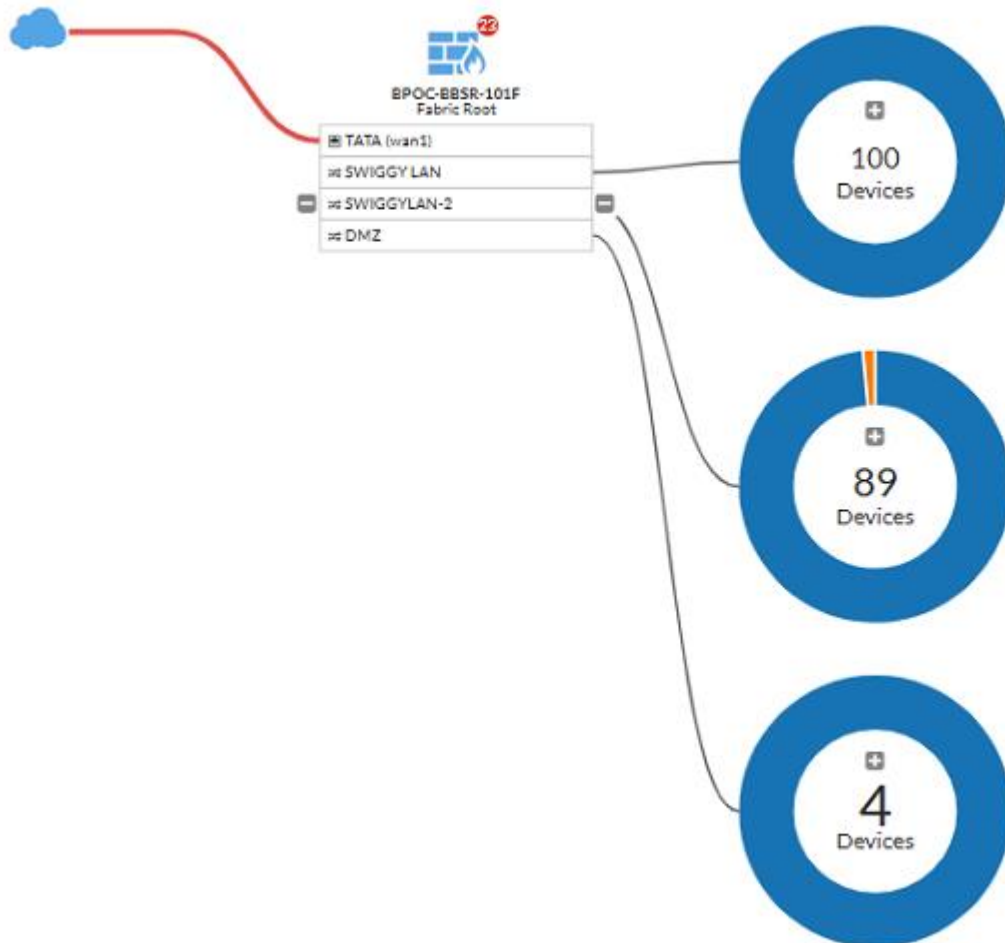
## 5. Test Result

Firewalls from different vendors can have large performance differences when tested with various realistic traffic profiles. Evaluating firewalls only from the datasheet is far from enough. Additionally, regular software update to the firewall requires retesting before putting into the production network again. Testing the firewall with Safire to verify how the upgrade reacts to realistic application traffic provides better foresight.

This section contains five main key performance metrics as follows:

- Goodput
- Concurrent Sessions
- Latency
- Error Percentage
- Malware Block Rate

Each section starts with the definition of the performance metric, followed by a discussion. Measurement result as a function of number of users are shown in both a chart and a table.



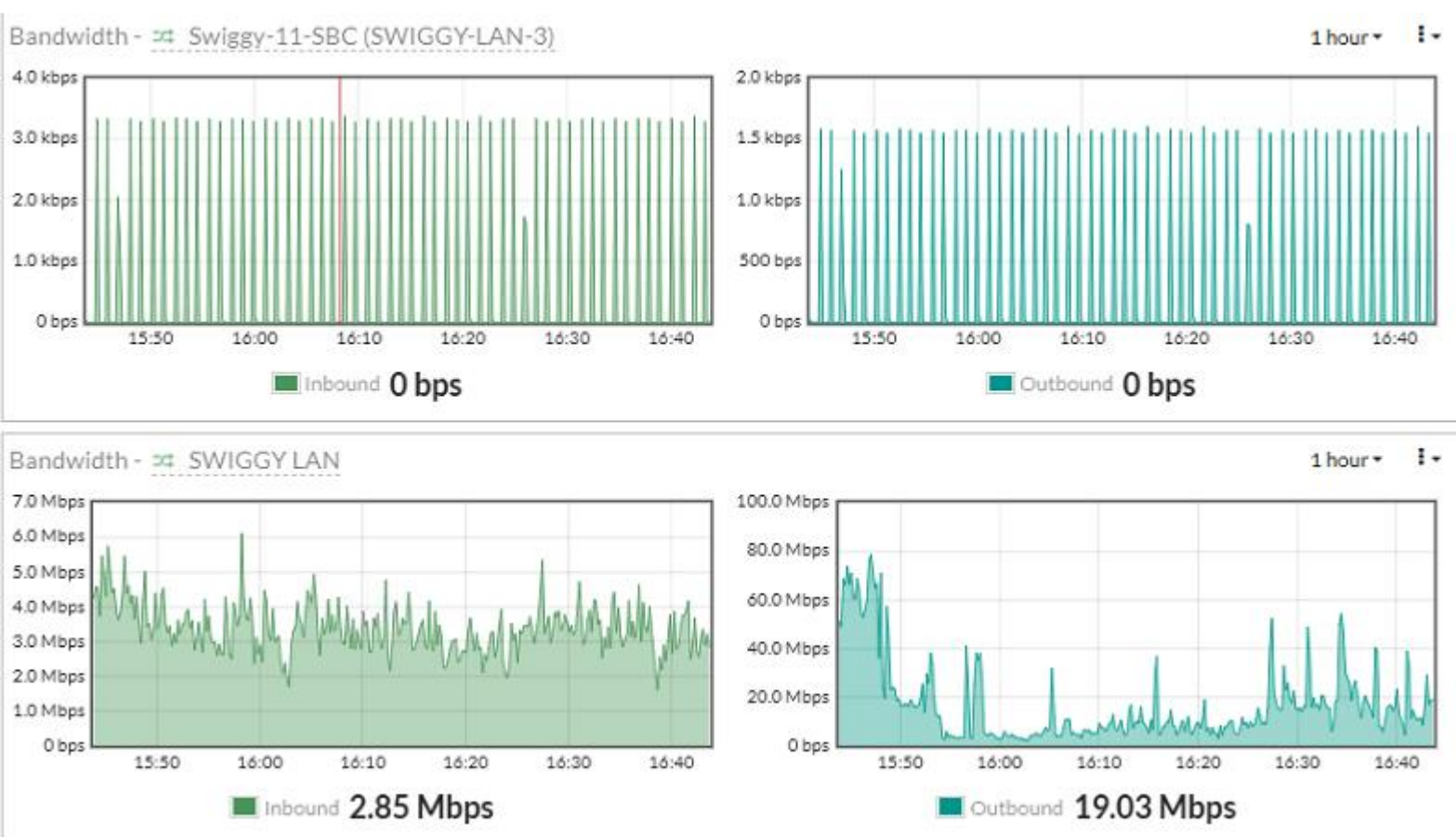
## 5.1 Goodput

Goodput (aggregated) is the application-level throughput defined as the useful amount of application data per unit of time that the application layer transports in both client-to-server (upstream) and server-to-client (downstream) directions, excluding protocol overhead bits as well as retransmitted data packets. The goodput is always lower than the layer-1 throughput (the gross bit rate that is transferred on the wire).

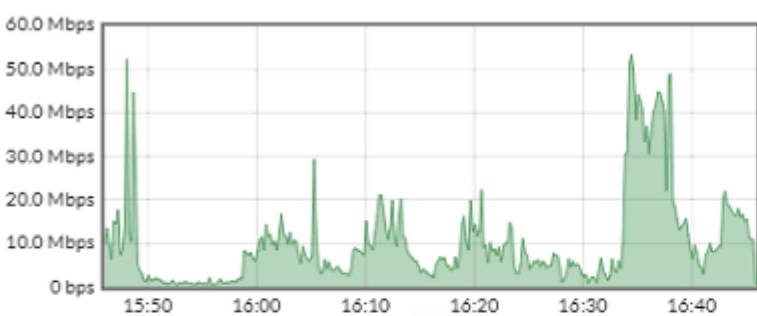
Factors that cause lower goodput than layer-1 throughput:

- Retransmission of lost or corrupt packets caused by bit errors or packet dropping in congested network devices, such as firewall, switches and routers.
- Transport layer flow control and congestion control.
- Protocol overhead: transport layer, network layer and data link layer protocol overhead is typically included in the throughput, but is excluded from the goodput.

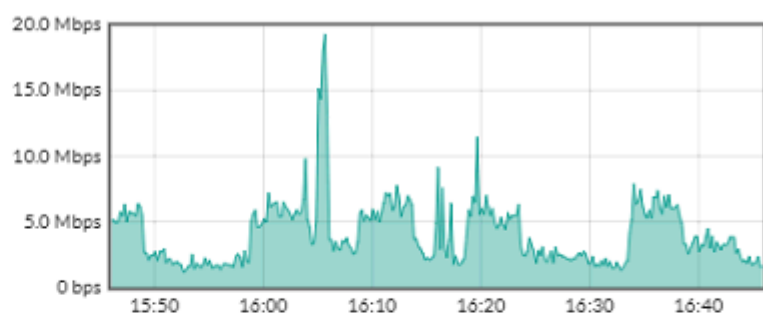
The chart below shows the goodput under different numbers of users, as well as layer-1 throughput rate. The goodput increases as the number of users increases. However, after a certain limit, the goodput will start converging. When this happens, it indicates that the firewall has reached its performance limit and cannot handle more traffic. Packets can get lost or misordered due to the congestion inside the firewall.



Bandwidth - TATA (wan1)

Inbound **579.89 kbps**

1 hour ▾

Outbound **1.51 Mbps**

Bandwidth - JIO (wan2)

Inbound **20.65 Mbps**

1 hour ▾

Outbound **5.13 Mbps**

Bandwidth - DMZ

Inbound **283.41 kbps**

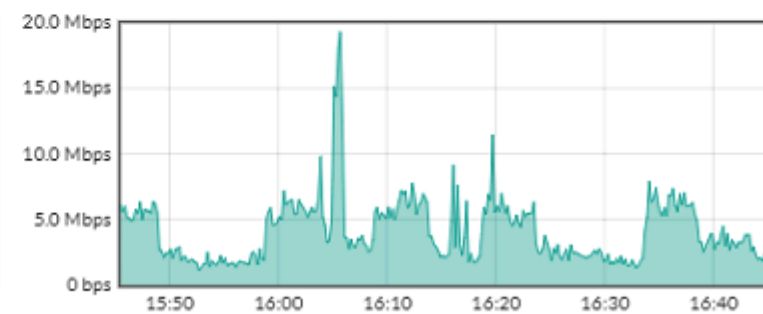
1 hour ▾

Outbound **2.49 Mbps**

Bandwidth - TATA (wan1)

Inbound **11.32 Mbps**

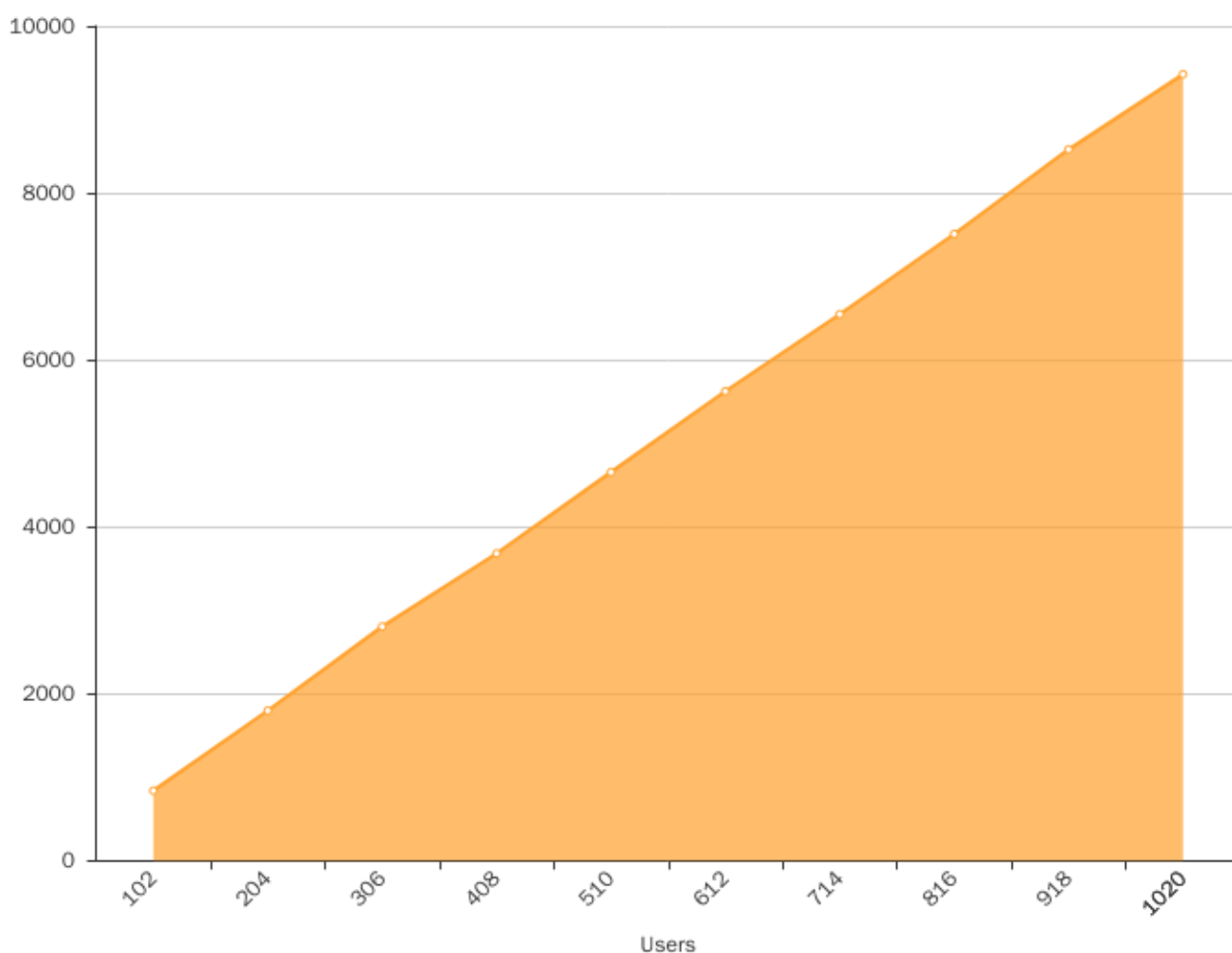
1 hour ▾

Outbound **1.89 Mbps**

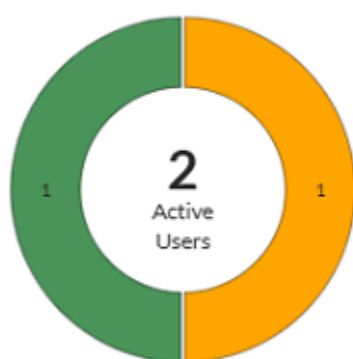
## 5.2 Concurrent Sessions

A session is defined by two uni-directional flows each uniquely identified by a 5-tuple key: source-address, destination-address, source-port, destination-port, and transport layer protocol. The concurrent session describes the maximum established/active sessions maintained at a given point in time by the firewall during each test.

The chart below shows the concurrent sessions under different numbers of users. The number of concurrent sessions increases as the number of users increases. However, after a certain limit, the number of concurrent sessions will start converging. When this happens, it indicates that the firewall has reached its limit and cannot handle more sessions due to the limited capacity of its session table.



SSL-VPN



Duration

- Connected < 1 Hour
- Connected < 10 Minutes



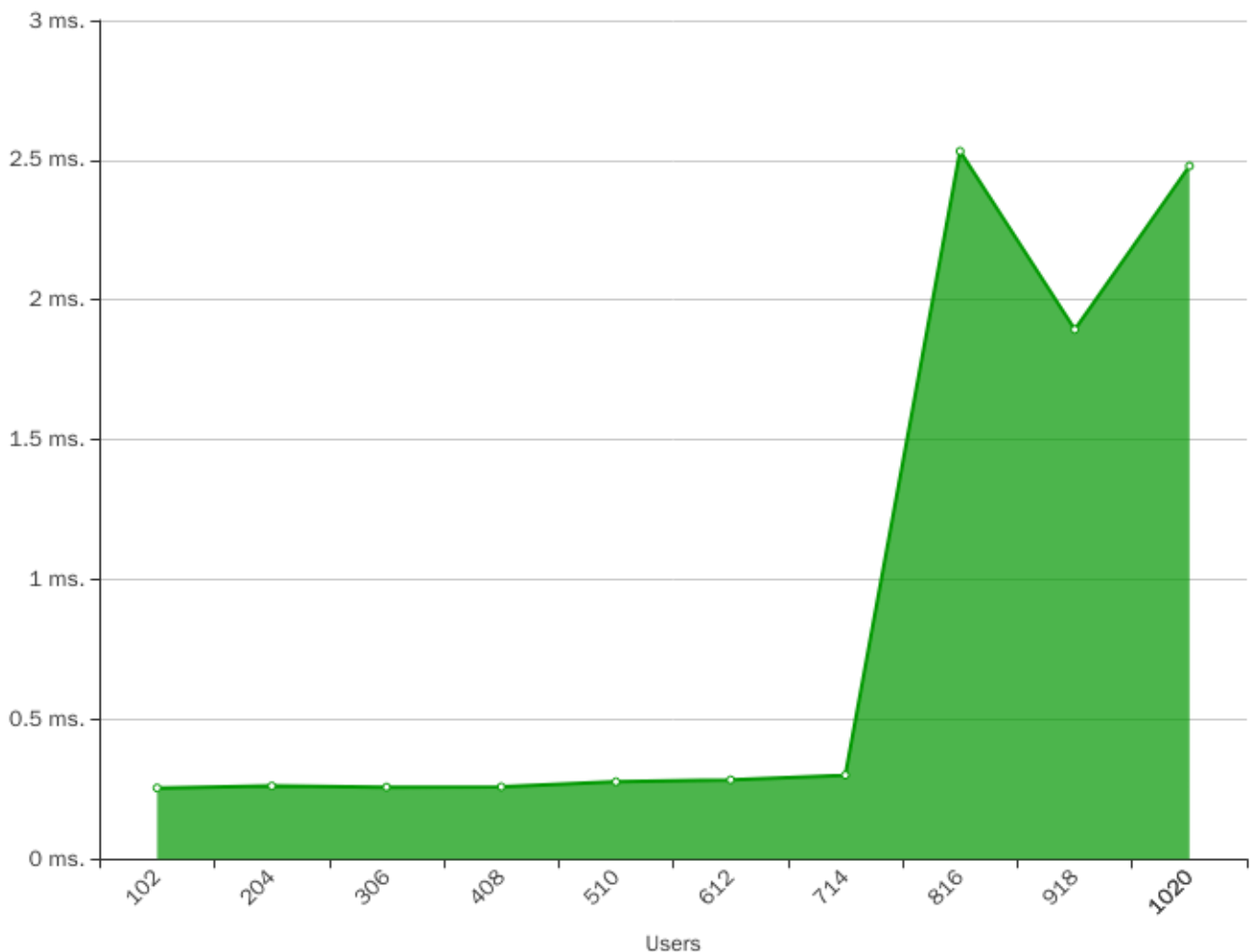
Connection Mode

- Tunnel

### 5.3 Latency

Latency is defined as the round-trip time (RTT) delay between the simulated clients and servers. The RTT latency measurement indicates how long for the data transmitter to receive the acknowledgement from the receiver. If packets are dropped by the firewall, TCP retransmission timeout will be triggered and will dramatically increase the RTT value.

The chart below shows the average RTT latency of the test scenario under different number of users. Latency increases with the growing number of users because the firewall needs to spend more time to process the incoming traffic. After a certain number of users, the latency may increase exponentially. This indicates that the firewall cannot handle the amount of traffic.

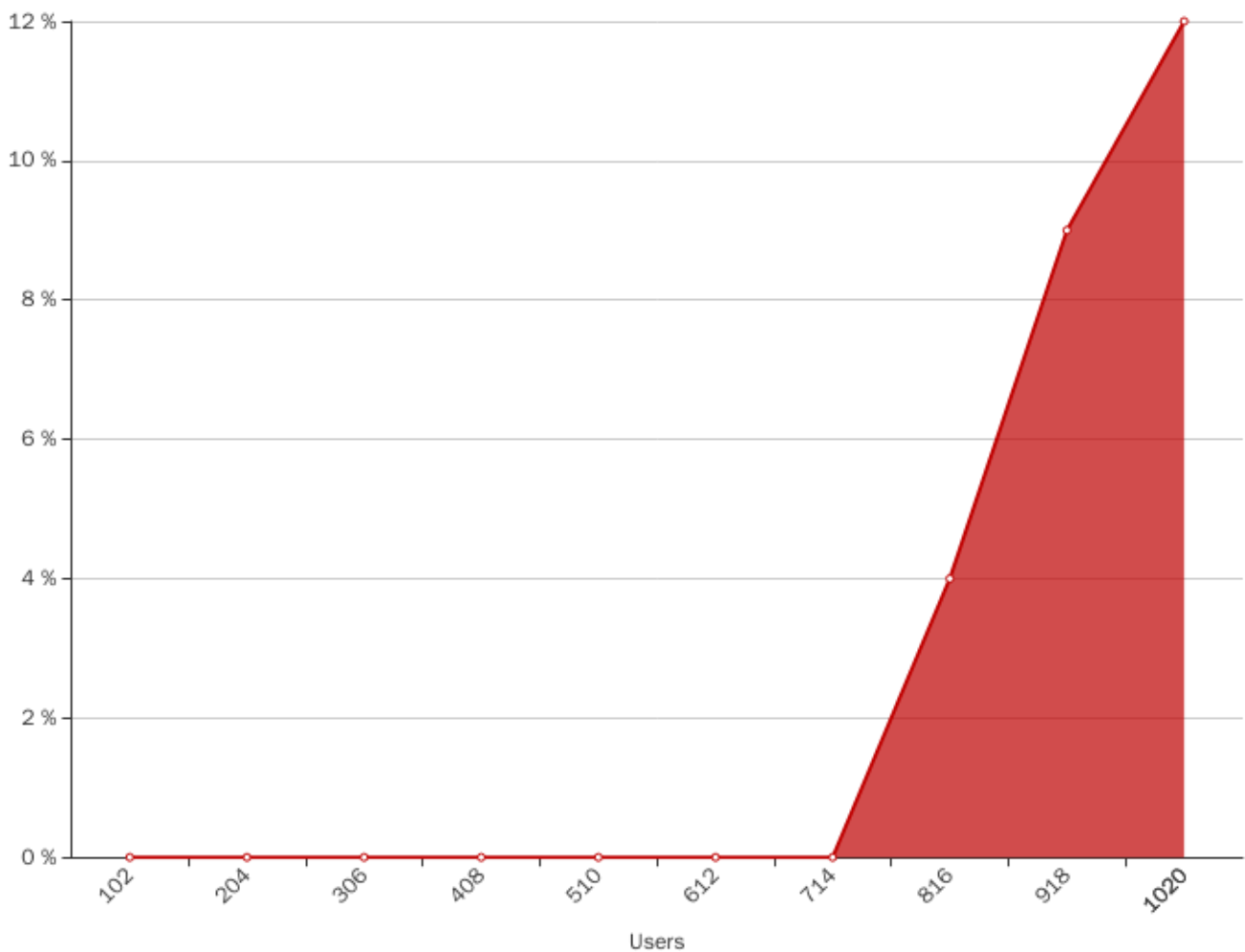


Number of Users	Latency (millisecond)
102	0.254 ms
204	0.261 ms
306	0.257 ms
408	0.258 ms
510	0.276 ms
612	0.283 ms
714	0.3 ms
816	2.532 ms
918	1.894 ms
1020	2.479 ms

## 5.4 Error Percentage

Error percentage is defined as the ratio between the number of retransmissions and the total number of packets transmitted. The retransmission includes both TCP SYN retransmissions, TCP fast retransmissions, FIN retransmissions, out-of-order packets, and duplicated ACKs.

TCP SYN retransmission indicates that the firewall fails to establish TCP connections before the timeout occurs. TCP fast retransmission indicates that transmitted packets are not received by the receiver due to packet dropping caused by the congested firewall.





Number of Users	Error Percentage
102	0 %
204	0 %
306	0 %
408	0 %
510	0 %
612	0 %
714	0 %
816	4 %
918	9 %
1020	12 %

## 5.5 Malware Block Rate

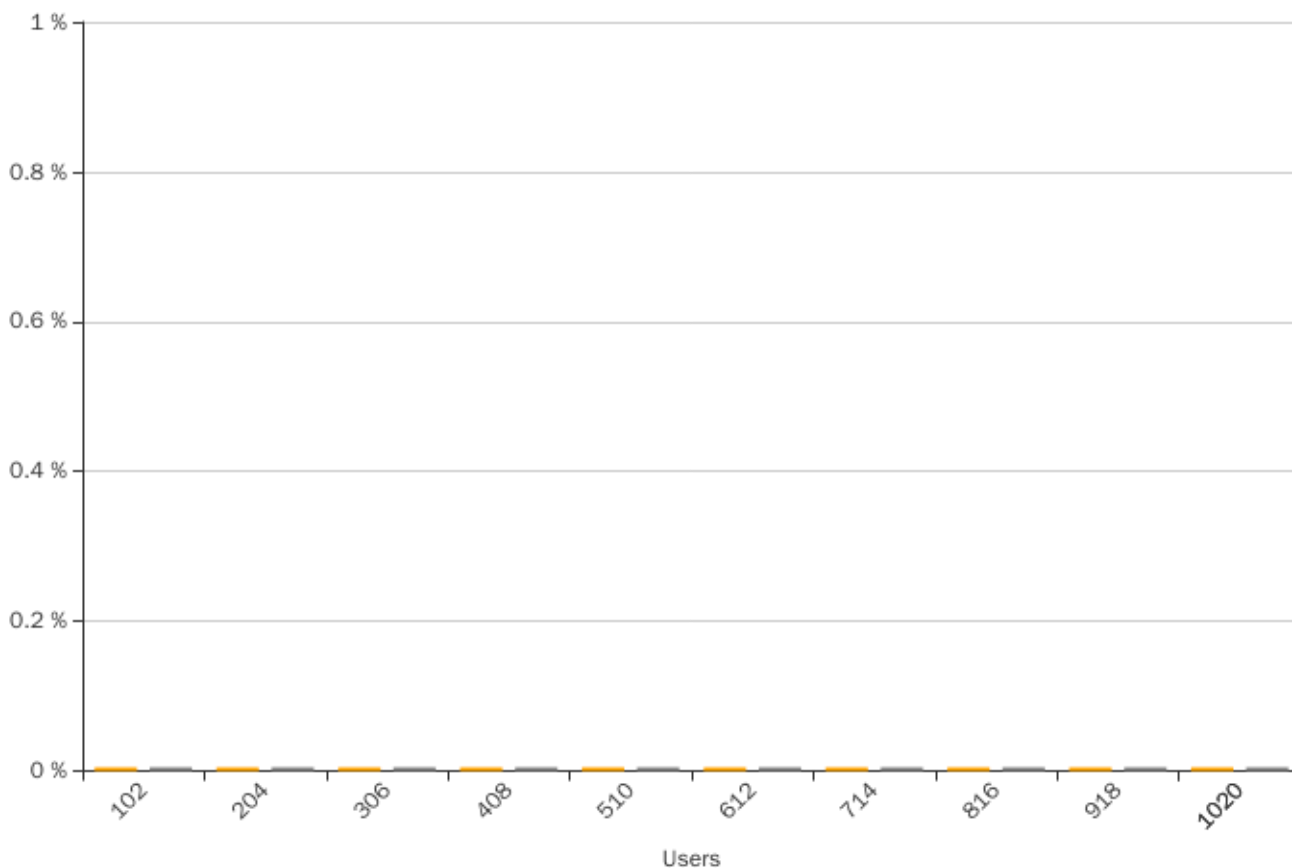
Malware block rate is defined as the ratio between number of successfully blocked malware and the total number of malware injected.

Malware (malicious software) is any software intentionally designed to cause damage to a computer, server, client or network. Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software. The code is described as computer viruses, worms, Trojan horse, ransomware, spyware, adware, etc.

A firewall without an anti-malware function enabled can place high risks on the network security for the enterprise. Thus, performance testing the firewall without keeping it busy with the work it is supposed to is invalid. In order to exercise the anti-malware engine, virus injection is used together with the simulated user traffic. The goal is not to test the security efficacy of the firewall but to keep the anti-malware engine busy so that the test result is convincing.

The test malware file used by Safire is safe, because it is not a virus, and does not include any fragments of viral code. Most security products react to it as if it were a virus. The file is a legitimate DOS program, and produces sensible results when run.

Anti-malware test traffic includes both non-encrypted malware injection (plaintext) and encrypted malware injection (TLS-encrypted). It requires the firewall to have anti-malware function enabled in order to successfully block the non-encrypted malware traffic. It requires the firewall to have anti-malware and SSL deep inspection functions enabled in order to successfully block the encrypted malware traffic. This is because when malware traffic is encrypted, the firewall won't be able to identify the threat but let it pass if the decryption function is off. A firewall with anti-malware function enabled should successfully block 100% of the non-encrypted malware under all circumstances. If not, it indicates the firewall has reached its bottleneck and the security function start being unstable.



Number of Users	Malware Block Rate (non-encrypted)	Malware Block Rate (encrypted)
102	0 %	0 %
204	0 %	0 %
306	0 %	0 %
408	0 %	0 %
510	0 %	0 %
612	0 %	0 %
714	0 %	0 %
816	0 %	0 %
918	0 %	0 %

Summary		Logs																																				
209,328 Events		<div>Disk</div> <div>1 hour</div>																																				
<div>Web Filter</div> <table> <tr> <th>Top Category</th><th>Action</th><th>Count</th></tr> <tr> <td>Freeware and Software Downloads</td><td>Passthrough</td><td>13,487</td></tr> <tr> <td>URL filter applied</td><td>Blocked</td><td>1,445</td></tr> <tr> <td>URL filter applied</td><td>Passthrough</td><td>296</td></tr> <tr> <td>Unrated</td><td>Blocked</td><td>53</td></tr> <tr> <td>File Sharing and Storage</td><td>Passthrough</td><td>47</td></tr> </table> <div>15,328 events</div>		Top Category	Action	Count	Freeware and Software Downloads	Passthrough	13,487	URL filter applied	Blocked	1,445	URL filter applied	Passthrough	296	Unrated	Blocked	53	File Sharing and Storage	Passthrough	47	<div>Application Control</div> <table> <tr> <th>Top Category</th><th>Action</th><th>Count</th></tr> <tr> <td>Network.Service</td><td>Pass</td><td>106,931</td></tr> <tr> <td>Web.Client</td><td>Pass</td><td>54,891</td></tr> <tr> <td>Business</td><td>Pass</td><td>15,529</td></tr> <tr> <td>Collaboration</td><td>Pass</td><td>10,769</td></tr> <tr> <td>Update</td><td>Pass</td><td>4,437</td></tr> </table> <div>193,984 events</div>	Top Category	Action	Count	Network.Service	Pass	106,931	Web.Client	Pass	54,891	Business	Pass	15,529	Collaboration	Pass	10,769	Update	Pass	4,437
Top Category	Action	Count																																				
Freeware and Software Downloads	Passthrough	13,487																																				
URL filter applied	Blocked	1,445																																				
URL filter applied	Passthrough	296																																				
Unrated	Blocked	53																																				
File Sharing and Storage	Passthrough	47																																				
Top Category	Action	Count																																				
Network.Service	Pass	106,931																																				
Web.Client	Pass	54,891																																				
Business	Pass	15,529																																				
Collaboration	Pass	10,769																																				
Update	Pass	4,437																																				

## 5.6 Policy Review

Policy	Policy Type	Source Interface	Destination Interface	Bytes	Sessions	Bandwidth
SWIGGY LAN_Airtel ILL (8)	Firewall	SWIGGY LAN	JIO (wan2)	1.21 GB	551	9.58 Mbps
SWIGGYLAN2-AirtelILL (30)	Firewall	SWIGGYLAN-2	JIO (wan2)	502.29 MB	575	3.50 Mbps
SWIGGYLAN2-AirtelILL(D) (31)	Firewall	SWIGGYLAN-2	JIO (wan2)	389.48 MB	1,921	4.18 Mbps
Test4 (93)	Firewall	SWIGGY LAN	JIO (wan2)	209.90 MB	1,003	1.53 Mbps
SSLVPN-AirtelILL (48)	Firewall	SSL-VPN tunnel interface (ssl.root)	JIO (wan2)	17.93 MB	84	349.58 kb...
SWIGGY LAN_Airtel ILL(DATA) (20)	Firewall	SWIGGY LAN	JIO (wan2)	10.70 MB	194	616.86 kb...
SWIGGYLAN2 TO DMZ (62)	Firewall	SWIGGYLAN-2	DMZ	1.61 MB	6,130	260.18 kb...
SWIGGY LAN_DMZ (9)	Firewall	SWIGGY LAN	DMZ	1.11 MB	4,182	163.30 kb...
SSLVPN - Airtel ILL (49)	Firewall	SSL-VPN tunnel interface (ssl.root)	JIO (wan2)	888.76 kB	21	44.09 kbps
DMZ_NertSat (4)	Firewall	DMZ	TATA (wan1)	480.63 kB	1,489	67.57 kbps
Implicit Deny	Firewall	SWIGGYLAN-2	JIO (wan2)	42.73 kB	3	336 bps
WAN TO LAN SBC (88)	Firewall	TATA (wan1)	Swiggy-11-SBC (SWIGGY-LAN-3)	25.40 kB	5	744 bps
ssl_vpn_lan (18)	Firewall	SSL-VPN tunnel interface (ssl.root)	DMZ	20.73 kB	85	1.70 kbps
DMZ TO SWIGGY LAN 2 (29)	Firewall	DMZ	SWIGGYLAN-2	17.43 kB	86	2.12 kbps
DMZ TO SWIGGY LAN (5)	Firewall	DMZ	SWIGGY LAN	7.67 kB	39	600 bps
DMZ-SSLVPN (45)	Firewall	DMZ	SSL-VPN tunnel interface (ssl.root)	1.55 kB	7	376 bps
Antivirus Server (24)	Firewall	TATA (wan1)	DMZ	224 B	1	0 bps

### 5.6.1 Fortinet Firewall Policy for Swiggy

#### Policy Overview

- This policy governs the firewall configuration and management for Swiggy's IT infrastructure, specifically utilizing **Fortinet Firewalls** (FortiGate series). The primary objective of this policy is to ensure the confidentiality, integrity, and availability of Swiggy's internal and external network traffic, protect customer data, and ensure compliance with industry standards.

### 5.6.2 General Policy Objectives

- Access Control:** Implement fine-grained control over network traffic to ensure only authorized communications are allowed.
- Segmentation:** Create secure network zones to separate internal systems, customer-facing services, and sensitive data.
- Threat Prevention:** Utilize FortiGate's advanced features (IPS, Antivirus, Web Filtering) to detect and prevent threats.
- Compliance:** Ensure adherence to relevant security frameworks and standards, such as **PCI-DSS**, **GDPR**, and **ISO 27001**.
- High Availability:** Ensure that firewall configurations are resilient and support load balancing and failover to guarantee continuous operations.

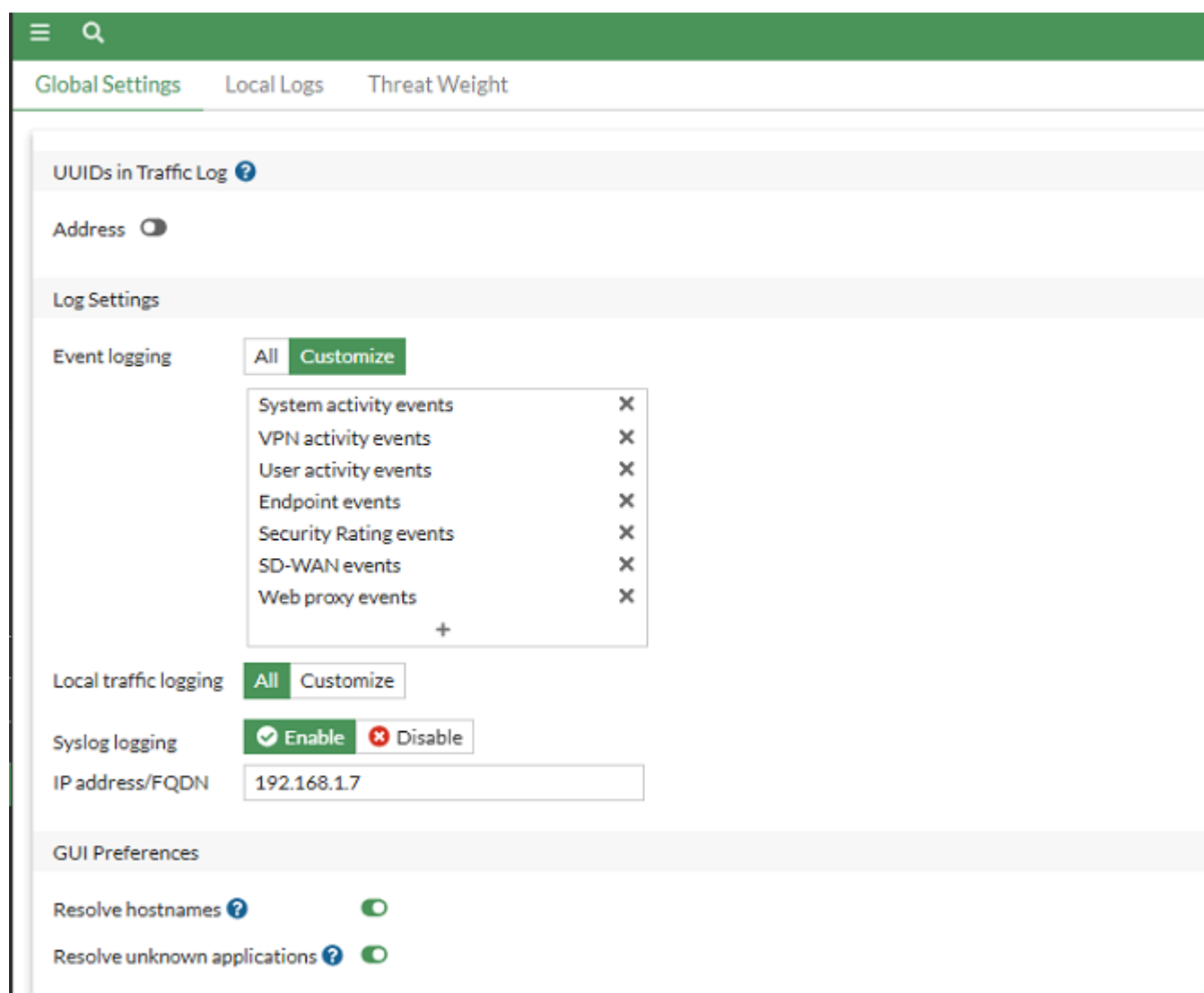
### 5.6.3. Access Control Lists (ACL) and Rule Configuration

- Objective:** Define explicit rules to restrict unauthorized access and ensure network traffic is appropriately filtered.
- Allow Traffic:**
  - Allow inbound HTTPS traffic (port 443) to the DMZ for user-facing applications (e.g., Swiggy's website and mobile apps).
  - Allow necessary outbound traffic from internal services to the internet (for updates, APIs, etc.).
- Deny Traffic:**
  - Deny all inbound traffic from untrusted sources (e.g., external IP addresses that are not whitelisted).

- Block unnecessary or unused ports (e.g., SMB, Telnet, FTP) to reduce attack vectors.
- Deny direct access from the guest network to the internal network.

### 5.6.7 Logging and Monitoring:

- Enable logging for all firewall policies to monitor access attempts, intrusions, or malicious activity.
- Create real-time alerts for suspicious activities, including brute-force attempts, DDoS, or unusual traffic spikes.



The screenshot shows the FortiGate GUI with the 'Global Settings' tab selected. The 'Local Logs' sub-tab is active, displaying the 'Log Settings' section. The 'UUIDs in Traffic Log' section has a toggle for 'Address' set to 'Off'. The 'Event logging' section has a dropdown menu set to 'All', with a 'Customize' button. The dropdown menu lists the following events with checkboxes: System activity events, VPN activity events, User activity events, Endpoint events, Security Rating events, SD-WAN events, and Web proxy events. The 'Local traffic logging' section has a dropdown menu set to 'All', with a 'Customize' button. The 'Syslog logging' section has a toggle set to 'Enable'. The 'IP address/FQDN' field is set to '192.168.1.7'. The 'GUI Preferences' section has two toggles: 'Resolve hostnames' and 'Resolve unknown applications', both set to 'On'.

### 5.6.8 Intrusion Prevention System (IPS) Policy

- **Objective:** Prevent attacks and intrusions by inspecting and blocking malicious traffic in real-time.
- **Policy Configuration:**
- Enable FortiGate's **IPS feature** to detect and block a wide range of known threats (e.g., SQL injection, cross-site scripting, buffer overflow).
- Apply predefined FortiGuard signatures for known vulnerabilities and threats.
- Use custom IPS rules where needed to protect critical business applications and assets.

- **Attack Prevention:**
- Enable detection of Distributed Denial of Service (DDoS) attacks to prevent any disruptions to Swiggy's services.
- Set thresholds for anomaly detection to automatically block traffic when unusual patterns are detected.

Edit IPS Sensor

Name

IPS\_PREVENTION

Comments

Write a comment... 0/255

Block malicious URLs
☐

IPS Signatures and Filters

+ Create New
Edit
Delete

Details	Exempt IPs	Action	Packet Logging
<div> <div>SEV</div> <div> <div></div> <div></div> <div></div> <div></div> <div></div> </div> </div> <div> <div>SEV</div> <div> <div></div> <div></div> <div></div> <div></div> <div></div> </div> </div> <div> <div>SEV</div> <div> <div></div> <div></div> <div></div> <div></div> <div></div> </div> </div>		<div> <div></div> Block </div>	<div> <div></div> Disabled </div>
ABUS.TVIP.Cameras.Admin.Command.Injection AAEH.Botnet AARC.Botnet ABNR.Botnet +9189	0	<div> <div></div> Block </div>	<div> <div></div> Disabled </div>

Botnet C&C

Scan Outgoing Connections to Botnet Sites

Disable
Block
Monitor

3674 IP Addresses in botnet package.

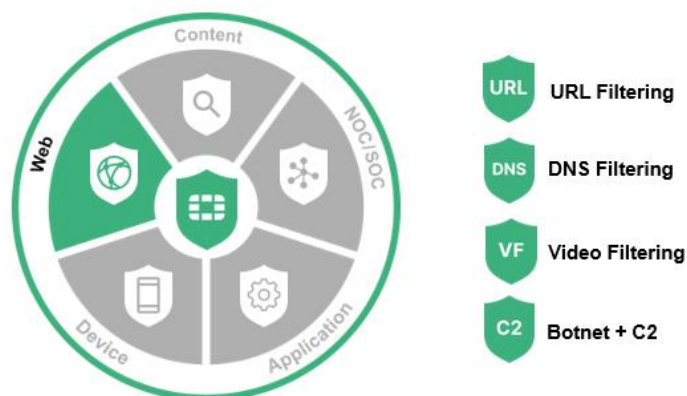
```

BPOC-BBSR-101F # diagnose ips anomaly list
list nids meter:
total # of nids meters: 0.

BPOC-BBSR-101F #

```

## 5.6.9 Web Filtering and Application Control Policy



- **Objective:** Enforce safe browsing for employees and ensure that malicious or inappropriate web content is blocked.

### 5.6.10 Web Filtering:

- 
- Enable **FortiGuard Web Filtering** to block access to harmful websites, including phishing sites and malicious domains.
- Configure categories to block sites that are irrelevant to business operations, such as social media and gaming sites, during working hours (unless necessary).
- **Application Control:**
- Limit access to specific applications and cloud services that are needed for business operations (e.g., Slack, Zoom).
- Block or limit access to unauthorized applications such as peer-to-peer services, torrenting apps, or games.

- AntiVirus
- Web Filter ☆
- Video Filter
- DNS Filter
- Application Control
- Intrusion Prevention
- File Filter
- SSL/SSH Inspection
- Application Signatures
- IPS Signatures
- Web Rating Overrides
- Web Profile Overrides
- VPN >
- User & Authentication >
- WiFi & Switch Controller >
- System 1 >
- Security Fabric >
- Log & Report >

Reverse Proxy
Flow Based
Proxy Based

● FortiGuard Category Based Filter

✓ Allow
👁 Monitor
🚫 Block
⚠ Warning
👤 Authenticate

Name	Action
Local Categories <span style="background-color: #0070c0; color: white; border-radius: 50%; padding: 2px 5px;">2</span>	
custom1	🚫 Block
custom2	🚫 Block
Potentially Liable <span style="background-color: #0070c0; color: white; border-radius: 50%; padding: 2px 5px;">12</span>	
Drug Abuse	🚫 Block
Hacking	🚫 Block
Illegal or Unethical	🚫 Block
Discrimination	🚫 Block
Explicit Violence	🚫 Block

0% 95

**Category Usage Quota** P i

+ Create New
✎ Edit
🗑 Delete

## 6. System Health Status:

```
CLI Console (1)
BPOC-BBSR-101F # get system performance status
CPU states: 2% user 0% system 0% nice 98% idle 0% iowait 0% irq 0% softirq
CPU0 states: 4% user 0% system 0% nice 96% idle 0% iowait 0% irq 0% softirq
CPU1 states: 1% user 0% system 0% nice 99% idle 0% iowait 0% irq 0% softirq
CPU2 states: 4% user 0% system 0% nice 96% idle 0% iowait 0% irq 0% softirq
CPU3 states: 3% user 1% system 0% nice 96% idle 0% iowait 0% irq 0% softirq
CPU4 states: 1% user 1% system 0% nice 98% idle 0% iowait 0% irq 0% softirq
CPU5 states: 4% user 0% system 0% nice 96% idle 0% iowait 0% irq 0% softirq
CPU6 states: 2% user 0% system 0% nice 98% idle 0% iowait 0% irq 0% softirq
CPU7 states: 2% user 1% system 0% nice 97% idle 0% iowait 0% irq 0% softirq
Memory: 7769676k total, 3189312k used (41.0%), 2973916k free (38.3%), 1606448k freeable (20.7%)
Average network usage: 37102 / 39300 kbps in 1 minute, 37467 / 39109 kbps in 10 minutes, 36823 / 38629 kbps in 30 minutes
Maximal network usage: 65881 / 68502 kbps in 1 minute, 83428 / 86197 kbps in 10 minutes, 130958 / 134068 kbps in 30 minutes
Average sessions: 18700 sessions in 1 minute, 18435 sessions in 10 minutes, 17490 sessions in 30 minutes
Maximal sessions: 18969 sessions in 1 minute, 19485 sessions in 10 minutes, 19489 sessions in 30 minutes
Average session setup rate: 141 sessions per second in last 1 minute, 143 sessions per second in last 10 minutes, 131 sessions per second in last 30 minutes
Maximal session setup rate: 215 sessions per second in last 1 minute, 288 sessions per second in last 10 minutes, 289 sessions per second in last 30 minutes
Average NPU sessions: 4211 sessions in last 1 minute, 3116 sessions in last 10 minutes, 3612 sessions in last 30 minutes
Maximal NPU sessions: 4304 sessions in last 1 minute, 4304 sessions in last 10 minutes, 4304 sessions in last 30 minutes
Average nTurbo sessions: 2909 sessions in last 1 minute, 2172 sessions in last 10 minutes, 2625 sessions in last 30 minutes
Maximal nTurbo sessions: 2968 sessions in last 1 minute, 2968 sessions in last 10 minutes, 3267 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 55 days, 11 hours, 17 minutes

BPOC-BBSR-101F #
```

### 6.1 System Status

```
CLI Console (1)
BPOC-BBSR-101F # get system status
Version: FortiGate-101F v7.2.10,build1706,240918 (GA.M)
Security Level: 1
Firmware Signature: certified
Virus-DB: 93.02157(2025-04-03 03:26)
Extended DB: 93.02157(2025-04-03 03:25)
AV AI/ML Model: 4.01118(2025-04-03 03:45)
IPS-DB: 31.00981(2025-04-02 00:50)
IPS-ETDB: 0.00000(2001-01-01 00:00)
APP-DB: 31.00980(2025-04-01 00:22)
FMWP-DB: 25.00022(2025-02-19 15:56)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 5.00371(2025-04-02 10:49)
IoT-Detect: 0.00000(2022-08-17 17:31)
Serial-Number: FG101FTK21020759
BIOS version: 05000024
System Part-Number: P24605-21
Log hard disk: Available
Hostname: BPOC-BBSR-101F
Private Encryption: Disable
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 1706
Release Version Information: GA
System time: Thu Apr 3 17:56:10 2025
--More--
```