VMware Edge Enhanced Firewall Service (EFS) – IDS/IPS Beta Test Plan
Version 1.0

vmware

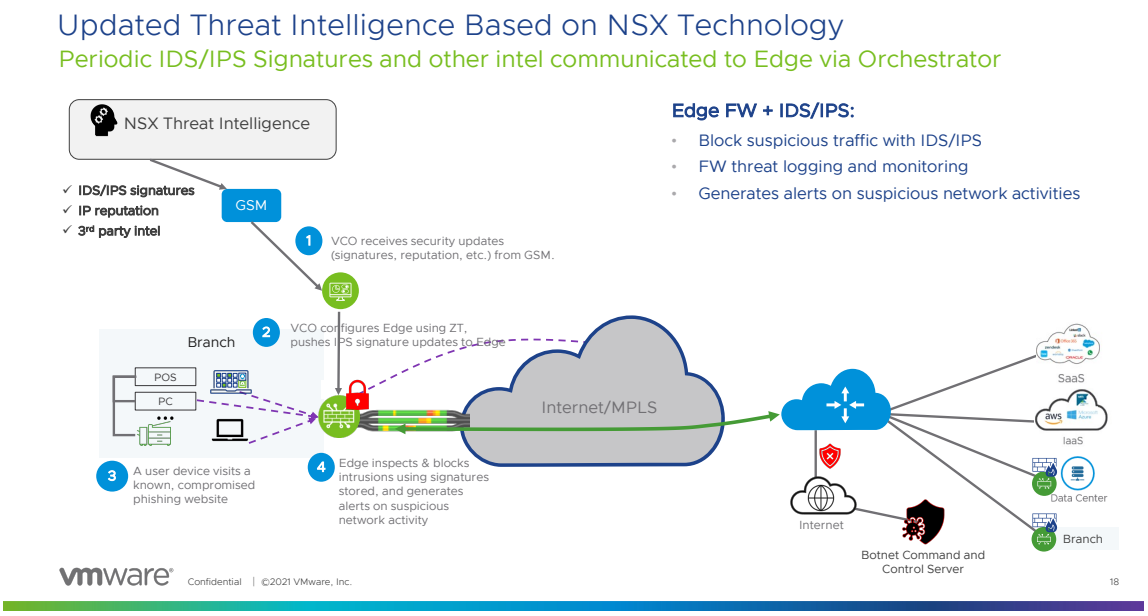
Contents

1. Overview

This document provides sample test cases to conduct a Beta Test for the VMware Edge Enhanced Firewall Service (EFS) - IDS/IPS.

This document does not cover test cases for existing Firewall features for example, Stateful Firewall or Network Flood Protection. The configuration and setup for existing firewall features is found at https://docs.vmware.com/en/VMware-SD-WAN/5.1/VMware-SD-WAN-Administration-Guide/GUID-0763C0A6-7E57-4C5B-A856-BBEC76344730.html

2. VMware Edge Enhanced Firewall Service Overview



VMware Edge EFS is a feature that extends the on-premise edge firewall capabilities to include Intrusion Detection and Prevention services. The IDS/IPS services protect edge traffic across Branch to Branch, Branch to Hub or Branch to Internet traffic patterns. If the traffic flow is detected as malicious, an alert will be logged and if IPS is enabled, the traffic will also be blocked.

3. Pre-requisites and Success Criteria

The following sections define pre-requisites, requirements and success criteria as agreed upon between customer and VMware.

Pre-requisites	Met? (Yes/No)
VMware edge activated to the Beta VCO	
Edge version is at least 5.2.0 release	
Laptops, PC connected to VMware edge	
Ensure the EFS feature is enabled at the Enterprise level. An Operator can activate the EFS feature from SD WAN -> Global Settings -> Customer Configuration -> SD-WAN settings.	

Ensure the Firewall Logging feature is enabled at the Enterprise level. An Operator can activate the Firewall Logging feature from SD WAN -> Global Settings -> Customer Configuration -> Global settings.	
With EFS enabled on the Edge, static LAN addressing must be configured for the IDS/IPS functionality to work.	

Success Criteria

Success Criteria	Met? Yes/No)
Edge EFS can **detect** intrusions and generate an alert in the firewall logs.	
Edge EFS can **prevent** intrusions and generate an alert in the firewall logs.	
Edge EFS can provide **visibility** into user traffic across their edges and enterprise	

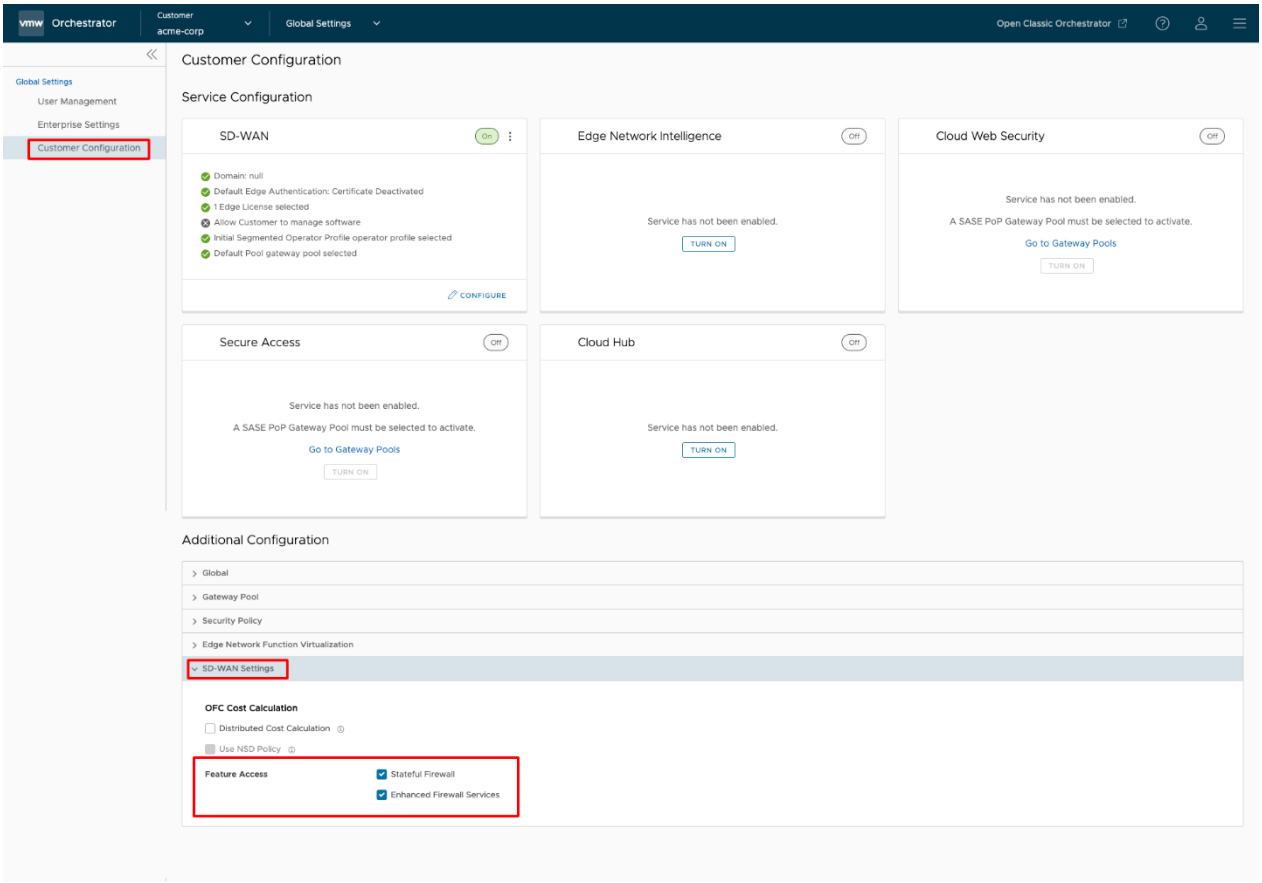
4. Edge EFS Configuration and Monitoring

The following section describes how to enable the Edge EFS and Firewall Logging configuration at the Enterprise level. This is normally done by the Operator user and for customers should be configured already before they start testing the Intrusion Detection and Prevention capabilities.

4.1 Enterprise Level: Enable Enhanced Firewall Services (EFS)

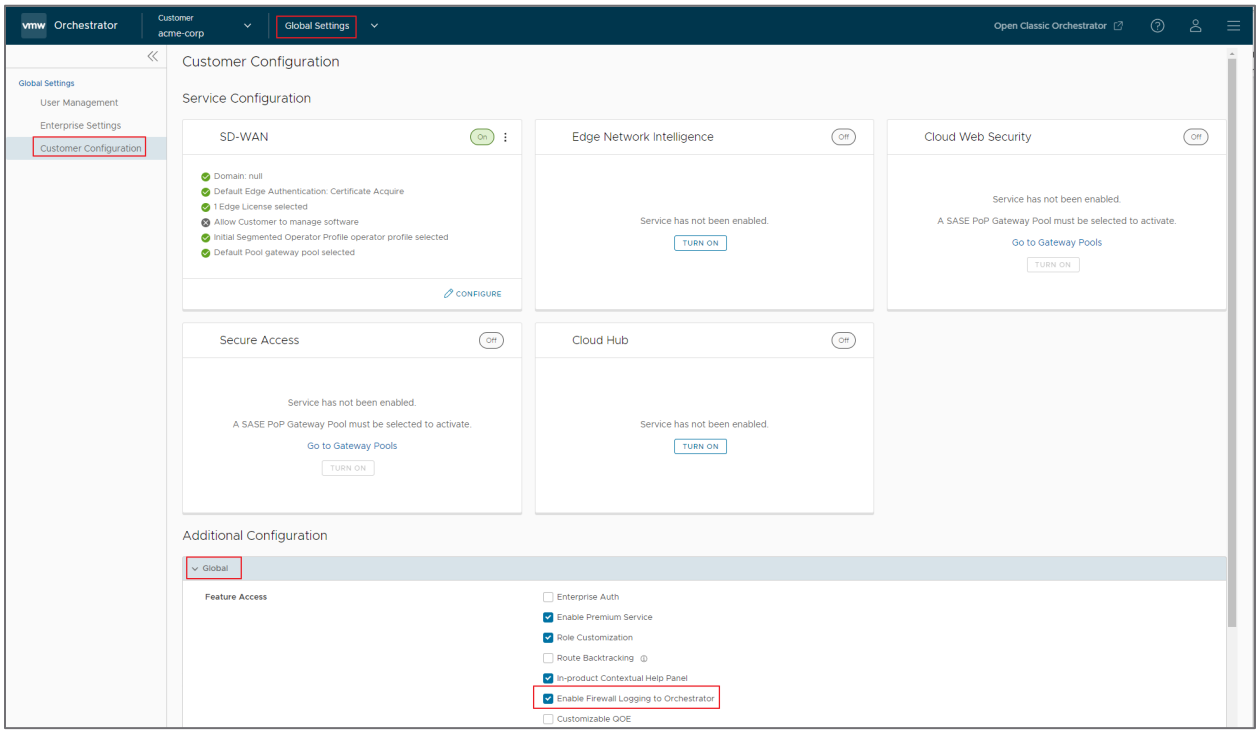
1. Login to the Beta VCO as operator user
2. For a specific Enterprise customer, go to **Global Settings -> Customer Configuration -> SD-WAN Settings**
3. Under the Feature Access section. Check and enable the **Enhanced Firewall Services**.

Note that Stateful Firewall checkbox is also enabled by default



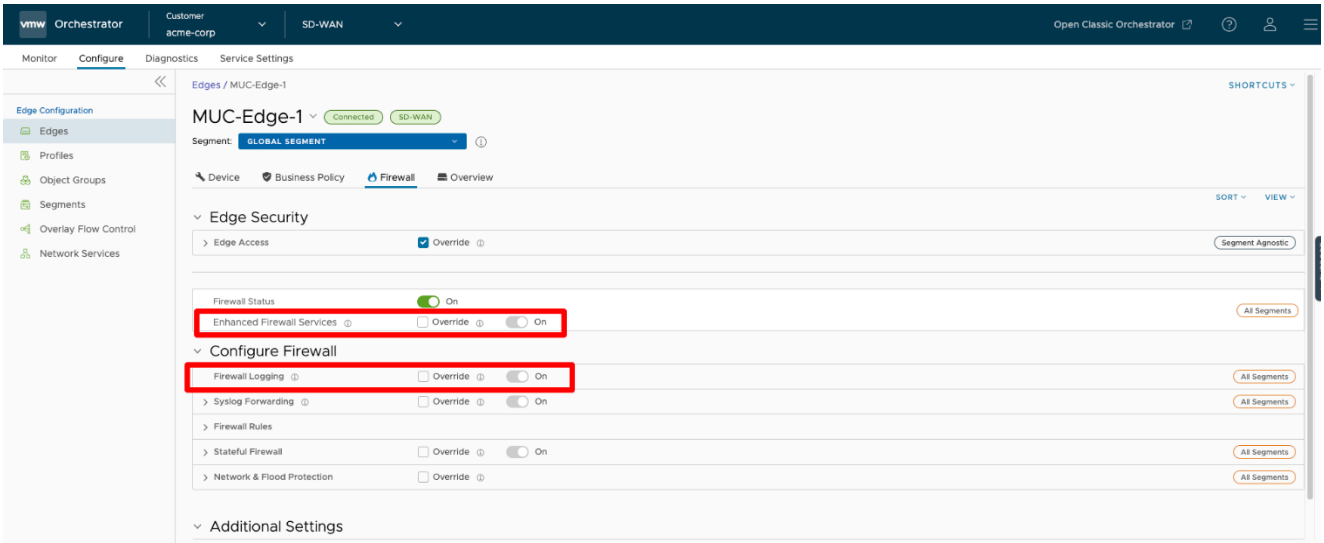
4.2 Enterprise Level: Enable Firewall Logging

1. Login to Beta VCO as Operator user
2. For a specific Enterprise customer, go to **Global Settings -> Customer Configuration -> Global**
3. Under the Feature Access section, Check and enable the **Enable Firewall Logging to Orchestrator**

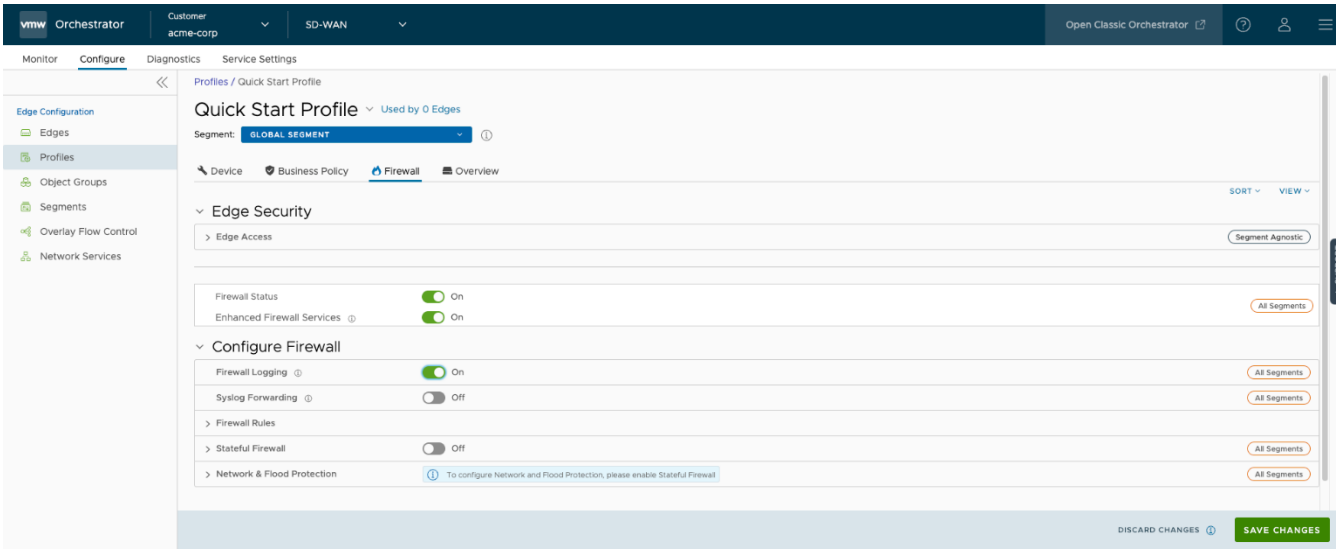


4.3 Configure Profile/Edge for Enhanced Firewall Services

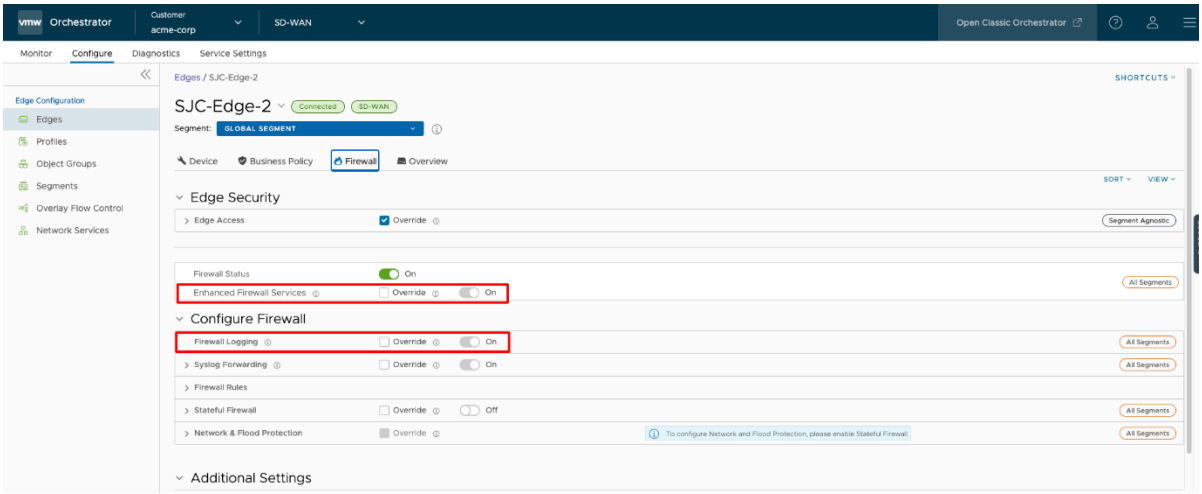
1. In the Enterprise portal SD-WAN page, Navigate to **Configure > Profile**. The Profiles page displays the existing Profiles.
2. To configure a **Profile**, click the link to an existing Profile or Add a new Profile.
3. Click the Firewall tab.
4. Enhanced Firewall Services is default set to disable. Toggle to enable it.
5. Firewall logging is default set to disable. When enabled, the default retention is 7 days or a maximum of 15Gb, whichever comes first. Toggle to enable monitoring of firewall logs in orchestrator UI.



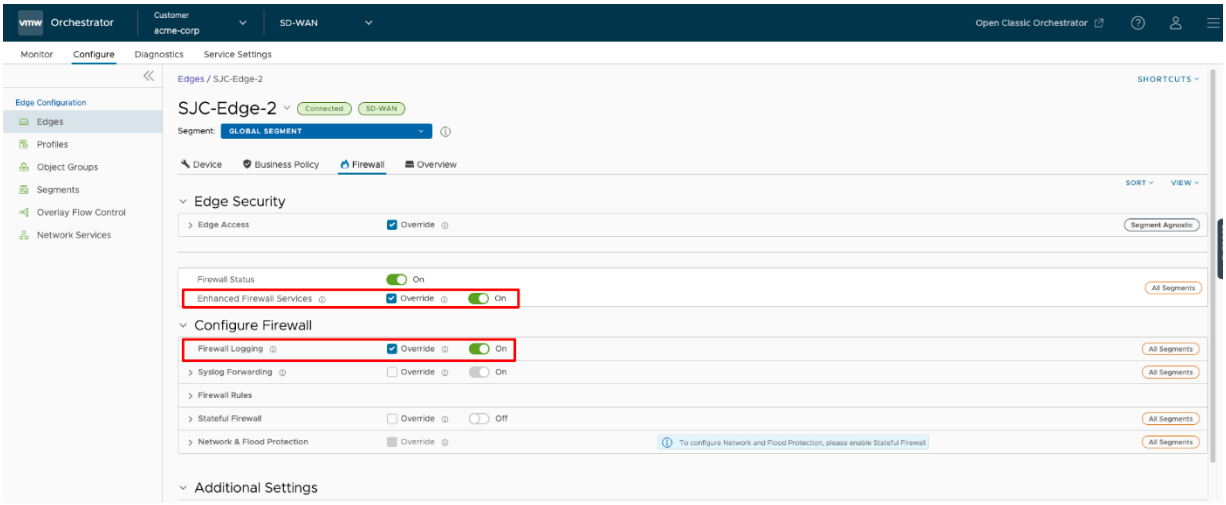
6. Once Enabled at Profile level, click on Save Changes in the bottom right of the screen.



7. Note that when you navigate to an Edge where this Profile has been applied, the Edge would inherit the configuration from the Profile and the toggle button will be **On** though the option would show a gray tone.



8. Enhanced Firewall Services and Firewall Logging can also be enabled at the **Edge** level. In this scenario, the enterprise admin would check the Override checkbox and toggle the respective settings to On.



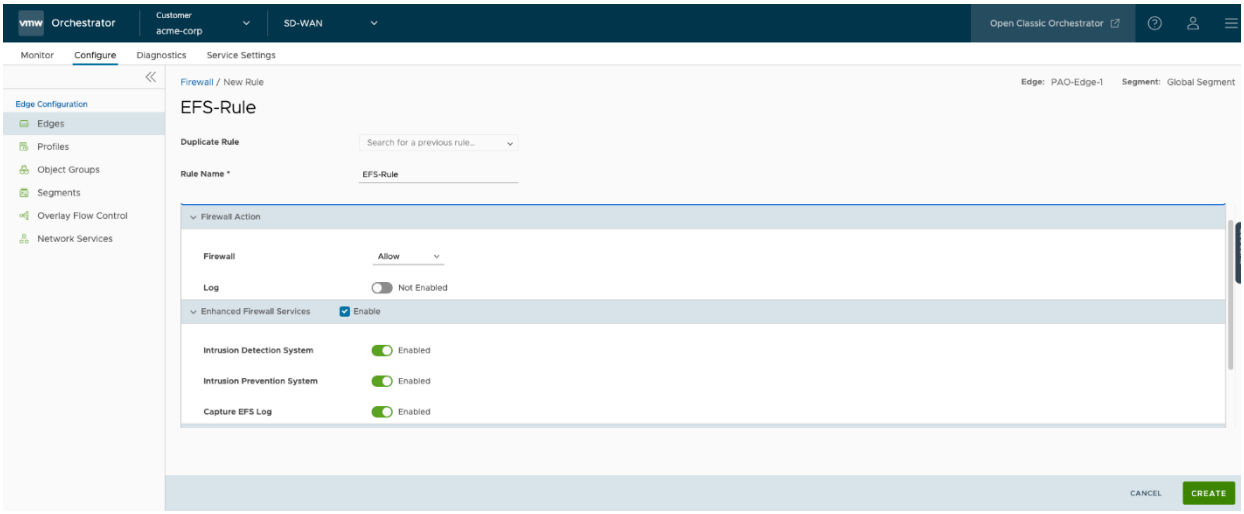
4.4 Configure Enhanced Firewall Service Firewall Rules

This section covers the configuration of EFS firewall rules. For configuration of generic firewall rules, please see https://docs.vmware.com/en/VMware-SD-WAN/5.1/VMware-SD-WAN-Administration-Guide/GUID-D12A4E23-7866-461F-9194-A031662E62CD.html

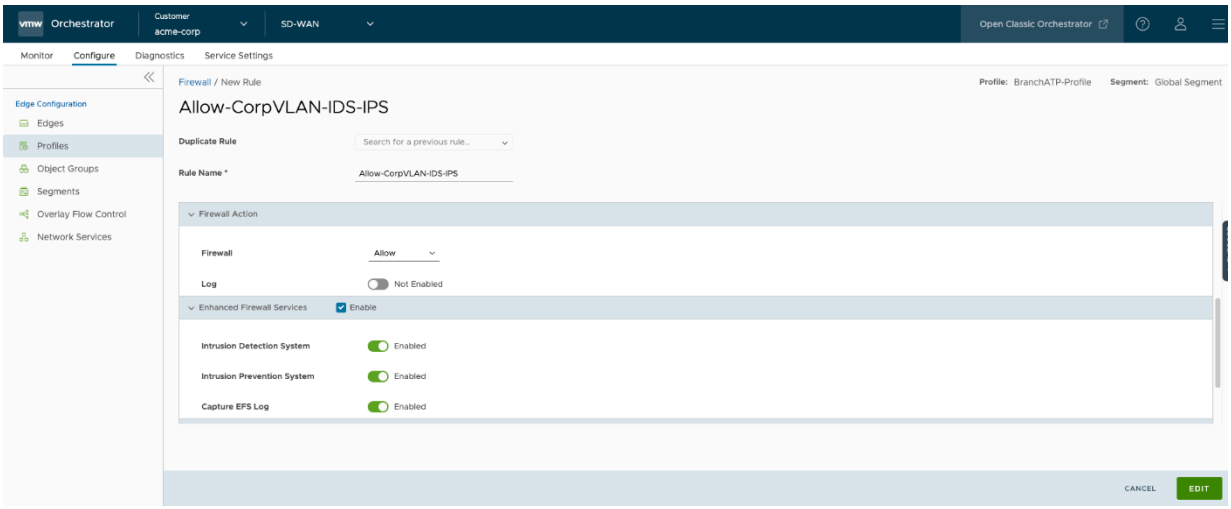
1. In the Enterprise portal, go to Configure -> Profiles. The Profiles page displays the existing Profiles.
2. To configure a **Profile**, click the link to an existing Profile or Add a new Profile.
3. Click the Firewall tab.
4. Toggle On the Enhanced Firewall Services to activate EFS. By default, this feature is not activated.
5. Under Firewall Rules, you can create a new EFS firewall rule or modify an existing firewall rule.
    a. To create a new EFS firewall rule, click on New Rule.
    b. Enter a unique **Rule Name** in the text box. You may also create a firewall rule from an existing rule by selecting the rule from the Duplicate Rule drop down menu.
    c. Configure the associated **Match** conditions and **Firewall Action** to be performed.
    d. Select the **Enhanced Firewall Services** checkbox and configure the following EFS settings.

    Note that the EFS engine inspects traffic sent/received through the Edges and matches content against the signatures configured in the engine.

    Note that EFS can be activated in the rule only if the Firewall action is Allow
6. Intrusion Detection System – When IDS is activated on Edges, the Edges detect if the traffic flow is malicious or not based on the signatures in the engine. If an attack is detected, the EFS engine generates an alert in the firewall log. If no attack is detected, the EFS engine forwards the traffic.
7. Intrusion Prevention System – When IPS is activated on Edges, the Edges detect if the traffic flow is malicious or not based on the signatures in the engine. If an attack is detected, the EFS engine generates an alert in the firewall log and blocks the traffic flow. IPS can only be activated when IDS is enabled. When IDS is not enabled, toggling IPS to enabled will toggle both IPS and IDS to enabled as well.
8. Enable **Capture EFS Log** to ensure that the IDS/IPS alerts are sent to the firewall log in the Orchestrator UI.
9. Add a comment for the rule if needed and click Create.

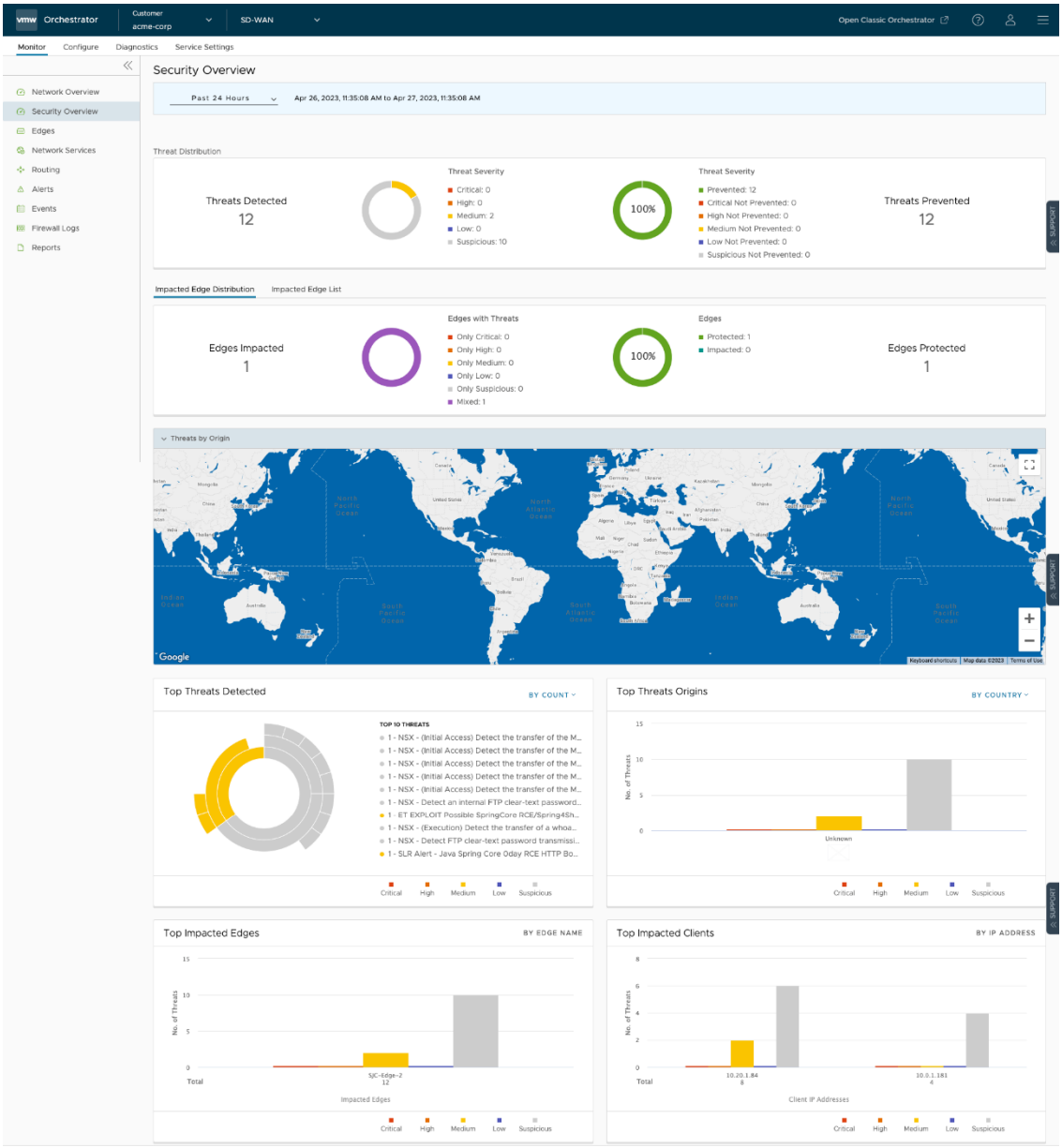


10. To modify an existing firewall rule (for e.g. Allow-CorpVLAN-IDS-IPS in this case) for EFS settings:
    a. Under the Firewall Rules area of the Profile -> Firewall tab page, click the rule name of an existing firewall rule to be modified.
    b. Modify the Enhanced Firewall Services settings and click Edit.



4.5 Monitoring Enhanced Firewall Services - Enterprise

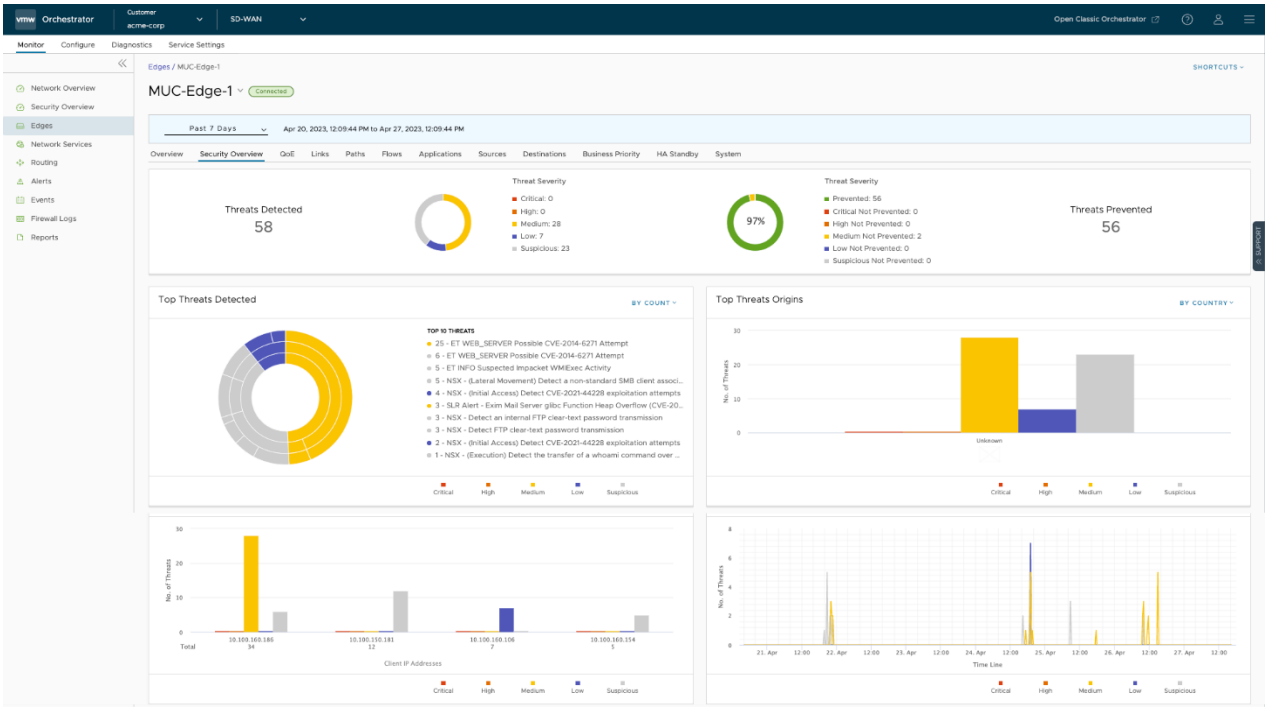
1. To view the EFS details for an Enterprise, click **Monitor -> Security Overview**
2. The Security Overview page shows a number of dashboards for the EFS IDS/IPS metrics collected for the Enterprise based on the selected time frame
    a. Threat Distribution – Summary count of Threats Detected and Prevented
    b. Impacted Edge Distribution – Summary count of Edges Impacted and Protected
    c. Impacted Edge List – List of all Edges and the associated Threat Impact(Severity)
    d. Top Threats Detected filtered by **Count**(Default) or by **Impact**
    e. Top Threat Origins filtered by **IP Address** (Default) or by **Country**
    f. Top Impacted Edges filtered by **Edge Name** or **IP Address**
    g. Top Impacted Clients filtered by **IP Address** or by **Country**



4.6 Monitoring Enhanced Firewall Services - Edge

1. To view the EFS details for an Edge, click **Monitor -> Edges**
2. Select an Edge from the table by clicking on the Edge. The Network Overview page appears by default. Select the **Security Overview** tab
3. The Security Overview page shows a number of dashboards for the EFS IDS/IPS metrics collected for the selected Edge based on the selected time frame.
    a. Summary count of Threats Detected and Prevented for the Edge
    b. Top Threats Detected filtered by Count (Default) or by Impact
    c. Top Threat Origins filtered by Country (Default) or by IP Address
    d. Top Impacted Clients filtered by IP Address (Default) or by Country

e. Histogram Trend of Threats for the past selected time frame.



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.