VMware SD-WAN Design Guide for Enhanced Firewall Services

VMware SD-WAN

vmware by Broadcom

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

https://docs.vmware.com/

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

Contents

VMware SD-WAN Design Guide for Enhanced Firewall Services

1

Read the following topics next:

Overview

A significant number of network breaches originate in branch offices. Branch offices are vulnerable to a variety of attack vectors, including sophisticated phishing campaigns, lax physical security, and insider threats from disgruntled or careless users. These threats can be used to gain access to the network. With proper defenses, the damage from these attacks can be limited to the branch office and prevented from spreading to more sensitive areas of the network, such as the data center. VMware Enhanced Firewall Services (EFS) are natively integrated security services in the VMware SD-WAN Edge that can help protect branch offices from attacks.

Purpose

This design guide outlines how an organization can use the EFS feature set to enhance its security footprint. The topic areas covered in this design guide include:

- Identified use cases
- Architecture
- Design considerations
- Traffic patterns
- Security best practices
- Deployment strategy

The guide provides detailed information on each topic, as well as recommendations for how to implement EFS in a secure manner.

Target Audience

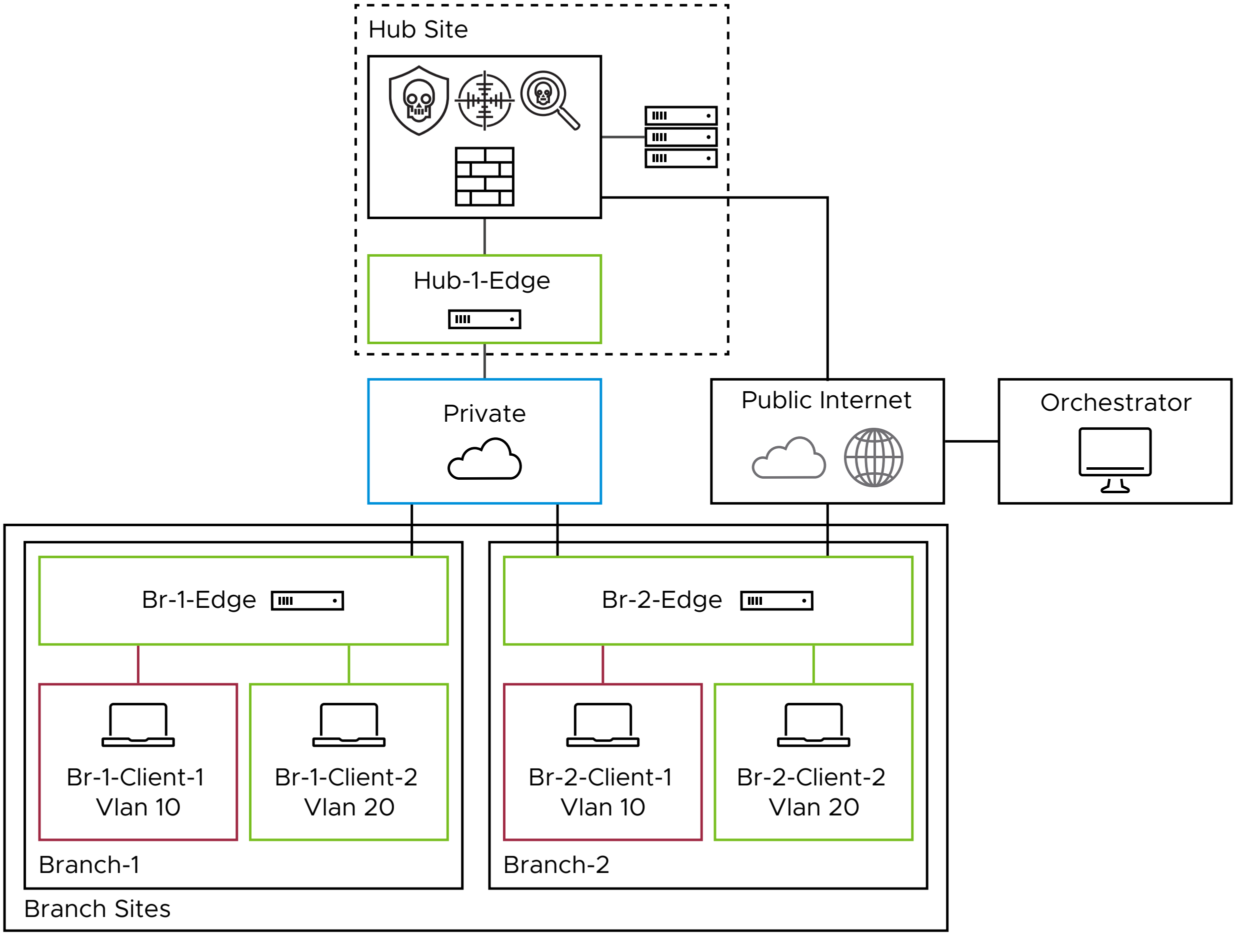
This design guide is intended for all network and security architects, engineers, and administrators who design, deploy, or maintain a VMware SASE™ solution.

Reference Architecture

The reference architecture describes the basic topology, use cases, and functionality of the EFS components when activated for accessing applications in a multi-cloud environment, whether it be for branch-to-branch traffic, branch-to-hub traffic, or when accessing SaaS applications on the public cloud.

Topology

This guide will use the following topology. The topology illustrates use of the SD-WAN Edge at the branches and at the hub site with EFS functionality in play.



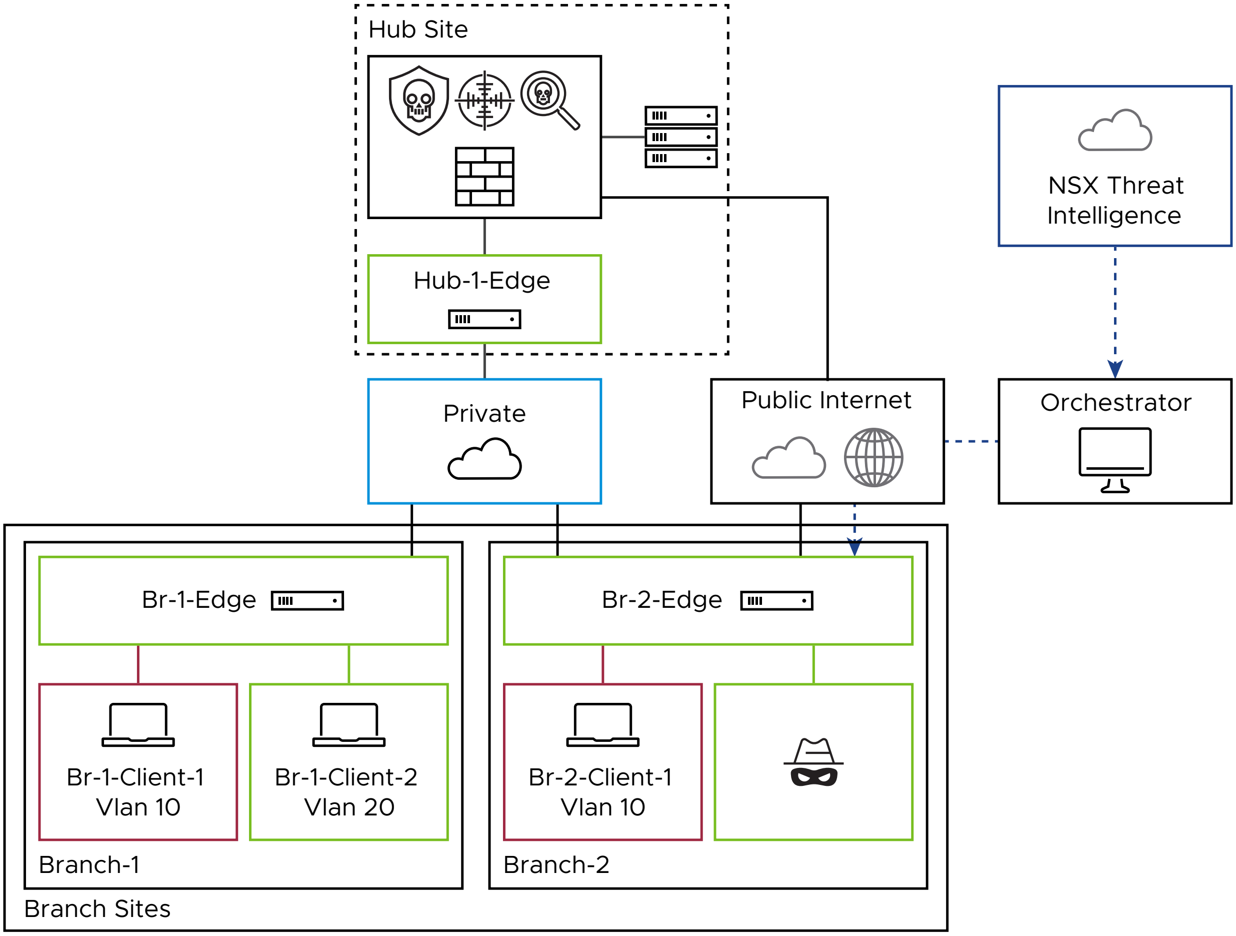
Use Cases

Use Case	Description
Private Access	Private Access refers to those inter and intra-branch communications. While perimeter security is essential, internal traffic protection with VMware EFS ensures that potential threats within the network are promptly identified and neutralized, thus maintaining the integrity and confidentiality of organizational assets.
Internet Access (without CWS)	Direct Internet Access (DIA) provides direct connectivity to the Internet, which can improve efficiency and user experience. However, it also introduces new security challenges. VMware EFS can help to mitigate these risks by providing a secure and controlled way for users to access the Internet. This can help to safeguard your enterprise from potential threats.
Internet Access (with CWS)	A more comprehensive approach for securing Internet/SaaS traffic would be to pair VMware EFS with VMware Cloud Web Security (CWS) and its many security capabilities, such as sandboxing, SSL decryption, URL and content filtering, Data Loss Prevention (DLP), and Cloud Access Security Broker (CASB).

EFS Features

IDS/IPS

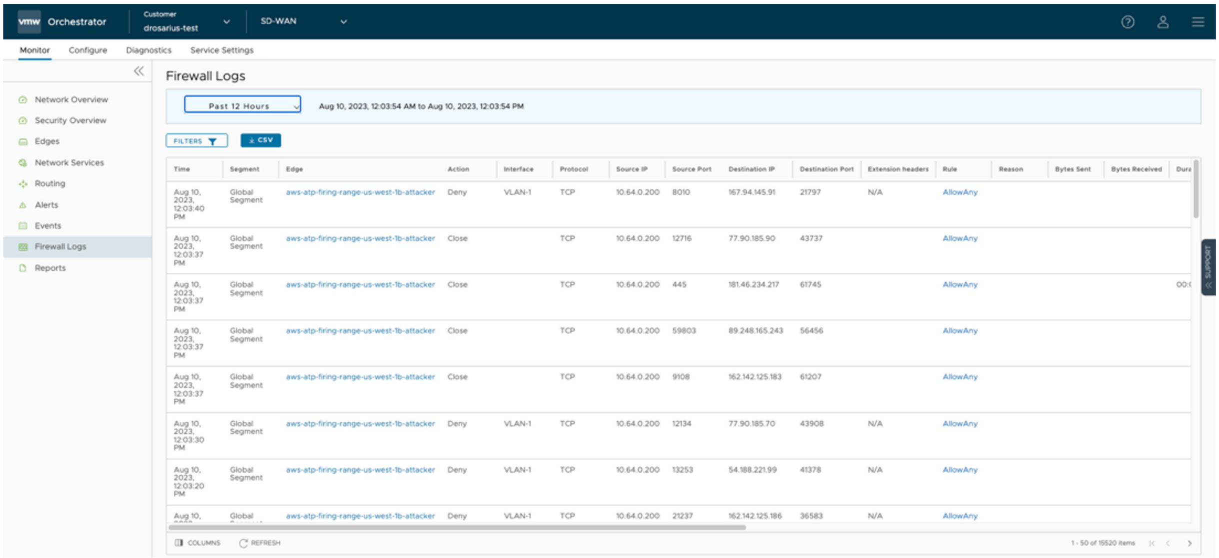
The following diagram illustrates the signature flow. The Edge employs the same IDPS engine, Suricata, as the NSX Distributed Firewall, sharing identical IDPS signatures. The NSX Security Team creates these signatures, developing custom ones and obtaining others from third-party agencies. Each signature is carefully curated and verified by the NSX Security Team. To ensure the Edge has the most up-to-date signatures, the Orchestrator queries the NSX Threat Intelligence cloud every 4 hours.



VMware Hosted Logging

Regionally hosted logging is included in the base VMware SD-WAN license. This means that logs are stored in the same region as the Orchestrator (virtual controller). By default, 15 GB of logs per Enterprise or seven days of logs per Edge, whichever comes first, will be kept. Logs can be viewed under the **Firewall Logs** section of the dashboard. There are options to search and filter for the specific data needed for troubleshooting or investigating. From this view, there is also a button to export the logs locally into a CSV format.

Figure 1-1. Hosted Logging View



Firewall Logs

Past 12 Hours Aug 10, 2023, 12:03:54 AM to Aug 10, 2023, 12:03:54 PM

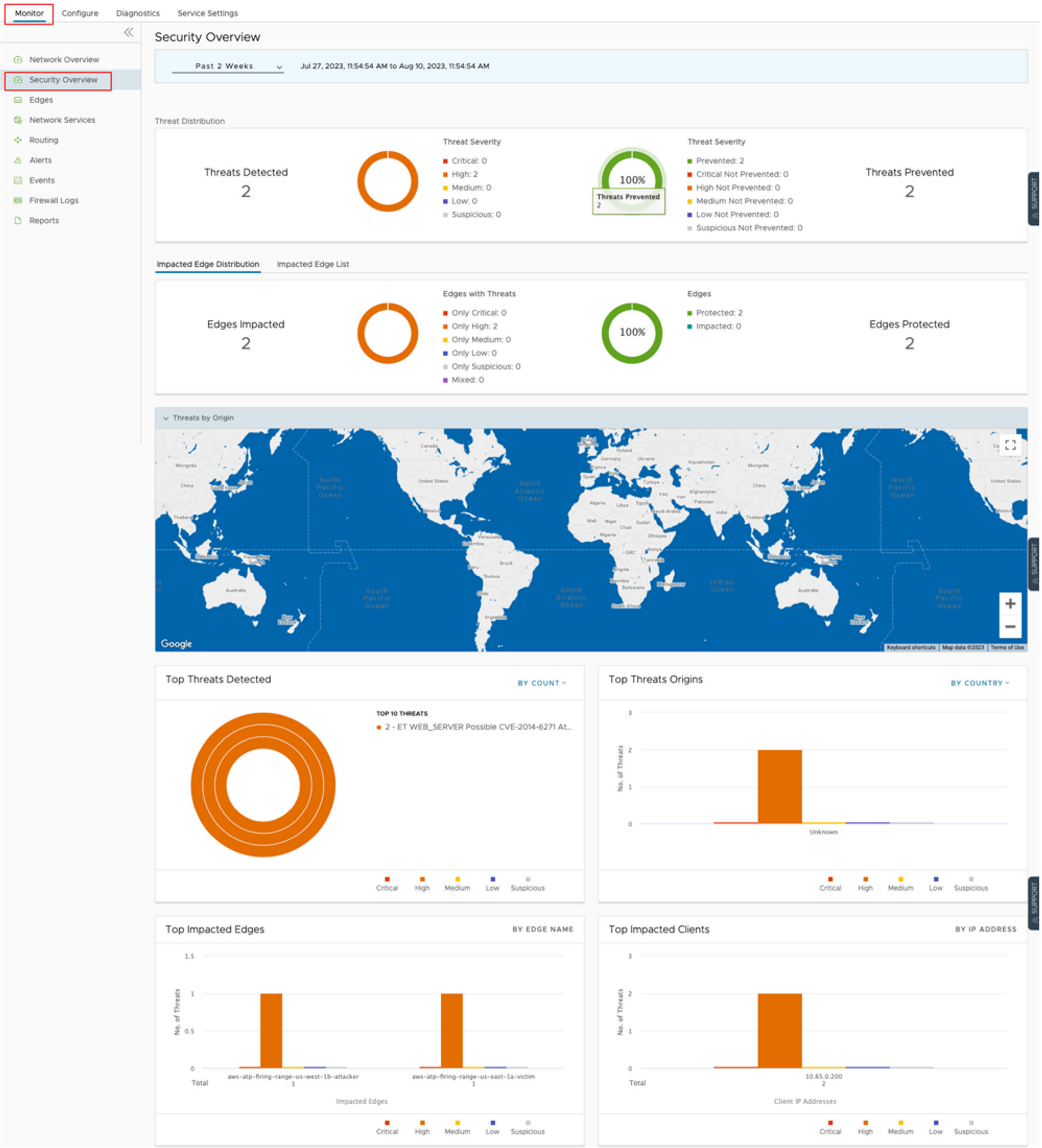
Time	Segment	Edge	Action	Interface	Protocol	Source IP	Source Port	Destination IP	Destination Port	Extension headers	Rule	Reason	Bytes Sent	Bytes Received	Dura
Aug 10, 2023, 12:03:40 PM	Global Segment	aws-atp-firing-range-us-west-1b-attacker	Deny	VLAN-1	TCP	10.64.0.200	8010	167.94.145.91	21797	N/A	AllowAny				
Aug 10, 2023, 12:03:37 PM	Global Segment	aws-atp-firing-range-us-west-1b-attacker	Close		TCP	10.64.0.200	12716	77.90.185.90	43737		AllowAny				
Aug 10, 2023, 12:03:37 PM	Global Segment	aws-atp-firing-range-us-west-1b-attacker	Close		TCP	10.64.0.200	445	181.46.234.217	61745		AllowAny				00:0
Aug 10, 2023, 12:03:37 PM	Global Segment	aws-atp-firing-range-us-west-1b-attacker	Close		TCP	10.64.0.200	59803	89.248.165.243	56456		AllowAny				
Aug 10, 2023, 12:03:37 PM	Global Segment	aws-atp-firing-range-us-west-1b-attacker	Close		TCP	10.64.0.200	9108	162.142.125.183	61207		AllowAny				
Aug 10, 2023, 12:03:30 PM	Global Segment	aws-atp-firing-range-us-west-1b-attacker	Deny	VLAN-1	TCP	10.64.0.200	12134	77.90.185.70	43908	N/A	AllowAny				
Aug 10, 2023, 12:03:20 PM	Global Segment	aws-atp-firing-range-us-west-1b-attacker	Deny	VLAN-1	TCP	10.64.0.200	13253	54.188.221.99	41378	N/A	AllowAny				
Aug 10,	Global	aws-atp-firing-range-us-west-1b-attacker	Deny	VLAN-1	TCP	10.64.0.200	21237	162.142.125.186	36583	N/A	AllowAny				

1 - 50 of 15520 items

Security Overview Dashboard

The **Security Overview** dashboard provides a comprehensive overview of your Enterprise's threat landscape. A quick response is essential in addressing threats. This dashboard displays threats and their severity, the source of attacks, and the affected Edges, allowing you to take corrective action quickly.

Figure 1-2. Security Overview Dashboard



Security Overview

Past 2 Weeks — Jul 27, 2023, 11:54:54 AM to Aug 10, 2023, 11:54:54 AM

Threat Distribution

Threats Detected 2

Threat Severity
- Critical: 0
- High: 2
- Medium: 0
- Low: 0
- Suspicious: 0

100% Threats Prevented 2

Threat Severity
- Prevented: 2
- Critical Not Prevented: 0
- High Not Prevented: 0
- Medium Not Prevented: 0
- Low Not Prevented: 0
- Suspicious Not Prevented: 0

Threats Prevented 2

Impacted Edge Distribution | Impacted Edge List

Edges Impacted 2

Edges with Threats
- Only Critical: 0
- Only High: 2
- Only Medium: 0
- Only Low: 0
- Only Suspicious: 0
- Mixed: 0

100%

Edges
- Protected: 2
- Impacted: 0

Edges Protected 2

Top Threats Detected

TOP 10 THREATS
- 2 - ET WEB_SERVER Possible CVE-2014-6271 At...

Top Threats Origins

Top Impacted Edges

aws-atp-firing-range-us-west-1b-attacker 1
aws-atp-firing-range-us-east-1a-victim 1

Top Impacted Clients

10.65.0.200 2

Solution Components

- VMware Edge Cloud Orchestrator (Hosted by VMware or On-prem)
  - On-prem deployments require additional conversation and configuration. Contact the SD-WAN support Team.
- VMware SD-WAN Edge. All actively selling Edge types (physical and virtual) support Enhanced Firewall Services (EFS).

System Requirements

To benefit from Enhanced Firewall Services (EFS), an additional license (*VCX-EFW-100M-12P-C*) must be purchased and activated.

Design Considerations

Although Enhanced Firewall Services (EFS) can be set up with a few mouse clicks, a thorough understanding of the network, traffic flows, and current configurations is required before activating and configuring the feature.

Performance Impact

Traffic inspected by the IDPS with Stateful Firewall may experience a performance impact. Performance numbers can be found here. There is a balancing act between securing the network and making it performant. By understanding your network, EFS can be applied to the appropriate traffic.

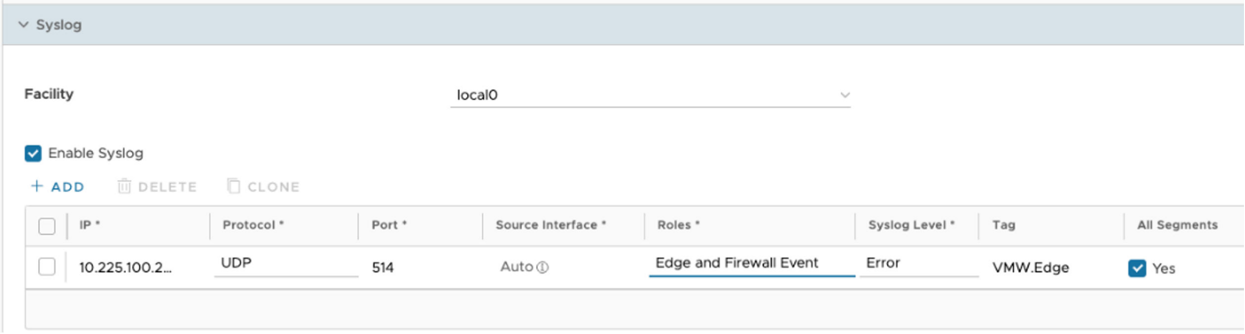
Logging

Logging is essential when it comes to troubleshooting issues, investigating threats, and complying with PCI DSS, NIST, and others. VMware SD-WAN accomplishes this by utilizing regionally hosted logging infrastructure and/or exporting logs via syslog to a central log server, Security Orchestration, Automation and Response (SOAR), or Security Information and Event Management (SIEM) such as Splunk or IBM's QRadar. These two features are not mutually exclusive, so both can be used together.

Syslog

Companies with an existing central log server, SIEM, or SOAR can export the logs via syslog into those solutions. The following image depicts the syslog configuration. You can configure the feature at the Profile or Edge level. It is important to note that syslog traffic is not encrypted.

Figure 1-3. Syslog Configuration



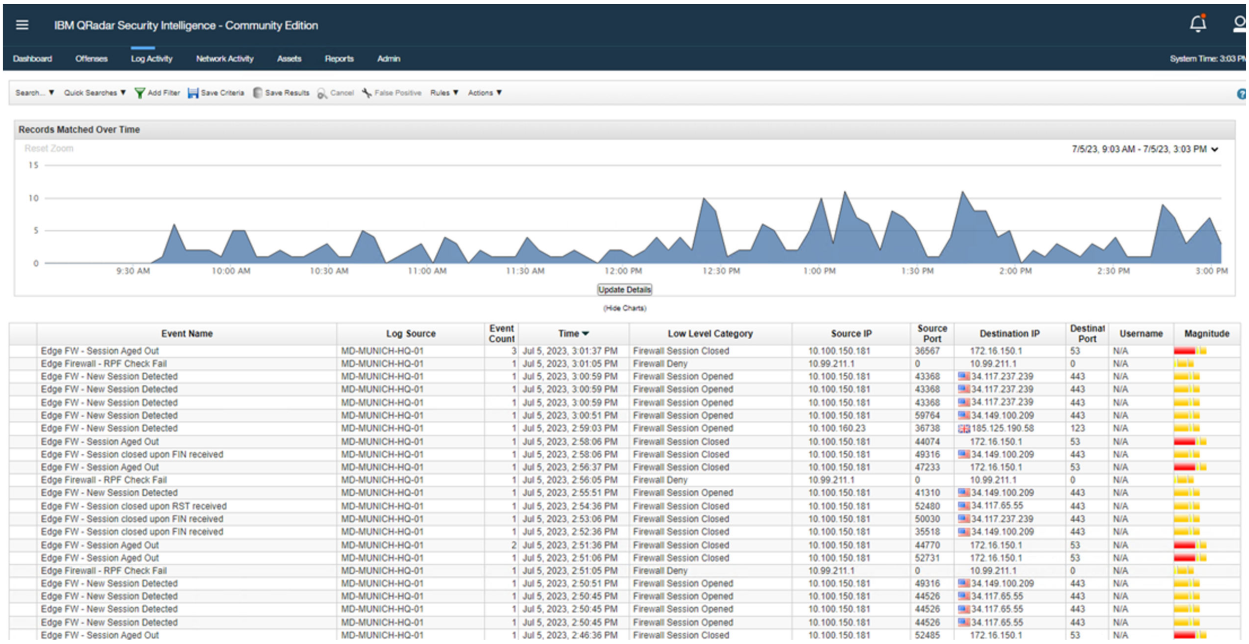
Facility: local0

☑ Enable Syslog

□	IP *	Protocol *	Port *	Source Interface *	Roles *	Syslog Level *	Tag	All Segments
□	10.225.100.2...	UDP	514	Auto ⓘ	Edge and Firewall Event	Error	VMW.Edge	☑ Yes

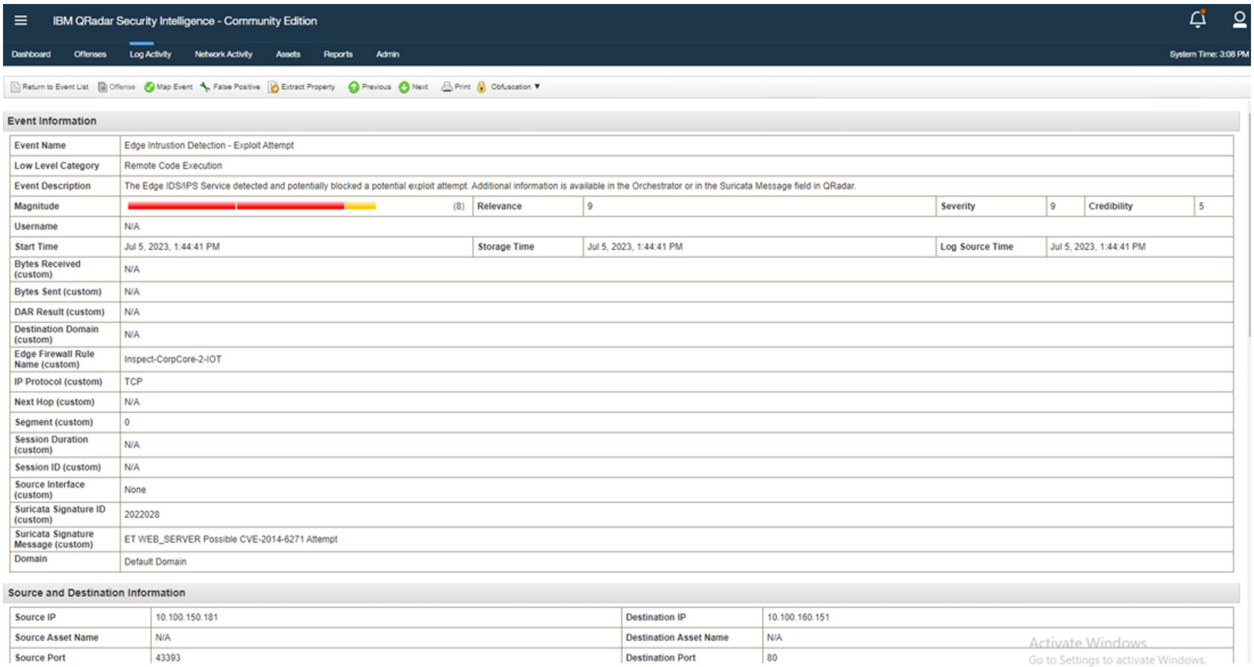
The following images are examples of an IBM QRadar instance receiving logs from an Edge device.

Figure 1-4. IBM QRadar View - Example 1



Event Name	Log Source	Event Count	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destinat Port	Username	Magnitude
Edge FW - Session Aged Out	MD-MUNICH-HQ-01	3	Jul 5, 2023, 3:01:37 PM	Firewall Session Closed	10.100.150.181	36567	172.16.150.1	53	N/A	🟥🟨
Edge Firewall - RPF Check Fail	MD-MUNICH-HQ-01	1	Jul 5, 2023, 3:01:05 PM	Firewall Deny	10.99.211.1	0	10.99.211.1	0	N/A	🟨
Edge FW - New Session Detected	MD-MUNICH-HQ-01	1	Jul 5, 2023, 3:00:59 PM	Firewall Session Opened	10.100.150.181	43368	34.117.237.239	443	N/A	🟨
Edge FW - New Session Detected	MD-MUNICH-HQ-01	1	Jul 5, 2023, 3:00:59 PM	Firewall Session Opened	10.100.150.181	43368	34.117.237.239	443	N/A	🟨
Edge FW - New Session Detected	MD-MUNICH-HQ-01	1	Jul 5, 2023, 3:00:59 PM	Firewall Session Opened	10.100.150.181	43368	34.117.237.239	443	N/A	🟨
Edge FW - New Session Detected	MD-MUNICH-HQ-01	1	Jul 5, 2023, 3:00:51 PM	Firewall Session Opened	10.100.150.181	59764	34.149.100.209	443	N/A	🟨
Edge FW - New Session Detected	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:59:03 PM	Firewall Session Opened	10.100.160.23	36738	185.125.190.58	123	N/A	🟨
Edge FW - Session Aged Out	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:58:06 PM	Firewall Session Closed	10.100.150.181	44074	172.16.150.1	53	N/A	🟥🟨
Edge FW - Session closed upon FIN received	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:58:06 PM	Firewall Session Closed	10.100.150.181	49316	34.149.100.209	443	N/A	🟨
Edge FW - Session Aged Out	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:56:37 PM	Firewall Session Closed	10.100.150.181	47233	172.16.150.1	53	N/A	🟥🟨
Edge Firewall - RPF Check Fail	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:56:05 PM	Firewall Deny	10.99.211.1	0	10.99.211.1	0	N/A	🟨
Edge FW - New Session Detected	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:55:51 PM	Firewall Session Opened	10.100.150.181	41310	34.149.100.209	443	N/A	🟨
Edge FW - Session closed upon RST received	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:54:36 PM	Firewall Session Closed	10.100.150.181	52480	34.117.65.55	443	N/A	🟨
Edge FW - Session closed upon FIN received	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:53:06 PM	Firewall Session Closed	10.100.150.181	50030	34.117.237.239	443	N/A	🟨
Edge FW - Session closed upon FIN received	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:52:36 PM	Firewall Session Closed	10.100.150.181	35518	34.149.100.209	443	N/A	🟨
Edge FW - Session Aged Out	MD-MUNICH-HQ-01	2	Jul 5, 2023, 2:51:36 PM	Firewall Session Closed	10.100.150.181	44770	172.16.150.1	53	N/A	🟥🟨
Edge FW - Session Aged Out	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:51:06 PM	Firewall Session Closed	10.100.150.181	52731	172.16.150.1	53	N/A	🟥🟨
Edge Firewall - RPF Check Fail	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:51:05 PM	Firewall Deny	10.99.211.1	0	10.99.211.1	0	N/A	🟨
Edge FW - New Session Detected	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:50:51 PM	Firewall Session Opened	10.100.150.181	49316	34.149.100.209	443	N/A	🟨
Edge FW - New Session Detected	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:50:45 PM	Firewall Session Opened	10.100.150.181	44526	34.117.65.55	443	N/A	🟨
Edge FW - New Session Detected	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:50:45 PM	Firewall Session Opened	10.100.150.181	44526	34.117.65.55	443	N/A	🟨
Edge FW - New Session Detected	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:50:45 PM	Firewall Session Opened	10.100.150.181	44526	34.117.65.55	443	N/A	🟨
Edge FW - Session Aged Out	MD-MUNICH-HQ-01	1	Jul 5, 2023, 2:46:36 PM	Firewall Session Closed	10.100.150.181	52485	172.16.150.1	53	N/A	🟥🟨

Figure 1-5. IBM QRadar View - Example 2



Event Information

Event Name	Edge Intrustion Detection - Exploit Attempt						
Low Level Category	Remote Code Execution						
Event Description	The Edge IDS/IPS Service detected and potentially blocked a potential exploit attempt. Additional information is available in the Orchestrator or in the Suricata Message field in QRadar.						
Magnitude	🟥🟥🟨 (8)	Relevance	9	Severity	9	Credibility	5
Username	N/A						
Start Time	Jul 5, 2023, 1:44:41 PM	Storage Time	Jul 5, 2023, 1:44:41 PM	Log Source Time	Jul 5, 2023, 1:44:41 PM		
Bytes Received (custom)	N/A						
Bytes Sent (custom)	N/A						
DAR Result (custom)	N/A						
Destination Domain (custom)	N/A						
Edge Firewall Rule Name (custom)	Inspect-CorpCore-2-IOT						
IP Protocol (custom)	TCP						
Next Hop (custom)	N/A						
Segment (custom)	0						
Session Duration (custom)	N/A						
Session ID (custom)	N/A						
Source Interface (custom)	None						
Suricata Signature ID (custom)	2022028						
Suricata Signature Message (custom)	ET WEB_SERVER Possible CVE-2014-6271 Attempt						
Domain	Default Domain						

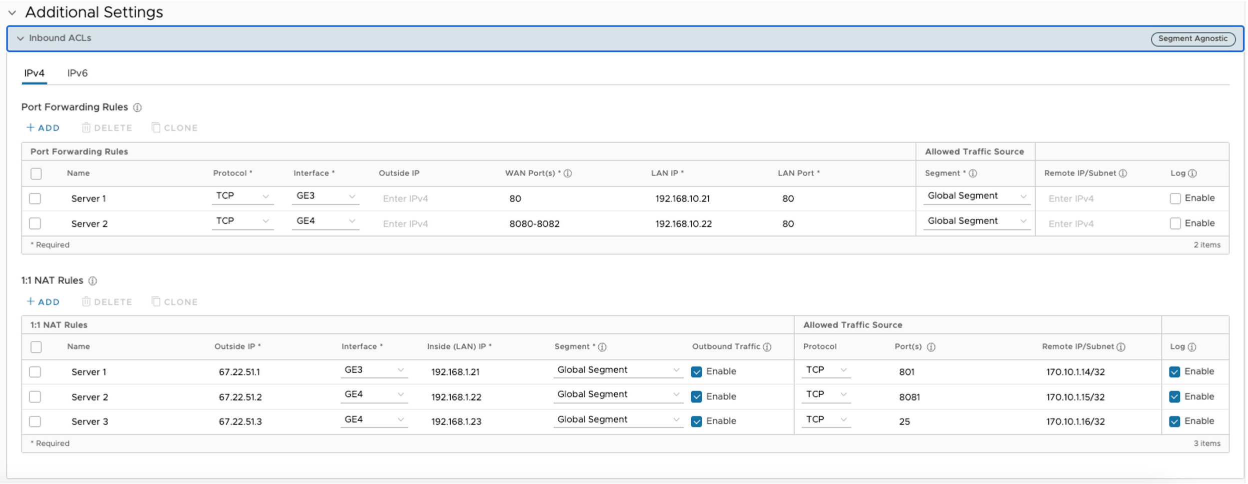
Source and Destination Information

Source IP	10.100.150.181	Destination IP	10.100.160.151
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	43393	Destination Port	80

Known Limitations

In 5.2 release, traffic that hits a 1:1 NAT or Port Forwarding rule will not be inspected by the IDPS Engine. This limitation will be addressed in a future release.

Figure 1-6. 1:1 NAT and Port Forwarding Configuration



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 ⓘ
☐	Server 1	TCP	GE3	Enter IPv4	80	192.168.10.21	80	Global Segment	Enter IPv4	☐ Enable
☐	Server 2	TCP	GE4	Enter IPv4	8080-8082	192.168.10.22	80	Global Segment	Enter IPv4	☐ Enable

* Required 2 items

1:1 NAT Rules ⓘ

+ ADD DELETE CLONE

1:1 NAT Rules							Allowed Traffic Source			
☐	Name	Outside IP *	Interface *	Inside (LAN) IP *	Segment * ⓘ	Outbound Traffic ⓘ	Protocol	Port(s) ⓘ	Remote IP/Subnet ⓘ	Log ⓘ
☐	Server 1	67.22.51.1	GE3	192.168.1.21	Global Segment	☑ Enable	TCP	801	170.10.1.14/32	☑ Enable
☐	Server 2	67.22.51.2	GE4	192.168.1.22	Global Segment	☑ Enable	TCP	8081	170.10.1.15/32	☑ Enable
☐	Server 3	67.22.51.3	GE4	192.168.1.23	Global Segment	☑ Enable	TCP	25	170.10.1.16/32	☑ Enable

* Required 3 items

Traffic Patterns

This section describes about monitoring and inspecting network traffic patterns to detect threats and troubleshoot performance issues.

The Branch Attack Surface

An adversary has numerous ways to gain initial access into an Enterprise's network. Some of those ways include the following:

- Internet of Things (IoT) - These devices have become ubiquitous as there seems to be a race to turn everything “smart.” Everything wants access to the network, such as sensors, printers, security cameras, door locks, and so on. Unfortunately, security is usually an afterthought when creating these devices.

- Employees - Employees are prime targets for adversaries to leverage for initial access. Disgruntled employees can sell access to your network, and inattentive employees can be susceptible to phishing campaigns.

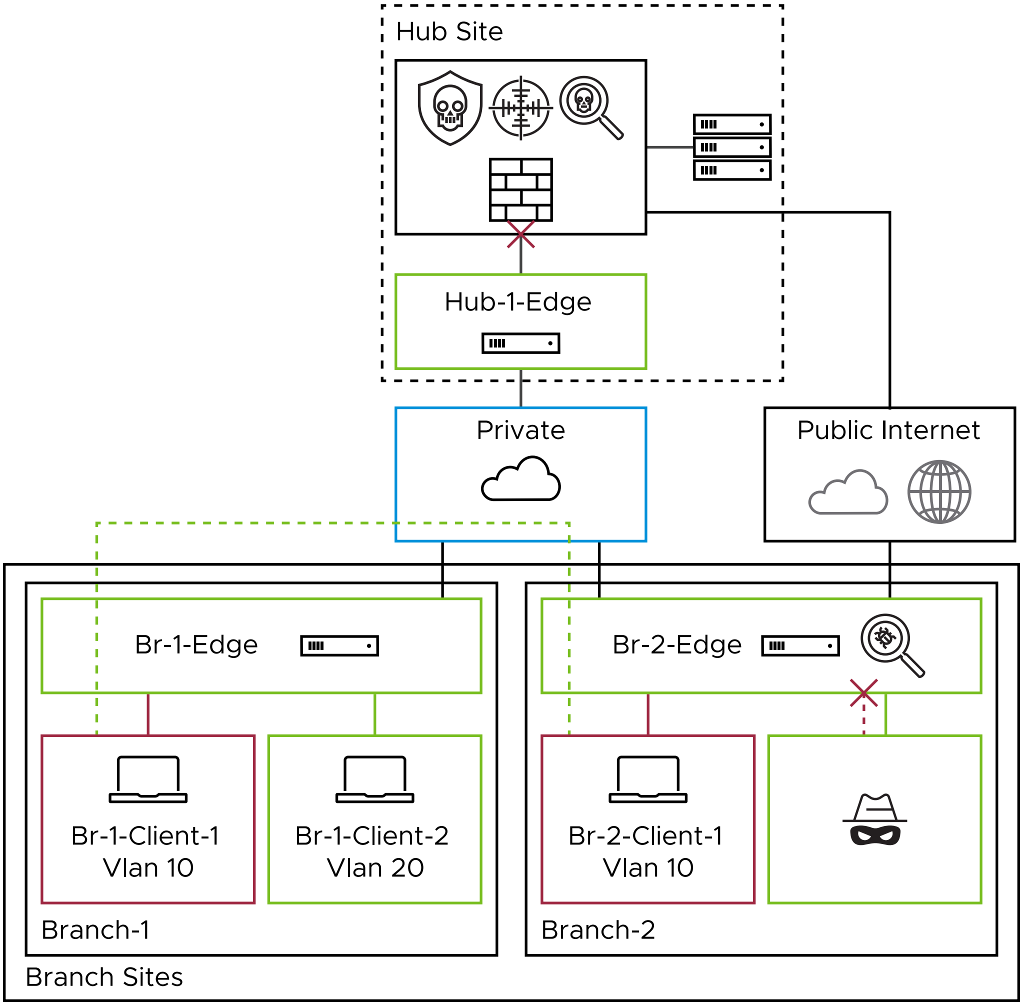
- Physical Security - Physical security vulnerabilities could provide opportunities for malicious actors to gain access to machines or open ports. This could allow them to steal data, launch attacks, or disrupt operations. It is important to implement strong physical security measures to protect against these risks.

- Network Devices - Network devices that are not patched offer adversaries the means to spread through the network. This is because unpatched devices may contain vulnerabilities that can be exploited by attackers. Once an attacker has gained access to an unpatched device, they can then use it to move laterally through the network and gain access to other devices. This can lead to a data breach, financial loss, or even physical damage. Therefore, it is important to keep all network devices up to date with the latest security patches.

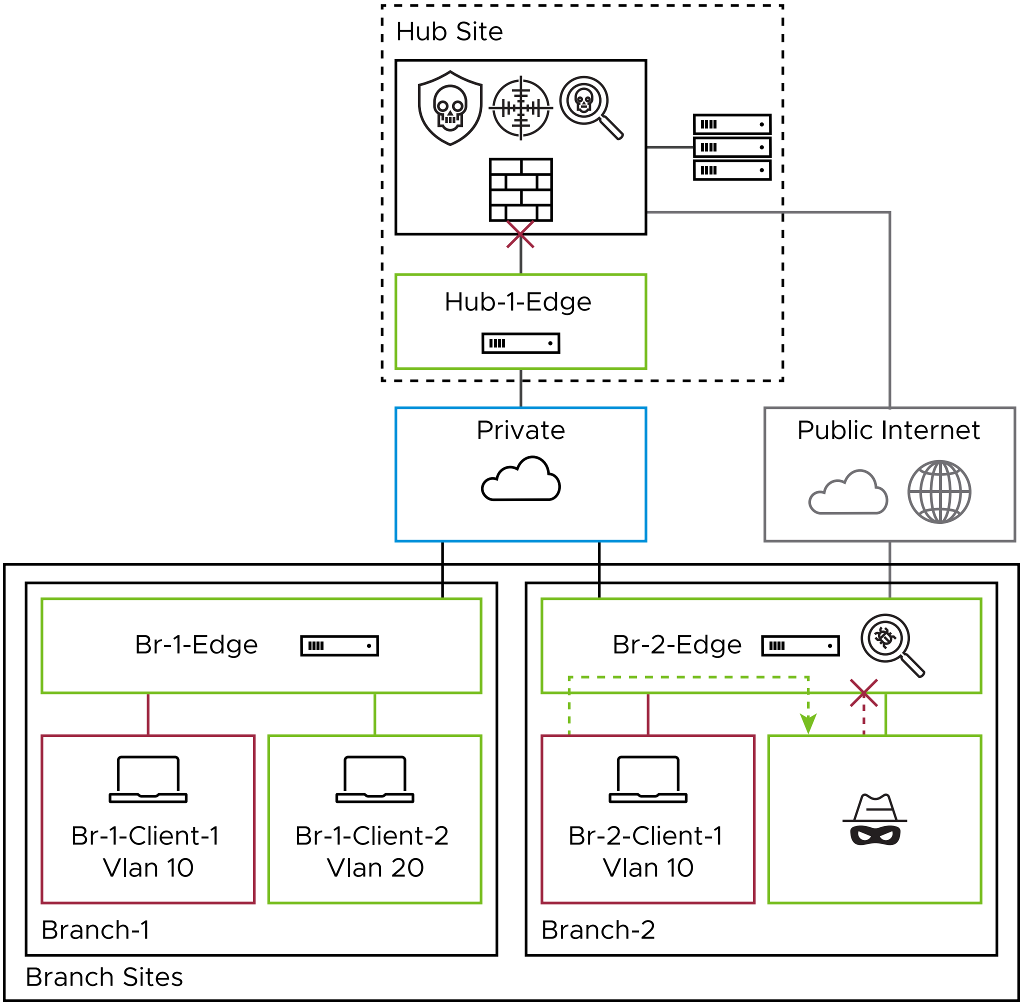
Protecting internal traffic is as important as securing the network perimeter. Adversaries have multiple methods of bypassing a robust security stack that protects the boundary between the internal network and the outside world. Without a layered defense, a threat actor essentially has free rein over the internal network. A solid understanding of network segmentation will make it easier to create firewall policies that add the appropriate level of security without compromising performance.

Private Access

Inter-Branch Communication



Intra-Branch Communication



Examples of Inter-branch and Intra-branch traffic:

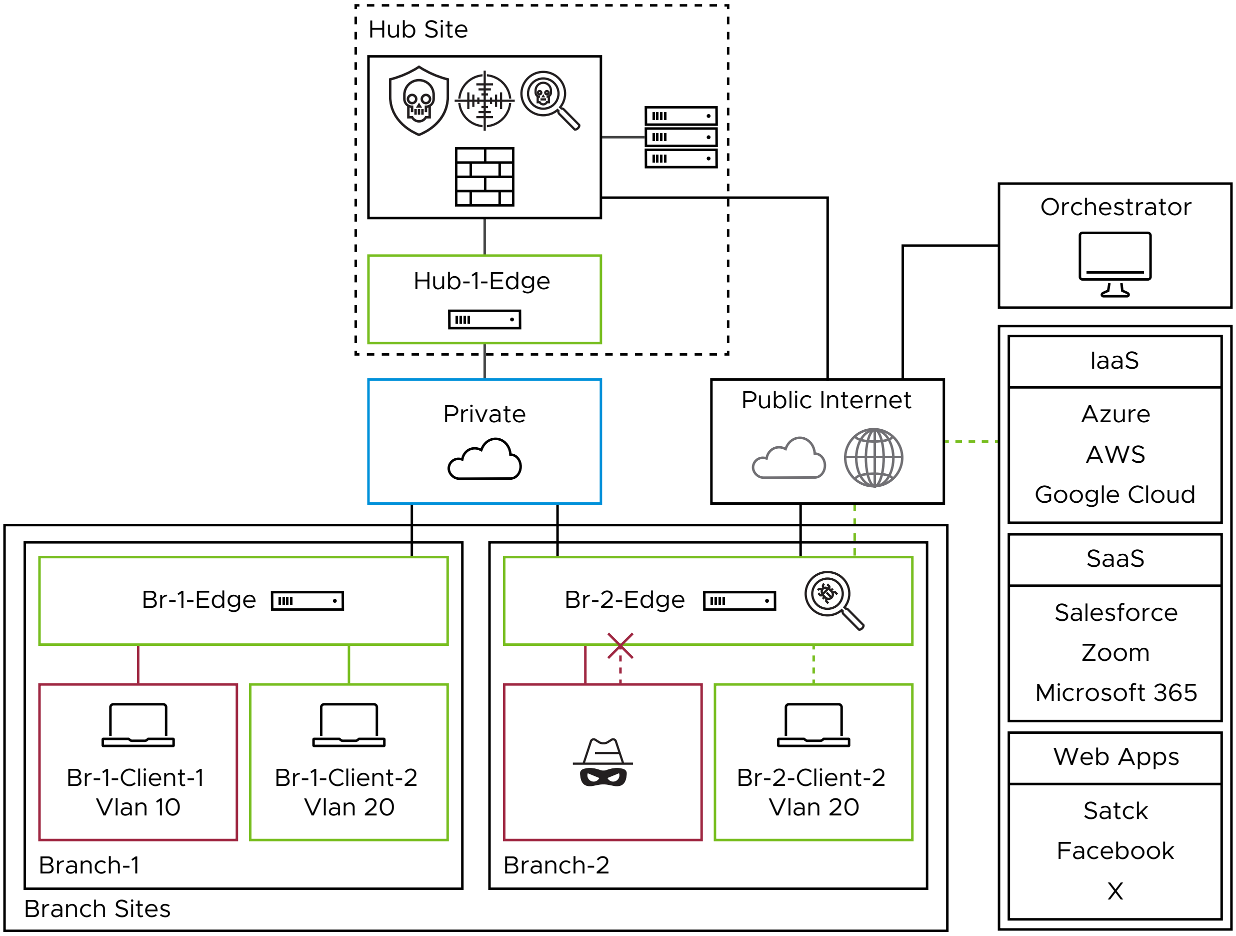
- Doctors' office downloading MRI images from Imaging Center
- IoT device communications
- Application traffic

As branch sites typically have less security in place than hubs, it would be more prudent to add additional security checks for this traffic flow. The goal of EFS is to easily add these checks to secure the branch and limit the blast radius of an attack, thus hindering a hacker's ability to use techniques such as lateral movement.

Once an attacker gains access to a machine on an internal network, they will typically need to find a way to move laterally through the network in order to find sensitive information. One common way that an attacker might move laterally is by exploiting vulnerabilities in software that is used internally by the company. VMware EFS can detect and prevent malicious movement that uses known exploits.

Internet Access without CWS

Figure 1-7. Direct Internet Access



Branch with Private Access Only

Branches without a direct Internet connection typically access the Internet through a hub site. Hub sites often have dedicated next-generation firewalls (NGFWs) at the perimeter. Leveraging these existing firewalls at the hub can be a more efficient approach.

Branch with Direct Internet Access (DIA)

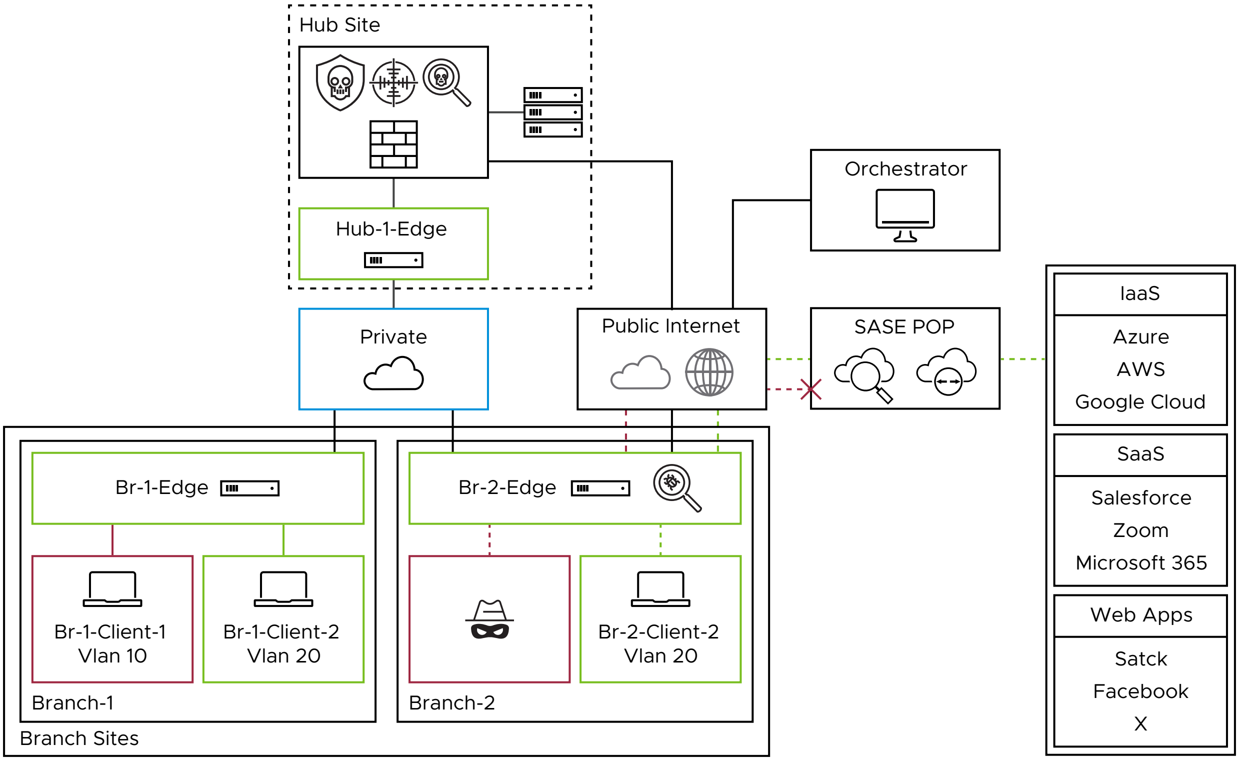
Direct Internet Access (DIA) offers a number of advantages for Enterprises, including:

- Improved performance for cloud-based applications, as traffic does not need to be backhauled to a hub site.
- Potential cost savings, as DIA is typically cheaper than a private MPLS connection.
- The ability to deploy sites quickly, as getting a private MPLS link installed at a branch can take months.

These benefits come with trade-offs concerning security. By adding DIA, you are bypassing the perimeter security. VMware EFS provides similar protection as you would find on the perimeter, so you realize all the benefits that come with DIA while stopping malicious activity.

Branch with Internet Access Through CWS

Figure 1-8. Internet Access through VMware CWS



VMware EFS can be combined with VMware Cloud Web Security (CWS) to provide a more well-rounded security approach. VMware EFS protects your network from malicious activity by analyzing traffic patterns against signatures of known threats and anomalous behavior. In contrast, CWS primarily focuses on Internet-bound traffic, with features such as SSL Decryption, DLP, CASB, and URL and Content Filtering. Together, they provide a multi-tiered defense, protecting internal network operations and external web interactions from various cyber threats.

To configure a CWS policy, see here.

Best Practices

The deployment of VMware EFS, or any new feature, requires careful consideration and planning.

Understanding your network:

- Common traffic flows - Analyzing the primary direction of your network traffic (branch-to-branch, branch-to-hub, or branch-to-internet) can help you determine the best starting point for deploying EFS.

- Known security measures - Understanding the placement of firewalls with capabilities similar to EFS within your network can inform your decisions regarding traffic inspection. It might be more efficient to leverage existing security hardware.
- Performance pain points - As networks expand, a location that initially began as a small branch might evolve into a medium or even large branch. If the Edge, originally designed for the smaller branch, has not been updated, it might be inadequately equipped to handle EFS, potentially compromising the site's performance.

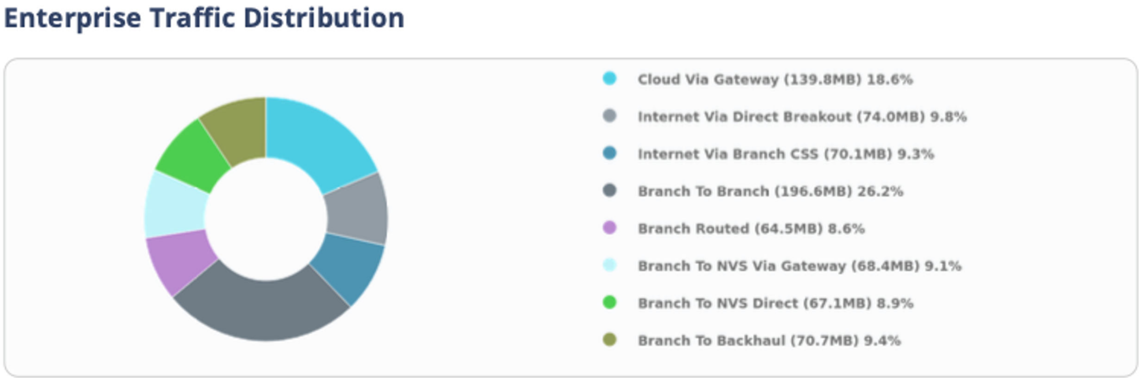
Some of these factors can be understood through experience with the network, while others will require some investigative work. The VMware Orchestrator provides you with easy-to-use tools and dashboards to accurately formulate a deployment strategy.

Deployment Strategy

The following is a simple guide on what tools are available in the Orchestrator, how to use the tools, and how to activate EFS to start inspecting traffic.

Day 0 Plan

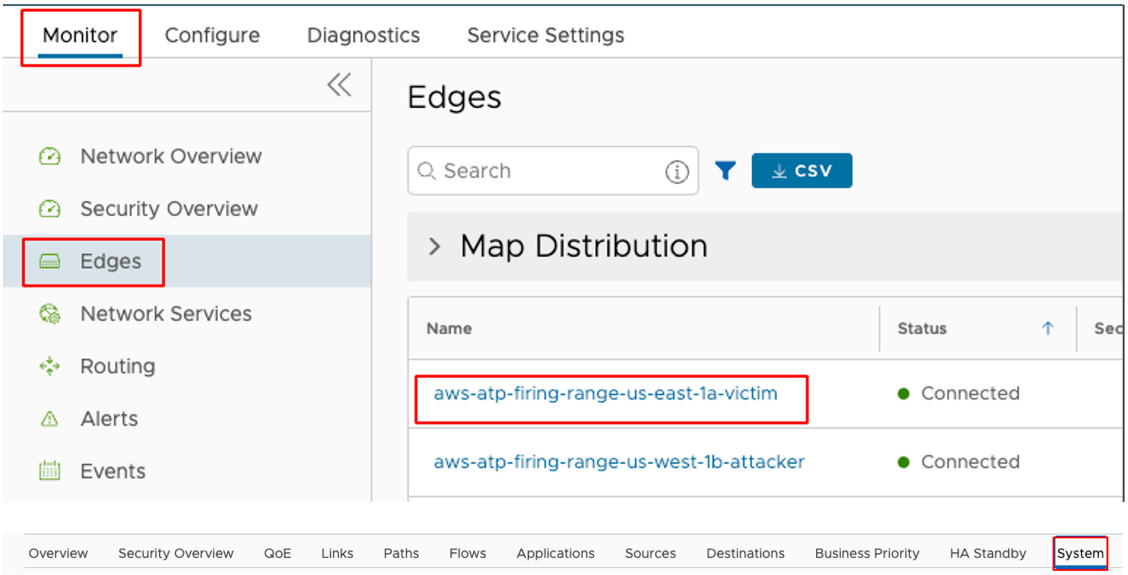
- Run Reports
  - Running a Report for the entire VMware SD-WAN network or even a single Edge can give you a quick glimpse of the types of traffic patterns and the corresponding percentage of the total traffic.
  - To run a Report, see Monitor Enterprise Reports. The report will show the Enterprise Traffic Distribution as shown below.



- Investigate Edge Utilization

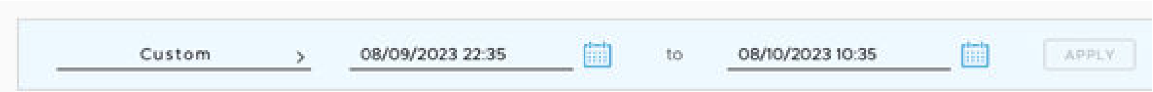
  Note To speed up the following process, contact your VMware representative to get the Edge utilization metrics of your entire VMware SD-WAN network.

  - Analyzing key utilization metrics such as CPU and memory usage, throughput, and flow count can help you make informed decisions about whether and how to deploy EFS. These metrics can provide insights into your current infrastructure usage and help you identify potential bottlenecks.
  - To view the CPU, memory usage, and flow counts, go to **Monitor** > **Edges** > Select the Edge you are investigating > **System**.



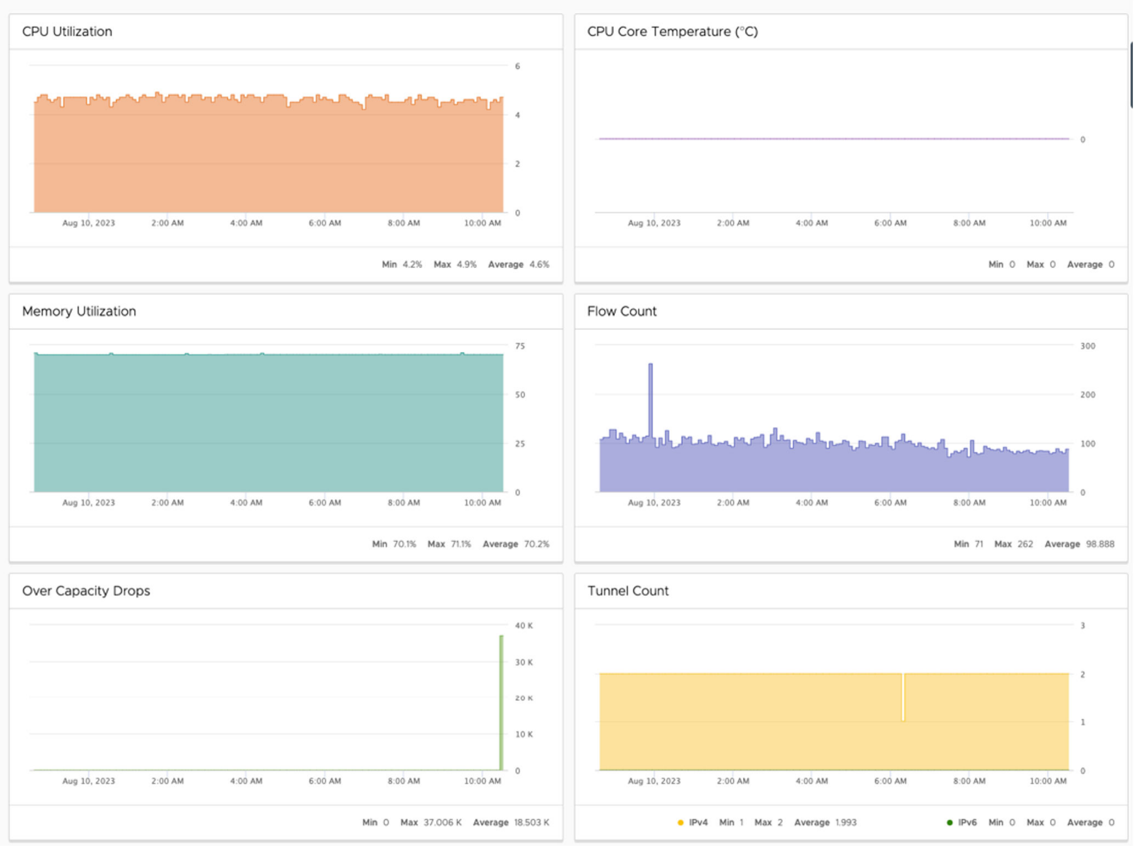
Name	Status	Sec
aws-atp-firing-range-us-east-1a-victim	● Connected	
aws-atp-firing-range-us-west-1b-attacker	● Connected	

  - Select a time range tfor analysis based on the type of Enterprise and the desired sample size. For example, a one-month time range may be sufficient for a small business, while a full year may be necessary for a large corporation.

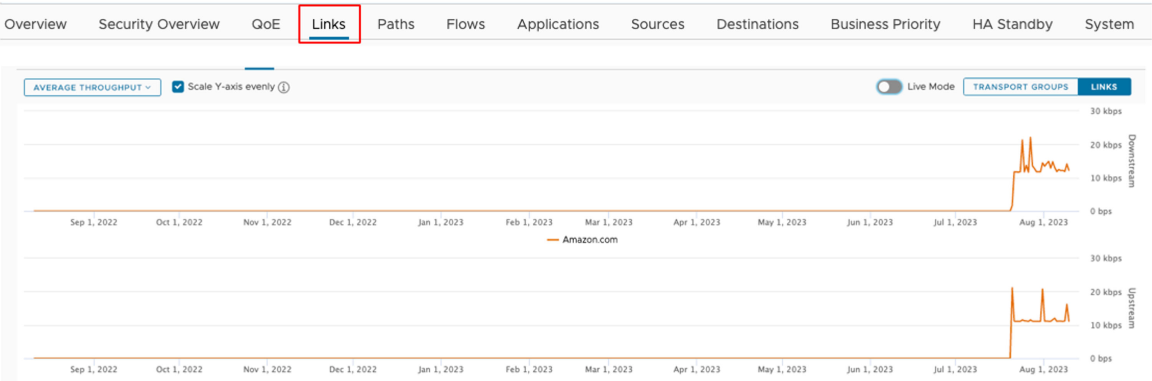


Custom > 08/09/2023 22:35 to 08/10/2023 10:35

  - The most important metrics for planning are CPU, Memory, flow count, and Over Capacity Drops. Specifically, the maximum and average values. It is important to cross-check the flow counts with the VMware SD-WAN Edge platform specifications..


CPU Utilization
6
4
2
0
Aug 10, 2023
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
Min 4.2% Max 4.9% Average 4.6%
CPU Core Temperature (°C)
0
Min 0 Max 0 Average 0
Memory Utilization
75
50
25
0
Min 70.1% Max 71.1% Average 70.2%
Flow Count
300
200
100
0
Min 71 Max 262 Average 98.888
Over Capacity Drops
40 K
30 K
20 K
10 K
0
Min 0 Max 37.006 K Average 18.503 K
Tunnel Count
3
2
1
0
● IPv4 Min 1 Max 2 Average 1.993
● IPv6 Min 0 Max 0 Average 0

- To view Average Throughput, select the **Links** tab.



- Make sure to cross-check these numbers with the VMware SD-WAN Edge platform specifications..

Adequate planning is essential for a smooth deployment. Now that you have investigated the branch site using the above tools, you can now develop a deployment strategy. Your strategy can be as simple as inspecting all traffic, assuming the branch has capacity, or gradually adding inspection to traffic and monitoring.

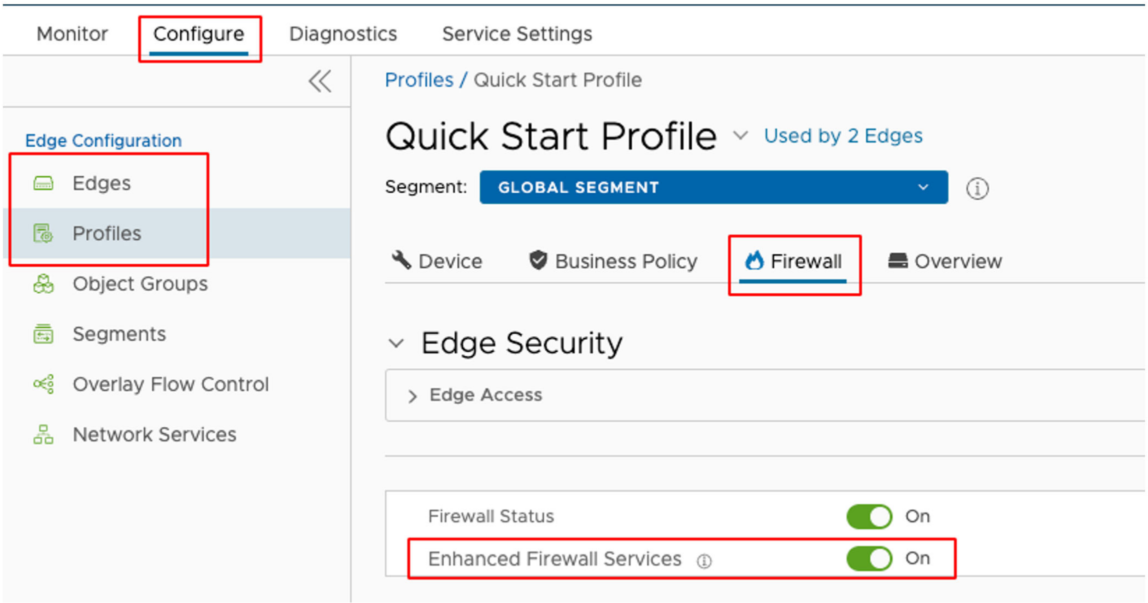
Day 1 Deploy

Activate EFS

Note Enhanced Firewall Services (EFS) is a licensed feature. EFS will only show up in a properly licensed environment.

Caution Activating or deactivating EFS may cause a disruption in network traffic.

- Enabling EFS can be done on either the Profile or Edge level.
- Go to **Configure** > **Profile** or **Edge** > Select the Profile or Edge you want to configure > **Firewall**. Make sure the **Enhanced Firewall Services** toggle is set to "On".

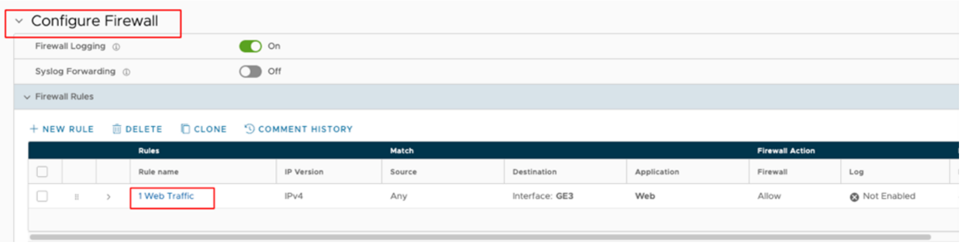


Segment: GLOBAL SEGMENT

Firewall Status On

Enhanced Firewall Services On

- Go to **Firewall Rules** and select an **ALLOW** firewall rule you would want EFS to inspect.

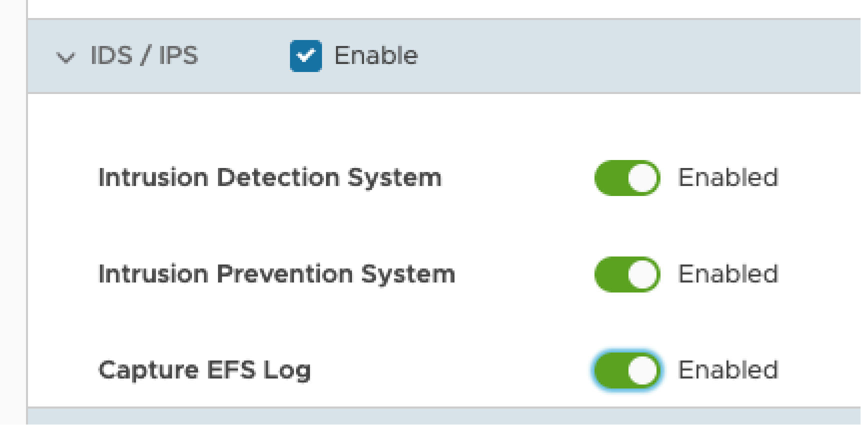


Firewall Logging On

Syslog Forwarding Off

			Rules		Match			Firewall Action	
□			Rule name	IP Version	Source	Destination	Application	Firewall	Log
□	⠿	›	1 Web Traffic	IPv4	Any	Interface: **GE3**	**Web**	Allow	⊗ Not Enabled

- Click the **Rule** link that you want to inspect and go to the **IDS/IPS** section. Select **Enable** check box and then configure the following options as required:



IDS / IPS ☑ Enable

Intrusion Detection System: Enabled

Intrusion Prevention System: Enabled

Capture EFS Log: Enabled

- **Intrusion Detection System** if you want for malicious traffic to be allowed but alerted.
- **Intrusion Prevention System** if you want EFS to alert and prevent malicious traffic.
- **Capture EFS Log** to log any traffic that is seen as malicious by the EFS.

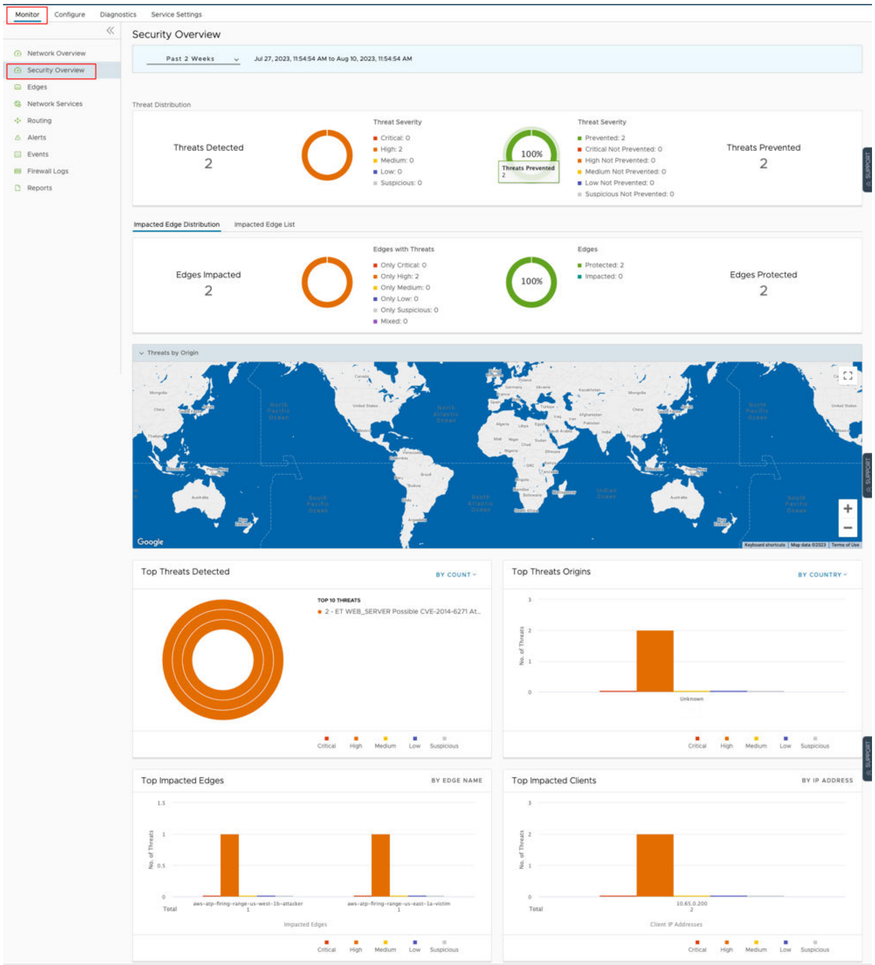
Day 2 Monitor and Optimize

After EFS has been activated and applied to ALLOW firewall rules, it is important to monitor the site for abnormalities. Utilizing the same metrics used for planning can provide a good indication of whether or not a site is stable. In addition to the tools provided by the Orchestrator, it is important to also be on the lookout for trouble tickets that relate to the site you worked on. If any metrics increase significantly, or if you observe Event log entries like EDGE_MEMORY_USAGE by navigating to **Monitor** > **Events**, or if there is a surge in user complaints from the site, you may need to roll back the changes and reevaluate.

Day N Maintain

Now that EFS has been deployed it is important to monitor your network for malicious activity. Integrating with a SIEM solution and/or monitoring the **Security Overview** dashboard can notify you of malicious events. The **Security Overview** dashboard offers a holistic view of your Enterprise's threat landscape, allowing you to quickly react to attacks.

- Go to **Monitor** > **Security Overview**.



Security Overview

Past 2 Weeks Jul 27, 2023, 11:54:54 AM to Aug 10, 2023, 11:54:54 AM

Threat Distribution

Threats Detected 2

Threat Severity
- Critical: 0
- High: 2
- Medium: 0
- Low: 0
- Suspicious: 0

100% Threats Prevented 2

Threat Severity
- Prevented: 2
- Critical Not Prevented: 0
- High Not Prevented: 0
- Medium Not Prevented: 0
- Low Not Prevented: 0
- Suspicious Not Prevented: 0

Threats Prevented 2

Impacted Edge Distribution | Impacted Edge List

Edges Impacted 2

Edges with Threats
- Only Critical: 0
- Only High: 2
- Only Medium: 0
- Only Low: 0
- Only Suspicious: 0
- Mixed: 0

100%

Edges
- Protected: 2
- Impacted: 0

Edges Protected 2

Threats by Origin

Top Threats Detected

TOP 10 THREATS
- 2 - ET WEB_SERVER Possible CVE-2014-6271 At...

Top Threats Origins

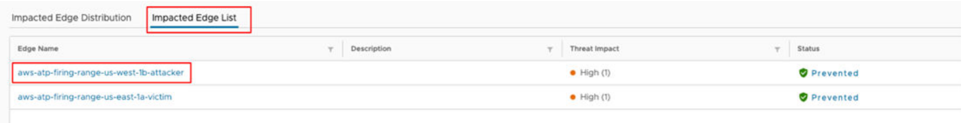
Top Impacted Edges

aws-atp-firing-range-us-west-1b-attacker 1
aws-atp-firing-range-us-east-1a-victim 1

Top Impacted Clients

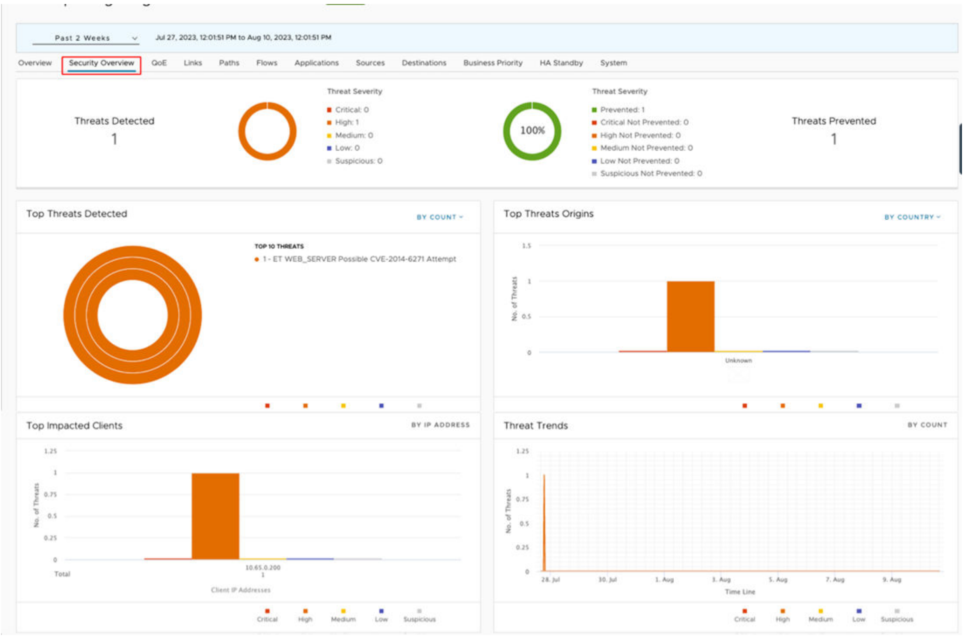
10.65.0.200 2

- If you want to investigate a single Edge. On this dashboard, select **Impacted Edge List** > select an Edge > **Security Overview** .



Impacted Edge Distribution | Impacted Edge List

Edge Name	Description	Threat Impact	Status
aws-atp-firing-range-us-west-1b-attacker		● High (1)	✓ Prevented
aws-atp-firing-range-us-east-1a-victim		● High (1)	✓ Prevented



Past 2 Weeks

Jul 27, 2023, 12:01:51 PM to Aug 10, 2023, 12:01:51 PM

Threats Detected 1

Threat Severity: Critical: 0, High: 1, Medium: 0, Low: 0, Suspicious: 0

Threat Severity: Prevented: 1, Critical Not Prevented: 0, High Not Prevented: 0, Medium Not Prevented: 0, Low Not Prevented: 0, Suspicious Not Prevented: 0

Threats Prevented 1

TOP 10 THREATS

1 - ET WEB_SERVER Possible CVE-2014-6271 Attempt

False Positive Workarounds

A False Positive, with regards to IDS/IPS, is a situation where legitimate traffic is being blocked/flagged by the IDS/IPS.

If you believe that the IDS/IPS might be incorrectly blocking legitimate traffic, follow the steps outlined below, starting from granular approaches and moving to more broad solutions, to resolve the problem.

In all cases, submit a support ticket outlining the type of traffic being dropped and the Signature ID that the traffic is hitting. To collect the appropriate data to submit in your support ticket, refer to the Firewall logs or your logging infrastructure that is collecting your syslogs.

If you use the Orchestrator-hosted logging, navigate to **Monitor** > **Firewall Logs** and find the suspected traffic. From these logs, gather the Source IP, Destination IP, Application, and Signature ID and add that to your support ticket.

Caution Activating and deactivating the Enhanced Firewall Service (EFS) may cause a disruption in network traffic.

Method 1: Create a More Targeted Firewall Rule Above the Offending Firewall Rule

The most specific solution is to create a more targeted firewall rule above the offending firewall rule by performing the following steps:

- Navigate to **Monitor** > **Firewall Logs** and filter the log entries to match the incorrectly blocked traffic. Note the Source/Destination IP/Port, Protocol, and Application. You will use that information to create a new firewall rule. Also note the Rule and Edge Name.
- Under the **Configure** tab, navigate to the **Edges** view and select the affected Edge.
- Navigate to the **Firewall** tab and expand the **Firewall Rules** area.

- Select **+ New Rule** and create a more specific rule based on the data you collected from the logs. Make sure to not activate IDS/IPS and then click **Create**.
- Select the firewall rule you just created and drag it to right above the offending firewall rule.
- Click **Save Changes**.
- Verify the change is working as intended and the traffic is not being blocked.

Method 2: Deactivate EFS at the Rule level

To further limit the scope of change you can select the offending rule and deactivate EFS at the firewall rule level. To deactivate EFS at the Rule level:

- Navigate to **Monitor** > **Firewall Logs** and select the appropriate log entry. From the **Rule** and **Edge** columns, note the Rule name and the Edge name.
- Under the **Configure** tab, navigate to the **Edges** view and select the affected Edge.
- Navigate to the **Firewall** tab and expand the **Firewall Rules** area.
- Find the offending Rule and select it. If the Rule is under the **Rules From Profile** area then you will need to navigate to the Profile and edit the rule from there. The steps to edit the rule at the Profile level are same as editing the rule at the Edge level.
- After selecting the Rule, scroll down to the **IDS/IPS** section. From the **IDS/IPS** section you can deactivate both IDS/IPS or you can just deactivate IPS.
- To deactivate both IPS and IDS, unselect the **Enable** check box.
- To deactivate only the IPS, toggle the **Enable** button next to **Intrusion Prevention System**.
- Verify the change is working as intended and the traffic is not being blocked.

Method 3: Deactivate EFS at the Edge level

If the issue is isolated at a single branch, then to limit the scope of changes, it might be best to deactivate EFS on the affected Edge. To deactivate EFS at the Edge level:

- Navigate to **Configure** > **Edges** and select the appropriate Edge to deactivate EFS.
- Navigate to the **Firewall** tab.
- In the **Enhanced Firewall Services** area, select the **Override** check box and then toggle the **Enhanced Firewall Services** button to **Off**.
- Verify the change is working as intended and the traffic is not being blocked.

Method 4: Deactivate EFS at the Profile level

If the issue is seen across several branches, then it might be prudent to deactivate EFS at the Profile level. To deactivate EFS at the Profile level:

- Navigate to **Configure** > **Profiles** and select the Profile that covers the desired Edges.
- From the Profile view, click the **Firewall** tab.
- Toggle the **Enhanced Firewall Services** button to **Off**.

- Verify the change is working as intended and the traffic is not being blocked.

References

- VMware SD-WAN Edge platform specifications
- VMware Cloud Web Security Configuration Guide
- Monitor Enterprise Reports