Enhanced Firewall Services

vmware

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Firewall Overview

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. SD-WAN Orchestrator supports configuration of Stateless, Stateful, and Enhanced Firewall Services (EFS) rules for Profiles and Edges.

Stateful Firewall

A Stateful firewall monitors and tracks the operating state and characteristics of every network connection coming through the firewall and uses this information to determine which network packets to allow through the firewall. The Stateful firewalls build a state table and use this table to allow only returning traffic from connections currently listed in the state table. After a connection is removed from the state table, no traffic from the external device of this connection is permitted.

The Stateful firewall feature provides the following benefits:

- Prevent attacks such as denial of service (DoS) and spoofing
- More robust logging
- Improved network security

The main differences between a Stateful firewall and a Stateless firewall are:

- Matching is directional. For example, you can allow hosts on VLAN 1 to initiate a TCP session with hosts on VLAN 2 but deny the reverse. Stateless firewalls translate into simple ACLs (Access lists) which do not allow for this kind of granular control.

Enhanced Firewall Services

Enhanced Firewall Services (EFS) provide additional EFS security functionalities on VMware SD-WAN Edges. The NSX Security powered EFS functionality supports Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) services on VMware SD-WAN Edges. The Edge Enhanced Firewall Services (EFS) protect Edge traffic from intrusions across Branch to Branch, Branch to Hub, or Branch to Internet traffic patterns.

Currently, SD-WAN Edge Firewall provides stateful inspection along with application identification without additional EFS security features. While the stateful Firewall SD-WAN Edge provides security, it is not adequate and creates a gap in providing EFS security integrated natively with VMware SD-WAN. Edge EFS address these security gaps and offers enhanced threat protection natively on the SD-WAN Edge in conjunction with VMware SD-WAN.

Firewall Logs

With the Stateful Firewall and Enhanced Firewall Services (EFS) features activated, more information can be reported in the firewall logs. The firewall logs will contain the following fields: Time, Segment, Edge, Action, Interface, Protocol, Source IP, Source Port, Destination IP, Destination Port, Extension Headers, Rule, Reason, Bytes Received, Bytes Sent, Duration, Application, Destination Domain, Destination Name, Session ID, Signature, IPS Alert, IDS Alert, Signature ID, Category, Attack Source, Attack Target, and Severity.

Note Not all fields will be populated for all firewall logs. For example, Reason, Bytes Received/ Sent and Duration are fields included in logs when sessions are closed. Signature, IPS Alert, IDS Alert, Signature ID, Category, Attack Source, Attach Target, and Severity are populated only for EFS alerts, not for firewall logs.

Firewall logs are generated:

- When a flow is created (on the condition that the flow is accepted)
- When the flow is closed
- When a new flow is denied
- When an existing flow is updated (due to a firewall configuration change)

You can view the firewall logs by using the following firewall features:

- **Firewall Logging** - By default, Edges cannot send their Firewalls logs to Orchestrator.

  Note For an Edge to send the Firewall logs to Orchestrator, ensure that the "**Enable Firewall Logging to Orchestrator**" customer capability is activated at the Customer level under "Global Settings" UI page. Customers must contact your Operator if you would want the Firewall Logging feature to be activated.

  You can view the Edge Firewall logs in Orchestrator from the **Monitor** > **Firewall Logs** page. For more information, see Monitor Firewall Logs.

- **Syslog Forwarding** - Allows you to view the logs by sending the logs originating from enterprise SD-WAN Edge to one or more configured remote servers. By default, the **Syslog Forwarding** feature is deactivated for an enterprise. To forward the logs to remote Syslog collectors, you must:

  a Activate **Syslog Forwarding** feature under **Configure > Edges/Profile > Firewall** tab.

Configure Profile Firewall

A Firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. SD-WAN Orchestrator supports configuration of stateless and stateful Firewalls for Profiles and Edges.

For more information on Firewall, see Firewall Overview.

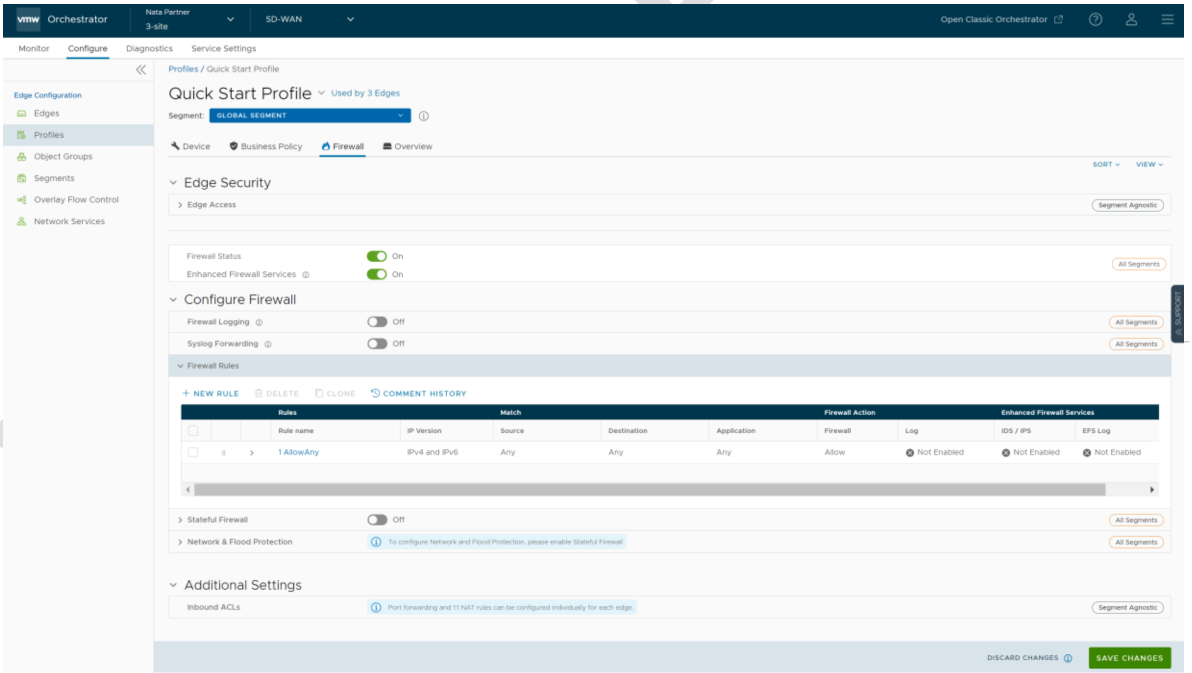
Configure Profile Firewall

To configure Profile Firewall:

1 In the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.

2 To configure a Profile Firewall, click the link to the Profile and click the **Firewall** tab. Alternatively, you can click the **View** link in the **Firewall** column of the Profile.

3 The **Firewall** page appears.



Edge Security

Edge Access — Segment Agnostic

Firewall Status: On

Enhanced Firewall Services: On — All Segments

Configure Firewall

Firewall Logging: Off — All Segments

Syslog Forwarding: Off — All Segments

Firewall Rules

Rules		Match				Firewall Action		Enhanced Firewall Services	
Rule name	IP Version	Source	Destination	Application		Firewall	Log	IDS / IPS	EFS Log
1 AllowAny	IPv4 and IPv6	Any	Any	Any		Allow	Not Enabled	Not Enabled	Not Enabled

Stateful Firewall: Off — All Segments

Network & Flood Protection: To configure Network and Flood Protection, please enable Stateful Firewall — All Segments

Additional Settings

Inbound ACLs: Port forwarding and 1:1 NAT rules can be configured individually for each edge. — Segment Agnostic

4 From the **Firewall** tab, you can configure the following Edge Security and Firewall capabilities:

Field	Description
Edge Access	Allows you to configure a Profile for Edge access. You must make sure to select the appropriate option for Support access, Console access, USB port access, SNMP access, and Local Web UI access under Firewall settings to make the Edge more secure. This will prevent any malicious user from accessing the Edge. By default, Support access, Console access, SNMP access, and Local Web UI access are deactivated for security reasons. For more information, see Configure Edge Access.
Firewall Status	Allows you to turn ON or OFF the Firewall rules, configure Firewall settings, and in-bound ACLs for all Edges associated with the Profile. **Note** By default, this feature is activated. You can deactivate the Firewall function for Profiles by turning the **Firewall Status** to OFF.
Enhanced Firewall Services	Allows you to turn ON or OFF the Enhanced Firewall Services (EFS) feature for all Edges associated with the Profile. **Note** By default, this feature is not activated. For more information, see Configure Enhanced Firewall Services.
Firewall Logging	Allows you to turn ON or OFF the Firewall Logging feature for all Edges associated with the Profile. By default, Edges cannot send their Firewalls logs to Orchestrator. **Note** For an Edge to send the Firewall logs to Orchestrator, ensure that the "**Enable Firewall Logging to Orchestrator**" customer capability is activated at the Customer level under "Global Settings" UI page. Customers must contact your Operator if you would want the Firewall Logging feature to be activated. You can view the Edge Firewall logs in Orchestrator from the **Monitor** > **Firewall Logs** page. For more information, see Monitor Firewall Logs.
Syslog Forwarding	By default, the Syslog Forwarding feature is deactivated for an Enterprise. To collect SD-WAN Orchestrator bound events and Firewall logs originating from Enterprise SD-WAN Edge to one or more centralized remote Syslog collectors (Servers), an Enterprise user must activate this feature at the Edge/ Profile level. **Note** You can view both IPv4 and IPv6 Firewall logging details in a IPv4-based Syslog Server.

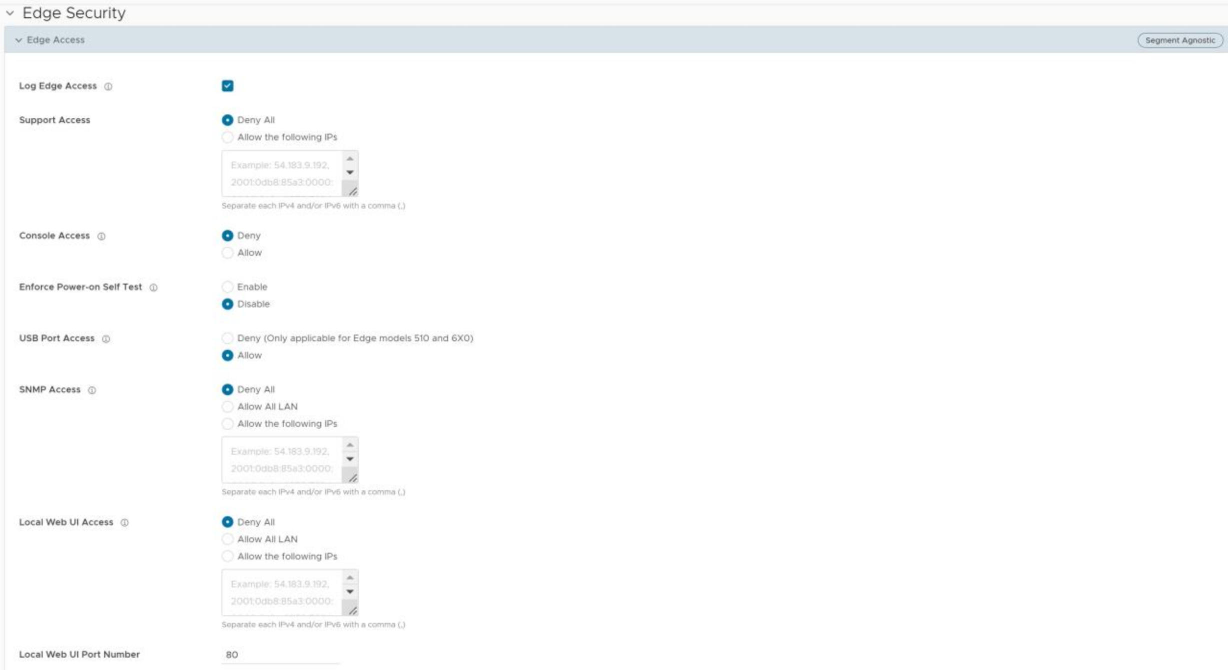
Field	Description
Firewall Rules	The existing pre-defined Firewall rules are displayed. You can click **+ NEW RULE** to create a new Firewall rule. For more information, see Configure Firewall Rule. To delete existing Firewall rules, select the checkboxes prior to the rules and click **DELETE**. To duplicate a Firewall rule, select the rule and click **CLONE**. While creating or updating a Firewall rule, you can add comments about the rule in the **New Comment** field in the **Comment History** tab. A maximum of 50 characters is allowed and you can add any number of comments for the same rule.
Stateful Firewall	By default, the Stateful Firewall feature is deactivated for an Enterprise. SD-WAN Orchestrator allows you to set session timeout for established and non-established TCP flows, UDP flows, and other flows at the Profile level. Optionally, you can also override the Stateful firewall settings at the Edge level. For more information, see Configure Stateful Firewall Settings.
Network & Flood Protection	To secure all connection attempts in an Enterprise network, VMware SD-WAN Orchestrator allows you to configure Network and Flood Protection settings at the Profile and Edge levels, to protect against the various types of attacks. For more information, see Configure Network & Flood Protection Settings.

Configure Edge Access

To configure Edge access for Profiles, perform the following steps:

1 From the SD-WAN Orchestrator, go to **Configure** > **Profiles** > **Firewall**.

2 Under **Edge Security**, click the **Edge Access** expand icon.



Log Edge Access ☑

Support Access ● Deny All ○ Allow the following IPs

Example: 54.183.9.192, 2001:0db8:85a3:0000:

Separate each IPv4 and/or IPv6 with a comma (,)

Console Access ● Deny ○ Allow

Enforce Power-on Self Test ○ Enable ● Disable

USB Port Access ○ Deny (Only applicable for Edge models 510 and 6X0) ● Allow

SNMP Access ● Deny All ○ Allow All LAN ○ Allow the following IPs

Example: 54.183.9.192, 2001:0db8:85a3:0000:

Separate each IPv4 and/or IPv6 with a comma (,)

Local Web UI Access ● Deny All ○ Allow All LAN ○ Allow the following IPs

Example: 54.183.9.192, 2001:0db8:85a3:0000:

Separate each IPv4 and/or IPv6 with a comma (,)

Local Web UI Port Number 80

3 You can configure one or more of the following Edge Access options, and click **Save Changes**:

Field	Description
Log Edge Access	When activated, all access to the Edge is logged, including successful and failed attempts.
Support Access	Select **Allow the following IPs** if you want to explicitly specify the IP addresses from where you can SSH into this Edge. You can enter both IPv4 and IPv6 addresses separated by comma (,). By default, **Deny All** is selected.
Console Access	Select **Allow** to activate Edge access through Physical Console (Serial Port or Video Graphics Array (VGA) Port). By default, **Deny** is selected and Console login is deactivated after Edge activation. **Note** Whenever the console access setting is changed from **Allow** to **Deny** or vice-versa, the Edge must be rebooted manually.
Enforce Power-on Self Test	When activated, a failed Power-on Self Test will deactivate the Edge. You can recover the Edge by running factory reset and then reactivate the Edge.

Field	Description
USB Port Access	Select **Allow** to activate and select **Deny** to deactivate the USB port access on Edges. This option is available only for Edge models 510 and 6x0. **Note** Whenever the USB port access setting is changed from **Allow** to **Deny** or vice-versa, you must reboot the Edge manually if you have access to the Edge and if the Edge is in a remote site, restart the Edge using SD-WAN Orchestrator.
SNMP Access	Allows Edge access from routed interfaces/WAN through SNMP. Select one of the following options: ■ **Deny All** - By default, SNMP access is deactivated for all devices connected to an Edge. ■ **Allow All LAN** - Allows SNMP access for all devices connected to the Edge through a LAN network. ■ **Allow the following IPs** - Allows you to explicitly specify the IP addresses from where you can access the Edge through SNMP. Separate each IPv4 or IPv6 addresses with a comma (,).
Local Web UI Access	Allows Edge access from routed interfaces/WAN through a Local Web UI. Select one of the following options: ■ **Deny All** - By default, Local Web UI access is deactivated for all devices connected to an Edge. ■ **Allow All LAN** - Allows Local Web UI access for all devices connected to the Edge through a LAN network. ■ **Allow the following IPs** - Allows you to explicitly specify the IP addresses from where you can access the Edge through Local Web UI. Separate each IPv4 or IPv6 addresses with a comma (,).
Local Web UI Port Number	Enter the port number of the local Web UI from where you can access the Edge. The default value is 80.

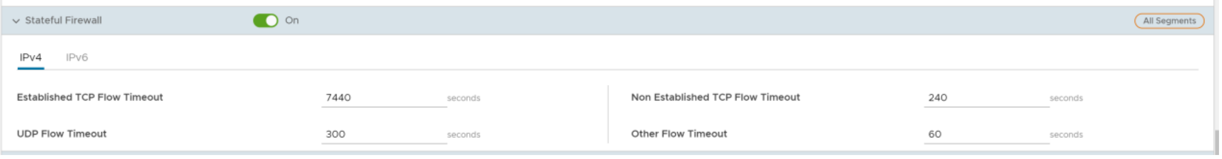
If you want to override the Edge access settings for a specific Edge, use **Enable Edge Override** option available on the **Edge Firewall** page.

Configure Stateful Firewall Settings

To configure Stateful Firewall Settings for Profiles, perform the following steps:

1 From the SD-WAN Orchestrator, go to **Configure** > **Profiles** > **Firewall**.

2 Under **Configure Firewall**, turn on the **Stateful Firewall** toggle button and then click the expand icon. By default, the timeout sessions are applied for IPv4 addresses.



Established TCP Flow Timeout 7440 seconds

Non Established TCP Flow Timeout 240 seconds

UDP Flow Timeout 300 seconds

Other Flow Timeout 60 seconds

3 You can configure the following Stateful Firewall settings, and click **Save Changes**:

Field	Description
Established TCP Flow Timeout (seconds)	Sets the inactivity timeout period (in seconds) for established TCP flows, after which they are no longer valid. The allowable value ranges from 60 seconds through 15999999 seconds. The default value is 7440 seconds.
Non Established TCP Flow Timeout (seconds)	Sets the inactivity timeout period (in seconds) for non-established TCP flows, after which they are no longer valid. The allowable value ranges from 60 seconds through 604800 seconds. The default value is 240 seconds.
UDP Flow Timeout (seconds)	Sets the inactivity timeout period (in seconds) for UDP flows, after which they are no longer valid. The allowable value ranges from 60 seconds through 15999999 seconds. The default value is 300 seconds.
Other Flow Timeout (seconds)	Sets the inactivity timeout period (in seconds) for other flows such as ICMP, after which they are no longer valid. The allowable value ranges from 60 seconds through 15999999 seconds. The default value is 60 seconds.

Note The configured timeout values apply only when the memory usage is below the soft limit. Soft limit corresponds to anything below 60 percent of the concurrent flows supported by the platform in terms of memory usage.

Configure Network & Flood Protection Settings

VMware SD-WAN provides detection and protection against following types of attacks to combat exploits at all stages of their execution:

- Denial-of-Service (DoS) attack
- TCP-based attacks - Invalid TCP Flags, TCP Land, and TCP SYN Fragment
- ICMP-based attacks - ICMP Ping of Death and ICMP Fragment
- IP-based attacks - IP Unknown Protocol, IP Options, IPv6 Unknown Protocol, and IPv6 Extension Header.

Attack Type	Description
Denial-of-Service (DoS) attack	A denial-of-service (DoS) attack is a type of network security attack that overwhelms the targeted device with a tremendous amount of bogus traffic so that the target becomes so preoccupied processing the bogus traffic that legitimate traffic cannot be processed. The target can be a firewall, the network resources to which the firewall controls access, or a specific hardware platform or operating system of an individual host. The DoS attack attempts to exhaust the target device's resources, making the target device unavailable to legitimate users. There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Other DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the system.
Invalid TCP Flags	Invalid TCP flags attack occurs when a TCP packet has a bad or invalid flag combination. A vulnerable target device will crash due to invalid TCP flag combinations and therefore it is recommended to filter them out. Invalid TCP flags guards against: ■ Packet that has no flags set in its TCP header such as SYN, FIN, ACK, etc., ■ TCP header that has SYN and FIN flags combined, which are mutually exclusive flags in reality
TCP Land	A Land attack is a Layer 4 DoS attack in which, a TCP SYN packet is created such that the source IP address and port are set to be the same as the destination IP address and port, which in turn is set to point to an open port on a target device. A vulnerable target device would receive such a message and reply to the destination address effectively sending the packet for reprocessing in an infinite loop. Thus, the device CPU is consumed indefinitely causing the vulnerable target device to crash or freeze.

TCP SYN Fragment	The Internet Protocol (IP) encapsulates a Transmission Control Protocol (TCP) SYN segment in the IP packet to initiate a TCP connection and invoke a SYN/ACK segment in response. Because the IP packet is small, there is no legitimate reason for it to be fragmented. A fragmented SYN packet is anomalous, and as such suspect. In a TCP SYN fragment attack, a target server or host is flooded with TCP SYN packet fragments. The host catches the fragments and waits for the remaining packets to arrive so it can reassemble them. By flooding a server or host with connections that cannot be completed, the host's memory buffer overflows and therefore no further legitimate connections are possible, causing damage to the target host's operating system.

Attack Type	Description
ICMP Ping of Death	An Internet Control Message Protocol (ICMP) Ping of Death attack involves the attacker sending multiple malformed or malicious pings to a target device. While ping packets are generally small used for checking reachability of network hosts, they could be crafted larger than the maximum size of 65535 bytes by attackers. When a maliciously large packet is transmitted from the malicious host, the packet gets fragmented in transit and when the target device attempts to reassemble the IP fragments into the complete packet, the total exceeds the maximum size limit. This could overflow memory buffers initially allocated for the packet, causing system crash or freeze or reboot, as they cannot handle such huge packets.
ICMP Fragment	An ICMP Fragmentation attack is a common DoS attack which involves the flooding of fraudulent ICMP fragments that cannot be defragmented on the target server. As defragmentation can only take place when all fragments are received, temporary storage of such fake fragments takes up memory and may exhaust the available memory resources of the vulnerable target server, resulting in server unavailability.
IP Unknown Protocol	Enabling IP Unknown Protocol protection blocks IP packets with the protocol field containing a protocol ID number of 143 or greater, as it could lead to crash if not handled properly on the end device. A cautious stance would be to block such IP packets from entering the protected network.

IP Options	Attackers sometimes configure IP option fields within an IP packet incorrectly, producing either incomplete or malformed fields. Attackers use these malformed packets to compromise vulnerable hosts on the network. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing a packet containing a specific crafted IP option in the packet's IP header. Enabling IP Insecure Options protection blocks transit IP packets with incorrectly formatted IP option field in the IP packet header.

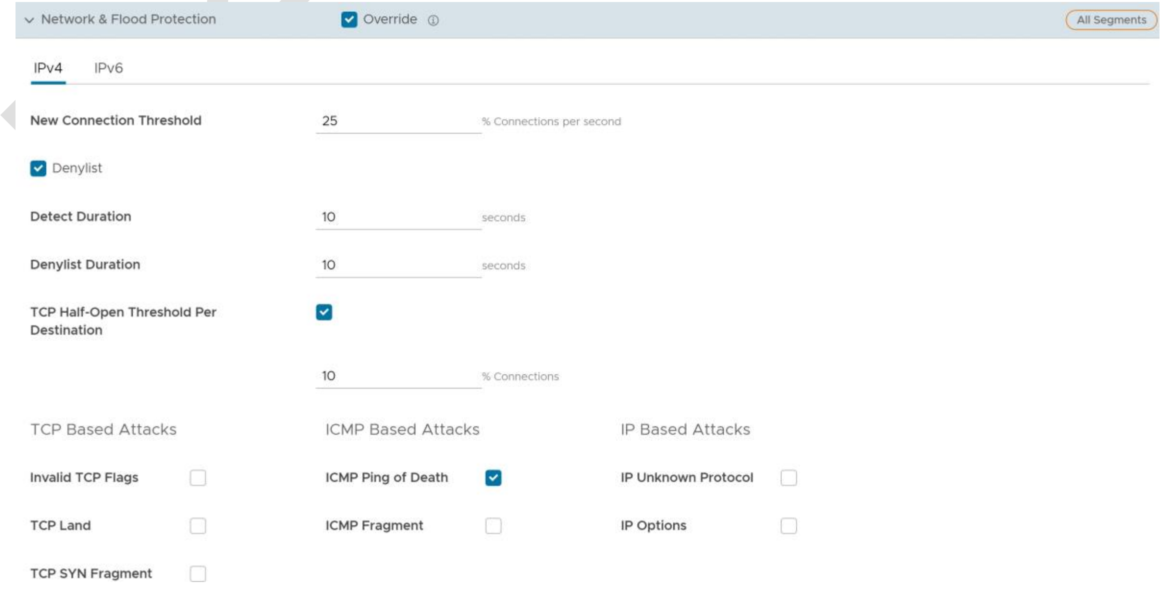
Attack Type	Description
IPv6 Unknown Protocol	Enabling IPv6 Unknown Protocol protection blocks IPv6 packets with the protocol field containing a protocol ID number of 143 or greater, as it could lead to crash if not handled properly on the end device. A cautious stance would be to block such IPv6 packets from entering the protected network.
IPv6 Extension Header	IPv6 Extension Header attack is a DoS attack that occurs due to mishandling of extension headers in an IPv6 packet. The mishandling of IPv6 extension headers creates new attack vectors that could lead to DoS, and which can be exploited for different purposes, such as creating covert channels and routing header 0 attacks. Enabling this option would drop IPv6 packet with any extension header except fragmentation headers.

To configure Network and Flood Protection Settings for Profiles, perform the following steps:

1 From the SD-WAN Orchestrator, go to **Configure** > **Profiles** > **Firewall**.

2 Under **Configure Firewall**, ensure to turn on the **Stateful Firewall** feature.

3 Click the **Network & Flood Protection** expand icon.



Network & Flood Protection ☑ Override

IPv4 | IPv6

New Connection Threshold: 25 % Connections per second

☑ Denylist

Detect Duration: 10 seconds

Denylist Duration: 10 seconds

TCP Half-Open Threshold Per Destination: ☑ 10 % Connections

TCP Based Attacks		ICMP Based Attacks		IP Based Attacks	
Invalid TCP Flags	□	ICMP Ping of Death	☑	IP Unknown Protocol	□
TCP Land	□	ICMP Fragment	□	IP Options	□
TCP SYN Fragment	□				

4 You can configure the following Network and Flood Protection settings, and click **Save Changes**:

Note By default, the network and flood protection settings are applied for IPv4 addresses.

Field	**Description**
New Connection Threshold (connections per second)	The maximum number of new connections that is allowed from a single source IP per second. The allowable value ranges from 10 percentage through 100 percentage. The default value is 25 percentage.
Denylist	Select the checkbox to block a source IP address, which is violating the new connection threshold by sending flood traffic either due to misconfiguration of network or malicious user attacks. **Note** The **New Connection Threshold (connections per second)** settings will not work unless **Denylist** is selected.
Detect Duration (seconds)	Before blocking a Source IP address, it is the grace time duration for which the violating source IP is allowed to send traffic flows. If a host sends flood traffic of new connection requests (port scan, TCP SYN flood, etc.,) exceeding the maximum allowed connection per second (CPS) for this duration, it will be considered as eligible for denylisting instead of immediately denylisting it as soon as it exceeds the CPS per source once. For example, consider that the maximum allowed CPS is 10 with detect duration of 10 seconds, if the host floods new connection requests greater than 100 requests for 10 seconds, then the host will be denylisted. The allowable value ranges from 10 seconds through 100 seconds. The default value is 10 seconds.
Denylist Duration (seconds)	The time duration for which the violated source IP is blocked from sending any packets. The allowable value ranges from 10 seconds through 86400 seconds. The default value is 10 seconds.
TCP Half-Open Threshold Per Destination	The maximum number of half-open TCP connections that is allowed per destination. The allowable value ranges from 1 percentage through 100 percentage.
TCP Based Attacks	Supports protection from the following TCP-based attacks by enabling the respective checkboxes: ■ Invalid TCP Flags ■ TCP Land ■ TCP SYN Fragment

Configure Edge Firewall

By default, all the Edges inherit the Firewall rules, Enhanced Firewall Services (EFS) settings, Stateful Firewall settings, Network and Flood Protection settings, Firewall Logging, Syslog Forwarding, and Edge access configurations from the associated Profile.

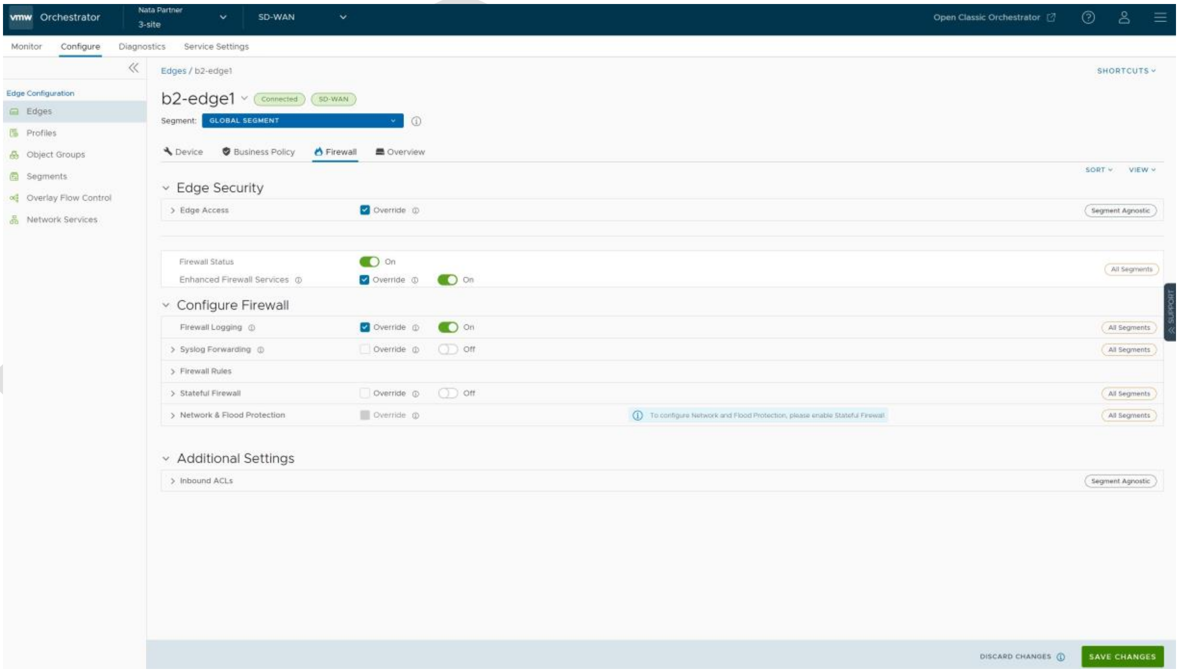
Under the **Firewall** tab of the **Edge Configuration** dialog, you can view all the inherited Firewall rules in the **Rule From Profile** area. Optionally, at the Edge-level, you can also override the inherited Firewall rules and various Firewall settings.

1 In the Enterprise portal, go to **Configure > Edges**.

2 Select an Edge for which you want to override the inherited Firewall settings and click on the **Firewall** tab.

3 Select the **Override** checkbox against the various Firewall settings if you want to modify the inherited Firewall rules and settings for the selected Edge.

Note The Edge override rules will take priority over the inherited Profile rules for the Edge. Any Firewall override match value that is the same as any Profile Firewall rule will override that Profile rule.



Segment: GLOBAL SEGMENT

Edge Security

- Edge Access ☑ Override — Segment Agnostic

Firewall Status: On — All Segments
Enhanced Firewall Services ☑ Override: On

Configure Firewall

- Firewall Logging ☑ Override: On — All Segments
- Syslog Forwarding ☐ Override: Off — All Segments
- Firewall Rules
- Stateful Firewall ☐ Override: Off — All Segments
- Network & Flood Protection ☐ Override — To configure Network and Flood Protection, please enable Stateful Firewall — All Segments

Additional Settings

- Inbound ACLs — Segment Agnostic

4 At the Edge level, you can configure Port Forwarding and 1:1 NAT IPv4 or IPv6 rules individually by navigating to **Additional Settings** > **Inbound ACLs**. For detailed information, see Port Forwarding Rules and 1:1 NAT Settings.

Note By default, all inbound traffic will be blocked unless the Port Forwarding and 1:1 NAT Firewall Rules are configured. The outside IP will always be that of WAN IP or IP address from WAN IP subnet.

Note When configuring IPv6 Port Forwarding and 1:1 NAT rules, you can enter only Global or Unicast IP address and cannot enter Link Local Address.

Port Forwarding and 1:1 NAT Firewall Rules

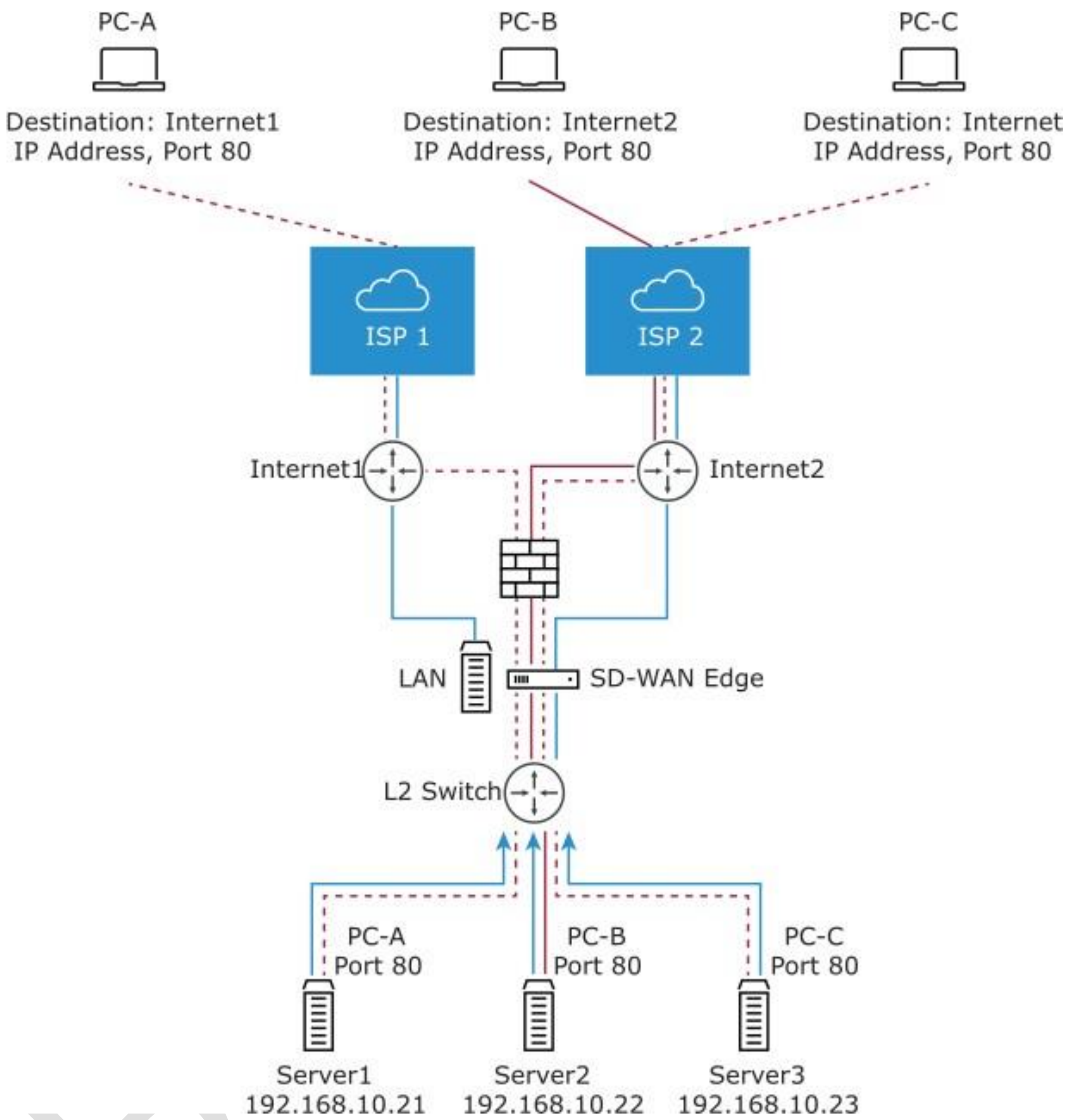
Note You can configure Port Forwarding and 1:1 NAT rules individually only at the Edge level.

Port Forwarding and 1:1 NAT firewall rules gives Internet clients access to servers connected to an Edge LAN interface. Access can be made available through either Port Forwarding Rules or 1:1 NAT (Network Address Translation) rules.

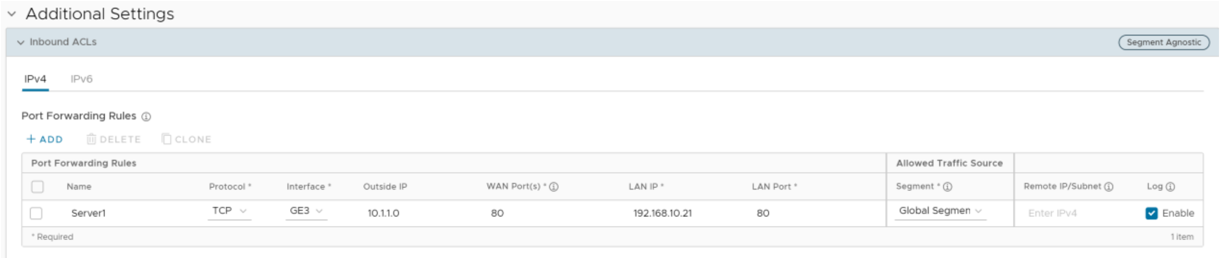
Port Forwarding Rules

Port forwarding rules allows you to configure rules to redirect traffic from a specific WAN port to a device (LAN IP/ LAN Port) within the local subnet. Optionally, you can also restrict the inbound traffic by an IP or a subnet. Port forwarding rules can be configured with the Outside IP which is on the same subnet of the WAN IP. It can also translate outside IP addresses in different subnets than the WAN interface address if the ISP routes traffic for the subnet towards the SD-WAN Edge.

The following figure illustrates the port forwarding configuration.



In the **Port Forwarding Rules** section, you can configure port forwarding rules with IPv4 or IPv6 address by clicking the **+Add** button and then entering the following details.


Additional Settings

Inbound ACLs

Segment Agnostic

IPv4 IPv6

Port Forwarding Rules

+ ADD DELETE CLONE

Port Forwarding Rules							Allowed Traffic Source		
□	Name	Protocol *	Interface *	Outside IP	WAN Port(s) *	LAN IP *	LAN Port *	Segment *	Remote IP/Subnet	Log
□	Server1	TCP	GE3	10.1.1.0	80	192.168.10.21	80	Global Segmen	Enter IPv4	☑ Enable

* Required

1 item

1 In the **Name** text box, enter a name (optional) for the rule.

2 From the **Protocol** drop-down menu, select either TCP or UDP as the protocol for port forwarding.

3 From the **Interface** drop-down menu, select the interface for the inbound traffic.

4 In the **Outside IP** text box, enter the IPv4 or IPv6 address using which the host (application) can be accessed from the outside network.

5 In the WAN Ports text box, enter a WAN port or a range of ports separated with a dash (-), for example 20-25.

6 In the **LAN IP** and **LAN Port** text boxes, enter the IPv4 or IPv6 address and port number of the LAN, where the request will be forwarded.

7 From the **Segment** drop-down menu, select a segment the LAN IP will belong to.

8 In the **Remote IP/subnet** text box, specify an IP address of an inbound traffic that you want to be forwarded to an internal server. If you do not specify any IP address, then it will allow any traffic.

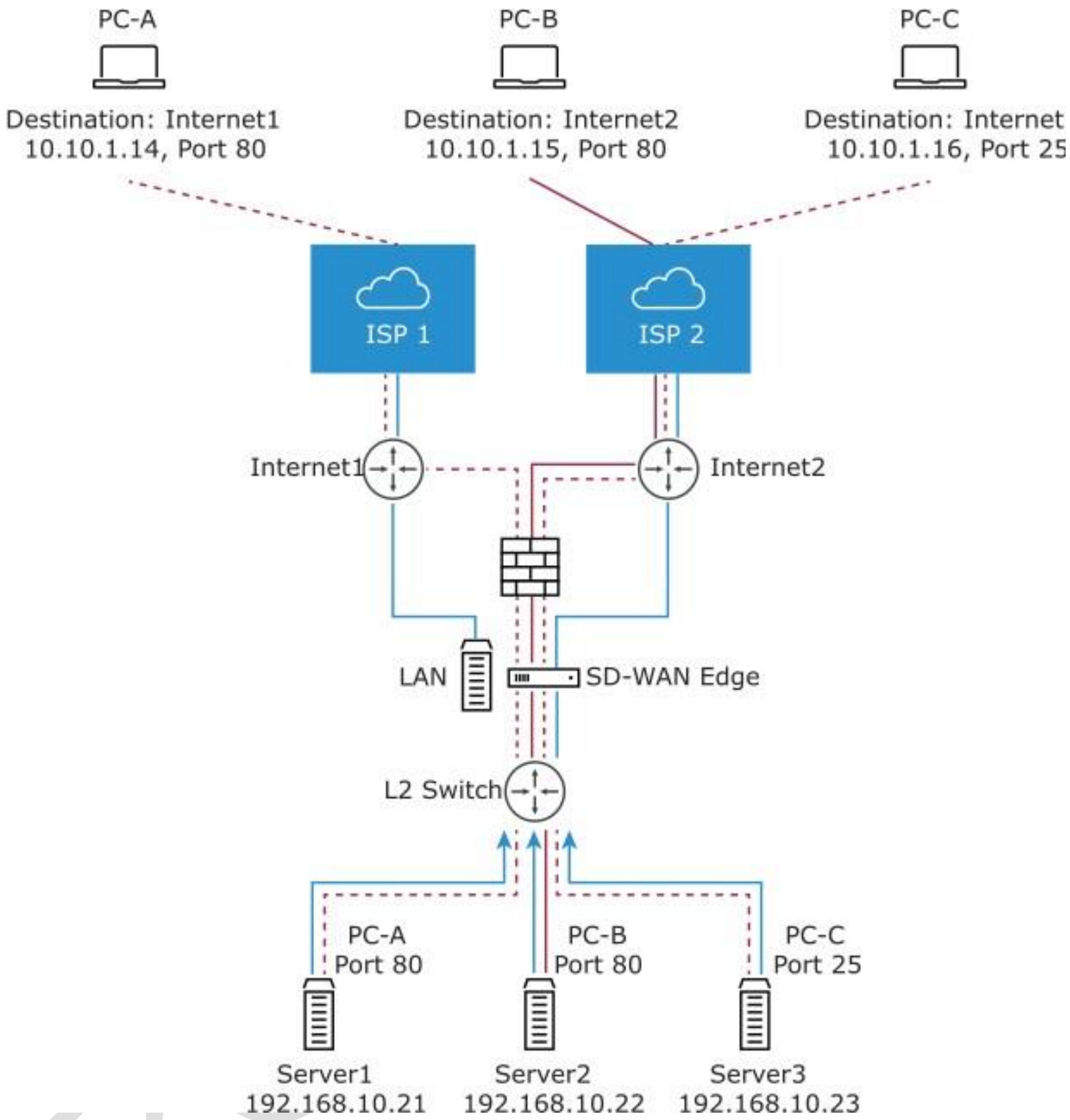
9 Select the **Log** check box to activate logging for this rule.

10 Click **Save Changes**.

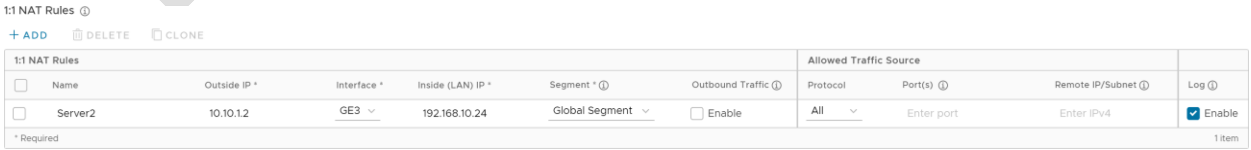
1:1 NAT Settings

These are used to map an Outside IP address supported by the SD-WAN Edge to a server connected to an Edge LAN interface (for example, a web server or a mail server). It can also translate outside IP addresses in different subnets than the WAN interface address if the ISP routes traffic for the subnet towards the SD-WAN Edge. Each mapping is between one IP address outside the firewall for a specific WAN interface and one LAN IP address inside the firewall. Within each mapping, you can specify which ports will be forwarded to the inside IP address. The **'+'** icon on the right can be used to add additional 1:1 NAT settings.

The following figure illustrates the 1:1 NAT configuration.



In the **1:1 NAT Rules** section, you can configure 1:1 NAT rules with IPv4 address or IPv6 address by clicking the **+Add** button and then entering the following details.



1:1 NAT Rules							Allowed Traffic Source			
□	Name	Outside IP *	Interface *	Inside (LAN) IP *	Segment * ⓘ	Outbound Traffic ⓘ	Protocol	Port(s) ⓘ	Remote IP/Subnet ⓘ	Log ⓘ
□	Server2	10.10.1.2	GE3	192.168.10.24	Global Segment	□ Enable	All	Enter port	Enter IPv4	☑ Enable

* Required

1 item

1 In the **Name** text box, enter a name for the rule.

Configure Firewall Rule

You can configure Firewall rules at the Profile and Edge levels to allow, drop, reject, or skip inbound and outbound traffic. If stateful firewall feature is activated, the firewall rule will be validated to filter both inbound and outbound traffic. With stateless firewall, you can control to filter only outbound traffic. The firewall rule matches parameters such as IP addresses, ports, VLAN IDs, Interfaces, MAC addresses, domain names, protocols, object groups, applications, and DSCP tags. When a data packet matches the match conditions, the associated action or actions are taken. If a packet matches no parameters, then a default action is taken on the packet.

To configure a firewall rule at the Profile level, perform the following steps.

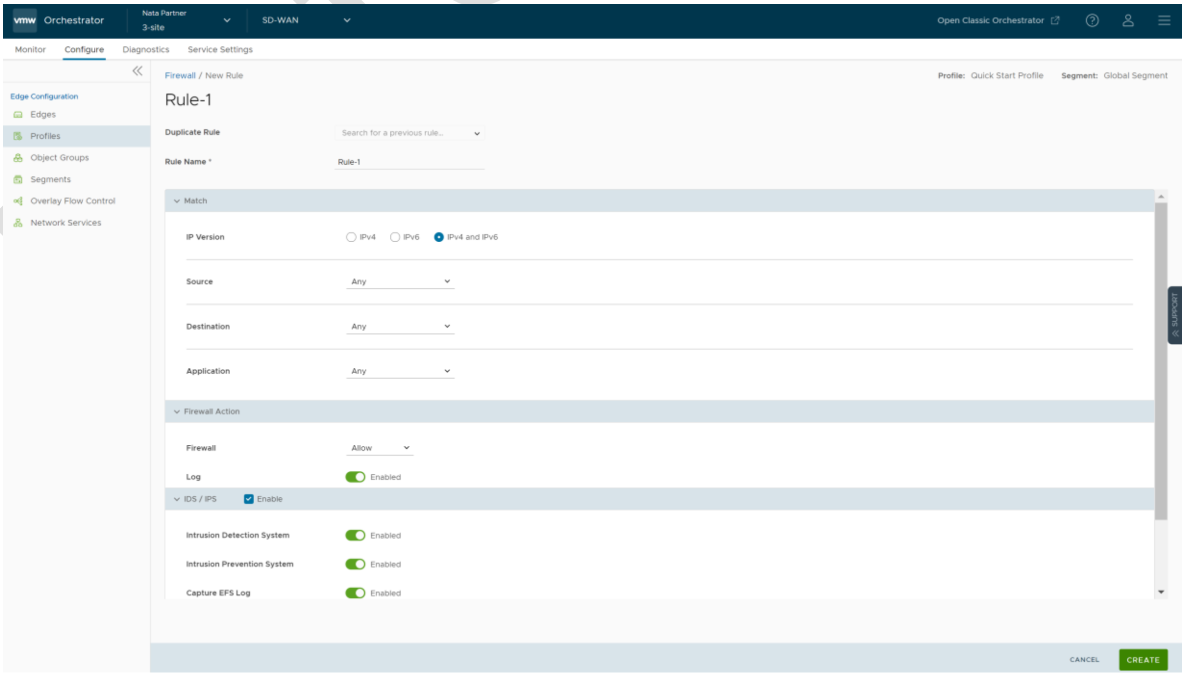
Procedure

1 In the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.

2 Select a Profile to configure a firewall rule, and click the **Firewall** tab.

From the **Profiles** page, you can navigate to the **Firewall** page directly by clicking the **View** link in the **Firewall** column of the Profile.

3 Go to the **Configure Firewall** section and under **Firewall Rules** area, click **+ NEW RULE**. The **Configure Rule** dialog box appears.



Profile: Quick Start Profile Segment: Global Segment

Rule-1

Duplicate Rule: Search for a previous rule...

Rule Name *: Rule-1

Match

IP Version: ○ IPv4 ○ IPv6 ● IPv4 and IPv6

Source: Any

Destination: Any

Application: Any

Firewall Action

Firewall: Allow

Log: Enabled

IDS / IPS ☑ Enable

Intrusion Detection System: Enabled

Intrusion Prevention System: Enabled

Capture EFS Log: Enabled

4 In the **Rule Name** text box, enter a unique name for the Rule. To create a firewall rule from an existing rule, select the rule to be duplicated from the **Duplicate Rule** drop-down menu.

5 In the **Match** section, configure the match conditions for the rule:

Field	Description
IP Version	By default, IPv4 and IPv6 address type is selected. You can configure the Source and Destination IP addresses according to the selected Address Type, as follows: ■ **IPv4** – Allows to configure only IPv4 addresses as Source and Destination. ■ **IPv6** – Allows to configure only IPv6 addresses as Source and Destination. ■ **IPv4 and IPv6** – Allows to configure both IPv4 and IPv6 addresses in the matching criteria. If you choose this mode, you cannot configure Source or Destination IP address. **Note** When you upgrade, the firewall rules from previous versions are moved to IPv4 mode.
Source	Allows to specify the source for packets. Select any of the following options: ■ **Any** - Allows all source addresses by default. ■ **Object Group** - Allows you to select a combination of address group and service group. **Note** If the selected address group contains any domain names, then they would be ignored when matching for the source. ■ **Define** - Allows you to define the source traffic to a specific VLAN, Interface, IPv4 or IPv6 Address, MAC Address, or Transport Port. Select one of the following options: ■ **VLAN** - Matches traffic from the specified VLAN, selected from the drop-down menu. ■ **Interface and IP Address** - Matches traffic from the specified interface and IPv4 or IPv6 address, selected from the drop-down menu. **Note** If an interface cannot be selected, then the interface is either not activated or not assigned to this segment. **Note** If you select **IPv4 and IPv6** (Mixed mode) as the Address Type, then the traffic is matched based on only the specified interface. Along with the IP address, you can specify one of the following address types to match the source traffic: ■ **CIDR prefix** - Choose this option if you want the network defined as a CIDR value (for

example: `172.10.0.0 /16`).

Field	Description
	■ **Subnet mask** - Choose this option if you want the network defined based on a Subnet mask (for example, `172.10.0.0 255.255.0.0`). ■ **Wildcard mask** - Choose this option if you want the ability to narrow the enforcement of a policy to a set of devices across different IP subnets that share a matching host IP address value. The Wildcard mask matches an IP, or a set of IP addresses based on the inverted Subnet mask. A '0' within the binary value of the mask means the value is fixed and a '1' within the binary value of the mask means the value is wild (can be 1 or 0). For example, a Wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111) with an IP Address of 172.0.0, the first three octets are fixed values, and the last octet is a variable value. This option is available only for IPv4 address. ■ **Mac Address** - Matches traffic based on the specified MAC address. ■ **Transport Port** - Matches traffic from the specified source port or port range.

Field	Description
Destination	Allows to specify the destination for packets. Select any of the following options: ■ **Any** - Allows all destination addresses by default. ■ **Object Group** - Allows you to select a combination of address group and service group. ■ **Define** - Allows you to define the destination traffic to a specific VLAN, Interface, IPv4 or IPv6 Address, Domain Name, Protocol, or Port. Select one of the following options: ■ **VLAN** - Matches traffic from the specified VLAN, selected from the drop-down menu. ■ **Interface** - Matches traffic from the specified interface, selected from the drop-down menu. **Note** If an interface cannot be selected, then the interface is either not activated or not assigned to this segment. ■ **IP Address** - Matches traffic for the specified IPv4 or IPv6 address and Domain name. **Note** If you select **IPv4 and IPv6** (Mixed mode) as the Address Type, then you cannot specify IP address as the destination. Along with the IP address, you can specify one of the following address types to match the source traffic: **CIDR prefix**, **Subnet mask**, or **Wildcard mask**. Use the **Domain Name** field to match the entire domain name or a portion of the domain name. For example, \"salesforce\" will match traffic to \"mixe\". ■ **Transport** - Matches traffic from the specified source port or port range. **Protocol** - Matches traffic for the specified protocol, selected from the drop-down menu. The supported protocols are GRE, ICMP, TCP, and UDP. **Note** ICMP is not supported in Mixed mode (IPv4 and IPv6).
Application	Select any of the following options: ■ **Any** - Applies the firewall rule to any application by default.

Field	Description
	■ **Define** - Allows to select an application and Differentiated Services Code Point (DSCP) flag to apply a specific firewall rule. **Note** When creating firewall rules matching an application, the firewall depends on the DPI (Deep Packet Inspection) Engine to identify the application to which a particular flow belongs. Generally, the DPI will not be able to determine the application based on the first packet. The DPI Engine usually needs the first 5-10 packets in the flow to identify the application, but the firewall needs to classify and forward the flow from the very first packet. This may cause the first flow to match a more generalized rule in the firewall list. Once the application has been correctly identified, any future flows matching the same tuples will be reclassified automatically and hit the correct rule.

6 In the **Action** section, configure the actions to be performed when the traffic matches the defined criteria.

Field	Description
Firewall	Select any of the following action the firewall should perform on packets, when the conditions of the rule are met: ■ **Allow** - Allows the data packets by default. ■ **Drop** - Drops the data packets silently without sending any notification to the source.
Log	Select this checkbox if you want a log entry to be created when this rule is triggered.

7 Select the **IDS/IPS** checkbox and activate either IDS or IPS toggle to create the Firewall. When user activates only IPS, IDS will be automatically activated. EFS engine inspects traffic sent/received through the Edges and matches content against signatures configured in the EFS engine. IDS/IPS Signatures are updated on a continuous basis with a valid EFS license. For more information about EFS, see Enhanced Firewall Services Overview.

Note EFS can be activated in the rule only if the Firewall action is **Allow**. If the Firewall action is anything other than **Allow**, EFS will be deactivated.

- **Intrusion Detection System** - When IDS is activated on Edges, the Edges detect if the traffic flow is malicious or not based on certain signatures configured in the engine. If attack is detected, the EFS engine generates an alert and sends the alert message to SD-WAN Orchestrator/Syslog Server if Firewall logging is activated in Orchestrator, and will not drop any packets.
- **Intrusion Prevention System** - When IPS is activated on Edges, the Edges detect if the traffic flow is malicious or not based on certain signatures configured in the engine. If

Enhanced Firewall Services

This section provides details about how to configure and monitor Enhanced Firewall Services (EFS).

Enhanced Firewall Services Overview

Enhanced Firewall Services (EFS) service provides additional EFS security functionalities on VMware SD-WAN Edges. The NSX Security powered EFS functionality supports Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) services on VMware SD-WAN Edges. The Edge Firewall EFS protect Edge traffic from intrusions across Branch to Branch, Branch to Hub, or Branch to Internet traffic patterns.

Currently, SD-WAN Edge Firewall provides stateful inspection along with application identification without additional EFS security features. While the stateful Firewall SD-WAN Edge provides security, it is not adequate and creates a gap in providing EFS security integrated natively with VMware SD-WAN. Edge EFS address these security gaps and offers enhanced firewall services natively on the SD-WAN Edge in conjunction with VMware SD-WAN.

Customer can configure and manage the EFS using the Firewall functionality in VMware SD-WAN Orchestrator.

Limitations

- When EFS is activated, only static addressing is supported. Do not use the Dynamic address on LAN networks such as DHCPv4 Client, DHCPv6 Client, DHCPv6 PD, and IPv6 SLAAC.

If the dynamic addressing is used and the address range is outside the private address range in case of IPv4 and ULA address range in case of IPv6 described in RFC1918, rule matching might not happen due to the address not being part of HOME_NETWORK setting in suricata.yaml.

Configure Enhanced Firewall Services

Customers can configure and manage the Enhanced Firewall Services (EFS) using the Firewall functionality in VMware SD-WAN Orchestrator

Before You Begin

For the EFS feature to work:

- Ensure the Edge version is upgraded to 5.2.0.0.
- Ensure the EFS feature is activated at the Enterprise level. Contact your Operator if you would want the EFS feature to be activated. An Operator can activate the EFS feature from the **SD-WAN** > **Global Settings** > **Customer Configuration** > **SD-WAN Settings** > **Feature**

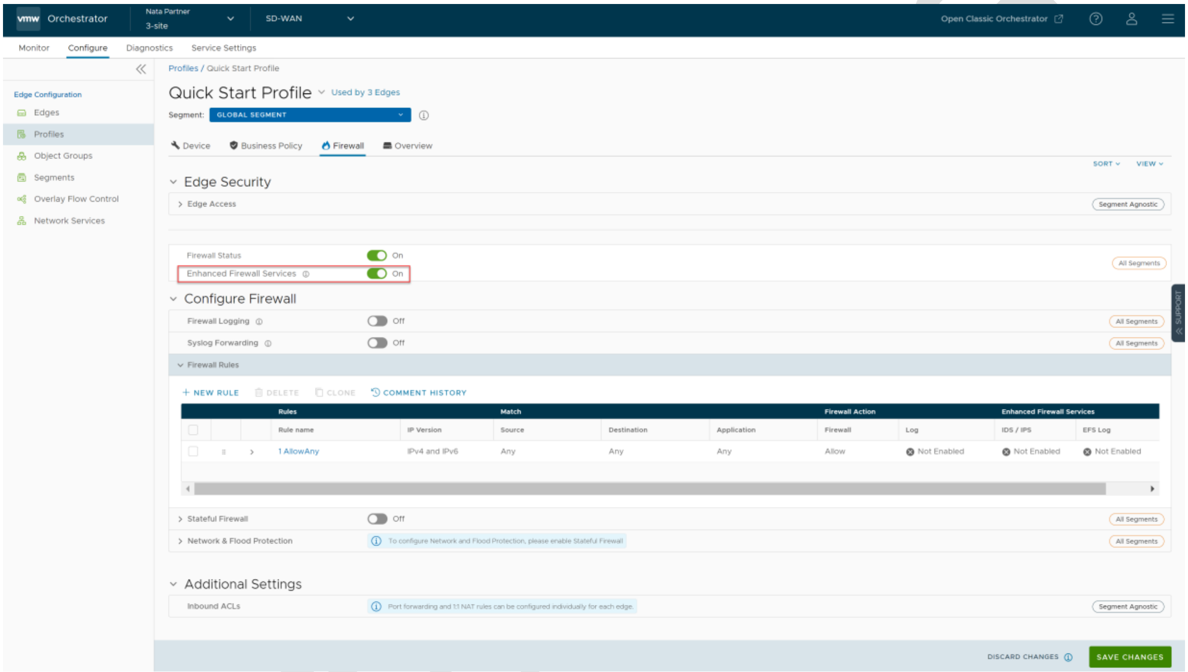
Access UI page.

Configure EFS Rule Settings at the Profile Level

1 In the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.

2 To configure a Profile Firewall, click the link to the Profile and then click the **Firewall** tab. Alternatively, you can also click the **View** link in the **Firewall** column of the Profile.

3 The **Firewall** page appears.



Quick Start Profile

Segment: GLOBAL SEGMENT

Edge Security

Edge Access — Segment Agnostic

Firewall Status — On

Enhanced Firewall Services — On — All Segments

Configure Firewall

Firewall Logging — Off — All Segments

Syslog Forwarding — Off — All Segments

Firewall Rules

Rules				Match				Firewall Action		Enhanced Firewall Services	
□			Rule name	IP Version	Source	Destination	Application	Firewall	Log	IDS / IPS	EFS Log
□	≡	›	1 AllowAny	IPv4 and IPv6	Any	Any	Any	Allow	⊗ Not Enabled	⊗ Not Enabled	⊗ Not Enabled

Stateful Firewall — Off — All Segments

Network & Flood Protection — To configure Network and Flood Protection, please enable Stateful Firewall — All Segments

Additional Settings

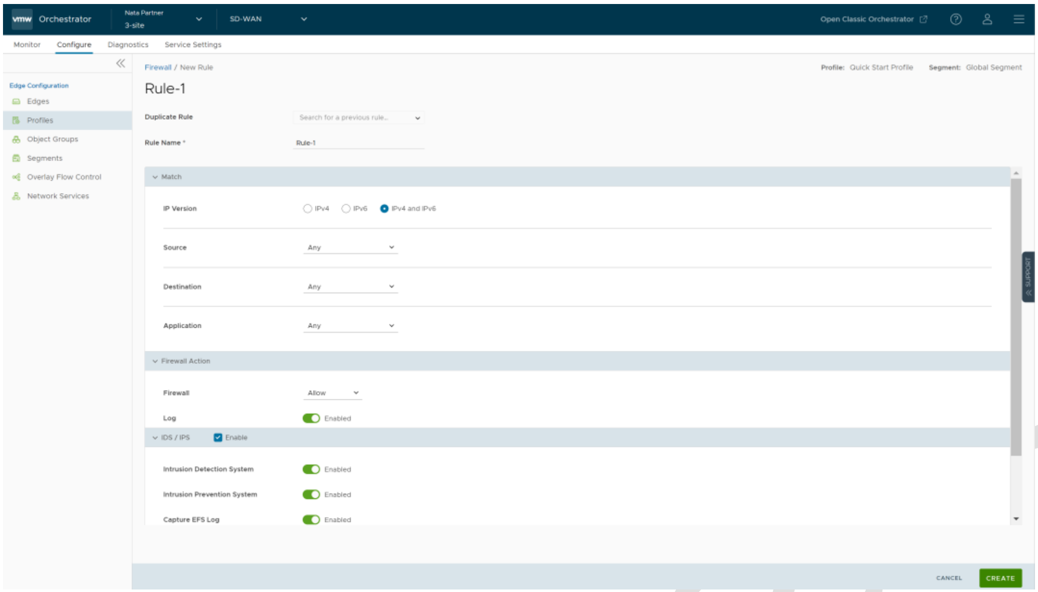
Inbound ACLs — Port forwarding and 1:1 NAT rules can be configured individually for each edge. — Segment Agnostic

4 Turn ON the **Enhanced Firewall Services** toggle button to activate the EFS feature for all Edges associated with the Profile. By default, this feature is not activated.

5 Under **Firewall Rules**, you can create a new EFS rule or modify an existing firewall rule for EFS settings.

- To create a new EFS rule:

  1 Click the **+ New Rule** button.



Profile: Quick Start Profile   Segment: Global Segment

Rule-1

Duplicate Rule: Search for a previous rule...

Rule Name *: Rule-1

Match

IP Version: ○ IPv4 ○ IPv6 ● IPv4 and IPv6

Source: Any

Destination: Any

Application: Any

Firewall Action

Firewall: Allow

Log: Enabled

IDS / IPS ☑ Enable

Intrusion Detection System: Enabled

Intrusion Prevention System: Enabled

Capture EFS Log: Enabled

2 In the **Rule Name** text box, enter a unique name for the Rule. To create a firewall rule from an existing rule, select the rule to be duplicated from the **Duplicate Rule** drop-down menu.

3 Configure the **Match** conditions and **Firewall Actions** to be performed when the traffic matches the defined match criteria. For more information, see Configure Firewall Rule.

4 Select the **IDS/IPS** checkbox and activate either IDS or IPS toggle to create the Firewall. When user activates only IPS, IDS will be automatically activated. EFS engine inspects traffic sent/received through the Edges and matches content against signatures configured in the EFS engine.

Note EFS can be activated in the rule only if the Firewall action is **Allow**. If the Firewall action is anything other than **Allow**, EFS will be deactivated.

- **Intrusion Detection System** - When IDS is activated on Edges, the Edges detect if the traffic flow is malicious or not based on certain signatures configured in the engine. If attack is detected, the EFS engine generates an alert and sends the alert message to SD-WAN Orchestrator/Syslog Server if Firewall logging is activated in Orchestrator, and will not drop any packets.

- **Intrusion Prevention System** - When IPS is activated on Edges, the Edges detect if the traffic flow is malicious or not based on certain signatures configured in the engine. If attack is detected, the EFS engine generates an alert and blocks the traffic flow to the client only if the signature rule has action as "Reject", matched by the malicious traffic. If the action in the signature rule is "Alert", the traffic will be allowed without dropping any packets even if you configure IPS.

Note VMware recommends customer to not activate VNF when IDS/IPS is activated on Edges.

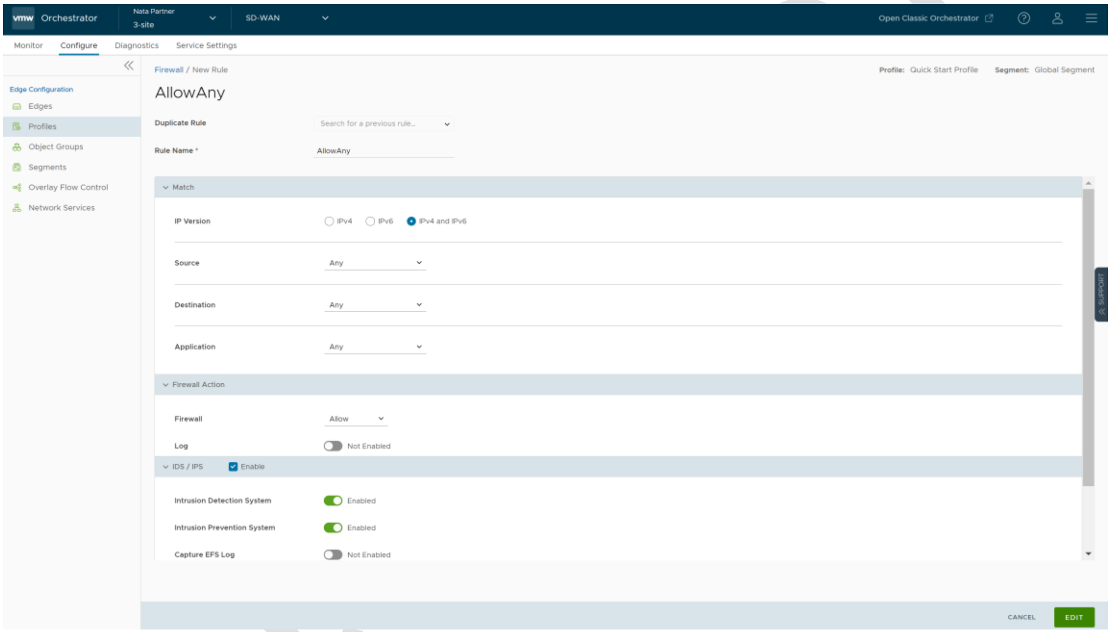
5 To send the EFS logs to Orchestrator, turn on the **Capture EFS Log** toggle button.

> **Note** For an Edge to send the Firewall logs to Orchestrator, ensure that the “Enable Firewall Logging to Orchestrator” customer capability is activated at the Customer level under “Global Settings” UI page. Customers must contact your Operator if you would want the Firewall Logging feature to be activated.

    6. Click **Create**.

- To modify an existing firewall rule for EFS settings:

    1. Under the **Firewall Rules** area of the **Profile Firewall** page, click the link under the **Rule name** column of an existing firewall to be modified.
    2. Modify the **IDS/IPS** settings and click **Edit**.



Firewall / New Rule

Profile: Quick Start Profile Segment: Global Segment

AllowAny

Duplicate Rule: Search for a previous rule...

Rule Name *: AllowAny

Match

IP Version: ○ IPv4 ○ IPv6 ● IPv4 and IPv6

Source: Any

Destination: Any

Application: Any

Firewall Action

Firewall: Allow

Log: Not Enabled

IDS / IPS ☑ Enable

Intrusion Detection System: Enabled

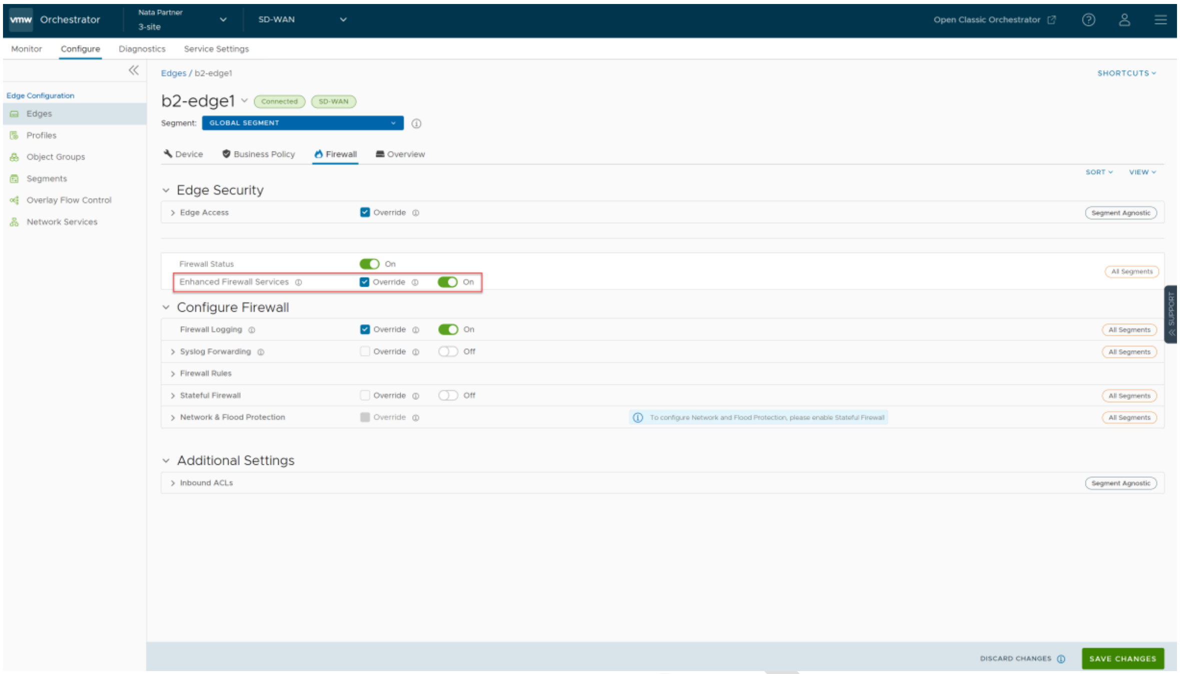
Intrusion Prevention System: Enabled

Capture EFS Log: Not Enabled

6. Click **Save Changes**.

Configure EFS Rule Settings at the Edge Level

1. In the Enterprise portal, go to **Configure > Edges**. The **Edges** page displays the existing Edges.
2. To configure an Edge, click the link to the Edge or click the **View** link in the **Firewall** column of the Edge.
3. Click the **Firewall** tab.



b2-edge1

Segment: GLOBAL SEGMENT

Edge Security

Edge Access	☑ Override		Segment Agnostic
Firewall Status		On	All Segments
Enhanced Firewall Services	☑ Override	On	

Configure Firewall

Firewall Logging	☑ Override	On	All Segments
Syslog Forwarding	□ Override	Off	All Segments
Firewall Rules			
Stateful Firewall	□ Override	Off	All Segments
Network & Flood Protection	□ Override	To configure Network and Flood Protection, please enable Stateful Firewall	All Segments

Additional Settings

Inbound ACLs	Segment Agnostic

4 To override the inherited EFS settings for a specific Edge, select the **Override** checkbox and turn on the toggle button next to the **Enhanced Firewall Services** UI label.

5 Under **Firewall Rules** area of the **Edge Firewall** page, you can create a new EFS rule or override the inherited EFS rule settings for the Edge. Follow the procedure as described in the Step 5 of the Configure EFS Rule Settings at the Profile Level section.

6 After you have overridden the EFS rule settings, click **Save Changes**.

Note Firewall rules of the existing Edges that are not upgraded to the 5.2.0 release will not have any impact when you activate the EFS service at the global setting level or per rule level with IDS/IPS.

Monitor Enhanced Firewall Services Threats

You can monitor Enhanced Firewall Services (EFS) Threats based on the metrics collected using the EFS Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) for a specific Edge or an Enterprise.

Note The monitoring pages related to EFS will only be visible if the EFS feature is activated in Global Settings.

Monitor EFS - Edge View

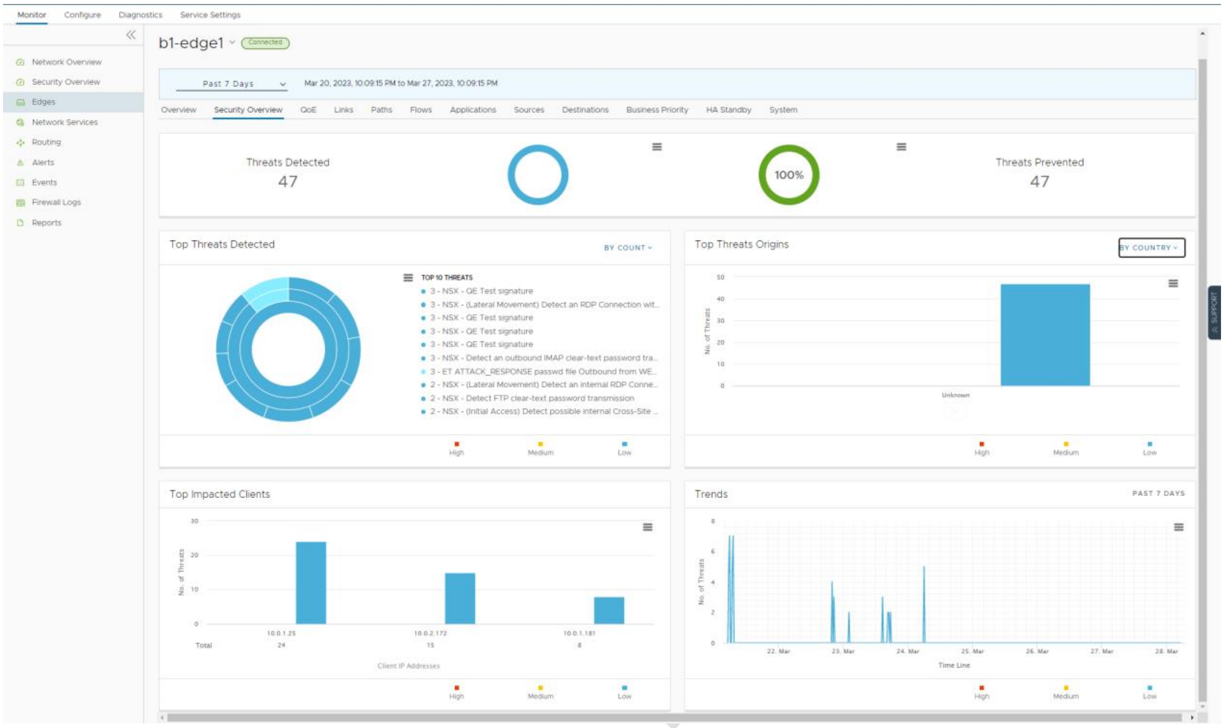
To view the EFS Threats details for a specific Edge:

1 In the Enterprise portal, click **Monitor** > **Edges**. The list of Edges associated with the Enterprise appears.

2 Select an Edge by clicking the link to an Edge. The **Network Overview** page (default page view) appears.

3 Click the **Security Overview** tab.

The **Security Overview** page appears. In addition, you can select the time frame for the overview page by 12 hours, 24 hours, and so on.



The **Security Overview** page is a graphical representation of cumulative data of the following EFS Threats details, based on the metrics collected using the EFS (IDS/IPS) for the selected Edge.

- Total count of Threats Detected
- Total count of Threats Prevented
- Top Threats Detected filtered "By Count" (Default) or "By Impact"
- Top Threat Origins filtered By "IP Address" (Default) or "By Country"
- Top Impacted Clients filtered By "IP Address" (Default) or "By Country"
- Histogram Trend of Threats for selected time frame.

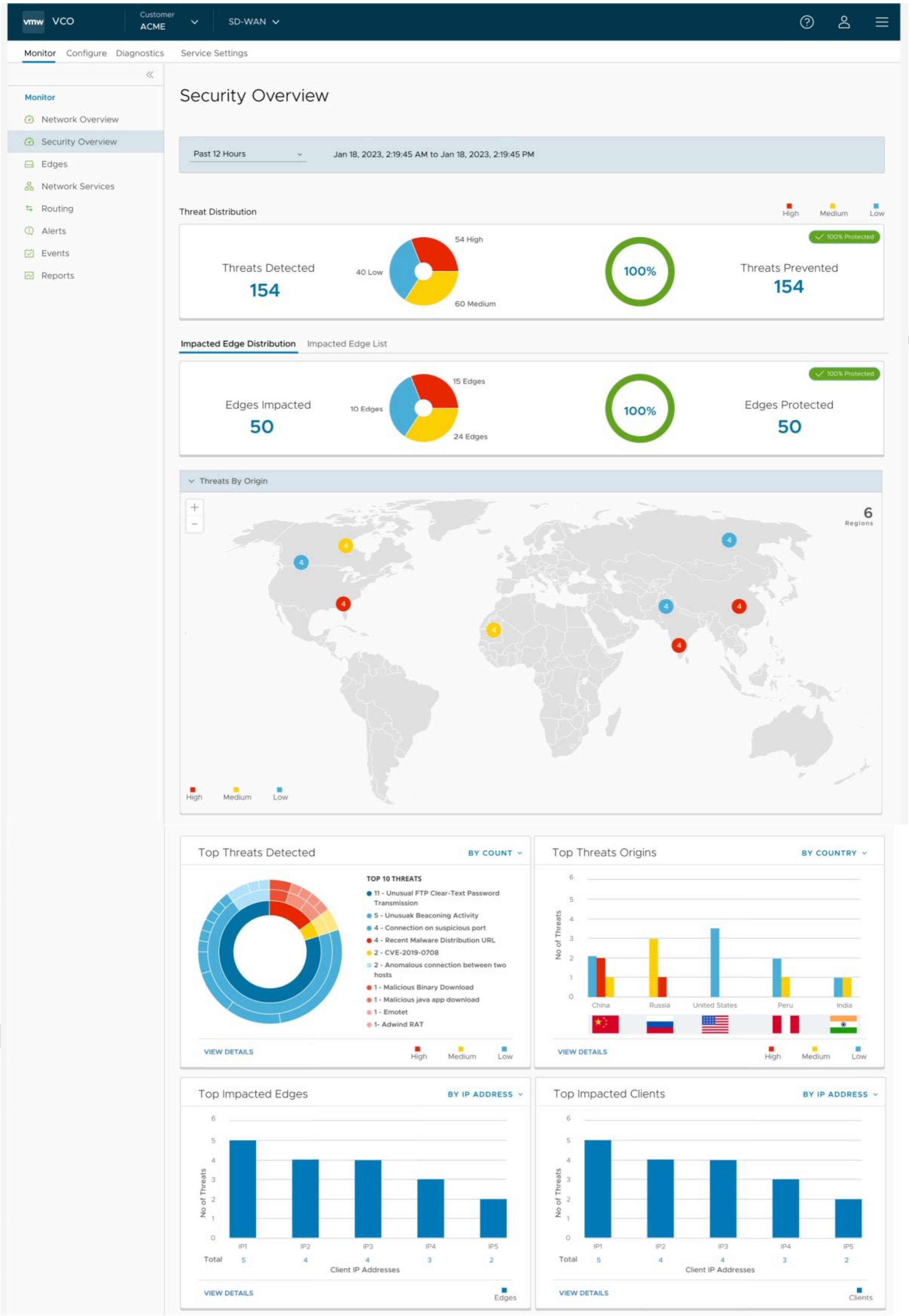
Under each graphical representation, clicking the **View Details** link displays detailed EFS information for the selected Edge, based on the selected metric type.

Monitor EFS - Enterprise View

To view the EFS Threats details for an Enterprise, click **Monitor** > **Security Overview**.

The **Security Overview** page is a graphical representation of Threat distribution based on the metrics collected using the EFS (IDS/IPS) for all Edges within an Enterprise. You can view the Threat distribution of all the Edges using the following two views:

- **Impacted Edge Distribution** – Represents a map view of all the EFS Impacted Edges (by severity) and Protected Edges. The page graphically displays the following EFS Threats details for an Enterprise:
  - Total count of Edges Impacted
  - Total count of Edges Protected
  - Top Threats Detected filtered "By Count" (Default) or "By Impact"
  - Top Threat Origins filtered By "IP Address" (Default) or "By Country"
  - Top Impacted Edges filtered By "IP Edge Name" (Default) or "IP Address"
  - Top Impacted Clients filtered By "IP Address" (Default) or "By Country"



Security Overview

Past 12 Hours

Jan 18, 2023, 2:19:45 AM to Jan 18, 2023, 2:19:45 PM

Threat Distribution

Threats Detected 154

Threats Prevented 154

Impacted Edge Distribution

Impacted Edge List

Edges Impacted 50

Edges Protected 50

Threats By Origin

Top Threats Detected

BY COUNT

TOP 10 THREATS

- 11 - Unusual FTP Clear-Text Password Transmission
- 5 - Unusuak Beaconing Activity
- 4 - Connection on suspicious port
- 4 - Recent Malware Distribution URL
- 2 - CVE-2019-0708
- 2 - Anomalous connection between two hosts
- 1 - Malicious Binary Download
- 1 - Malicious java app download
- 1 - Emotet
- 1- Adwind RAT

Top Threats Origins

BY COUNTRY

Top Impacted Edges

BY IP ADDRESS

	IP1	IP2	IP3	IP4	IP5
Total	5	4	4	3	2

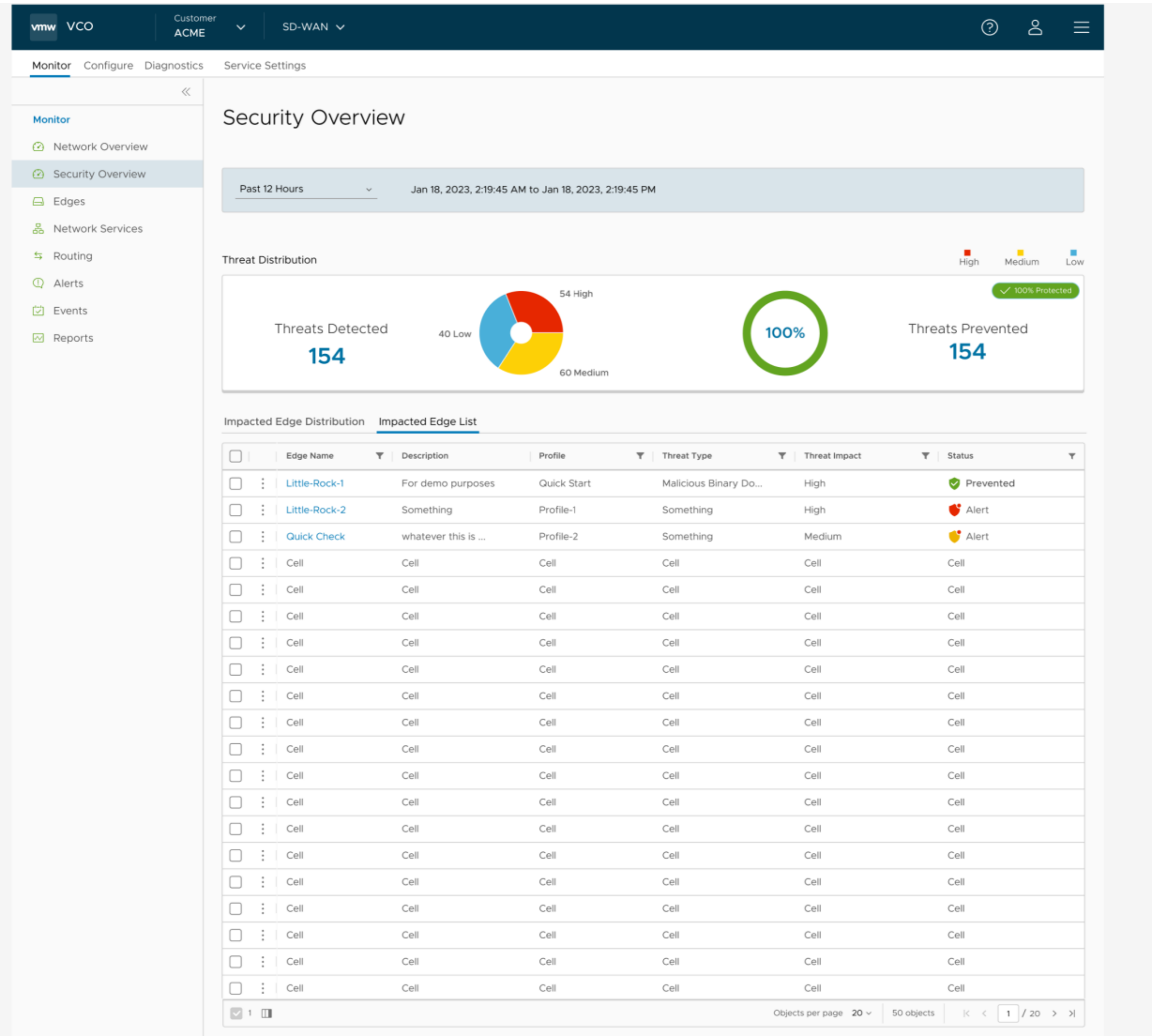
Top Impacted Clients

BY IP ADDRESS

	IP1	IP2	IP3	IP4	IP5
Total	5	4	4	3	2

- **Impacted Edge List** – Represents a tabular view of all the EFS impacted Edges along with

Threat details. The page displays the following details: Name and Description of the impacted Edge, Name of the Profile to which the impacted Edge is associated with, Threat Type, Threat Impact on Edge, and Status of impacted Edge.



Security Overview

Past 12 Hours Jan 18, 2023, 2:19:45 AM to Jan 18, 2023, 2:19:45 PM

Threat Distribution

Threats Detected 154

Threats Prevented 154

□		Edge Name	Description	Profile	Threat Type	Threat Impact	Status
□	⋮	Little-Rock-1	For demo purposes	Quick Start	Malicious Binary Do...	High	✓ Prevented
□	⋮	Little-Rock-2	Something	Profile-1	Something	High	Alert
□	⋮	Quick Check	whatever this is ...	Profile-2	Something	Medium	Alert
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell
□	⋮	Cell	Cell	Cell	Cell	Cell	Cell

☑ 1 Objects per page 20 50 objects 1 / 20

Enhanced Firewall Services Alerts and Events

Describes details about Enhanced Firewall Services (EFS) related Enterprise and Operator Orchestrator events.

Enterprise-level EFS Events

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
MGD_ATPUP_INVALID_IDPS_SIGNA	MGD_ATPUP_INVALID_IDPS_SIGNATURE	ERROR	SD-WAN Edge (MGD)	Generated when there is an invalid	5.2	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
TURE				suricata package.		
MGD_ATPUP_DOWNLOAD_IDPS_SIGNATURE_FAILED	MGD_ATPUP_DOWNLOAD_IDPS_SIGNATURE_FAILED	ERROR	SD-WAN Edge (MGD)	Generated when downloading of suricata package fails.	5.2	
MGD_ATPUP_DECRYPT_IDPS_SIGNATURE_FAILED	MGD_ATPUP_DECRYPT_IDPS_SIGNATURE_FAILED	ERROR	SD-WAN Edge (MGD)	Generated when unpacking of suricata package fails.	5.2	
MGD_ATPUP_APPLY_IDPS_SIGNATURE_FAILED	MGD_ATPUP_APPLY_IDPS_SIGNATURE_FAILED	ERROR	SD-WAN Edge (MGD)	Generated due to error in applying Suricata files.	5.2	
MGD_ATPUP_APPLY_IDPS_SIGNATURE_SUCCEEDED	MGD_ATPUP_APPLY_IDPS_SIGNATURE_SUCCEEDED	INFO	SD-WAN Edge (MGD)	Generated when suricata files are successfully applied.	5.2	
MGD_ATPUP_STANDBY_UPDATE_START	MGD_ATPUP_STANDBY_UPDATE_START	INFO	SD-WAN Edge (MGD)	Generated when HA Standby update with new EFS IDPS Signature version is started.	5.2	
MGD_ATPUP_STANDBY_UPDATE_FAILED	MGD_ATPUP_STANDBY_UPDATE_FAILED	ERROR	SD-WAN Edge (MGD)	Generated when HA Standby update with new EFS IDP Signature version fails.	5.2	
MGD_ATPUP_STANDBY_UPDATED	MGD_ATPUP_STANDBY_UPDATED	INFO	SD-WAN Edge (MGD)	Generated when HA Standby update with new EFS IDPS Signature version is successfully applied.	5.2	

Operator-level EFS Events

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
IDPS_SIGNATURE_VCO_VERSION_CHECK_FAIL	Querying existing signature version from local DB failed	ERROR	SD-WAN Orchestrator	When SD-WAN Orchestrator backend poll job has failed to retrieve existing suricata signature version from Orchestrator's local database.	5.2.0	
IDPS_SIGNATURE_GSM_VERSION_CHECK_FAIL	Querying signature metadata from GSM failed	ERROR	SD-WAN Orchestrator	When SD-WAN Orchestrator backend poll job has failed to retrieve existing suricata signature metadata (that includes signature version) from GSM.	5.2.0	
IDPS_SIGNATURE_SKIP_DOWNLOAD_NO_UPDATE	Skipping signature download due to no change in signature version	INFO	SD-WAN Orchestrator	When SD-WAN Orchestrator backend poll job skips downloading suricata signature file due to no change in suricata signature file version.	5.2.0	

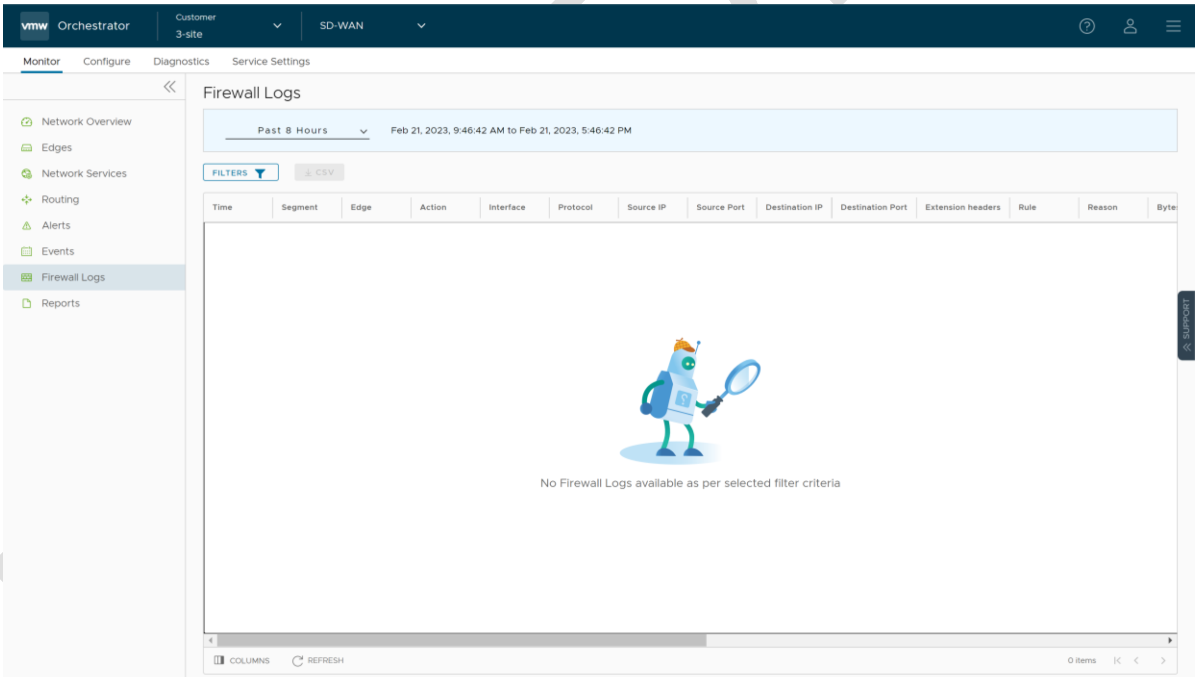
EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
IDPS_SIGNATURE_STORE_FAILURE_NO_PATH	Filestore path not set to store signature file	ERROR	SD-WAN Orchestrator	When SD-WAN Orchestrator backend poll job fails to store suricata signature file due to filestore path not being set.	5.2.0	
IDPS_SIGNATURE_DOWNLOAD_SUCCESS	Successfully downloaded signature file from GSM	INFO	SD-WAN Orchestrator	When SD-WAN Orchestrator backend poll job successfully downloads suricata signature file from GSM.	5.2.0	
IDPS_SIGNATURE_DOWNLOAD_FAILURE	Failed to download signature file from GSM	ERROR	SD-WAN Orchestrator	When SD-WAN Orchestrator backend poll job fails to download suricata signature file from GSM.	5.2.0	
IDPS_SIGNATURE_STORE_SUCCESS	Successfully stored the signature file in filestore	INFO	SD-WAN Orchestrator	When SD-WAN Orchestrator backend poll job successfully stores the suricata signature file in local file store.	5.2.0	
IDPS_SIGNATURE_STORE_SIGNATURE_FAILURE	Failed to store the signature file in filestore	ERROR	SD-WAN Orchestrator	When SD-WAN Orchestrator backend poll job fails to store the suricata signature file in local file store.	5.2.0	

Monitor Firewall Logs

The **Firewall Logs** page displays the details of firewall log originating from VMware SD-WAN Edges. By default, Edges cannot send their Firewalls logs to Orchestrator. For an Edge to send the Firewall logs to Orchestrator, ensure that the “**Enable Firewall Logging to Orchestrator**” customer capability is activated at the Customer level under “Global Settings” UI page. Customers must contact your Operator if you would want the Firewall Logging feature to be activated. By default, Orchestrator retains the Firewall logs until it reaches the maximum retention time of 7 days or maximum log size of 15 GB on a rotation basis.

To view the Edge Firewall logs in Orchestrator:

1 In the Enterprise portal, navigate to **Monitor** > **Firewall Logs**. The **Firewall Logs** page appears.



Firewall Logs

Past 8 Hours

Feb 21, 2023, 9:46:42 AM to Feb 21, 2023, 5:46:42 PM

Time	Segment	Edge	Action	Interface	Protocol	Source IP	Source Port	Destination IP	Destination Port	Extension headers	Rule	Reason	Byte

No Firewall Logs available as per selected filter criteria

The page displays the following Edge Firewall Log details: Time, Segment, Edge, Action, Interface, Protocol, Source IP, Source Port, Destination IP, Destination Port, Extension Headers, Rule, Reason, Bytes Received, Bytes Sent, Duration, Application, Destination Domain, Destination Name, Session ID, Signature, IPS Alert, IDS Alert, Signature ID, Category, Attack Source, Attack Target, and Severity.

Note Not all fields will be populated for all firewall logs. For example, Reason, Bytes Received/Sent and Duration are fields included in logs when sessions are closed. Signature, IPS Alert, IDS Alert, Signature ID, Category, Attack Source, Attach Target, and Severity are populated only for Enhanced Firewall Services (EFS) alerts, not for firewall logs.

Firewall Logs are generated:

- When a flow is created (on the condition that the flow is accepted)
- When the flow is closed
- When a new flow is denied
- When an existing flow is updated (due to a firewall configuration change)

EFS Alerts are generated:

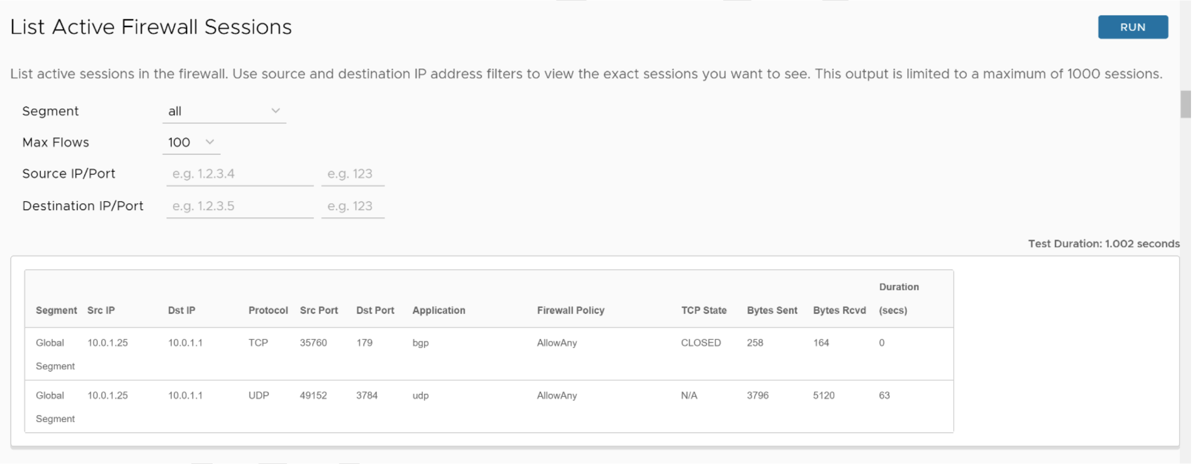
- Whenever the flow traffic matches any suricata signatures configured in the EFS engine.
- If firewall rule has only Intrusion Detection System (IDS) activated, the Edges detect if the traffic flow is malicious or not based on certain signatures configured in the engine. If attack is detected, the EFS engine generates an alert and sends the alert message to SD-WAN Orchestrator/Syslog Server if Firewall logging is activated in Orchestrator, and will not drop any packets.

Troubleshooting Firewall

You can collect the firewall diagnostic logs by running the remote diagnostic tests on an Edge.

For Edges running Release 3.4.0 or later which also have Stateful Firewall activated, you can use the following remote diagnostic tests to obtain firewall diagnostic information:

- **Flush Firewall Sessions** - Run this test on the required Edge by providing the Source and Destination IP addresses to flush the active firewalls session which needs to be reset. This is specifically for the Stateful Firewall. Running this test on an Edge not only flushes the firewall sessions, but actively send a TCP RST for the TCP-based sessions.
- **List Active Firewall Sessions** - Run this test to view the current state of the active firewall sessions (up to a maximum of 1000 sessions). You can filter by Source and Destination IP and Port as well as Segment to limit the number of sessions returned.



List Active Firewall Sessions

List active sessions in the firewall. Use source and destination IP address filters to view the exact sessions you want to see. This output is limited to a maximum of 1000 sessions.

Segment: all

Max Flows: 100

Source IP/Port: e.g. 1.2.3.4 e.g. 123

Destination IP/Port: e.g. 1.2.3.5 e.g. 123

Test Duration: 1.002 seconds

Segment	Src IP	Dst IP	Protocol	Src Port	Dst Port	Application	Firewall Policy	TCP State	Bytes Sent	Bytes Rcvd	Duration (secs)
Global Segment	10.0.1.25	10.0.1.1	TCP	35760	179	bgp	AllowAny	CLOSED	258	164	0
Global Segment	10.0.1.25	10.0.1.1	UDP	49152	3784	udp	AllowAny	N/A	3796	5120	63

Note You cannot see sessions that were denied as they are not active sessions. To troubleshoot those sessions, you will need to check the firewall logs.

For more information about how and when to run these remote diagnostics on an Edge, see VMware SD-WAN Troubleshooting guide available at https://docs.vmware.com/en/VMware-SD-WAN/index.html.