Integration Guide

VeloCloud SASE
QRadar SIEM

Services

Arista.com

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA +1-408-547-5500	+1-408-547-5502 +1-866-476-0000	+1-408-547-5501 +1-866-497-0000
www.arista.com/en/	support@arista.com	sales@arista.com

© Copyright 2025 Arista Networks, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos, and service marks ("Marks") displayed in this documentation are the property of Arista Networks in the United States and other countries. Use of the Marks is subject to the Arista Networks Terms of Use Policy, available at www.arista.com/en/terms-of-use. Use of marks belonging to other parties is for informational purposes only.

Contents

Chapter 1: Arista VeloCloud and QRadar SIEM Integration Guide..... 1

Chapter 2: Arista VeloCloud and QRadar SIEM Integration Overview.....2

Chapter 3: QRadar SIEM Integration Prerequisites.....5

Chapter 4: QRadar SIEM Integration Workflow..... 7

Chapter 5: How to Integrate VeloCloud Edge with QRadar SIEM.....16

Chapter 6: Troubleshooting and Diagnostics.....24

Appendix A: References.....28

A.1 QRadar SIEM Integration Device Support Module Files..... 29

A.1.1 Manifest..... 29

A.1.2 Device Support Module.....30

A.2 Related Documents.....52

Chapter 1

Arista VeloCloud and QRadar SIEM Integration Guide

This integration guide shows how QRadar SIEM and VeloCloud work together to give you a complete network security solution. QRadar has SIEM (Security Information and Event Management) capabilities that can analyze and alert you of any security issues in your network. VeloCloud featuring SD-WAN, has flexibility and scalability that can handle any network traffic and conditions. With this integration, you can see your network traffic in one place and deal with threats faster and better.

Chapter 2

Arista VeloCloud and QRadar SIEM Integration Overview

Arista VeloCloud SD-WAN integrates with QRadar SIEM to enable organizations with comprehensive cloud-enabled security, in addition to optimized connectivity.

General Overview

The cybersecurity landscape is constantly changing, with new threats emerging all the time. Cybercriminals can use different methods to attack, such as malware, ransomware, phishing attacks, and denial-of-service attacks. Cloud computing, mobile devices, and IoT endpoints have also created new ways for cybercriminals to attack.

Remote work has made it harder for organizations to protect their data and systems from attack. Employees working from home often use home networks that may not be as secure as the corporate network. They access corporate resources from these networks, which increases the risk of attack.

Integrating SIEM (Security Information and Event Management) platform with VeloCloud can help organizations monitor all traffic, no matter where it comes from, and quickly detect and respond to threats. VeloCloud provides a single point of control for all network traffic, including traffic on the public internet. SIEM can collect and analyze this traffic for signs of malicious activity.

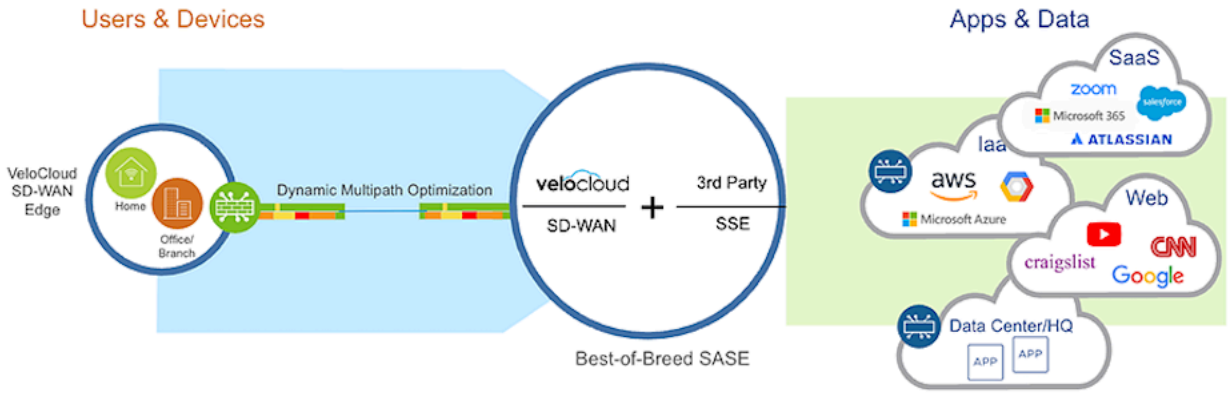
By integrating SIEM with VeloCloud, organizations can get a better view of their network traffic and spot threats faster. This can help them protect their data and systems from attack and improve their overall security posture.

This document will explain the technical aspects of integrating VeloCloud SD-WAN with QRadar SIEM. This will help organizations use VeloCloud capabilities faster and integrate them with their existing security ecosystem.

Arista VeloCloud Overview

VeloCloud™ leverages a Best-of-Breed SASE strategy by combining its industry-leading SD-WAN with seamless integration of leading Security Service Edge (SSE) solutions. This enables secure, reliable, and optimized connectivity for users—regardless of location—to applications across the edge, cloud, and data center. The solution enhances user experience, simplifies operations, and supports compliance risk mitigation.

Figure 2-1: VeloCloud Overview



You can deploy VeloCloud in diverse ways, such as a cloud-delivered service, a software-only solution, or a hybrid solution. This flexibility makes it a good option for organizations of any size and IT maturity level.

Some of the benefits of VeloCloud include:

- **Simplified connectivity management:** VeloCloud simplifies connectivity management through VeloCloud Orchestrator providing you a single place to manage your networking and security settings. This can help you reduce the complexity of your security infrastructure.
- **Improved security posture:** VeloCloud includes built-in security at the edge and combines several security technologies with third party SSE vendors to provide a comprehensive and flexible security approach. This can help you protect your organization from various threats.
- **Increased agility:** VeloCloud is a cloud-based solution, so you can easily scale it up or down as your needs change. This can help you be more agile in responding to changes in your business environment.

QRadar Overview

QRadar is a security information and event management (SIEM) solution that collects, analyzes, and correlates security data from various sources. This data can include logs, network traffic, and security alerts. QRadar uses this data to identify and respond to security threats and comply with industry regulations.

QRadar is a robust and scalable solution that organizations of any size can use. It is also a cloud-based solution, which you can easily deploy and scale to meet your organization's needs.

Some of the key features of QRadar include:

- **Data Collection from multiple sources:** QRadar can collect data from various sources, such as firewalls, intrusion detection systems, and web proxies. You can use this data to identify and respond to security threats.
- **Data Correlation:** QRadar uses machine learning and artificial intelligence to analyze and correlate data. This lets QRadar find patterns and anomalies that may indicate a security threat.
- **Threat Response:** You can use QRadar to respond to security threats. This can include automatically blocking malicious traffic, sending alerts to security analysts, and taking other actions to stop threats.
- **Regulatory Compliance:** You can use QRadar to help your organization comply with industry regulations. This can include PCI DSS, HIPAA, and SOX.

Chapter 3

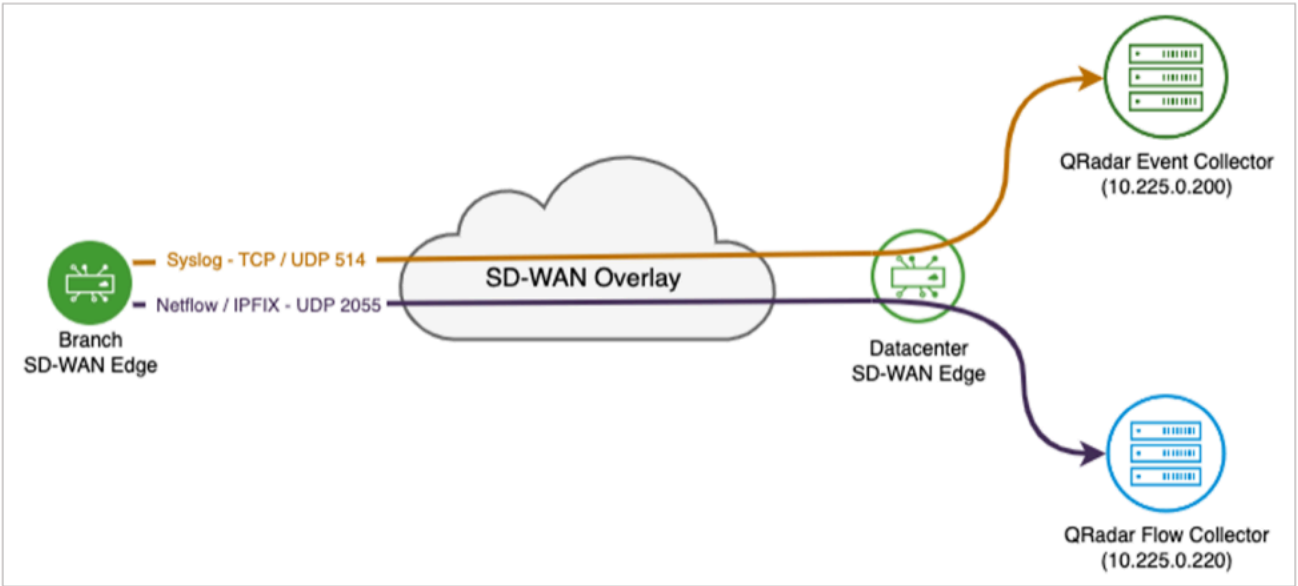
QRadar SIEM Integration Prerequisites

This document includes information on the supported data collection methods, QRadar SIEM and VeloCloud software versions, QRadar SIEM Device Support Modules, and SIEM license requirements.

Data Collection Methods supported from Arista VeloCloud

VeloCloud consists of multiple services. In this guide, we will describe integration between the SD-WAN Edge appliances and QRadar SIEM, using Syslog and IPFIX Data. Other types of integrations might be delivered in the future. This guide will use the following network connectivity between Edges and QRadar Collector Nodes

Figure 3-1: Edge to QRadar Collector Node Connectivity



Software Version Matrix

The following table shows the versions of both VeloCloud and QRadar used in this guide:

Table 1: VeloCloud & QRadar Versions

VeloCloud & QRadar Versions Tested	
QRadar	7.3.3 Field Patch 6 or higher
Log Source Management	7.0.1 or higher
VeloCloud Orchestrator	5.2.0.0 or higher
VeloCloud Edge	5.2.0.0 or higher

QRadar SIEM Device Support Module (DSM) for VeloCloud

The QRadar DSM (Device Support Module) software component lets QRadar collect data from various devices, such as firewalls, intrusion detection systems, and web proxies. The DSM provides a standardized

interface for collecting data from these devices, which makes it easier for QRadar to ingest and analyze the data.

The QRadar DSM also has many features that help improve the performance of QRadar, such as data compression and filtering. This can help reduce the amount of data that QRadar needs to store and process, which can improve the system's performance.

For VeloCloud, you can download proprietary DSM modules from the Arista Developer portal or X-Force App Exchange. The DSM modules make sure that QRadar can format and display messages from VeloCloud services such as Edge devices. The DSM also contains event mappings to inject various VeloCloud events in a standard format message in your enterprise's overall IT security ecosystem.

Note: You can reference the Version 1.7.0 of the QRadar SIEM Device Support Module here: QRadar SIEM Integration - Arista VeloCloud Edge Device Support Module v1.7.0.

QRadar SIEM License Requirements

You do not need a special license to receive events from VeloCloud. The integration will use both events per second (EPS) and flow per minute (FPM) licenses:

- **Edge logs:** QRadar EPS (Events per Second) license required.
- **Edge Traffic Telemetry via IPFIX:** QRadar FPM (Flows per Minute) license required.

Make sure the event collectors that collect logs and flow data have enough license allocations in QRadar. After you onboard the service, monitor the license requirements and adjust allocations as needed under (QRadar) **Admin** > **System** > **System and License Management** > **License Pool Management**.

See this KB Article for more information on event and flow capacity management.

Chapter 4

QRadar SIEM Integration Workflow

This section discusses how to integrate QRadar SIEM with VeloCloud and includes instruction on creating a Log Source group, importing the VeloCloud Edge DSM module, and setting up VeloCloud Edges as Log Source records.

Before data can be onboarded from the VeloCloud solutions, the QRadar SIEM service must be prepared to accept the data. This requires the following steps:

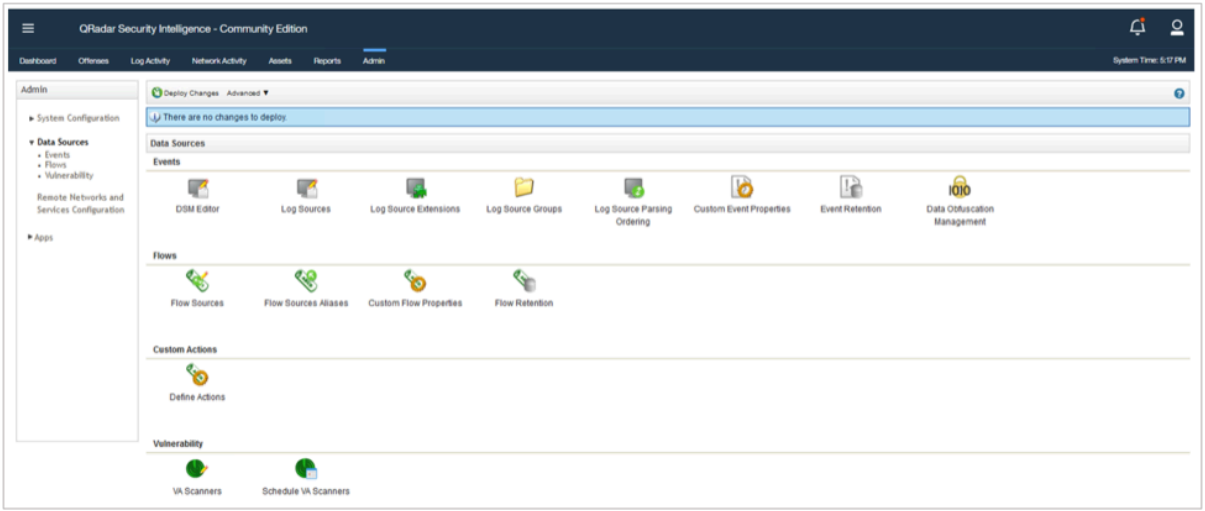
1. Create a Log Source Group for your Edge appliances.
2. Import the VeloCloud Edge DSM module.
3. Set up VeloCloud Edges as Log Source records.

Once these steps are ready, you can configure the VeloCloud Edges in the VeloCloud Orchestrator to send log messages and flow telemetry data to their designated event collectors.

1. **Create a Log Source Group for your VeloCloud Edge Appliances**:
   a. Log Source Groups help you manage larger-scale network deployments by associating default DSMs or Log Source Extensions with your network devices. Log source groups help filter event data to a particular group of devices.

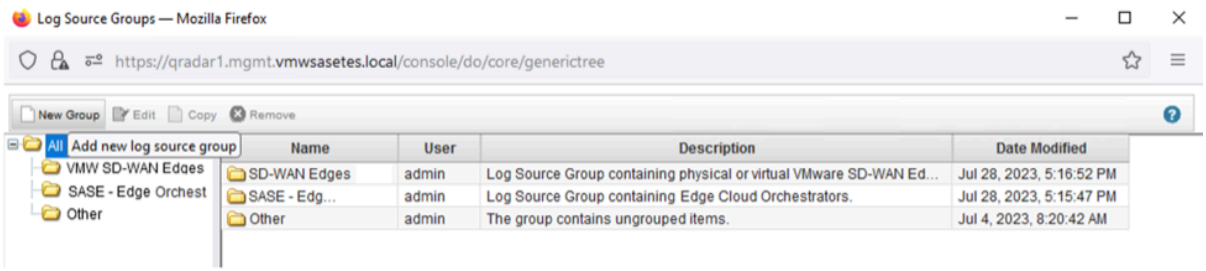
   b. To view or create a Log Source Group, go to **Admin** > **Data Sources** > **Events**. Depending on your system, you might see something similar:

   Figure 4-1: QRadar - Data Sources



c. In the main window, select **Log Source Groups**, then select **New Group** in the new window:

Figure 4-2: Log Source Group Management



d. A new window, titled **Group Properties** opens:

Figure 4-3: Log Source Group Properties

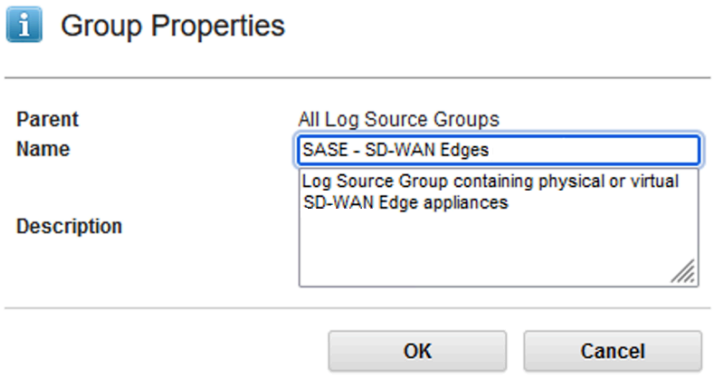


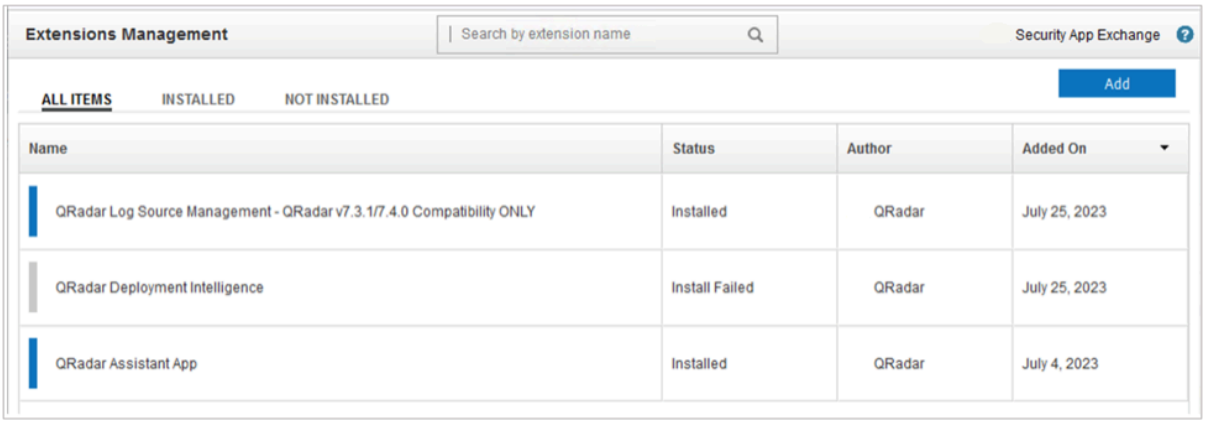
Table 2: Log Source Group Properties

QRadar – Log Source Group Properties	
Parent	The parent container for the newly created child object. Before you save your changes, make sure that the new Log Source Group is created under the correct container. QRadar supports nested Log Source Groups.
Name	Administrative name for the Log Source Group
Description	Summary of the log source group's function or its contents.

2. **Import the VeloCloud Edge DSM module into your QRadar Deployment**: Now that the Log Source Group is ready, we will import the custom DSM for VeloCloud Edge appliances. The DSM is delivered as a ZIP archive.

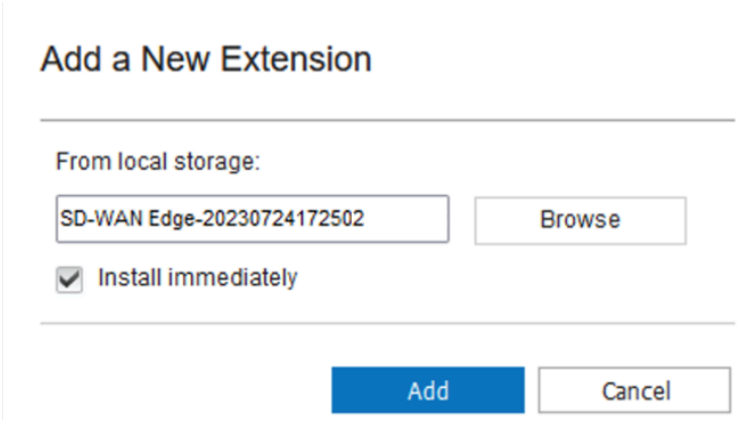
a. To start with the import process, navigate to **Admin** > **System Configuration**, then select **Extensions Management**:

Figure 4-4: Extensions Management



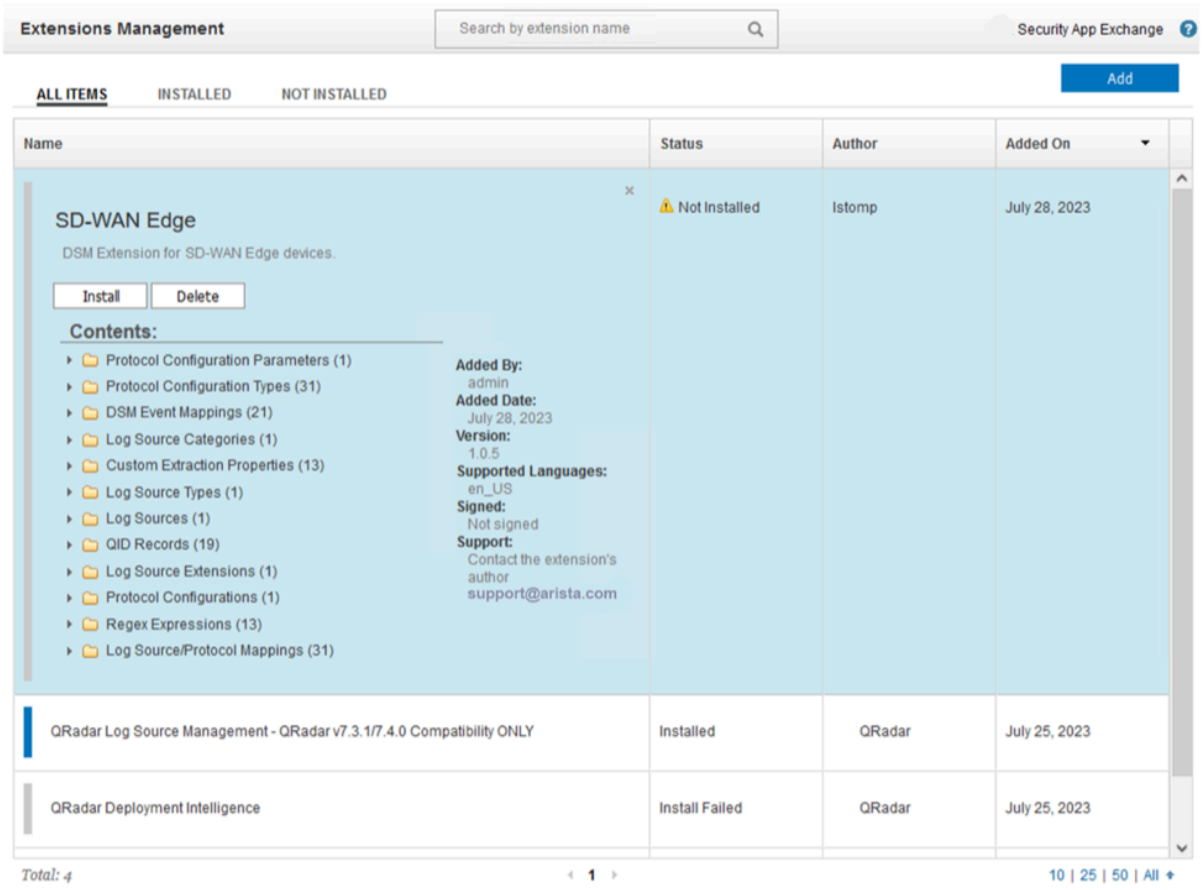
b. In this window, you will see a list of extension modules that enhance QRadar functionality and their installation statuses. The list of available modules depends on your deployment. To upload the ZIP archive, select the **Add** button in the top-right corner. If you want to install it right away, select **Install Immediately**:

Figure 4-5: Add New Extension



c. After the upload, a new line item will appear in the **Extensions Management** window. From here you can install the DSM (if you have not done it already), remove the module or look at its contents (the output might vary based on the DSM contents):

Figure 4-6: VeloCloud Edge DSM Contents

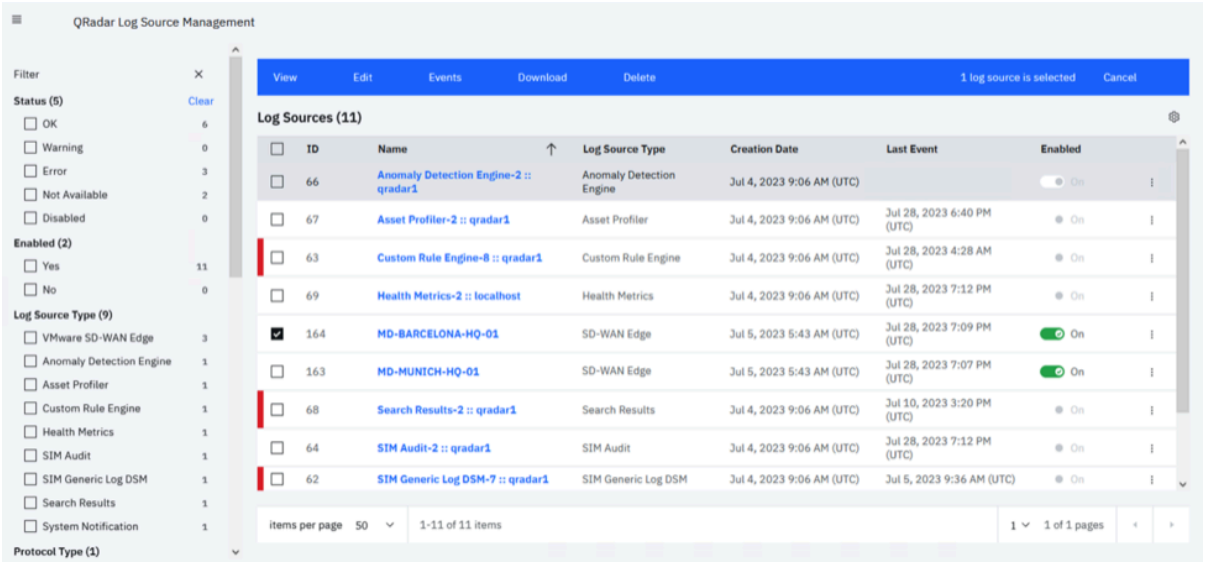


3. **Create a Log Source Record for Each VeloCloud Edge**:

   a. You need to create a log source record for each VeloCloud Edge to make them trusted sources of events. You can use an extension called **QRadar Log Source Management**to set up the Edge Syslog feeds. This extension may be different from the legacy **Log Source Management** interface, depending on your QRadar version.

b. To launch the application, go to **Admin** > **Apps** > **QRadar Log Source Management**.

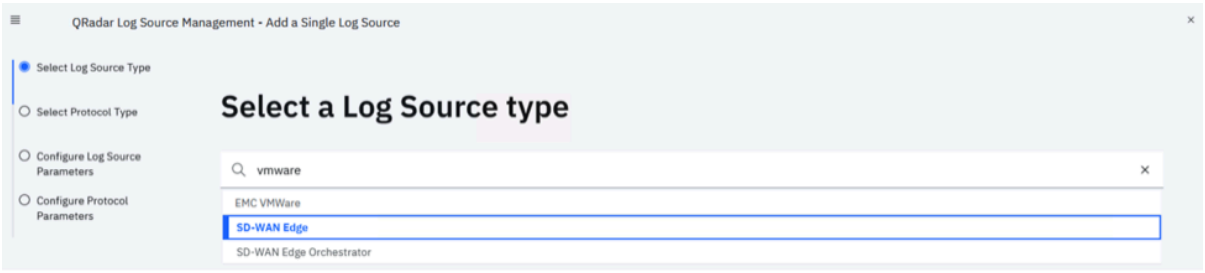
Figure 4-7: Log Source Management



c. After selecting on **+ New Log Source**, select **Single Log Source** (if you want to add just one Edge appliance), or **Multiple Log Sources** (if you need to create log sources in bulk).

d. Under **Select Log Source Type**, search for **SD-WAN Edge**:

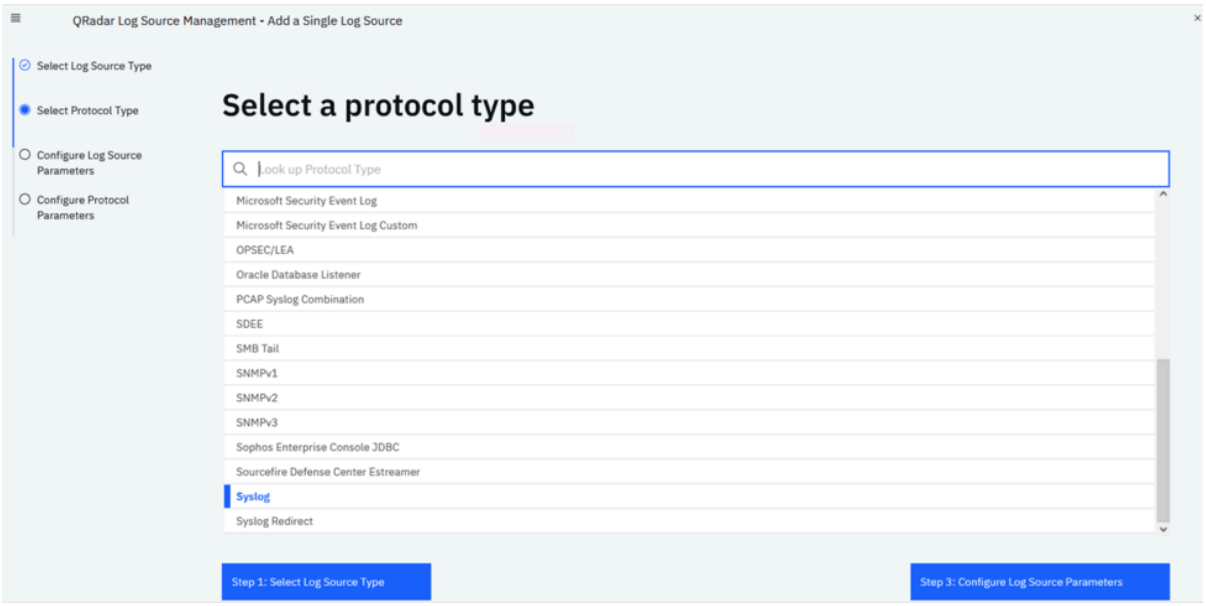
Figure 4-8: Select a Log Source Type



Note: If you cannot find the SD-WAN Edge option, check the **Admin** tab to see if changes are to be deployed, or you can do a **Deploy Full Configuration** from **Advanced**. After a few minutes, the log source type should show up.

e. Under **Select a Protocol Type**, it should default to Syslog, this is what we need:

Figure 4-9: Select a Protocol Type



f. On the **Log Source** parameters screen, you must complete all the device-specific details:

Figure 4-10: Log Source Parameters

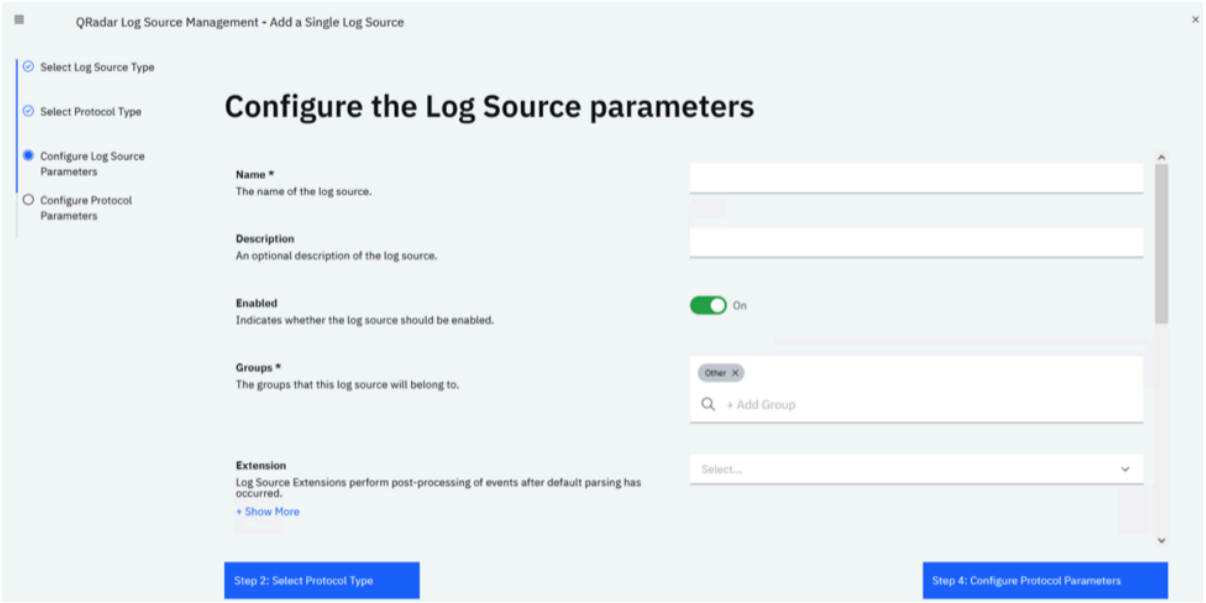
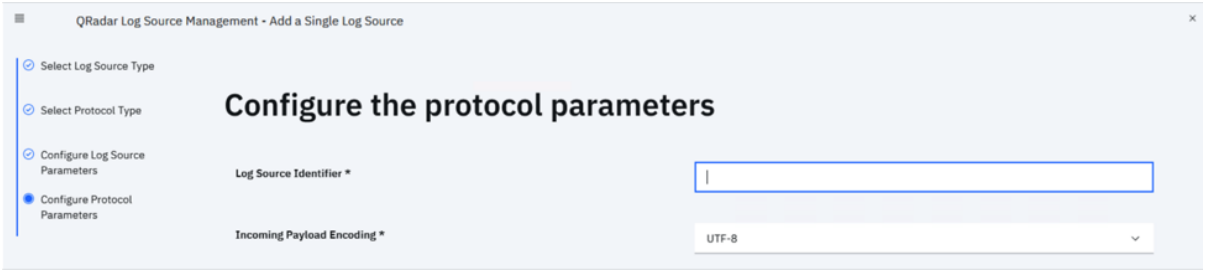


Table 3: Log Source Parameter Descriptions

Parameter Name	Description	Mandatory?
Name	The device name of the Edge (as appears in the Orchestrator).	Yes
Description	A brief description that helps identify the appliance sending events.	No
Enabled	This switch instructs QRadar to use this record to identify the log source, or not.	Yes
Groups	Assigns the device to a log source group. A device can be part of multiple groups if required. Grouping can help parse events faster or manage group members in a uniform fashion.	Yes
Extension	The associated DSM that helps to correctly format messages from the device and perform event mapping against logs. This should point to the SD-WAN Edge Extension.	No
Language	The language of the logs. Defaults to English.	Yes
Target Event Collector	Most of the QRadar deployments are distributed in nature. You can select the correct event collector that should accept Syslog messages from the Edges and parse them.	Yes
Credibility	An administrative measure on a scale of from 0 to 10, It is a measure of the log source's reliability.	Yes
Coalescing Events	If this feature is enabled, the SIEM will aggregate similar activities into a single entry.	No
Store Event Payload	If enabled, QRadar will record the payload of the Syslog messages. Typically enabled in production environments.	No

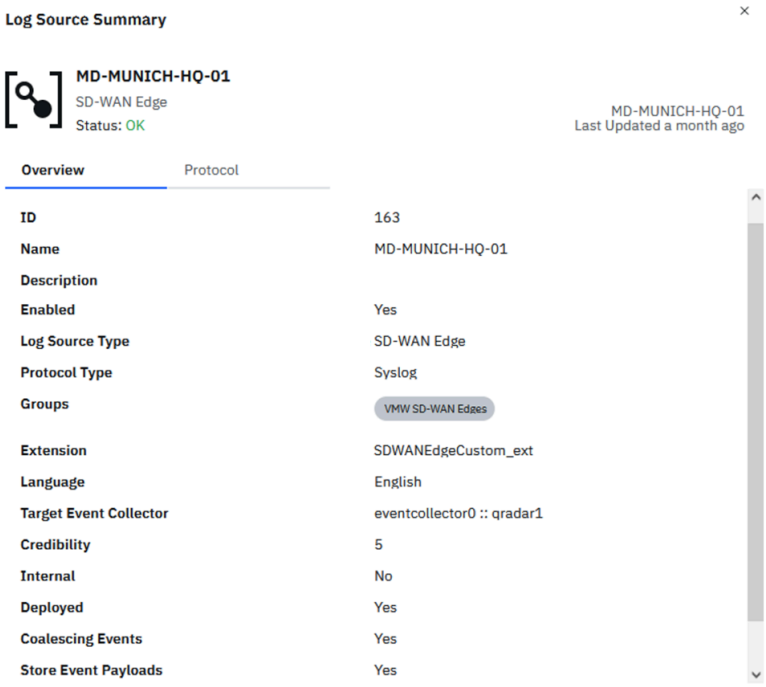
Once every parameter is set, you can progress to the next screen, selecting the **Protocol Parameters**. Encoding should be UTF-8, and the **Log Source Identifier** must be configured as the device name from the Orchestrator.

Figure 4-11: Protocol Parameters



Once all settings are set, select **Finish**. By selecting on the log source in the main screen, the **Log Source Summary** screen will open, and you can double-check the settings:

Figure 4-12: Log Source Summary of an Edge



Note: If you are using a distributed QRadar deployment (common in production environments), take note of the **Target Event Collector** setting, as you will set this up as a IPFIX and Syslog Target.

Event collectors might have multiple network interfaces that might have various assigned roles. See this KB article if you need assistance understanding how your QRadar deployment is connected to your enterprise network fabric.

4. **How to Integrate VeloCloud Edge with QRadar**: You have prepared QRadar to receive data from the VeloCloud Edge appliances. Now, you need to configure the QRadar Event Collectors as IPFIX and Syslog service endpoints. QRadar uses "Regular" network interfaces to collect log and flow data. If you are not sure what the interface IP address is, follow these steps:

   a. Go to **Admin** > **System Configuration** > **System and License Management**.

   b. In the **Display** field, select **Systems**.

   c. Select the **Event Collector** that you want to use as a target system.

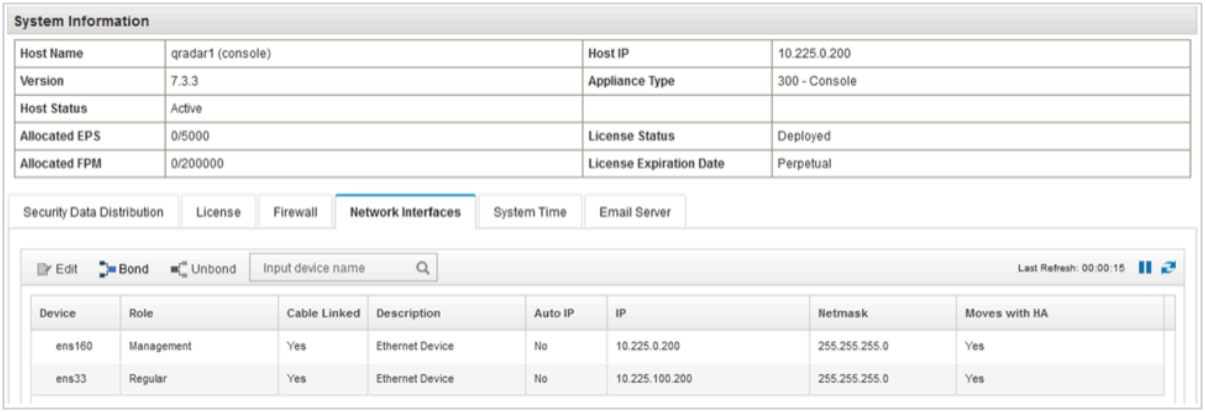
   d. Open the **Actions** drop-down menu from the top menu bar.

   e. Select **View and Manage System**.

   f. Select the **Network Interfaces** tab in the new window.

You will see a similar output for your node: Event Console node with two NICs, one used for OOB management, the regular NIC used for event and flow collection.

Figure 4-13: Network Interfaces



5. Now, you can switch from QRadar to the VeloCloud Orchestrator. Perform the following steps in the Orchestrator:

   a. On the Enterprise level, define the QRadar Flow Collectors as NetFlow/IPFIX Collectors.

   b. On the Edge or Profile level, enable the Edges to start the flow export process and send telemetry to the Flow Collectors defined in the previous step.

   c. While on the **Edge** or **Edge Profile** level, configure **Event Collectors** as **Syslog servers**.

   d. Enable the **Edge Firewall** or **Enhanced Firewall Services** logging.

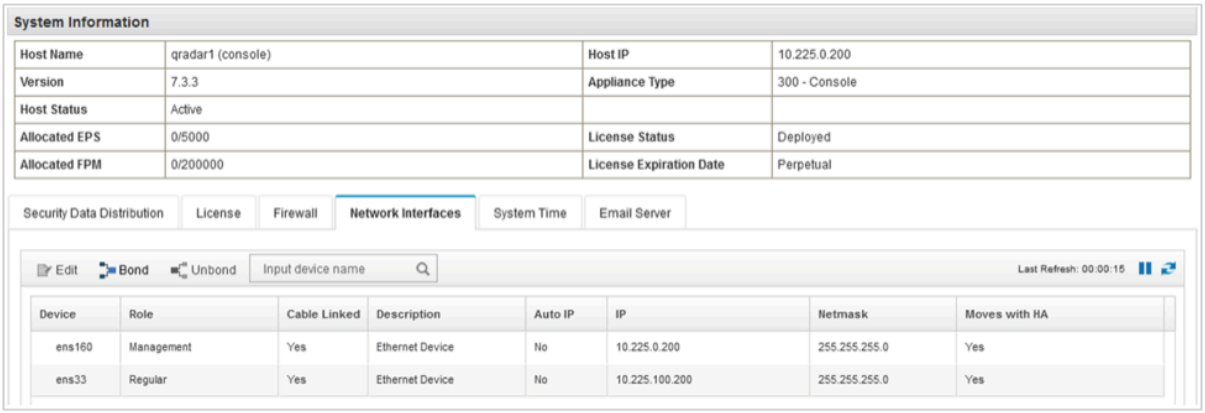
   e. Define a **Firewall Rule** with logging enabled.

Chapter 5

How to Integrate VeloCloud Edge with QRadar SIEM

This section explains how to integrate VeloCloud Edges with QRadar SIEM. It includes instructions on how to configure QRadar Event Collectors as IPFIX and Syslog service endpoints. This section also covers how to set up QRadar Flow Collectors as IPFIX Collectors in the VeloCloud Orchestrator, set up NetFlow in Edge Profiles, add the QRadar Event Collectors as Syslog Servers, turn on Syslog Forwarding for Edge Firewall and Enhanced Firewall Services, and create a Firewall Rule.

1. **How to Integrate VeloCloud Edges with QRadar**: You have prepared QRadar to receive data from the VeloCloud Edge appliances. Now, you need to configure the QRadar Event Collectors as IPFIX and Syslog service endpoints. QRadar uses "Regular" network interfaces to collect log and flow data. If you are not sure what the interface IP address is, please follow these steps:
   a. Go to **Admin** > **System Configuration** > **System and License Management**.
   b. In the **Display** field, select **Systems**.
   c. Select the **Event Collector** that you want to use as a target system.
   d. Open the **Actions** drop-down menu from the top menu bar.
   e. Select **View and Manage System**.
   f. Select the **Network Interfaces** tab in the new window.
      You may see a similar output for your node: Event Console node with two Network Interface Controllers (NICs), one used for OOB management, the regular NIC used for event and flow collection.
      Figure 5-1: Network Interfaces



   g. Now, you can switch from QRadar to the VeloCloud Orchestrator. Perform the following steps in the Orchestrator:
      1. On the **Enterprise** level, define the QRadar Flow Collectors as NetFlow/IPFIX Collectors.
      2. On the **Edge** or **Edge Profile** level, enable the Edges to start the flow export process and send telemetry to the Flow Collectors defined in the previous step.
      3. While on the **Edge** or **Edge Profile** level, configure **Event Collectors** as Syslog servers.

4. Enable the **Edge Firewall** or **Enhanced Firewall Services** logging.
5. Define a Firewall Rule with logging enabled.

2. **How to Set Up QRadar Flow Collectors as IPFIX Collectors in the VeloCloud Orchestrator**: The QRadar system can receive IPFIX updates by default on UDP port 2055. You need to define the system as a Flow Collector. You can do this at the enterprise (customer) level first. Follow these steps:
   a. Go to **Configure** > **Network Services** > **Network Management** > **NetFlow** > **Collectors** in the VeloCloud Orchestrator.
   b. Select **+ New**.
   c. Configure the settings as shown below:

Figure 5-2: New Flow Collector Configuration in the VeloCloud Orchestrator

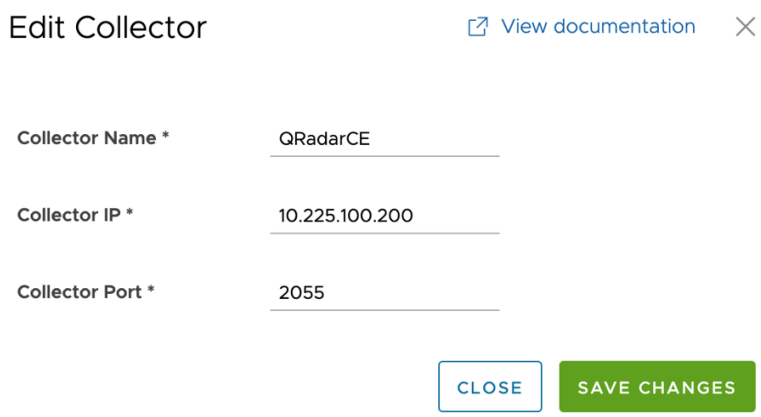


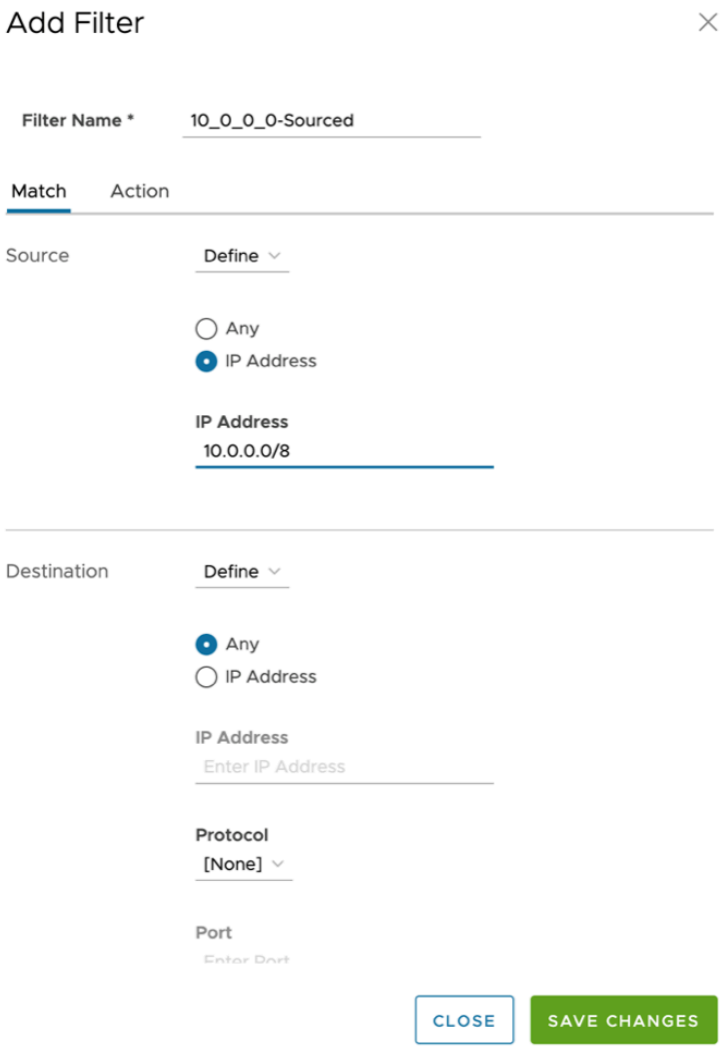
Table 4: Flow Collector Settings

Flow Collector Settings	
Collector Name	An administrative name of the collector that provides identification.
Collector IP	The destination IPv4 address that flow data will be sent. In case of QRadar, this will be the Regular NIC of the Flow Collector system.
Collector Port	The UDP port on which the Collector is listening for inbound flow data from network devices. In case of QRadar, this is UDP port 2055.

Note: If you use multiple QRadar Event Collectors for your VeloCloud SD-WAN fabric, ensure they are all added.

d. Once all the collectors are defined, you can create filters to reduce the number of flows sent by defining filters. To do this, select **+New** under **Filters** in the main Orchestrator screen:

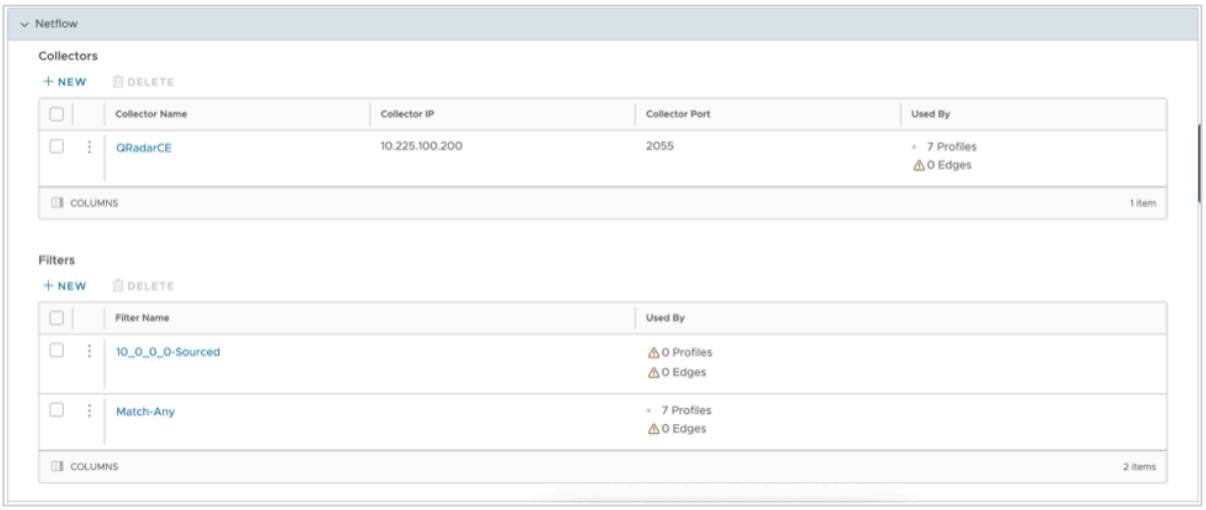
Figure 5-3: Add Filter



Filters work as match/set statements, you can select traffic sources in the **Match** tab, **Destinations** and even **Applications** (data derived from Deep Application Recognition or DAR), and based on the defined criteria, flow records can get exported to flow collectors or filtered. This is a helpful mechanism to save Flows per Minute (FPM), which helps you to spend your QRadar Flow licenses in the most optimal way.

When everything is set, please ensure that all settings are correct in the **Network Services** configuration screen:

Figure 5-4: NetFlow Settings Summary



While the IPFIX settings must be pre-defined on an enterprise level, Syslog settings can be applied without any previous definition (as of Release 5.2.0.x). In the next step, we will define the QRadar event collectors as Syslog targets and apply the IPFIX settings we created.

3. **Set up NetFlow in Edge Profiles**: You need to use one or more profiles to build your VeloCloud SD-WAN fabric. Profiles are like templates that help you apply common settings to many devices in your network. First, you need to find the profiles that you want to use for your deployment. You also need to set QRadar as a Flow Collector for each profile.

   a. Go to **Configure** > **Profiles** and select the profile you want to change.

   b. Go to the **Device** tab and select **Telemetry**. Then check the box for **Activate NetFlow**:

   Figure 5-5: Activate NetFlow

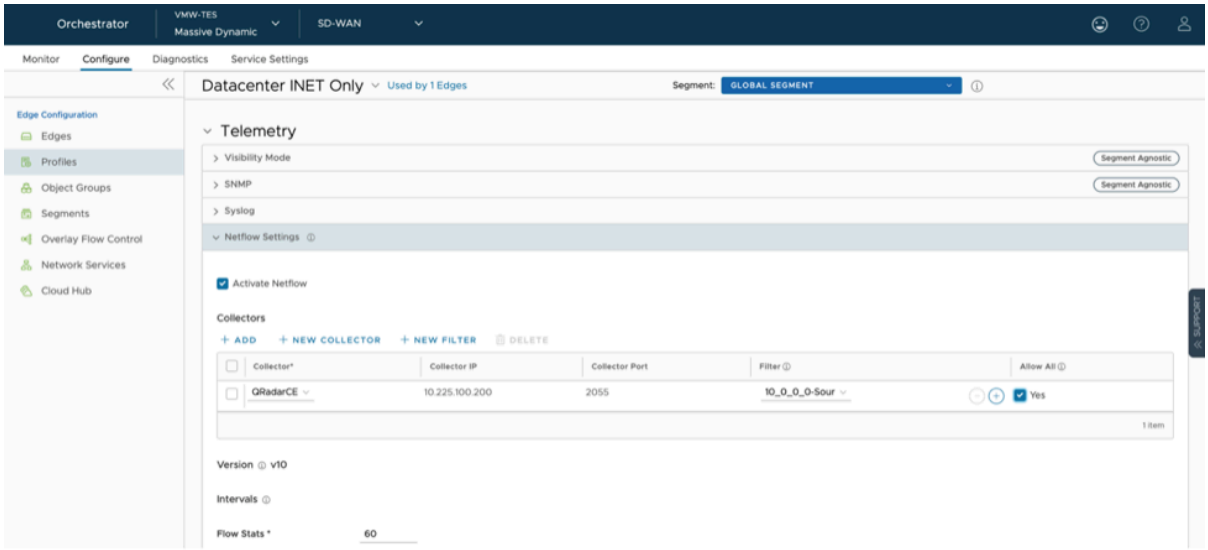


Table 5: Flow Collector Settings – Edge Profile View

Flow Collector Settings – Edge Profile View	
Collector	Select the collector that is the designated event collector for Edges using this profile.
Collector IP Address (Read-Only)	The destination IPv4 address that flow data will be sent. In the case of QRadar, this will be the Regular NIC of the Flow Collector system.
Collector Port (Read-Only)	The UDP port on which the Collector is listening for inbound flow data from network devices. In case of QRadar, this is UDP port 2055.
Filter	Select a pre-configured filter to ensure that only relevant flows will be exported to the Flow collector.
Allow All	If you are using a multi-segment (Multi-user) SD-WAN deployment, and you need to collect flows from traffic in other segments, check this option.
Version	VeloCloud SD-WAN only supports IPFIX (NetFlow Version 10) data export.
Intervals (Multi-line)	If you need to fine-tune the flow export operations, you can change the flow timers here. This configuration is only available if the Global Segment is selected in the segment selection drop-down box at the top.

c. After you make the changes, select **Save Changes**, and wait for them to take effect. You can see the progress of the changes from the **Events** view.

4. **Add the QRadar Event Collectors as Syslog Servers**: QRadar Event Collectors can receive Syslog data from Log Sources on UDP and TCP ports 514. To make sure that the Edges send log events to QRadar, not just Flow data, you should make most changes at the profile level. This will make sure that all Edges in your VeloCloud SD-WAN fabric have the same security configuration and can scale out easily. You need to find all the Edge Profiles that you want to use for your deployment first.

a. To set up Syslog services, go to **Configure** > **Profiles**, then choose the profile(s) you want to change, and then go to the **Device** tab and select **Telemetry**.

b. Under the **Syslog** section, check the box for **Enable Syslog**.

Figure 5-6: Enable Syslog

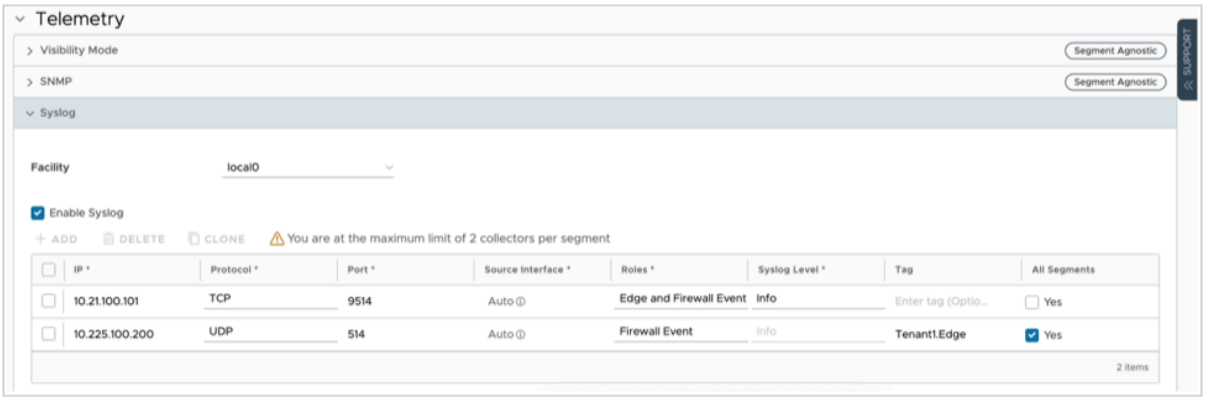


Table 6: Syslog Settings – Edge Profile View

Syslog Settings – Edge Profile View	
IP	Type in the IP address of the QRadar Event collector managing the edges associated with this profile. This is typically the same Event collector node that the Edge is using as a Flow Collector.
Protocol	The VeloCloud Edge supports both UDP and TCP protocols. Based on your QRadar deployment and network connectivity, you might prefer one or the other.
Port	By default, the QRadar Event Collectors listen to Syslog under port 514 (both TCP and UDP).
Roles	This setting supports Edge Events, Firewall Events and Edge and Firewall Events. In case of QRadar, both is supported in the DSM. In case you want to retrieve Edge Events (Interface status changes, Management and Control Plane updates, and so forth) using the Orchestrator API, you can select Firewall Events only.
Syslog Level	Based on the Level selected here, events classified on this level (or higher) will be sent to the Syslog server. If Firewall Events is set under Roles, this field will default to Info, as Firewall events are set as Informational messages.
Tag	Each Syslog message can be appended with a custom tag in the header. Some systems can identify tenants and other service details from this tag. In QRadar, this tag has no relevance.
All Segments	If you have a multi-segment (Multi-user) SD-WAN fabric, and need to export firewall events from all segments, you should select this box.

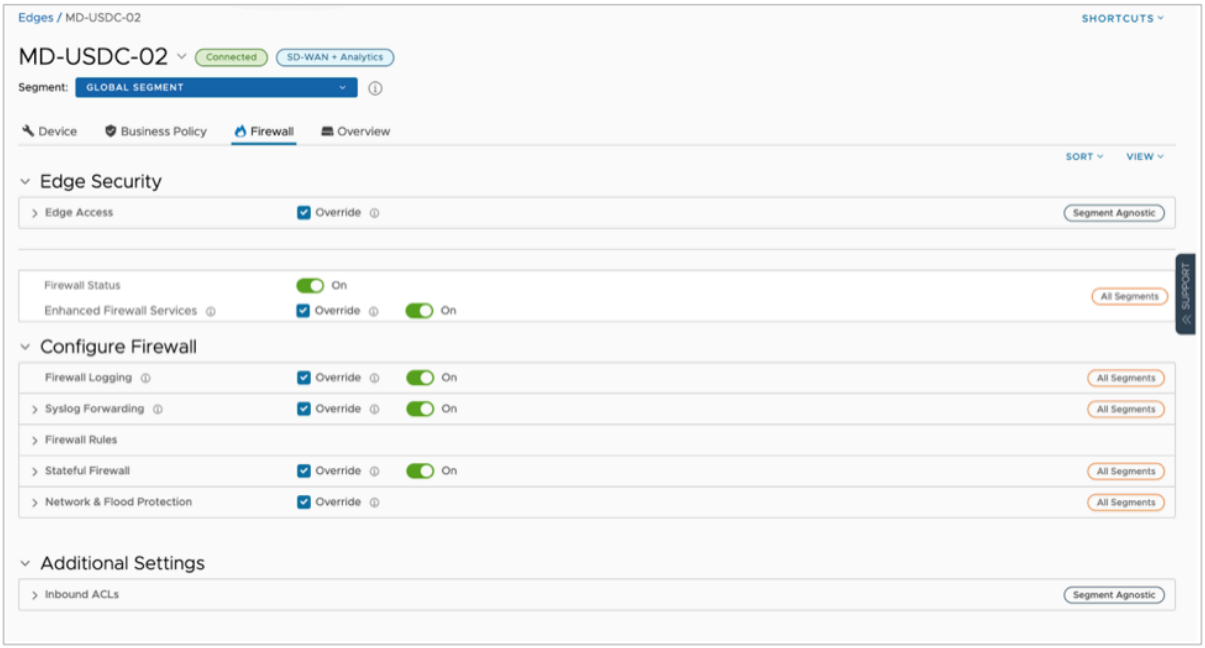
c. Make sure you **Save Changes** to complete your configuration.

5. **Turn on Syslog Forwarding for Edge Firewall and Enhanced Firewall Services**: Now you can send Edge events (like configuration changes, interface changes, and so on) to QRadar, but you also need to send firewall events. You can do this on the Profile or Edge level. Usually, it is better to do this on the profile level to make sure it works for all devices in your network. But sometimes, you may have different firewall rules for each Edge, so in this guide, we will show you how to do it on the Edge level.

   a. Go to **Configure** > **Edges** and choose the Edge that you want to change.

   b. Select on the **Firewall** tab.

Figure 5-7: Edge Firewall Settings



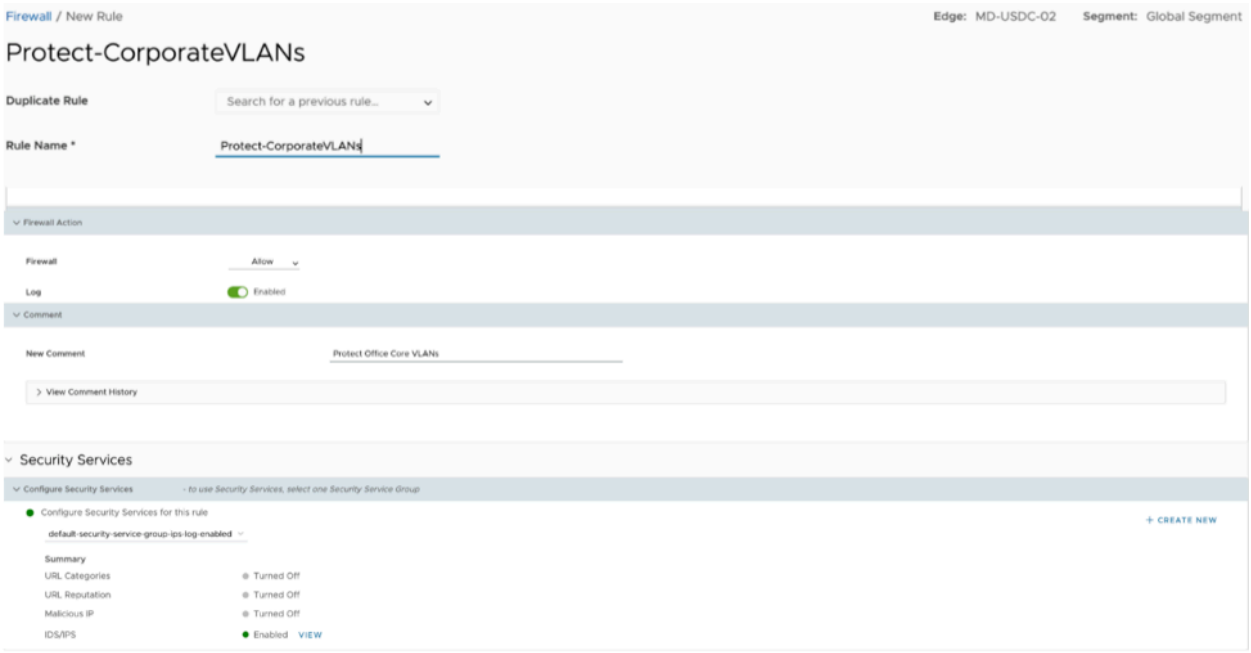
c. On the **Firewall** tab, ensure these settings are turned on:

- **Firewall Status**
- **Enhanced Security > Intrusion Detection / Prevention** (6.x+ versions) or **Enhanced Firewall Services** (5.2.x to 6.0 versions) if you need IDS/IPS service.
- **Firewall Logging** (if you want to send a copy of the log events to the hosted logging service).
- **Syslog Forwarding**
- **Stateful Firewall**
- **Network and Flood Protection** (if you want to protect the Control/Management Plane).

The **Firewall Logging** and **Syslog Forwarding** settings control the event logging for the Edge Firewall services. Under the **Syslog Forwarding** section, you can see the Syslog server settings that come from your profile and Edge override configurations.

6. **Make a Firewall Rule with Logging Turned On**: The last step is to make a Firewall Rule with Logging turned on for the Edge. This will make sure that events are sent to QRadar. You can add or change rules under the **Firewall Rules** section.

Figure 5-8: Firewall Rule with IDPS and Logging Enabled



Make sure the following fields are enabled for Firewall events to be sent to the QRadar system:

Table 7: Firewall Rule – Logging Settings per Rule

Firewall Rule – Logging Settings per Rule	
Firewall Action > **Log**	If this field is enabled, the Edge will generate a log event (locally and to the Syslog server) whenever a flow matches the firewall rule. This is useful for troubleshooting and monitoring purposes.
Security Services > Select a Security Services group that has IDS/IPS engine enabled along with its logging. (6.x version and higher)	If further inspection is necessary to determine whether a flow is malicious, the IDS/IPS system must be enabled. In this case, the Intrusion Detection System must be in the Enabled state for an IDS event to be generated. When this field is enabled, the Edge will generate an event. Both a local message and a Syslog message, enriched with the IDS/IPS event, will be recorded. This field is only required if the IDS/IPS service is enabled for the rule.

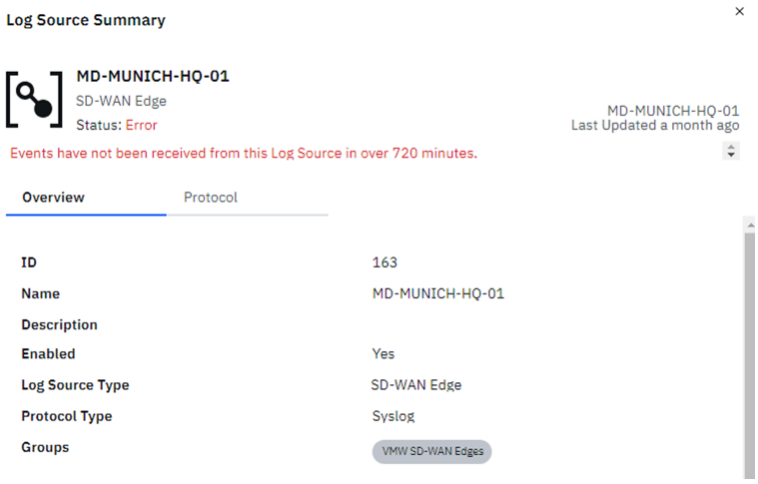
Chapter 6

Troubleshooting and Diagnostics

This section provides troubleshooting steps for an QRadar SIEM and VeloCloud deployment, including how to fix Log Source errors when no events are received, check that Syslog packets are coming from the correct interface on the VeloCloud Edge, override the Source Interface Selection in the Orchestrator, and verify that messages are being received by the QRadar Event Collector.

1. **How to fix Log Source errors when no events are received for more than 720 minutes**: Sometimes, VeloCloud Edges may not send events to the QRadar Event Collector for a long time. This can depend on your Firewall policy, flow characteristics and log settings. If this happens, some Edge appliances may show an error in the **Log Source Management App**:

   Figure 6-1: Errored state for inactive VeloCloud Edge in QRadar

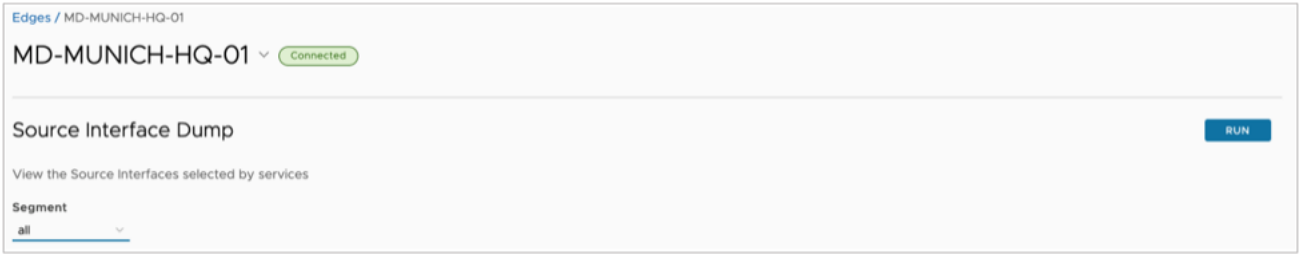
   To fix this, you may need to change a system-wide setting called **Syslog Event Timeout** parameter. You can find out how to do this in this KB article.

2. **Check that Syslog packets come from the right interface on the VeloCloud Edge**:

   a. In production environments, you may have one or more firewalls that filter traffic between your SD-WAN Fabric and the QRadar Event Collector nodes. An Edge may have many interfaces that can send syslog messages, so you need to make sure that the configuration is right on both the Edges and the firewalls that protect the Event Collector. You can check the source interface for each service on the VeloCloud Orchestrator. To do this, go to the Edge appliance using **Diagnostics** > **Remote Diagnostics**.

b. Choose the Edge you want to check, and after the connection is made, select the **Source Interface Dump** diagnostic:

Figure 6-2: Source Interface Dump



c. After selecting **Run**, you get a list of the services that the Edge is configured to support:
VeloCloud Edge is configured to support a large number of services as displayed in the Orchestrator:

Figure 6-3: Source Interface Table

Source Interface Table

Segment	Service	Source Interface	Source Selection	Source IP	Destination IP	Destination Port	Destination route
Global Segment	SD-WAN Mgmt	VLAN-1	Automatic	10.99.211.1	13.56.127.15	443	0.0.0.0/0 via vcg32-lhr4
Global Segment	SD-WAN Mgmt	VLAN-1	Automatic	10.99.211.1	54.157.32.184	443	0.0.0.0/0 via vcg32-lhr4
Global Segment	NYANSA_EP	VLAN-1	Automatic	10.99.211.1	35.160.178.114	443	0.0.0.0/0 via vcg32-lhr4
Global Segment	ZSCALER_L7	VLAN-1	Automatic	10.99.211.1	165.225.72.39	7000	0.0.0.0/0 via vcg32-lhr4
Global Segment	NYANSA_EP	VLAN-1	Automatic	10.99.211.1	44.232.141.196	443	0.0.0.0/0 via vcg32-lhr4
Global Segment	DNS	None	Automatic	::	2001:4860:4860::8888	53	::/0 via vcg32-lhr4
Global Segment	NYANSA_EP	VLAN-1	Automatic	10.99.211.1	52.25.6.138	443	0.0.0.0/0 via vcg32-lhr4
Global Segment	RADIUS	VLAN-1	Automatic	10.99.211.1	192.168.88.160	1812	0.0.0.0/0 via vcg32-lhr4
Global Segment	NTP	None	Automatic	0.0.0.0	0.0.0.0	123	0.0.0.0/32 via vcg32-lhr4
Global Segment	NYANSA_EP	VLAN-1	Automatic	10.99.211.1	34.208.245.198	443	0.0.0.0/0 via vcg32-lhr4
Global Segment	SD-WAN Mgmt	None	Automatic	::	2620:df:4000:105:b748:49be:adbc:7393	443	::/0 via vcg32-lhr4
Global Segment	DNS	VLAN-1	Automatic	10.99.211.1	8.8.8.8	53	0.0.0.0/0 via vcg32-lhr4
Global Segment	NYANSA_EP	VLAN-1	Automatic	10.99.211.1	35.80.226.90	443	0.0.0.0/0 via vcg32-lhr4
Global Segment	RSYSLOG	VLAN-1	Automatic	10.99.211.1	10.225.100.200	514	10.225.100.0/24 via vcg32-lhr4
Global Segment	NYANSA_EP	VLAN-1	Automatic	10.99.211.1	44.228.140.69	443	0.0.0.0/0 via vcg32-lhr4
Global Segment	DNS	VLAN-1	Automatic	10.99.211.1	8.8.4.4	53	0.0.0.0/0 via vcg32-lhr4
Global Segment	ZSCALER_L7	VLAN-1	Automatic	10.99.211.1	104.129.194.39	7001	0.0.0.0/0 via vcg32-lhr4
Global Segment	DNS	None	Automatic	::	2001:4860:4860::8844	53	::/0 via vcg32-lhr4
Global Segment	Netflow	VLAN-1	Automatic	10.99.211.1	10.225.100.200	2055	10.225.100.0/24 via vcg32-lhr4

This widget lets you see all the configurations that the Edge got from the Orchestrator. For the QRadar SIEM integration, you should look for two types of service. Please make sure that these are correct:

Table 8: Source Interface Output

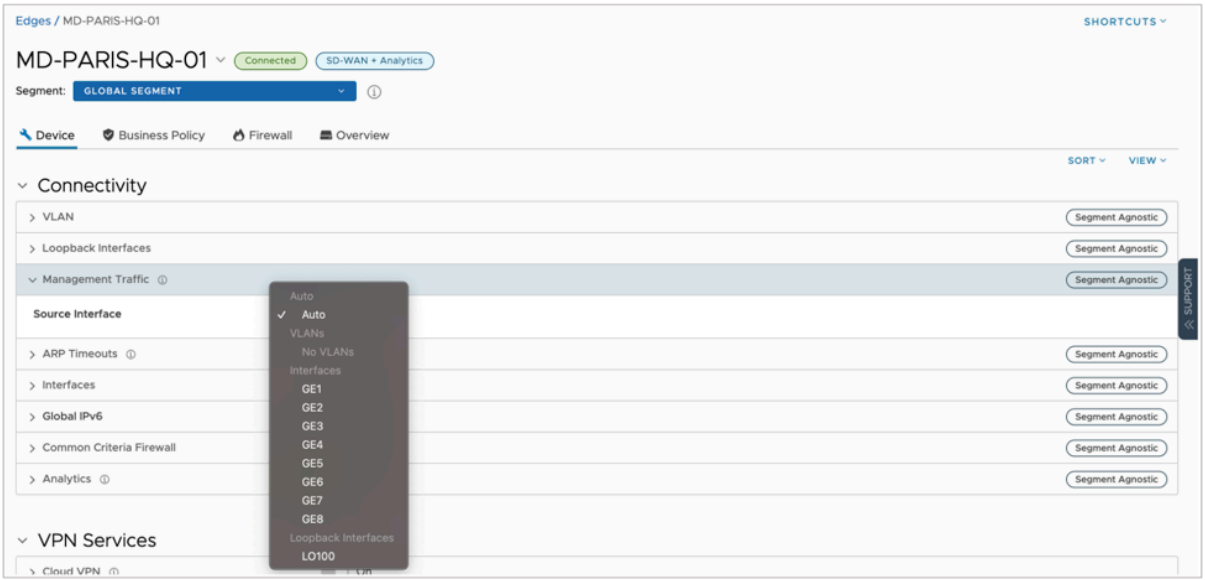
Source Interface Output	
Service	This should be either RSYSLOG or NetFlow.
Source Interface	This field represents the source interface from which the events or flows will be sent from.
Source Selection	By default, the Edges allocate source interfaces automatically. This behavior can be overridden, and a source interface (such as a Loopback interface) can be set manually.
Source IP	This field specifies the IPv4 or IPv6 address from which messages will originate.
Destination IP	This field specifies the IPv4 or IPv6 address to which flows or events will be sent. In the case of QRadar, this may be the same destination or separate systems in a distributed setup.
Destination Port	This field represents the port number on the destination system that packets will be sent to. In the case of QRadar default settings, 2055 should be used for the IPFIX protocol and 514 for RSYSLOG.
Destination Route	The VeloCloud Edge performs a route lookup for the destination IP address. The system will then display the prefix and next hop information. The Event and Flow collector can be placed in subnets connected to the Edge LAN interfaces (either directly routed, or connected using static routing, OSPF or BGP), in the Underlay (for example, if you are using MPLS as a transit), or in the Underlay (accessible via Gateways or a designated Hub location), depending on the SD-WAN fabric design.

3. **Override the Source Interface Selection in the Orchestrator**:

   a. The SD-WAN Edges automatically choose the source interfaces for traffic that they generate (based on their routing information and interface layout). Like any network appliance, physical interfaces can change states, and even if there is another path to the collector nodes, the source IP address may change. To make sure that Management traffic always comes from the same IP address and the interface stays up no matter what happens to the physical network, it is best to use Loopback interfaces for this type of traffic.

   b. To change the default, automatic interface assignment, you can go to **Configure** > **Edges**, choose the Edge that you want to change, then on the **Device** tab, go to and open the **Management Traffic** section, and select the interface you want from the **Source Interface** drop-down menu:

   Figure 6-4: Management Traffic- Source Interface selection in the Orchestrator



> **Note:** This change affects all services that are classified as management traffic.

4. **Check if messages are coming in on the QRadar Event Collector**: Now that we have made sure that communication between the SD-WAN Edges and the Event or Flow Collector nodes is using the right path and source and destination IP addresses, we can check if the Collectors are getting Syslog and IPFIX messages. A quick way to check is to run a packet capture on the collector interface.

   a. For this, you need SSH access to the Collector node you are troubleshooting. After logging in to the system, you can check the IP addresses and interface layout with a simple “ip address” or “ip a” command.

```
[root@qradar1 ~]# ip address <output omitted> 2: ens33: <BROADCAST,MULTICAST,PROMI
SC,UP,LOWER_UP> mtu 1500 qdisc prio state UP group default qlen 1000 link/ether
 00:50:56:94:90:ab brd ff:ff:ff:ff:ff:ff inet 10.225.100.200/24 brd 10.225.100.255 scope
 global ens33 valid_lft forever preferred_lft forever inet6 fe80::250:56ff:fe94:90ab/64
 scope link valid_lft forever preferred_lft forever 3: ens160: <BROADCAST,MULTICAST,UP,LO
WER_UP> mtu 1500 qdisc prio state UP group default qlen 1000 link/ether 00:50:56:94:d1:c4
 brd ff:ff:ff:ff:ff:ff inet 10.225.0.200/24 brd 10.225.0.255 scope global ens160 valid_lft
 forever preferred_lft forever inet6 fe80::250:56ff:fe94:d1c4/64 scope link valid_lft
 forever preferred_lft forever <output omitted>
```

   b. You can also see the interface name and role assignment in the QRadar Console. After you confirm which interface is set up for event or flow collection, you can use the “tcpdump” command to start a packet capture. Here is an example of this command and its parameters:

```
sudo tcpdump -i <interface name> -s0 -vv -nn src <log source IP address> and dst port <514
 or 2055>
```

   c. The example below captures packets that arrive on interface ens33 from IP address 10.99.211.1, going to the QRadar Collector on port 514:

```
# sudo tcpdump -i ens33 -s0 -vv -nn src 10.99.211.1 and dst port 514 tcpdump: listening on
 ens33, link-type EN10MB (Ethernet), capture size 262144 bytes 14:29:26.751712 IP (tos 0x0,
 ttl 61, id 54724, offset 0, flags [none], proto UDP (17), length 243) 10.99.211.1.50142 >
 10.225.100.200.514: [udp sum ok] SYSLOG, length: 215 Facility local0 (16), Severity info
 (6) Msg: Aug 14 14:29:30 MD-MUNICH-HQ-01 VMW.Edge: ACTION=VCF Drop SEGMENT=0 PROTO=IPv6-IC
MP SRC=fe80::ffff:ffff:ffff:ffff DST=ff02::1 REASON=IPv6: Reverse path forwarding check fail
 SEGMENT_NAME=Global Segment COUNT=89 <output omitted>
```

We have verified that the Collector node is getting raw Syslog and IPFIX data at this point. If you need more troubleshooting, see this. KB Articles.

Appendix A

References

- QRadar SIEM Integration Device Support Module Files
- Related Documents

A.1 QRadar SIEM Integration Device Support Module Files

- Manifest
- Device Support Modules Samples

A.1.1 Manifest

Device Support Module (DSM) for QRadar SIEM

VeloCloud-SD-WAN-Edge-Device-Support-Module-v1.7.0-master


```
{
"doc" : {
"extension_manifest" : {
"min_qradar_version" : "2020.7.0.20201113144954",
"authored_by" : "sathya.thammanur",
"authored_by_email" : "velocloud@arista.com",
"package_size" : "0",
"supported_language_set" : [ "en-US" ],
"extension_name" : "extension.name",
"extension_long_description" : "extension.long.description",
"locale" : {
"en-US" : {
"extension.long.description" : "This DSM contains security event mappings for VeloCloud SD-WAN
 Edge appliances.",
"extension.name" : "VeloCloud SD-WAN Edge"
}
},
"version" : "1.7.0"
}
},
"_id" : "sathya.thammanur:VeloCloud SD-WAN Edge"
}
```

A.1.2 Device Support Module

Device Support Module (DSM) for QRadar SIEM solutions samples.

`Arista SD-WAN Edge-20231004023738.xml`

```
<content><qradarversion>2020.7.0.20201113144954</qradarversion>
 <sensorprotocol>
  <gatewaysupported>true</gatewaysupported>
  <autodiscoverable>true</autodiscoverable>
  <plugin_version>20211115162</plugin_version>
  <protocoldescription>TLS Syslog</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>true</inbound>
  <protocolname>TLSSyslog</protocolname>
  <bulk_addable>false</bulk_addable>
  <latest_version>20230615170057</latest_version>
  <transmissionprotocol>TCP</transmissionprotocol>
  <id>22</id>
  <autodiscoveryport>0</autodiscoveryport>
  <configurable>true</configurable>
  <listenportkey>tlsListenPort</listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>true</gatewaysupported>
  <autodiscoverable>true</autodiscoverable>
  <plugin_version>+20221031125+</plugin_version>
  <protocoldescription>TCP Multiline Syslog</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>true</inbound>
  <protocolname>TCPMultilineSyslog</protocolname>
  <bulk_addable>false</bulk_addable>
  <latest_version>202210311125147</latest_version>
  <transmissionprotocol>TCP</transmissionprotocol>
  <id>23</id>
  <autodiscoveryport>0</autodiscoveryport>
  <listenprotocolkey>@protocol.listenprotocolkey@</listenprotocolkey>
  <configurable>true</configurable>
  <listenportkey>tcpMultilinePort</listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>true</gatewaysupported>
  <autodiscoverable>true</autodiscoverable>
  <plugin_version>20210705183</plugin_version>
  <protocoldescription>UDP Multiline Syslog</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>true</inbound>
  <protocolname>UDPMultilineSyslog</protocolname>
  <bulk_addable>false</bulk_addable>
  <latest_version>202107051183817</latest_version>
  <transmissionprotocol>UDP</transmissionprotocol>
  <id>24</id>
  <autodiscoveryport>0</autodiscoveryport>
  <configurable>true</configurable>
  <listenportkey>listenPort</listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>true</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>20191218165</plugin_version>
  <protocoldescription>Syslog Redirect</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>true</inbound>
  <protocolname>SyslogRedirect</protocolname>
  <bulk_addable>false</bulk_addable>
  <transmissionprotocol>UDP,TCP</transmissionprotocol>
  <id>50</id>
  <autodiscoveryport>0</autodiscoveryport>
  <listenprotocolkey>protocol</listenprotocolkey>
  <configurable>true</configurable>
  <listenportkey>listenPort</listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>+20230208183+</plugin_version>
  <protocoldescription>HTTP Receiver</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>true</inbound>
  <protocolname>HTTPReceiver</protocolname>
  <bulk_addable>false</bulk_addable>
  <latest_version>20230208183459</latest_version>
  <transmissionprotocol>TCP</transmissionprotocol>
  <id>51</id>
  <autodiscoveryport>0</autodiscoveryport>
  <listenprotocolkey>@protocol.listenprotocolkey@</listenprotocolkey>
  <configurable>true</configurable>
  <listenportkey>listenPort</listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>+20220516182+</plugin_version>
  <protocoldescription>Microsoft Security Event Log (End of life)</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>false</inbound>
  <protocolname>WindowsEventLog</protocolname>
  <bulk_addable>true</bulk_addable>
  <latest_version>20220516182406</latest_version>
  <transmissionprotocol>TCP</transmissionprotocol>
  <id>30</id>
  <autodiscoveryport>514</autodiscoveryport>
  <listenprotocolkey>@protocol.listenprotocolkey@</listenprotocolkey>
  <configurable>true</configurable>
  <listenportkey>@protocol.listenportkey@</listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>20191218165</plugin_version>
  <protocoldescription>Microsoft Security Event Log Custom</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>false</inbound>
  <protocolname>WindowsEventLogCustom</protocolname>
  <bulk_addable>true</bulk_addable>
```

```
  <transmissionprotocol>TCP</transmissionprotocol>
  <id>31</id>
  <autodiscoveryport>514</autodiscoveryport>
  <configurable>true</configurable>
  <listenportkey></listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>true</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>20191218165</plugin_version>
  <protocoldescription>Amazon Web Services</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>false</inbound>
  <protocolname>AmazonWebServices</protocolname>
  <bulk_addable>false</bulk_addable>
  <transmissionprotocol></transmissionprotocol>
  <id>76</id>
  <autodiscoveryport>0</autodiscoveryport>
  <configurable>true</configurable>
  <listenportkey></listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>20191218165</plugin_version>
  <protocoldescription>SMB Tail</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>false</inbound>
  <protocolname>SmbTailProtocol</protocolname>
  <bulk_addable>false</bulk_addable>
  <transmissionprotocol></transmissionprotocol>
  <id>32</id>
  <autodiscoveryport>0</autodiscoveryport>
  <configurable>true</configurable>
  <listenportkey></listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>20191218165</plugin_version>
  <protocoldescription>SNMPv3</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>true</inbound>
  <protocolname>SNMPv3</protocolname>
  <bulk_addable>false</bulk_addable>
  <transmissionprotocol>UDP</transmissionprotocol>
  <id>10</id>
  <autodiscoveryport>162</autodiscoveryport>
  <configurable>true</configurable>
  <listenportkey>listenPort</listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>7.0</plugin_version>
  <encoding_enabled>false</encoding_enabled>
  <inbound>false</inbound>
  <protocolname>AnomalyDetectionEngine</protocolname>
  <bulk_addable>false</bulk_addable>
  <id>33</id>
  <configurable>false</configurable>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>20191218165</plugin_version>
  <protocoldescription>SNMPv1</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>true</inbound>
  <protocolname>SNMPv1</protocolname>
  <bulk_addable>false</bulk_addable>
  <transmissionprotocol>UDP</transmissionprotocol>
  <id>11</id>
  <autodiscoveryport>162</autodiscoveryport>
  <configurable>true</configurable>
  <listenportkey></listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>6.0</plugin_version>
  <encoding_enabled>false</encoding_enabled>
  <inbound>true</inbound>
  <protocolname>Forwarded</protocolname>
  <bulk_addable>false</bulk_addable>
  <transmissionprotocol>TCP</transmissionprotocol>
  <id>12</id>
  <autodiscoveryport>0</autodiscoveryport>
  <configurable>false</configurable>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>20210913151</plugin_version>
  <protocoldescription>EMC VMWare</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>false</inbound>
  <protocolname>EMCVmWareProtocol</protocolname>
  <bulk_addable>false</bulk_addable>
  <transmissionprotocol></transmissionprotocol>
  <id>34</id>
  <autodiscoveryport>0</autodiscoveryport>
  <configurable>true</configurable>
  <listenportkey></listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>+20230330194+</plugin_version>
  <protocoldescription>Microsoft Azure Event Hubs</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>false</inbound>
  <protocolname>MicrosoftAzureEventHubs</protocolname>
  <bulk_addable>false</bulk_addable>
  <latest_version>20230503181429</latest_version>
  <transmissionprotocol>@protocol.transmissionprotocol@</transmissionprotocol>
  <id>78</id>
  <autodiscoveryport>0</autodiscoveryport>
  <listenprotocolkey>@protocol.listenprotocolkey@</listenprotocolkey>
  <configurable>true</configurable>
  <listenportkey>@protocol.listenportkey@</listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>20191218165</plugin_version>
  <protocoldescription>Cisco NSEL</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
```

```
   <inbound>true</inbound>
   <protocolname>Cisco NSEL</protocolname>
   <bulk_addable>false</bulk_addable>
   <transmissionprotocol>UDP</transmissionprotocol>
   <id>35</id>
   <autodiscoveryport>0</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey>collectorPort</listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>20191218165</plugin_version>
   <protocoldescription>PCAP Syslog Combination</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>true</inbound>
   <protocolname>PCAPSyslog</protocolname>
   <bulk_addable>false</bulk_addable>
   <transmissionprotocol>UDP</transmissionprotocol>
   <id>36</id>
   <autodiscoveryport>0</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey>pcapPort</listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>20210716173</plugin_version>
   <protocoldescription>Sophos Enterprise Console JDBC</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>false</inbound>
   <protocolname>JdbcSophos</protocolname>
   <bulk_addable>false</bulk_addable>
   <latest_version>20210716173434</latest_version>
   <transmissionprotocol></transmissionprotocol>
   <id>37</id>
   <autodiscoveryport>0</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey></listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>20191218165</plugin_version>
   <protocoldescription>Log File</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>false</inbound>
   <protocolname>LogFileProtocol</protocolname>
   <bulk_addable>false</bulk_addable>
   <latest_version>20230518134525</latest_version>
   <transmissionprotocol></transmissionprotocol>
   <id>15</id>
   <autodiscoveryport>0</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey></listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>20191218165</plugin_version>
   <protocoldescription>Microsoft Exchange</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>false</inbound>
   <protocolname>WindowsExchangeProtocol</protocolname>
   <bulk_addable>false</bulk_addable>
   <transmissionprotocol></transmissionprotocol>
   <id>16</id>
   <autodiscoveryport>0</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey></listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>20191218165</plugin_version>
   <protocoldescription>Microsoft DHCP</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>false</inbound>
   <protocolname>WindowsDHCPProtocol</protocolname>
   <bulk_addable>false</bulk_addable>
   <transmissionprotocol></transmissionprotocol>
   <id>17</id>
   <autodiscoveryport>0</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey></listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>20191218165</plugin_version>
   <protocoldescription>Microsoft IIS</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>false</inbound>
   <protocolname>WindowsIISProtocol</protocolname>
   <bulk_addable>false</bulk_addable>
   <transmissionprotocol></transmissionprotocol>
   <id>18</id>
   <autodiscoveryport>0</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey></listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>20220420193</plugin_version>
   <protocoldescription>Cisco Firepower eStreamer</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>false</inbound>
   <protocolname>CiscoFirepowerEstreamer</protocolname>
   <bulk_addable>false</bulk_addable>
   <latest_version>20221031121312</latest_version>
   <transmissionprotocol></transmissionprotocol>
   <id>19</id>
   <autodiscoveryport>0</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey></listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>true</autodiscoverable>
   <plugin_version>20191218165</plugin_version>
   <protocoldescription>Syslog</protocoldescription>
   <encoding_enabled>true</encoding_enabled>
   <inbound>true</inbound>
   <protocolname>Syslog</protocolname>
   <bulk_addable>true</bulk_addable>
   <transmissionprotocol>UDP,TCP</transmissionprotocol>
   <id>0</id>
```

```
  <autodiscoveryport>514</autodiscoveryport>
  <configurable>true</configurable>
  <listenportkey></listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>20191218165</plugin_version>
  <protocoldescription>SNMPv2</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>true</inbound>
  <protocolname>SNMPv2</protocolname>
  <bulk_addable>false</bulk_addable>
  <transmissionprotocol>UDP</transmissionprotocol>
  <id>1</id>
  <autodiscoveryport>162</autodiscoveryport>
  <configurable>true</configurable>
  <listenportkey>listenPort</listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>20210212181</plugin_version>
  <protocoldescription>OPSEC/LEA</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>false</inbound>
  <protocolname>LEA</protocolname>
  <bulk_addable>false</bulk_addable>
  <latest_version>202102121281229</latest_version>
  <transmissionprotocol></transmissionprotocol>
  <id>2</id>
  <autodiscoveryport>0</autodiscoveryport>
  <configurable>true</configurable>
  <listenportkey></listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>6.0</plugin_version>
  <encoding_enabled>false</encoding_enabled>
  <inbound>true</inbound>
  <protocolname>SOAP</protocolname>
  <bulk_addable>false</bulk_addable>
  <transmissionprotocol>TCP</transmissionprotocol>
  <id>3</id>
  <autodiscoveryport>8081</autodiscoveryport>
  <configurable>false</configurable>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>6.0</plugin_version>
  <encoding_enabled>false</encoding_enabled>
  <inbound>true</inbound>
  <protocolname>CLASSIFY</protocolname>
  <bulk_addable>false</bulk_addable>
  <id>4</id>
  <configurable>false</configurable>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>6.0</plugin_version>
  <encoding_enabled>false</encoding_enabled>
  <inbound>false</inbound>
  <protocolname>Event CRE</protocolname>
  <bulk_addable>false</bulk_addable>
  <id>5</id>
  <configurable>false</configurable>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>6.0</plugin_version>
  <encoding_enabled>false</encoding_enabled>
  <inbound>false</inbound>
  <protocolname>JDBC:SiteProtector</protocolname>
  <bulk_addable>false</bulk_addable>
  <id>6</id>
  <configurable>false</configurable>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>202009211172</plugin_version>
  <protocoldescription>SDEE</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>false</inbound>
  <protocolname>SDEE</protocolname>
  <bulk_addable>false</bulk_addable>
  <latest_version>202009211172617</latest_version>
  <transmissionprotocol></transmissionprotocol>
  <id>7</id>
  <autodiscoveryport>0</autodiscoveryport>
  <configurable>true</configurable>
  <listenportkey></listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>false</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>+20230307171+</plugin_version>
  <protocoldescription>JDBC</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>false</inbound>
  <protocolname>JDBC</protocolname>
  <bulk_addable>false</bulk_addable>
  <latest_version>20230307171530</latest_version>
  <transmissionprotocol>""</transmissionprotocol>
  <id>8</id>
  <autodiscoveryport>0</autodiscoveryport>
  <listenprotocolkey>@protocol.listenprotocolkey@</listenprotocolkey>
  <configurable>true</configurable>
  <listenportkey>""</listenportkey>
 </sensorprotocol>
 <sensorprotocol>
  <gatewaysupported>true</gatewaysupported>
  <autodiscoverable>false</autodiscoverable>
  <plugin_version>+20230209180+</plugin_version>
  <protocoldescription>Apache Kafka</protocoldescription>
  <encoding_enabled>false</encoding_enabled>
  <inbound>false</inbound>
  <protocolname>ApacheKafka</protocolname>
  <bulk_addable>false</bulk_addable>
  <latest_version>20230209180636</latest_version>
  <transmissionprotocol>@protocol.transmissionprotocol@</transmissionprotocol>
  <id>80</id>
  <autodiscoveryport>0</autodiscoveryport>
  <listenprotocolkey>@protocol.listenprotocolkey@</listenprotocolkey>
```

```
   <configurable>true</configurable>
   <listenportkey>@protocol.listenportkey@</listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>20191218165</plugin_version>
   <protocoldescription>Juniper NSM</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>true</inbound>
   <protocolname>JuniperNSM</protocolname>
   <bulk_addable>false</bulk_addable>
   <transmissionprotocol>UDP</transmissionprotocol>
   <id>9</id>
   <autodiscoveryport>514</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey>inboundPort</listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>true</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>20191218165</plugin_version>
   <protocoldescription>Amazon AWS S3 REST API</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>false</inbound>
   <protocolname>AmazonAWSRESTAPI</protocolname>
   <bulk_addable>false</bulk_addable>
   <transmissionprotocol></transmissionprotocol>
   <id>62</id>
   <autodiscoveryport>0</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey></listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>20191218132</plugin_version>
   <protocoldescription>WinCollect File Forwarder</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>false</inbound>
   <protocolname>WinCollectFileForwarder</protocolname>
   <bulk_addable>true</bulk_addable>
   <transmissionprotocol>TCP</transmissionprotocol>
   <id>41</id>
   <autodiscoveryport>514</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey></listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>+20230109141+</plugin_version>
   <protocoldescription>Ariel REST API</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>false</inbound>
   <protocolname>ArielRESTAPI</protocolname>
   <bulk_addable>false</bulk_addable>
   <latest_version>202301091141812</latest_version>
   <transmissionprotocol>@protocol.transmissionprotocol@</transmissionprotocol>
   <id>63</id>
   <autodiscoveryport>0</autodiscoveryport>
   <listenprotocolkey>@protocol.listenprotocolkey@</listenprotocolkey>
   <configurable>true</configurable>
   <listenportkey>@protocol.listenportkey@</listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>true</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>+20230313132+</plugin_version>
   <protocoldescription>Google Cloud Pub/Sub</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>false</inbound>
   <protocolname>GoogleCloudPubSub</protocolname>
   <bulk_addable>false</bulk_addable>
   <latest_version>202303131132604</latest_version>
   <transmissionprotocol>@protocol.transmissionprotocol@</transmissionprotocol>
   <id>85</id>
   <autodiscoveryport>0</autodiscoveryport>
   <listenprotocolkey>@protocol.listenprotocolkey@</listenprotocolkey>
   <configurable>true</configurable>
   <listenportkey>@protocol.listenportkey@</listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>20200110201</plugin_version>
   <protocoldescription>JDBC - SiteProtector</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>false</inbound>
   <protocolname>SiteProtectorJDBC</protocolname>
   <bulk_addable>false</bulk_addable>
   <transmissionprotocol></transmissionprotocol>
   <id>20</id>
   <autodiscoveryport>0</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey></listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>20210716173</plugin_version>
   <protocoldescription>IBM Security Identity Manager JDBC</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>false</inbound>
   <protocolname>IBMSIMJDBC</protocolname>
   <bulk_addable>false</bulk_addable>
   <latest_version>202107161734434</latest_version>
   <transmissionprotocol></transmissionprotocol>
   <id>42</id>
   <autodiscoveryport>0</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey></listenportkey>
  </sensorprotocol>
  <sensorprotocol>
   <gatewaysupported>false</gatewaysupported>
   <autodiscoverable>false</autodiscoverable>
   <plugin_version>20191218165</plugin_version>
   <protocoldescription>Oracle Database Listener</protocoldescription>
   <encoding_enabled>false</encoding_enabled>
   <inbound>false</inbound>
   <protocolname>OracleDatabaseListener</protocolname>
   <bulk_addable>false</bulk_addable>
   <transmissionprotocol></transmissionprotocol>
   <id>21</id>
   <autodiscoveryport>0</autodiscoveryport>
   <configurable>true</configurable>
   <listenportkey></listenportkey>
  </sensorprotocol>
```

```
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630429</id>
 <unravelevent>0</unravelevent>
 <uuid>adebb22e-fad8-40b8-87f6-f136522f11ec</uuid>
 <qidmapid>699777</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Web Application Attack</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Open</deviceeventcategory>
 <customevent>true</customevent>
 <id>630423</id>
 <unravelevent>0</unravelevent>
 <uuid>d040df7f-2cac-48f6-8cf5-1b2699ba3af5</uuid>
 <qidmapid>699798</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>VCF Open</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630424</id>
 <unravelevent>0</unravelevent>
 <uuid>02f8ccdf-8cff-48ef-8b24-491eeab683d2</uuid>
 <qidmapid>699801</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Attempted Information Leak</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630421</id>
 <unravelevent>0</unravelevent>
 <uuid>954105fe-595f-4ac0-ba94-01fa2641a674</uuid>
 <qidmapid>699778</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Successful User Privilege Gain</deviceeventid>
</dsmevent>
<dsmevent>
 <routepoint>EP</routepoint>
 <credibility>5</credibility>
 <deviceeventcategory>unknown</deviceeventcategory>
 <customevent>false</customevent>
 <id>630388</id>
 <unravelevent>0</unravelevent>
 <qidmapid>699776</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>unknown</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Close</deviceeventcategory>
 <customevent>true</customevent>
 <id>630389</id>
 <unravelevent>0</unravelevent>
 <uuid>a253fd6a-a08f-4c0a-b643-c173e4526809</uuid>
 <qidmapid>699805</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>FIN-Received</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630422</id>
 <unravelevent>0</unravelevent>
 <uuid>2682418e-ca14-4e04-a891-0a4a60cc8601</uuid>
 <qidmapid>699795</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Indication of an active backdoor channel</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630427</id>
 <unravelevent>0</unravelevent>
 <uuid>6c876028-d580-4d0b-a1cd-3bea3044cdc1</uuid>
 <qidmapid>699802</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Attempted User Privilege Gain</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630428</id>
 <unravelevent>0</unravelevent>
 <uuid>aed4d65b-1ad6-4a87-97fb-2dfce668485e</uuid>
 <qidmapid>699777</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Non-specific potential web app attack</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630425</id>
 <unravelevent>0</unravelevent>
 <uuid>9dd662af-48bf-412f-a5ab-73dbad17b992</uuid>
 <qidmapid>699814</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Information Leak</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>MGD_CONFIG_APPLIED</deviceeventcategory>
 <customevent>true</customevent>
 <id>630426</id>
 <unravelevent>0</unravelevent>
 <uuid>623c4860-b538-47c4-8c75-b9985e84cefa</uuid>
 <qidmapid>699808</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Applied new configuration for firewall version</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>MGD_CONF_APPLIED</deviceeventcategory>
 <customevent>true</customevent>
 <id>630393</id>
 <unravelevent>0</unravelevent>
 <uuid>30a8b715-e88e-42c6-8609-742643423603</uuid>
```

```
 <qidmapid>699783</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Applied new configuration for deviceSettings</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Drop</deviceeventcategory>
 <customevent>true</customevent>
 <id>630394</id>
 <unravelevent>0</unravelevent>
 <uuid>3f150b89-70ec-4ba7-b575-d8171afa9395</uuid>
 <qidmapid>699813</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>IPv6: Reverse path forwarding check fail</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>MGD_CONF_APPLIED</deviceeventcategory>
 <customevent>true</customevent>
 <id>630391</id>
 <unravelevent>0</unravelevent>
 <uuid>b2e31112-31aa-404a-9213-bbfe5a5e6c1f</uuid>
 <qidmapid>699786</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Applied new configuration for analyticsSettings</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>Stored</deviceeventcategory>
 <customevent>true</customevent>
 <id>630392</id>
 <unravelevent>0</unravelevent>
 <uuid>bb0871a4-11b5-451e-8bec-4adead4d917a</uuid>
 <qidmapid>699806</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>unknown</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630430</id>
 <unravelevent>0</unravelevent>
 <uuid>5a23fa5a-d241-4f77-b1b6-2b15c22dfd83</uuid>
 <qidmapid>699796</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>A Suspicious Filename was Detected</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>MGD_DEVICE_CONFIG_WARNING</deviceeventcategory>
 <customevent>true</customevent>
 <id>630397</id>
 <unravelevent>0</unravelevent>
 <uuid>50767bcc-3975-4582-a8c6-7c72e561b03f</uuid>
 <qidmapid>699788</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Inconsistent device settings detected, continuing with warnings</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Close</deviceeventcategory>
 <customevent>true</customevent>
 <id>630431</id>
 <unravelevent>0</unravelevent>
 <uuid>92c26b21-2617-4bf8-8615-9efe099fc61a</uuid>
 <qidmapid>699812</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Aged-Out</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630398</id>
 <unravelevent>0</unravelevent>
 <uuid>43140a9f-53dd-4897-b46e-65fc2d4f3ee2</uuid>
 <qidmapid>699782</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Possible Social Engineering Attempted</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>EDGE_AUTO_SIM_SWITCH</deviceeventcategory>
 <customevent>true</customevent>
 <id>630395</id>
 <unravelevent>0</unravelevent>
 <uuid>5d1491f1-978b-4bd7-9b7c-255abe747920</uuid>
 <qidmapid>699792</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Autosim Switch Disabled</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630396</id>
 <unravelevent>0</unravelevent>
 <uuid>27d0f76c-6813-4c33-9952-b54e3ee118c9</uuid>
 <qidmapid>699781</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Possibly Unwanted Program Detected</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630390</id>
 <unravelevent>0</unravelevent>
 <uuid>8815aa90-6ecd-49be-a3cc-336add620d7a</uuid>
 <qidmapid>699810</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>A Network Trojan was Detected</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630434</id>
 <unravelevent>0</unravelevent>
 <uuid>929b6fc2-a034-431c-86b9-5ff0d01878ec</uuid>
 <qidmapid>699796</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Access to a Potentially Vulnerable Web Application</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
```

```
  <customevent>true</customevent>
  <id>630432</id>
  <unravelevent>0</unravelevent>
  <uuid>bae0e0c3-bef7-4d36-84b3-fa4d7a726e05</uuid>
  <qidmapid>699807</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>Attempted Denial of Service</deviceeventid>
 </dsmevent>
 <dsmevent>
  <credibility>0</credibility>
  <deviceeventcategory>VCF Deny</deviceeventcategory>
  <customevent>true</customevent>
  <id>630399</id>
  <unravelevent>0</unravelevent>
  <uuid>2fa4510c-cb13-4a14-a3f2-03118b79f2c2</uuid>
  <qidmapid>699806</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>Invalid-TCP-Open</deviceeventid>
 </dsmevent>
 <dsmevent>
  <credibility>0</credibility>
  <deviceeventcategory>VCF Alert</deviceeventcategory>
  <customevent>true</customevent>
  <id>630433</id>
  <unravelevent>0</unravelevent>
  <uuid>e53ece07-ddba-4c40-87f0-026968d996c2</uuid>
  <qidmapid>699780</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>Targeted Malicious Activity was Detected</deviceeventid>
 </dsmevent>
 <dsmevent>
  <credibility>0</credibility>
  <deviceeventcategory>VCF Drop</deviceeventcategory>
  <customevent>true</customevent>
  <id>681622</id>
  <unravelevent>0</unravelevent>
  <uuid>2fe0e8aa-e4c4-4df0-b69b-d97aeca3b15a</uuid>
  <qidmapid>699813</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>IP: Reverse path forwarding check fail</deviceeventid>
 </dsmevent>
 <dsmevent>
  <credibility>0</credibility>
  <deviceeventcategory>VCF Update</deviceeventcategory>
  <customevent>true</customevent>
  <id>681621</id>
  <unravelevent>0</unravelevent>
  <uuid>a7912126-8d62-428f-ad4a-cb8966eb89e9</uuid>
  <qidmapid>3070875</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>VCF Update</deviceeventid>
 </dsmevent>
 <dsmevent>
  <credibility>0</credibility>
  <deviceeventcategory>VCF Alert</deviceeventcategory>
  <customevent>true</customevent>
  <id>630409</id>
  <unravelevent>0</unravelevent>
  <uuid>7552d5d3-d47c-4806-bad6-3c1691eccd5f</uuid>
  <qidmapid>699787</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>Device Retrieving External IP Address Detected</deviceeventid>
 </dsmevent>
 <dsmevent>
  <credibility>0</credibility>
  <deviceeventcategory>VCF Alert</deviceeventcategory>
  <customevent>true</customevent>
  <id>630407</id>
  <unravelevent>0</unravelevent>
  <uuid>f5f372e0-d4a0-4389-8d47-cfb688c20155</uuid>
  <qidmapid>699807</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>Detection of a Denial of Service Attack</deviceeventid>
 </dsmevent>
 <dsmevent>
  <credibility>0</credibility>
  <deviceeventcategory>ATP_IDPS_RULE_RELOAD_SUCCESS</deviceeventcategory>
  <customevent>true</customevent>
  <id>630408</id>
  <unravelevent>0</unravelevent>
  <uuid>347ae13d-3f63-4119-84b5-3b57b36cd71d</uuid>
  <qidmapid>699800</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>Suricata Engine reload success</deviceeventid>
 </dsmevent>
 <dsmevent>
  <credibility>0</credibility>
  <deviceeventcategory>MGD_WEBSOCKET_CLOSE</deviceeventcategory>
  <customevent>true</customevent>
  <id>630401</id>
  <unravelevent>0</unravelevent>
  <uuid>7df9ea5f-89d4-459d-aafb-ab7a1e53b944</uuid>
  <qidmapid>699811</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>Close WebSocket</deviceeventid>
 </dsmevent>
 <dsmevent>
  <credibility>0</credibility>
  <deviceeventcategory>VCF Alert</deviceeventcategory>
  <customevent>true</customevent>
  <id>630402</id>
  <unravelevent>0</unravelevent>
  <uuid>ade86f32-acc1-4e09-8372-ba4d3061d107</uuid>
  <qidmapid>699784</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>Detection of a Network Scan</deviceeventid>
 </dsmevent>
 <dsmevent>
  <credibility>0</credibility>
  <deviceeventcategory>VCF Alert</deviceeventcategory>
  <customevent>true</customevent>
  <id>630400</id>
  <unravelevent>0</unravelevent>
  <uuid>699ad20f-cfd6-4ae7-9fed-1b02f9b86030</uuid>
  <qidmapid>699796</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>Misc Attack</deviceeventid>
 </dsmevent>
 <dsmevent>
  <credibility>0</credibility>
  <deviceeventcategory>VCF Alert</deviceeventcategory>
  <customevent>true</customevent>
  <id>630405</id>
  <unravelevent>0</unravelevent>
  <uuid>5f0ceed9-7812-460e-a8c4-3353f80c5ec0</uuid>
  <qidmapid>699785</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>Exploit Kit Activity Detected</deviceeventid>
```

```
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>MGD_WEBSOCKET_INIT</deviceeventcategory>
 <customevent>true</customevent>
 <id>630406</id>
 <unravelevent>0</unravelevent>
 <uuid>f5218817-0027-4ce4-aa51-89d4c8de7569</uuid>
 <qidmapid>699809</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Initiate WebSocket with VCO upload</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630403</id>
 <unravelevent>0</unravelevent>
 <uuid>ac8e79eb-a03d-4197-97ba-d08440039c99</uuid>
 <qidmapid>699793</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Domain Observed Used for C2 Detected</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630404</id>
 <unravelevent>0</unravelevent>
 <uuid>799b8153-e2da-44c3-9c28-74be9efd085c</uuid>
 <qidmapid>699797</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Potential Corporate Privacy Violation</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630418</id>
 <unravelevent>0</unravelevent>
 <uuid>d0af0853-7e52-4988-9bf0-8c2677439665</uuid>
 <qidmapid>699779</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Successful Administrator Privilege Gain</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630419</id>
 <unravelevent>0</unravelevent>
 <uuid>d3bce044-59cc-4b89-a429-17d17980d822</uuid>
 <qidmapid>699796</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Non-specific potential attack</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630412</id>
 <unravelevent>0</unravelevent>
 <uuid>101bbb5f-ea88-479d-ac4b-ba10f04f0d60</uuid>
 <qidmapid>699790</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Attempt to Login By a Default Username and Password</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630413</id>
 <unravelevent>0</unravelevent>
 <uuid>2980ed8e-c452-47f1-9e82-c3bcef09158b</uuid>
 <qidmapid>699803</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Attempt to exploit client-side web app vuln</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630410</id>
 <unravelevent>0</unravelevent>
 <uuid>357d177d-dcd3-414b-b304-e0af1f33f75c</uuid>
 <qidmapid>699796</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Misc activity</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630411</id>
 <unravelevent>0</unravelevent>
 <uuid>32ee689a-d34a-4e51-a015-5b690f0c423e</uuid>
 <qidmapid>699789</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Successful Credential Theft Detected</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630416</id>
 <unravelevent>0</unravelevent>
 <uuid>e974095d-005a-4269-8b24-471f691ecd0e</uuid>
 <qidmapid>699799</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Potentially Bad Traffic</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630417</id>
 <unravelevent>0</unravelevent>
 <uuid>86f55110-c590-4d0a-8e7b-750ac7ce5e1e</uuid>
 <qidmapid>699791</qidmapid>
 <devicetypeid>4001</devicetypeid>
 <deviceeventid>Crypto Currency Mining Activity Detected</deviceeventid>
</dsmevent>
<dsmevent>
 <credibility>0</credibility>
 <deviceeventcategory>VCF Alert</deviceeventcategory>
 <customevent>true</customevent>
 <id>630414</id>
 <unravelevent>0</unravelevent>
```

```
  <uuid>9cc4f9bb-9d4a-4bd7-850c-7f67e749f9c3</uuid>
  <qidmapid>699793</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>Malware Command and Control Activity Detected</deviceeventid>
 </dsmevent>
 <dsmevent>
  <credibility>0</credibility>
  <deviceeventcategory>VCF Alert</deviceeventcategory>
  <customevent>true</customevent>
  <id>630415</id>
  <unravelevent>0</unravelevent>
  <uuid>2f0a7233-5395-4ba3-be42-348e66d2b9b0</uuid>
  <qidmapid>699794</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>Attempted Administrator Privilege Gain</deviceeventid>
 </dsmevent>
 <dsmevent>
  <credibility>0</credibility>
  <deviceeventcategory>VCF Close</deviceeventcategory>
  <customevent>true</customevent>
  <id>630420</id>
  <unravelevent>0</unravelevent>
  <uuid>bd9bdfa0-3529-4075-811c-164081253726</uuid>
  <qidmapid>699804</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>RST-Received</deviceeventid>
 </dsmevent>
 <dsmevent>
  <routepoint>EP</routepoint>
  <credibility>5</credibility>
  <deviceeventcategory>Stored</deviceeventcategory>
  <customevent>false</customevent>
  <id>630387</id>
  <unravelevent>0</unravelevent>
  <qidmapid>699775</qidmapid>
  <devicetypeid>4001</devicetypeid>
  <deviceeventid>unknown</deviceeventid>
 </dsmevent>
 <sensordevicecategory>
  <categorydescription>Third party Software integration</categorydescription>
  <categoryname>SW/Integration</categoryname>
  <id>5</id>
 </sensordevicecategory>
 <ariel_regex_property>
  <tenant_id>0</tenant_id>
  <creationdate>1688549252647</creationdate>
  <propertyname>Session Duration</propertyname>
  <forceparse>false</forceparse>
  <deprecated>false</deprecated>
  <propertytype>string</propertytype>
  <languagetag>NULL::character varying</languagetag>
  <description></description>
  <autodiscovered>false</autodiscovered>
  <sequenceid>292</sequenceid>
  <database>events</database>
  <datepattern>NULL::character varying</datepattern>
  <id>207a1188-f381-4c6d-8a2a-6766e337a51b</id>
  <editdate>1692467164132</editdate>
  <username>admin</username>
 </ariel_regex_property>
 <ariel_regex_property>
  <tenant_id>0</tenant_id>
  <creationdate>1690838333493</creationdate>
  <propertyname>Edge FW Action</propertyname>
  <forceparse>true</forceparse>
  <deprecated>false</deprecated>
  <propertytype>string</propertytype>
  <languagetag>NULL::character varying</languagetag>
  <description>VMware SD-WAN Edge - Firewall module acttion can be allow/drop/reject/alert</description>
  <autodiscovered>false</autodiscovered>
  <sequenceid>293</sequenceid>
  <database>events</database>
  <datepattern>NULL::character varying</datepattern>
  <id>485023e9-452b-4897-b518-7e40a3a05288</id>
  <editdate>1692467164197</editdate>
  <username>admin</username>
 </ariel_regex_property>
 <ariel_regex_property>
  <tenant_id>0</tenant_id>
  <creationdate>1688544080938</creationdate>
  <propertyname>IP Protocol</propertyname>
  <forceparse>true</forceparse>
  <deprecated>false</deprecated>
  <propertytype>string</propertytype>
  <languagetag>NULL::character varying</languagetag>
  <description></description>
  <autodiscovered>false</autodiscovered>
  <sequenceid>294</sequenceid>
  <database>events</database>
  <datepattern>NULL::character varying</datepattern>
  <id>8999aa82-29d4-44c2-b9f9-e2829ff7bb39</id>
  <editdate>1692467164279</editdate>
  <username>admin</username>
 </ariel_regex_property>
 <ariel_regex_property>
  <tenant_id>0</tenant_id>
  <creationdate>1688542013690</creationdate>
  <propertyname>Segment</propertyname>
  <forceparse>true</forceparse>
  <deprecated>false</deprecated>
  <propertytype>numeric</propertytype>
  <languagetag>en-US</languagetag>
  <description></description>
  <autodiscovered>false</autodiscovered>
  <sequenceid>295</sequenceid>
  <database>events</database>
  <datepattern></datepattern>
  <id>c2e9607f-057b-46b7-a4d1-01816d6b583c</id>
  <editdate>1692467164249</editdate>
  <username>admin</username>
 </ariel_regex_property>
 <ariel_regex_property>
  <tenant_id>0</tenant_id>
  <creationdate>1688549143932</creationdate>
  <propertyname>Source Interface</propertyname>
  <forceparse>false</forceparse>
  <deprecated>false</deprecated>
  <propertytype>string</propertytype>
  <languagetag>NULL::character varying</languagetag>
  <description></description>
  <autodiscovered>false</autodiscovered>
  <sequenceid>296</sequenceid>
  <database>events</database>
  <datepattern>NULL::character varying</datepattern>
  <id>7b5d7aba-e249-4fa0-8f63-49d81c8f7abf</id>
  <editdate>1692467164216</editdate>
  <username>admin</username>
 </ariel_regex_property>
```

```
<ariel_regex_property>
 <tenant_id>0</tenant_id>
 <creationdate>1688549361218</creationdate>
 <propertyname>Bytes Received</propertyname>
 <forceparse>false</forceparse>
 <deprecated>false</deprecated>
 <propertytype>numeric</propertytype>
 <languagetag>NULL::character varying</languagetag>
 <description></description>
 <autodiscovered>false</autodiscovered>
 <sequenceid>298</sequenceid>
 <database>events</database>
 <datepattern>NULL::character varying</datepattern>
 <id>fa70435d-0389-4dd9-9f75-270b65263c23</id>
 <editdate>1692467164058</editdate>
 <username>admin</username>
</ariel_regex_property>
<ariel_regex_property>
 <tenant_id>0</tenant_id>
 <creationdate>1688548547680</creationdate>
 <propertyname>Next Hop</propertyname>
 <forceparse>true</forceparse>
 <deprecated>false</deprecated>
 <propertytype>string</propertytype>
 <languagetag>NULL::character varying</languagetag>
 <description>Defines an Underlay or Overlay path for the flow in the VMW SD-WAN Solution</description>
 <autodiscovered>false</autodiscovered>
 <sequenceid>297</sequenceid>
 <database>events</database>
 <datepattern>NULL::character varying</datepattern>
 <id>8c107314-a062-43ad-8409-b78d99cc6b2f</id>
 <editdate>1692467164108</editdate>
 <username>admin</username>
</ariel_regex_property>
<ariel_regex_property>
 <tenant_id>0</tenant_id>
 <creationdate>1688550769123</creationdate>
 <propertyname>Suricata Signature Message</propertyname>
 <forceparse>false</forceparse>
 <deprecated>false</deprecated>
 <propertytype>string</propertytype>
 <languagetag>NULL::character varying</languagetag>
 <description>This field contains a Human-readable description of the Suricata Signature triggered.</description>
 <autodiscovered>false</autodiscovered>
 <sequenceid>300</sequenceid>
 <database>events</database>
 <datepattern>NULL::character varying</datepattern>
 <id>bb14e276-15a7-42e8-afc6-e75ccb491a14</id>
 <editdate>1692467164263</editdate>
 <username>admin</username>
</ariel_regex_property>
<ariel_regex_property>
 <tenant_id>0</tenant_id>
 <creationdate>1688550695625</creationdate>
 <propertyname>Suricata Signature ID</propertyname>
 <forceparse>false</forceparse>
 <deprecated>false</deprecated>
 <propertytype>string</propertytype>
 <languagetag>NULL::character varying</languagetag>
 <description>This field represents the Signature ID in the Edge FW Suricata IPS Rule-set.</description>
 <autodiscovered>false</autodiscovered>
 <sequenceid>299</sequenceid>
 <database>events</database>
 <datepattern>NULL::character varying</datepattern>
 <id>62c9297f-15c4-4ab9-bfbc-6b6bb5567305</id>
 <editdate>1692467164329</editdate>
 <username>admin</username>
</ariel_regex_property>
<ariel_regex_property>
 <tenant_id>0</tenant_id>
 <creationdate>1688549552582</creationdate>
 <propertyname>DAR Result</propertyname>
 <forceparse>false</forceparse>
 <deprecated>false</deprecated>
 <propertytype>string</propertytype>
 <languagetag>NULL::character varying</languagetag>
 <description>This field represents the application discovered by the Edge using Deep Application Recognition.</description>
 <autodiscovered>false</autodiscovered>
 <sequenceid>301</sequenceid>
 <database>events</database>
 <datepattern>NULL::character varying</datepattern>
 <id>b412ed65-0448-4897-98c0-80bbcc65ea24</id>
 <editdate>1692467164158</editdate>
 <username>admin</username>
</ariel_regex_property>
<ariel_regex_property>
 <tenant_id>0</tenant_id>
 <creationdate>1688548679578</creationdate>
 <propertyname>Edge Firewall Rule Name</propertyname>
 <forceparse>true</forceparse>
 <deprecated>false</deprecated>
 <propertytype>string</propertytype>
 <languagetag>NULL::character varying</languagetag>
 <description>Represents a named FW Rule entry in the Edge FW Policy that was matched for the flow.</description>
 <autodiscovered>false</autodiscovered>
 <sequenceid>302</sequenceid>
 <database>events</database>
 <datepattern>NULL::character varying</datepattern>
 <id>873812fd-18aa-43e7-a10c-bcad77f5a662</id>
 <editdate>1692467164233</editdate>
 <username>admin</username>
</ariel_regex_property>
<ariel_regex_property>
 <tenant_id>0</tenant_id>
 <creationdate>1688547257627</creationdate>
 <propertyname>Session ID</propertyname>
 <forceparse>true</forceparse>
 <deprecated>false</deprecated>
 <propertytype>string</propertytype>
 <languagetag>NULL::character varying</languagetag>
 <description></description>
 <autodiscovered>false</autodiscovered>
 <sequenceid>303</sequenceid>
 <database>events</database>
 <datepattern>NULL::character varying</datepattern>
 <id>321d358d-1203-4a8f-b46e-74d818d7f761</id>
 <editdate>1692467164312</editdate>
 <username>admin</username>
</ariel_regex_property>
<ariel_regex_property>
 <tenant_id>0</tenant_id>
 <creationdate>1688548855664</creationdate>
 <propertyname>Destination Domain</propertyname>
 <forceparse>true</forceparse>
 <deprecated>false</deprecated>
 <propertytype>string</propertytype>
 <languagetag>NULL::character varying</languagetag>
 <description>Target domain name (if available)</description>
```

```
  <autodiscovered>false</autodiscovered>
  <sequenceid>304</sequenceid>
  <database>events</database>
  <datepattern>NULL::character varying</datepattern>
  <id>bd029346-adaf-422f-a17d-5a82a1e203d9</id>
  <editdate>1692467164180</editdate>
  <username>admin</username>
 </ariel_regex_property>
 <ariel_regex_property>
  <tenant_id>0</tenant_id>
  <creationdate>1688549348583</creationdate>
  <propertyname>Bytes Sent</propertyname>
  <forceparse>false</forceparse>
  <deprecated>false</deprecated>
  <propertytype>numeric</propertytype>
  <languagetag>NULL::character varying</languagetag>
  <description></description>
  <autodiscovered>false</autodiscovered>
  <sequenceid>305</sequenceid>
  <database>events</database>
  <datepattern>NULL::character varying</datepattern>
  <id>e2b48f1b-f8a6-4422-9aae-0d0e38cd4e66</id>
  <editdate>1692467164294</editdate>
  <username>admin</username>
 </ariel_regex_property>
 <sensordevicetype>
  <extension_id>1</extension_id>
  <uniqueperhost>false</uniqueperhost>
  <devicetypecredibility>5</devicetypecredibility>
  <uuid>d47fc6cb-d61b-44f0-a8d3-8fc76006eeee</uuid>
  <dsmparameter></dsmparameter>
  <devicecategoryid>5</devicecategoryid>
  <devicetypedescription>VMware SD-WAN Edge</devicetypedescription>
  <defaultlanguageid>1</defaultlanguageid>
  <id>4001</id>
  <devicetypename>VMwareSDWANEdgeCustom</devicetypename>
  <devicetypeoverride>4000</devicetypeoverride>
  <mask>0</mask>
 </sensordevicetype>
 <sensordevice>
  <deviceenabled>false</deviceenabled>
  <creationdate>1688535787225</creationdate>
  <bulk_added_id>0</bulk_added_id>
  <languageid>1</languageid>
  <deployed>true</deployed>
  <timestamp_last_seen>1690799325719</timestamp_last_seen>
  <devicecredibility>5</devicecredibility>
  <uuid>14f170b6-bfd3-465d-8f69-86163500933c</uuid>
  <hostname>MD-MUNICH-HQ-01</hostname>
  <timestamp_eps60s>2023-07-31T06:29:11.069-04:00</timestamp_eps60s>
  <peakeps60s>17</peakeps60s>
  <eccomponentid>-1</eccomponentid>
  <logonly>false</logonly>
  <id>162</id>
  <extension_use_condition>0</extension_use_condition>
  <devicedescription></devicedescription>
  <extension_id>1</extension_id>
  <store_event_payload>true</store_event_payload>
  <timestamp_peakeps60s>2023-07-26T08:31:11.066-04:00</timestamp_peakeps60s>
  <coalesce_events>true</coalesce_events>
  <eps60s>0</eps60s>
  <autodiscovered>false</autodiscovered>
  <bulk_added>false</bulk_added>
  <encoding>UTF-8</encoding>
  <devicetypeid>4001</devicetypeid>
  <eccomponentid_history>7</eccomponentid_history>
  <devicename>MD-MUNICH-HQ-01</devicename>
  <editdate>1692467485533</editdate>
  <gateway>false</gateway>
 </sensordevice>
 <qidmap>
  <severity>5</severity>
  <lowlevelcategory>1002</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250026</qid>
  <uuid>12a9adaf-8559-4201-a8bd-dd351b322d45</uuid>
  <ratethreshold>5</ratethreshold>
  <rateinterval>1000</rateinterval>
  <qdescription>The VMware SD-WAN Edge detected a potential Information Leak attempt. An attempted information leak is an attempt to acquire sensitive
 information from a system or network without authorization. Additional details are available under the event details or in the VMware Edge Cloud Orchestrator
 Security Overview and FW Logs view.</qdescription>
  <catpipename>Beta</catpipename>
  <ratelongwindow>86400</ratelongwindow>
  <qname>Edge Intrusion Detection - Attempted Information Leak</qname>
  <rateshortwindow>3600</rateshortwindow>
  <id>699801</id>
 </qidmap>
 <qidmap>
  <severity>7</severity>
  <lowlevelcategory>7065</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250014</qid>
  <uuid>11a73aed-3862-40e9-9ce6-d5aa0dbecc28</uuid>
  <ratethreshold>0</ratethreshold>
  <rateinterval>1000</rateinterval>
  <qdescription>The VMware SD-WAN Edge detected and raised a high-severity security event that indicates that an unauthorized user has successfully stolen
 credentials from a system or network and requires urgent attention.
Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
  <catpipename>Beta</catpipename>
  <ratelongwindow>86400</ratelongwindow>
  <qname>Edge Intrusion Detection - Successful Credential Theft Detected</qname>
  <rateshortwindow>3600</rateshortwindow>
  <id>699789</id>
 </qidmap>
 <qidmap>
  <severity>1</severity>
  <lowlevelcategory>19001</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250025</qid>
  <uuid>d79ed38e-dc19-41d3-b333-0b257a40e994</uuid>
  <ratethreshold>0</ratethreshold>
  <rateinterval>0</rateinterval>
  <qdescription>This event informs QRadar that the Suricata signature file has been updated on the VMware SD-WAN Edge. Further details are available in the
 Orchestrator.</qdescription>
  <catpipename>Echo</catpipename>
  <ratelongwindow>0</ratelongwindow>
  <qname>Edge Intrusion Detection - Signature File Updated</qname>
  <rateshortwindow>0</rateshortwindow>
  <id>699800</id>
 </qidmap>
 <qidmap>
  <severity>1</severity>
  <lowlevelcategory>19001</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250013</qid>
  <uuid>fe006000-c448-4ebc-8842-a27faa46620c</uuid>
  <ratethreshold>0</ratethreshold>
  <rateinterval>0</rateinterval>
```

```
  <qdescription>The Edge received a new configuration, however parts of the configuration (either coming from the profile or the edge) cannot be applied to
 the device. This is a fairly common alert with virtual edges, where the configuration might contain more NICs than what the virtual machine has. Further
 information is available in the SASE Orchestrator.</qdescription>
  <catpipename>Echo</catpipename>
  <ratelongwindow>0</ratelongwindow>
  <qname>Edge Management Plane - Configuration inconsistency detected</qname>
  <rateshortwindow>0</rateshortwindow>
  <id>699788</id>
 </qidmap>
 <qidmap>
  <severity>3</severity>
  <lowlevelcategory>7006</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250012</qid>
  <uuid>ab7bb607-9ec0-4280-8be1-ed0f41e0f530</uuid>
  <ratethreshold>5</ratethreshold>
  <rateinterval>1000</rateinterval>
  <qdescription>The VMware SD-WAN Edge detected suspicious flows that indicate that a device on your network is attempting to retrieve its external IP
 address. This is typically done by sending a request to a public DNS server.
While this is not necessarily malicious activity, it can be a sign of an attacker attempting to gather information about your network.
Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
  <catpipename>Beta</catpipename>
  <ratelongwindow>86400</ratelongwindow>
  <qname>Edge Intrusion Detection - Device Retrieving External IP Address Detected</qname>
  <rateshortwindow>3600</rateshortwindow>
  <id>699787</id>
 </qidmap>
 <qidmap>
  <severity>1</severity>
  <lowlevelcategory>4008</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250030</qid>
  <uuid>eec05d9b-120b-4a32-8aee-ab1ac5b189c3</uuid>
  <ratethreshold>0</ratethreshold>
  <rateinterval>0</rateinterval>
  <qdescription>The Edge observed a TCP session terminated by one of the peers using the TCP FIN flag.</qdescription>
  <catpipename>Echo</catpipename>
  <ratelongwindow>0</ratelongwindow>
  <qname>Edge FW - Session closed upon FIN received</qname>
  <rateshortwindow>0</rateshortwindow>
  <id>699805</id>
 </qidmap>
 <qidmap>
  <severity>1</severity>
  <lowlevelcategory>4007</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250040</qid>
  <uuid>30ba4c09-f966-4a97-8b86-227170412b9e</uuid>
  <ratethreshold>0</ratethreshold>
  <rateinterval>0</rateinterval>
  <qdescription>For all the ongoing sessions, the Update log message will appear if the firewall rule is either added or modified through Orchestrator. This
 can be due to a configuration change.
No futher action is required.</qdescription>
  <catpipename>Echo</catpipename>
  <ratelongwindow>0</ratelongwindow>
  <qname>Edge FW - Session Updated</qname>
  <rateshortwindow>0</rateshortwindow>
  <id>3070875</id>
 </qidmap>
 <qidmap>
  <severity>1</severity>
  <lowlevelcategory>4008</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250029</qid>
  <uuid>13e76fd2-ff4a-42c9-b885-4d16f9b707e6</uuid>
  <ratethreshold>0</ratethreshold>
  <rateinterval>0</rateinterval>
  <qdescription>The TCP session has been refused or terminated by one of the peers with a TCP Reset message.</qdescription>
  <catpipename>Echo</catpipename>
  <ratelongwindow>0</ratelongwindow>
  <qname>Edge FW - Session closed upon RST received</qname>
  <rateshortwindow>0</rateshortwindow>
  <id>699804</id>
 </qidmap>
 <qidmap>
  <severity>9</severity>
  <lowlevelcategory>5011</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250028</qid>
  <uuid>fbc9309f-c2ae-40e5-b9af-1e29c440469c</uuid>
  <ratethreshold>0</ratethreshold>
  <rateinterval>0</rateinterval>
  <qdescription>The Edge IPS service detected a potential exploit attempt targeting client-side Web applications. The Orchestrator or the Event details in
 QRadar will contain additional details.</qdescription>
  <catpipename>Alpha</catpipename>
  <ratelongwindow>0</ratelongwindow>
  <qname>Edge Intrusion Detection - Client-side Vulnerability Exploit Attempt</qname>
  <rateshortwindow>0</rateshortwindow>
  <id>699803</id>
 </qidmap>
 <qidmap>
  <severity>6</severity>
  <lowlevelcategory>4026</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250027</qid>
  <uuid>0fc2bd03-a0d4-4d19-869c-c4f09cc208cc</uuid>
  <ratethreshold>0</ratethreshold>
  <rateinterval>0</rateinterval>
  <qdescription>The VMware SD-WAN Edge detected a potential user privilege gain attempt. An attempted user privilege gain is an attempt by an unauthorized
 user to gain elevated privileges on a system or network. Additional details are available under the event details or in the VMware Edge Cloud Orchestrator
 Security Overview and FW Logs view.</qdescription>
  <catpipename>Echo</catpipename>
  <ratelongwindow>0</ratelongwindow>
  <qname>Edge Intrusion Detection - Attempted User Privilege Gain</qname>
  <rateshortwindow>0</rateshortwindow>
  <id>699802</id>
 </qidmap>
 <qidmap>
  <severity>1</severity>
  <lowlevelcategory>19017</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250034</qid>
  <uuid>74b41d72-2494-4490-b11a-7210cd22e3ac</uuid>
  <ratethreshold>0</ratethreshold>
  <rateinterval>0</rateinterval>
  <qdescription>The Edge reported data upload to the Orchestrator. This is usually part of normal operations, and no further action is required.</qd
escription>
  <catpipename>Echo</catpipename>
  <ratelongwindow>0</ratelongwindow>
  <qname>Edge Management Plane - Data stream to Orchestrator</qname>
  <rateshortwindow>0</rateshortwindow>
  <id>699809</id>
 </qidmap>
 <qidmap>
  <severity>1</severity>
  <lowlevelcategory>19018</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250033</qid>
```

```
   <uuid>673f789e-d568-499e-9e39-887c41a08cfc</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>This event shows that the Edge Firewall policy has been modified. More details are available on the Orchestrator.</qdescription>
   <catpipename>Echo</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge FW - Configuration changed</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699808</id>
  </qidmap>
  <qidmap>
   <severity>8</severity>
   <lowlevelcategory>2014</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250032</qid>
   <uuid>c78ab7ec-d1d8-449d-bb44-e9b58243a307</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>The VMware SD-WAN Edge detected a potential DoS attack attempt. An attempted DoS attack is a flood of traffic that aims to make a website or
  server unavailable. Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</
 qdescription>
   <catpipename>Beta</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Intrusion Detection - Attempted Denial of Service</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699807</id>
  </qidmap>
  <qidmap>
   <severity>3</severity>
   <lowlevelcategory>10009</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250031</qid>
   <uuid>21e3b7e6-dd2b-4895-9f15-da4ba4b1cf2b</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>VMware SD-WAN Edge Stored Event</qdescription>
   <ratelongwindow>0</ratelongwindow>
   <qname>VMware SD-WAN Edge Message</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699806</id>
  </qidmap>
  <qidmap>
   <severity>8</severity>
   <lowlevelcategory>6018</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250018</qid>
   <uuid>c3a02854-8c0a-4f6d-ac16-fb0bca4829ce</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>The VMware SD-WAN Edge firewall detected flows that are indicators that your system or network may be under attack by malware. This type of
  malware communicates with a remote server, known as a command and control (C&C) server, to receive instructions. The C&C server can then be used to control
  the infected system, such as downloading additional malware, stealing data, or launching denial-of-service attacks.
 Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
   <catpipename>Alpha</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Intrusion Detection - Malware Command and Control Activity Detected</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699793</id>
  </qidmap>
  <qidmap>
   <severity>1</severity>
   <lowlevelcategory>19001</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250017</qid>
   <uuid>e4a62615-445e-49f7-a240-161f73c4b780</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>The Edge reported that the Auto SIM Switch feature has been disabled. Unless this feature is required (the Edge has multiple cellular
  connections, for example), no additional action is required. Only certain hardware models support this feature.</qdescription>
   <catpipename>Echo</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Management Plane - Cellular failover disabled</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699792</id>
  </qidmap>
  <qidmap>
   <severity>1</severity>
   <lowlevelcategory>7072</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250016</qid>
   <uuid>f44feeea-f656-4af5-aae6-5fc5ac1ce561</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>The VMware SD-WAN Edge detected flows that indicates that your system or network may be infected with cryptocurrency mining malware. This
  type of malware uses your system's resources to mine cryptocurrency, which can have a number of negative consequences, including reduced system performance,
  increased power consumption, heat generation and security risks.
 Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
   <catpipename>Beta</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Intrusion Detection - Crypto Currency Mining Activity Detected</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699791</id>
  </qidmap>
  <qidmap>
   <severity>4</severity>
   <lowlevelcategory>3018</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250015</qid>
   <uuid>766be688-e3b8-4ae5-81f4-e06bcf3bc082</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>The VMware SD-WAN Edge observed and blocked login attempts that indicates that an unauthorized user is trying to access your system or network
  using default credentials. This could be a sign of a brute-force attack, which is an attempt to guess a password by trying a large number of possible
  combinations.
 Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
   <catpipename>Echo</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Intrusion Detection - Attempt to Login By a Default Username and Password</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699790</id>
  </qidmap>
  <qidmap>
   <severity>3</severity>
   <lowlevelcategory>10009</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250000</qid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>VMwareSDWANEdgeCustom Stored Event</qdescription>
   <ratelongwindow>0</ratelongwindow>
   <qname>VMware SD-WAN Edge Message</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699775</id>
  </qidmap>
  <qidmap>
   <severity>2</severity>
   <lowlevelcategory>9002</lowlevelcategory>
   <reverseip>false</reverseip>
```

```
   <qid>1002250022</qid>
   <uuid>e6035529-ccc1-4531-a05a-7694e11b669c</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>The Suricata IDPS engine of an Edge Firewall reported activity that is not part of the usual end-user behavior, and can be used to bypass the
  enterprise security measures. Additional information is available in the VMware SASE Orchestrator.</qdescription>
   <catpipename>Foxtrot</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Intrusion Detection - Policy Violation</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699797</id>
  </qidmap>
  <qidmap>
   <severity>3</severity>
   <lowlevelcategory>7006</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250021</qid>
   <uuid>3e1a1ec1-6465-4e7e-a6b0-04da30e1ab7c</uuid>
   <ratethreshold>5</ratethreshold>
   <rateinterval>1000</rateinterval>
   <qdescription>The Suricata IDPS engine detected flows that might belong to suspicious activity or hosts or applications that are misconfigured. These flows
  should be investigated. Additional information is available in the VMware SASE Orchestrator.</qdescription>
   <catpipename>Beta</catpipename>
   <ratelongwindow>86400</ratelongwindow>
   <qname>Edge Intrusion Detection - Suspicious Activity</qname>
   <rateshortwindow>3600</rateshortwindow>
   <id>699796</id>
  </qidmap>
  <qidmap>
   <severity>9</severity>
   <lowlevelcategory>6002</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250020</qid>
   <uuid>5cafce18-a694-433c-a813-74d6c209f068</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>The VMware SD-WAN Edge detected flows that are indication of an active backdoor being used and requires urgent attention.
 An indication of an active backdoor channel is any suspicious activity that suggests that an unauthorized user has gained access to your system or network and
  has created a way to communicate with your system or network without your knowledge.
 Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
   <catpipename>Beta</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Intrusion Detection - Indication of an active backdoor channel</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699795</id>
  </qidmap>
  <qidmap>
   <severity>9</severity>
   <lowlevelcategory>5032</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250019</qid>
   <uuid>37f5a738-99f5-4e1d-a0d0-b97b2c58d34a</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>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.</qdescription>
   <catpipename>Alpha</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Intrustion Detection - Exploit Attempt</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699794</id>
  </qidmap>
  <qidmap>
   <severity>10</severity>
   <lowlevelcategory>3007</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250004</qid>
   <uuid>e835a2ba-d4bf-49c2-89bf-588c9df92e96</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>The VMware SD-WAN Edge FW captured flows that indicate that an attacker has successfully gained administrator privileges on your system or
  network. Administrator privileges allow the attacker to do anything they want on your system, including installing malware, stealing data, and changing
  settings.
 Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
   <catpipename>Echo</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Intrusion Prevention - Successful Administrator Privilege Gain</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699779</id>
  </qidmap>
  <qidmap>
   <severity>1</severity>
   <lowlevelcategory>4008</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250037</qid>
   <uuid>011e95cc-d9e9-4bed-892f-075d2724608b</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>  </qdescription>
   <catpipename>Echo</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge FW - Session Aged Out</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699812</id>
  </qidmap>
  <qidmap>
   <severity>10</severity>
   <lowlevelcategory>3007</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250003</qid>
   <uuid>eb04f899-a123-4265-baae-77c6a43c2a7e</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>The VMware SD-WAN Edge block connectivity that indicates that an attacker has successfully gained administrator or root privileges on a system
  or network. This means that the attacker has complete control over the system or network, and they can do anything they want, including stealing data,
  installing malware, or disrupting operations.
 Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
   <catpipename>Echo</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Intrusion Detection - Successful User Privilege Gain</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699778</id>
  </qidmap>
  <qidmap>
   <severity>1</severity>
   <lowlevelcategory>19018</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250036</qid>
   <uuid>8030d208-2dd1-413e-bffb-cf6d668187a3</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>The Edge finished the websockets activity. Tipically this messages signals the end of data transfer from the Edge to the Orchestrator.</
 qdescription>
   <catpipename>Echo</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Management Plane - WebSocket closed</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699811</id>
```

```
  </qidmap>
  <qidmap>
   <severity>5</severity>
   <lowlevelcategory>14016</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250024</qid>
   <uuid>ea943744-6d26-4bfa-adb0-e94012be19d6</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>Potentially bad traffic is any traffic that is out of the ordinary and may be indicative of a security breach.
 The VMware SD-WAN Edge detected flows that are suspicious and could be part of recon activity, or indication of an ongoing exploit attempt and should be
  investigated.
 Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
   <catpipename>Beta</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Intrusion Detection - Potentially Bad Traffic</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699799</id>
  </qidmap>
  <qidmap>
   <severity>9</severity>
   <lowlevelcategory>5011</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250002</qid>
   <uuid>297dbf2f-165c-4172-8946-03d506292dae</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>The VMware SD-WAN Edge IDS/IPS service captured flows that indicate someone is attacking web applications.
 Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
   <catpipename>Alpha</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Intrusion Prevention - Web Application Attack</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699777</id>
  </qidmap>
  <qidmap>
   <severity>7</severity>
   <lowlevelcategory>6008</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250035</qid>
   <uuid>3a6f349f-8ba0-4718-b530-5a2150663bb5</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>  </qdescription>
   <catpipename>Beta</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge Intrusion Detection - Trojan Detected</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699810</id>
  </qidmap>
  <qidmap>
   <severity>3</severity>
   <lowlevelcategory>10001</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250001</qid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>Unknown</qdescription>
   <ratelongwindow>0</ratelongwindow>
   <qname>Unknown</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699776</id>
  </qidmap>
  <qidmap>
   <severity>1</severity>
   <lowlevelcategory>4007</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250023</qid>
   <uuid>272b740e-c9ec-48ff-9888-ac757feb2a3d</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>0</rateinterval>
   <qdescription>The Edge Firewall detected a new session opening.</qdescription>
   <catpipename>Echo</catpipename>
   <ratelongwindow>0</ratelongwindow>
   <qname>Edge FW - New Session Detected</qname>
   <rateshortwindow>0</rateshortwindow>
   <id>699798</id>
  </qidmap>
  <qidmap>
   <severity>3</severity>
   <lowlevelcategory>1021</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250039</qid>
   <uuid>f07cef4b-11a3-4d8e-a69c-2fa70ee2dc92</uuid>
   <ratethreshold>5</ratethreshold>
   <rateinterval>1000</rateinterval>
   <qdescription>The VMware SD-WAN Edge detected connectivity that an unauthorized user gained access to sensitive data.
 Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
   <catpipename>Beta</catpipename>
   <ratelongwindow>86400</ratelongwindow>
   <qname>Edge Intrusion Detection - Information Leak</qname>
   <rateshortwindow>3600</rateshortwindow>
   <id>699814</id>
  </qidmap>
  <qidmap>
   <severity>4</severity>
   <lowlevelcategory>4003</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250038</qid>
   <uuid>4f0f5000-43c1-4e70-816d-1d60c08f1ae5</uuid>
   <ratethreshold>25</ratethreshold>
   <rateinterval>100</rateinterval>
   <qdescription>  </qdescription>
   <catpipename>Echo</catpipename>
   <ratelongwindow>86400</ratelongwindow>
   <qname>Edge Firewall - RPF Check Fail</qname>
   <rateshortwindow>3600</rateshortwindow>
   <id>699813</id>
  </qidmap>
  <qidmap>
   <severity>7</severity>
   <lowlevelcategory>7065</lowlevelcategory>
   <reverseip>false</reverseip>
   <qid>1002250007</qid>
   <uuid>44053dd1-50cf-4f80-bfe9-3a052d2c7176</uuid>
   <ratethreshold>0</ratethreshold>
   <rateinterval>1000</rateinterval>
   <qdescription>The VMware SD-WAN Edge detected flows that indicate that an attacker may have attempted to use social engineering techniques to gain access to
  your system or network. Social engineering is a type of attack that relies on human interaction to trick the victim into providing sensitive information or
  taking actions that compromise their security.
 Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
   <catpipename>Beta</catpipename>
   <ratelongwindow>86400</ratelongwindow>
   <qname>Edge Intrusion Detection - Possible Social Engineering Attempted</qname>
   <rateshortwindow>3600</rateshortwindow>
   <id>699782</id>
  </qidmap>
  <qidmap>
```

```
  <severity>3</severity>
  <lowlevelcategory>20012</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250006</qid>
  <uuid>7ff4d9d2-342b-418f-8d8f-706fdfeb8e03</uuid>
  <ratethreshold>0</ratethreshold>
  <rateinterval>0</rateinterval>
  <qdescription>The VMware SD-WAN Edge detected flows that may belong to PUPs (Potentially Unwanted Programs).
PUPs are software programs that are not malicious in and of themselves, but they can be used to collect personal information or display unwanted ads.</qdescri
ption>
  <catpipename>Echo</catpipename>
  <ratelongwindow>0</ratelongwindow>
  <qname>Edge Intrusion Detection - Possibly Unwanted Program Detected</qname>
  <rateshortwindow>0</rateshortwindow>
  <id>699781</id>
 </qidmap>
 <qidmap>
  <severity>3</severity>
  <lowlevelcategory>7002</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250005</qid>
  <uuid>aaf78e01-5be3-4633-984e-a519925eab4f</uuid>
  <ratethreshold>5</ratethreshold>
  <rateinterval>1000</rateinterval>
  <qdescription>The VMware SD-WAN Edge detected flows that indicate that an attacker may be targeting your system or network. These alarms are triggered by
 signatures that are designed to detect known attack patterns.
Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
  <catpipename>Beta</catpipename>
  <ratelongwindow>86400</ratelongwindow>
  <qname>Edge Intrusion Detection - Targeted Malicious Activity was Detected</qname>
  <rateshortwindow>3600</rateshortwindow>
  <id>699780</id>
 </qidmap>
 <qidmap>
  <severity>1</severity>
  <lowlevelcategory>19030</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250011</qid>
  <uuid>bf4810bb-e0ee-48e2-9151-a92141929477</uuid>
  <ratethreshold>0</ratethreshold>
  <rateinterval>0</rateinterval>
  <qdescription>The Edge received an updated configuration file for its Crawler software component. This might have effect on the Edge throughput or the Edge
 Network Intelligence (ENI) operations.</qdescription>
  <catpipename>Echo</catpipename>
  <ratelongwindow>0</ratelongwindow>
  <qname>Edge Crawler - Configuration Change Detected</qname>
  <rateshortwindow>0</rateshortwindow>
  <id>699786</id>
 </qidmap>
 <qidmap>
  <severity>7</severity>
  <lowlevelcategory>13009</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250010</qid>
  <uuid>d4b08f0e-8004-4cdd-9795-1224a1f3ba51</uuid>
  <ratethreshold>0</ratethreshold>
  <rateinterval>0</rateinterval>
  <qdescription>The VMware SD-WAN Edge detected flows that indicates that an exploit kit has been used to attempt to compromise your system or network.
 Exploit kits are malicious software that are used to exploit vulnerabilities in software to gain access to a system or network.
Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
  <catpipename>Alpha</catpipename>
  <ratelongwindow>0</ratelongwindow>
  <qname>Edge Intrusion Detection - Exploit Kit Activity Detected</qname>
  <rateshortwindow>0</rateshortwindow>
  <id>699785</id>
 </qidmap>
 <qidmap>
  <severity>3</severity>
  <lowlevelcategory>7002</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250009</qid>
  <uuid>7fe179f4-9510-4973-b1cb-a746ea896bd3</uuid>
  <ratethreshold>5</ratethreshold>
  <rateinterval>1000</rateinterval>
  <qdescription>The VMware SD-WAN Edge firewall observed activity that might be part of network scanner tools such as NMAP.
Additional details are available under the event details or in the VMware Edge Cloud Orchestrator Security Overview and FW Logs view.</qdescription>
  <catpipename>Beta</catpipename>
  <ratelongwindow>86400</ratelongwindow>
  <qname>Edge Intrusion Detection - Detection of a Network Scan</qname>
  <rateshortwindow>3600</rateshortwindow>
  <id>699784</id>
 </qidmap>
 <qidmap>
  <severity>3</severity>
  <lowlevelcategory>19030</lowlevelcategory>
  <reverseip>false</reverseip>
  <qid>1002250008</qid>
  <uuid>386c86d9-4fc7-41bd-9a3b-abb8f6fd8f45</uuid>
  <ratethreshold>0</ratethreshold>
  <rateinterval>0</rateinterval>
  <qdescription>The Edge received an updated configuration that applied to the device settings. This configuration can contain modified connectivity details
 such as new IP addressing, additional VLANs, etc. Additional details can be found in the SASE Orchestrator.</qdescription>
  <catpipename>Echo</catpipename>
  <ratelongwindow>0</ratelongwindow>
  <qname>Edge Device Settings - Configuration Change Detected</qname>
  <rateshortwindow>0</rateshortwindow>
  <id>699783</id>
 </qidmap>
 <device_ext>
  <xml>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8bnMyOmRldmljZS1leHRlbnNpb24geG1sbnM6bnMyPSJldmVudF9wYXJzaW5nL2Rld
mljZV9leHRlbnNpb24iPgogICAgPHBhdHRlcm4gdXNlLWRlZmF1bHQtcGF0dGVybj0idHJ1ZSIgdHlwZT0iSmF2YVBhdHRlcm4iIGlkPSJEZXN0aW5hdGlvbklwLVBhdHRlcm4tMSI+RFNUPSgoPzpbMC05X
XsxLDN9XC4pezN9WzAtOV17MSwzfSlcczwvcGF0dGVybj4KICAgIDxwYXR0ZXJuIHVzZS1kZWZhdWx0LXBhdHRlcm49InRydWUiIHR5cGU9IkphdmFQYXR0ZXJuIiBpZD0iRGVzdGluYXRpb25Qb3J0LVBhd
HRlcm4tMSI+RFBUPSguKj8pXHM8L3BhdHRlcm4+CiAgICA8cGF0dGVybiB1c2UtZGVmYXVsdC1wYXR0ZXJuPSJ0cnVlIiB0eXBlPSJKYXZhUGF0dGVybiIgaWQ9IkV2ZW50Q2F0ZWdvcnktUGF0dGVybi0xI
j5BQ1RJT049KC4qPylccyguKj8pXHM8L3BhdHRlcm4+CiAgICA8cGF0dGVybiB1c2UtZGVmYXVsdC1wYXR0ZXJuPSJ0cnVlIiB0eXBlPSJKYXZhUGF0dGVybiIgaWQ9IkV2ZW50Q2F0ZWdvcnktUGF0dGVyb
i0yIj5NR0RfQ09ORl9BUFBMSUVEPC9wYXR0ZXJuPgogICAgPHBhdHRlcm4gdXNlLWRlZmF1bHQtcGF0dGVybj0idHJ1ZSIgdHlwZT0iSmF2YVBhdHRlcm4iIGlkPSJFdmVudENhdGVnb3J5LVBhdHRlcm4tM
yI+KE1HRF9XRUJTT0NLRVRfKSguKj8pOjwvcGF0dGVybj4KICAgIDxwYXR0ZXJuIHVzZS1kZWZhdWx0LXBhdHRlcm49InRydWUiIHR5cGU9IkphdmFQYXR0ZXJuIiBpZD0iRXZlbnRDYXRlZ29yeS1QYXR0Z
XJuLTQiPihBVFBfSURQU19SVUxFXykoLio/KTo8L3BhdHRlcm4+CiAgICA8cGF0dGVybiB1c2UtZGVmYXVsdC1wYXR0ZXJuPSJ0cnVlIiB0eXBlPSJKYXZhUGF0dGVybiIgaWQ9IkV2ZW50Q2F0ZWdvcnktU
GF0dGVybi01Ij5FREdFX0FVVE9fU0lNX1NXSVRDSDwvcGF0dGVybj4KICAgIDxwYXR0ZXJuIHVzZS1kZWZhdWx0LXBhdHRlcm49InRydWUiIHR5cGU9IkphdmFQYXR0ZXJuIiBpZD0iRXZlbnRDYXRlZ29ye
S1QYXR0ZXJuLTYiPk1HRF9ERVZJQ0VfQ09ORklHX1dBUk5JTkc8L3BhdHRlcm4+CiAgICA8cGF0dGVybiB1c2UtZGVmYXVsdC1wYXR0ZXJuPSJ0cnVlIiB0eXBlPSJKYXZhUGF0dGVybiIgaWQ9IkV2ZW50T
mFtZS1QYXR0ZXJuLTEiPlJFQVNPTj0oLio/KVxzW0EtWl0qKF98PSk8L3BhdHRlcm4+CiAgICA8cGF0dGVybiB1c2UtZGVmYXVsdC1wYXR0ZXJuPSJ0cnVlIiB0eXBlPSJKYXZhUGF0dGVybiIgaWQ9IkV2Z
W50TmFtZS1QYXR0ZXJuLTIiPkNBVEVHT1JZPSguKj8pXHNbQS1aXSooX3w9KTwvcGF0dGVybj4KICAgIDxwYXR0ZXJuIHVzZS1kZWZhdWx0LXBhdHRlcm49InRydWUiIHR5cGU9IkphdmFQYXR0ZXJuIiBpZ
D0iRXZlbnROYW1lLVBhdHRlcm4tMyI+TUdEX0NPTkZfQVBQTElFRDpccyguKj8pKFxzWzEtOV18XHN2ZXJzaW9uKTwvcGF0dGVybj4KICAgIDxwYXR0ZXJuIHVzZS1kZWZhdWx0LXBhdHRlcm49InRydWUiI
HR5cGU9IkphdmFQYXR0ZXJuIiBpZD0iRXZlbnROYW1lLVBhdHRlcm4tNCI+VkNNGIE9wZW48L3BhdHRlcm4+CiAgICA8cGF0dGVybiB1c2UtZGVmYXVsdC1wYXR0ZXJuPSJ0cnVlIiB0eXBlPSJKYXZhUGF0d
GVybiIgaWQ9IkV2ZW50TmFtZS1QYXR0ZXJuLTUiPk1HRF9XRUJTT0NLRVRfKC4qPyk6XHMoLio/KSQ8L3BhdHRlcm4+CiAgICA8cGF0dGVybiB1c2UtZGVmYXVsdC1wYXR0ZXJuPSJ0cnVlIiB0eXBlPSJKY
XZhUGF0dGVybiIgaWQ9IkV2ZW50TmFtZS1QYXR0ZXJuLTYiPkFUUF9JRFBTXyguKj8pOlxzKC4qPylcc3dpdGgoLio/KSQ8L3BhdHRlcm4+CiAgICA8cGF0dGVybiB1c2UtZGVmYXVsdC1wYXR0ZXJuPSJ0c
nVlIiB0eXBlPSJKYXZhUGF0dGVybiIgaWQ9IkV2ZW50TmFtZS1QYXR0ZXJuLTciPkVER0VfQVVUT19TSU1fU1dJVENIOlxzKC4qPykkPC9wYXR0ZXJuPgogICAgPHBhdHRlcm4gdXNlLWRlZmF1bHQtcGF0d
GVybj0idHJ1ZSIgdHlwZT0iSmF2YVBhdHRlcm4iIGlkPSJFdmVudE5hbWUtUGF0dGVybi04Ij5NR0RfREVWSUNFX0NPTkZJR19XQVJOSU5HOlxzKC4qPykkPC9wYXR0ZXJuPgogICAgPHBhdHRlcm4gdXNlL
WRlZmF1bHQtcGF0dGVybj0idHJ1ZSIgdHlwZT0iSmF2YVBhdHRlcm4iIGlkPSJFdmVudE5hbWUtUGF0dGVybi05Ij5WQ0YgVXBkYXRlPC9wYXR0ZXJuPgogICAgPHBhdHRlcm4gdXNlLWRlZmF1bHQtcGF0d
GVybj0idHJ1ZSIgdHlwZT0iSmF2YVBhdHRlcm4iIGlkPSJEZXN0aW5hdGlvbklwdjYtUGF0dGVybi0xIj5EU1Q9KCgoWzAtOWEtZkEtRl17MSw0fTopezcsN31bMC05YS1mQS1GXXsxLDR9fChbMC05YS1mQ
S1GXXsxLDR9Oil7MSw3fTp8KFswLTlhLWZBLUZdezEsNH06KXsxLDZ9OlswLTlhLWZBLUZdezEsNH18KFswLTlhLWZBLUZdezEsNH06KXsxLDV9KDpbMC05YS1mQS1GXXsxLDR9KXsxLDJ9fChbMC05YS1mQ
S1GXXsxLDR9Oil7MSw0fSg6WzAtOWEtZkEtRl17MSw0fSl7MSwzfXwoWzAtOWEtZkEtRl17MSw0fTopezEsM30oOlswLTlhLWZBLUZdezEsNH0pezEsNH18KFswLTlhLWZBLUZdezEsNH06KXsxLDJ9KDpbM
C05YS1mQS1GXXsxLDR9KXsxLDV9fFswLTlhLWZBLUZdezEsNH06KCg6WzAtOWEtZkEtRl17MSw0fSl7MSw2fSl8OigoOlswLTlhLWZBLUZdezEsNH0pezEsN318Oil8ZmU4MDooOlswLTlhLWZBLUZdezAsN
H0pezAsNH0lWzAtOWEtekEtWl17MSx9fDo6KGZmZmYoOjB7MSw0fSl7MCwxfTopezAsMX0oKDI1WzAtNV18KDJbMC00XXwxezAsMX1bMC05XSl7MCwxfVswLTldKVwuKXszLDN9KDI1WzAtNV18KDJbMC00X
XwxezAsMX1bMC05XSl7MCwxfVswLTldKXwoWzAtOWEtZkEtRl17MSw0fTopezEsNH06KCgyNVswLTVdfCgyWzAtNF18MXswLDF9WzAtOV0pezAsMX1bMC05XSlcLil7MywzfSgyNVswLTVdfCgyWzAtNF18M
XswLDF9WzAtOV0pezAsMX1bMC05XSkpKVxzPC9wYXR0ZXJuPgogICAgPHBhdHRlcm4gdXNlLWRlZmF1bHQtcGF0dGVybj0idHJ1ZSIgdHlwZT0iSmF2YVBhdHRlcm4iIGlkPSJTb3VyY2VJcHY2LVBhdHRlc
m4tMSI+U1JDPSgoKFswLTlhLWZBLUZdezEsNH06KXs3LDd9WzAtOWEtZkEtRl17MSw0fXwoWzAtOWEtZkEtRl17MSw0fTopezEsN306fChbMC05YS1mQS1GXXsxLDR9Oil7MSw2fTpbMC05YS1mQS1GXXsxL
DR9fChbMC05YS1mQS1GXXsxLDR9Oil7MSw1fSg6WzAtOWEtZkEtRl17MSw0fSl7MSwyfXwoWzAtOWEtZkEtRl17MSw0fTopezEsNH0oOlswLTlhLWZBLUZdezEsNH0pezEsM318KFswLTlhLWZBLUZdezEsN
H06KXsxLDN9KDpbMC05YS1mQS1GXXsxLDR9KXsxLDR9fChbMC05YS1mQS1GXXsxLDR9Oil7MSwyfSg6WzAtOWEtZkEtRl17MSw0fSl7MSw1fXxbMC05YS1mQS1GXXsxLDR9OigoOlswLTlhLWZBLUZdezEsN
```

```
H0pezEsNn0pfDooKDpbMC05YS1mQS1GXXsxLDR9KXsxLDd9fDopfGZlODA6KDpbMC05YS1mQS1GXXswLDR9KXswLDR9JVswLTlhLXpBLVpdezEsfXw6OihmZmZmKDowezEsNH0pezAsMX06KXswLDF9KCgyN
VswLTVdfCgyWzAtNF18MXswLDF9WzAtOV0pezAsMX1bMC05XSlcLil7MywzfSgyNVswLTVdfCgyWzAtNF18MXswLDF9WzAtOV0pezAsMX1bMC05XSl8KFswLTlhLWZBLUZdezEsNH06KXsxLDR9OigoMjVbM
C01XXwoMlswLTRdfDF7MCwxfVswLTldKXswLDF9WzAtOV0pXC4pezMsM30oMjVbMC01XXwoMlswLTRdfDF7MCwxfVswLTldKXswLDF9WzAtOV0pKSlcczwvcGF0dGVybj4KICAgIDxwYXR0ZXJuIHVzZS1kZ
WZhdWx0LXBhdHRlcm49InRydWUiIHR5cGU9IkphdmFQYXR0ZXJuIiBpZD0iUHJvdG9jb2wtUGF0dGVybi0xIj5QUk9UTz0oLio/KVxzPC9wYXR0ZXJuPgogICAgPHBhdHRlcm4gdXNlLWRlZmF1bHQtcGF0d
GVybj0idHJ1ZSIgdHlwZT0iSmF2YVBhdHRlcm4iIGlkPSJTb3VyY2VJcC1QYXR0ZXJuLTEiPlNSQz0oKD86WzAtOV17MSwzfVwuKXszfVswLTldezEsM30pXHM8L3BhdHRlcm4+CiAgICA8cGF0dGVybiB1c
2UtZGVmYXVsdC1wYXR0ZXJuPSJ0cnVlIiB0eXBlPSJKYXZhUGF0dGVybiIgaWQ9IlNvdXJjZVBvcnQtUGF0dGVybi0xIj5TUFQ9KC4qPylcczwvcGF0dGVybj4KICAgIDxwYXR0ZXJuIHR5cGU9IkphdmFQY
XR0ZXJuIiBpZD0iQWxsRXZlbnRzIj4oLio/KTwvcGF0dGVybj4KICAgIDxtYXRjaC1ncm91cCBkZXZpY2UtdHlwZS1pZC1vdmVycmlkZT0iNDAwMSIgb3JkZXI9IjEiPgogICAgICAgIDxtYXRjaGVyIG9yZ
GVyPSIxIiBlbmFibGUtc3Vic3RpdHV0aW9ucz0idHJ1ZSIgY2FwdHVyZS1ncm91cD0iXDEiIHBhdHRlcm4taWQ9IkRlc3RpbmF0aW9uSXAtUGF0dGVybi0xIiBmaWVsZD0iRGVzdGluYXRpb25JcCIvPgogI
CAgICAgIDxtYXRjaGVyIG9yZGVyPSIxIiBlbmFibGUtc3Vic3RpdHV0aW9ucz0idHJ1ZSIgY2FwdHVyZS1ncm91cD0iXDEiIHBhdHRlcm4taWQ9IkRlc3RpbmF0aW9uUG9ydC1QYXR0ZXJuLTEiIGZpZWxkP
SJEZXN0aW5hdGlvblBvcnQiLz4KICAgICAgICA8bWF0Y2hlciBvcmRlcj0iMSIgZW5hYmxlLXN1YnN0aXR1dGlvbnM9InRydWUiIGNhcHR1cmUtZ3JvdXA9IlwxIFwyIiBwYXR0ZXJuLWlkPSJFdmVudENhd
GVnb3J5LVBhdHRlcm4tMSIgZmllbGQ9IkV2ZW50Q2F0ZWdvcnkiLz4KICAgICAgICA8bWF0Y2hlciBvcmRlcj0iMiIgZW5hYmxlLXN1YnN0aXR1dGlvbnM9InRydWUiIGNhcHR1cmUtZ3JvdXA9IlwwIiBwY
XR0ZXJuLWlkPSJFdmVudENhdGVnb3J5LVBhdHRlcm4tMiIgZmllbGQ9IkV2ZW50Q2F0ZWdvcnkiLz4KICAgICAgICA8bWF0Y2hlciBvcmRlcj0iMyIgZW5hYmxlLXN1YnN0aXR1dGlvbnM9InRydWUiIGNhc
HR1cmUtZ3JvdXA9IlwxXDIiIHBhdHRlcm4taWQ9IkV2ZW50Q2F0ZWdvcnktUGF0dGVybi0zIiBmaWVsZD0iRXZlbnRDYXRlZ29yeSIvPgogICAgICAgIDxtYXRjaGVyIG9yZGVyPSI0IiBlbmFibGUtc3Vic
3RpdHV0aW9ucz0idHJ1ZSIgY2FwdHVyZS1ncm91cD0iXDFcMiIgcGF0dGVybi1pZD0iRXZlbnRDYXRlZ29yeS1QYXR0ZXJuLTQiIGZpZWxkPSJFdmVudENhdGVnb3J5Ii8+CiAgICAgICAgPG1hdGNoZXIgb
3JkZXI9IjUiIGVuYWJsZS1zdWJzdGl0dXRpb25zPSJ0cnVlIiBjYXB0dXJlLWdyb3VwPSJcMCIgcGF0dGVybi1pZD0iRXZlbnRDYXRlZ29yeS1QYXR0ZXJuLTUiIGZpZWxkPSJFdmVudENhdGVnb3J5Ii8+C
iAgICAgICAgPG1hdGNoZXIgb3JkZXI9IjYiIGVuYWJsZS1zdWJzdGl0dXRpb25zPSJ0cnVlIiBjYXB0dXJlLWdyb3VwPSJcMCIgcGF0dGVybi1pZD0iRXZlbnRDYXRlZ29yeS1QYXR0ZXJuLTYiIGZpZWxkP
SJFdmVudENhdGVnb3J5Ii8+CiAgICAgICAgPG1hdGNoZXIgb3JkZXI9IjEiIGVuYWJsZS1zdWJzdGl0dXRpb25zPSJ0cnVlIiBjYXB0dXJlLWdyb3VwPSJcMSIgcGF0dGVybi1pZD0iRXZlbnROYW1lLVBhd
HRlcm4tMSIgZmllbGQ9IkV2ZW50TmFtZSIvPgogICAgICAgIDxtYXRjaGVyIG9yZGVyPSIyIiBlbmFibGUtc3Vic3RpdHV0aW9ucz0idHJ1ZSIgY2FwdHVyZS1ncm91cD0iXDEiIHBhdHRlcm4taWQ9IkV2Z
W50TmFtZS1QYXR0ZXJuLTIiIGZpZWxkPSJFdmVudE5hbWUiLz4KICAgICAgICA8bWF0Y2hlciBvcmRlcj0iMyIgZW5hYmxlLXN1YnN0aXR1dGlvbnM9InRydWUiIGNhcHR1cmUtZ3JvdXA9IlwxIiBwYXR0Z
XJuLWlkPSJFdmVudE5hbWUtUGF0dGVybi0zIiBmaWVsZD0iRXZlbnROYW1lIi8+CiAgICAgICAgPG1hdGNoZXIgb3JkZXI9IjQiIGVuYWJsZS1zdWJzdGl0dXRpb25zPSJ0cnVlIiBjYXB0dXJlLWdyb3VwP
SJcMCIgcGF0dGVybi1pZD0iRXZlbnROYW1lLVBhdHRlcm4tNCIgZmllbGQ9IkV2ZW50TmFtZSIvPgogICAgICAgIDxtYXRjaGVyIG9yZGVyPSI1IiBlbmFibGUtc3Vic3RpdHV0aW9ucz0idHJ1ZSIgY2Fwd
HVyZS1ncm91cD0iXDIiIHBhdHRlcm4taWQ9IkV2ZW50TmFtZS1QYXR0ZXJuLTUiIGZpZWxkPSJFdmVudE5hbWUiLz4KICAgICAgICA8bWF0Y2hlciBvcmRlcj0iNiIgZW5hYmxlLXN1YnN0aXR1dGlvbnM9I
nRydWUiIGNhcHR1cmUtZ3JvdXA9IlwyIiBwYXR0ZXJuLWlkPSJFdmVudE5hbWUtUGF0dGVybi02IiBmaWVsZD0iRXZlbnROYW1lIi8+CiAgICAgICAgPG1hdGNoZXIgb3JkZXI9IjciIGVuYWJsZS1zdWJzd
Gl0dXRpb25zPSJ0cnVlIiBjYXB0dXJlLWdyb3VwPSJcMSIgcGF0dGVybi1pZD0iRXZlbnROYW1lLVBhdHRlcm4tNyIgZmllbGQ9IkV2ZW50TmFtZSIvPgogICAgICAgIDxtYXRjaGVyIG9yZGVyPSI4IiBlb
mFibGUtc3Vic3RpdHV0aW9ucz0idHJ1ZSIgY2FwdHVyZS1ncm91cD0iXDEiIHBhdHRlcm4taWQ9IkV2ZW50TmFtZS1QYXR0ZXJuLTgiIGZpZWxkPSJFdmVudE5hbWUiLz4KICAgICAgICA8bWF0Y2hlciBvc
mRlcj0iOSIgZW5hYmxlLXN1YnN0aXR1dGlvbnM9InRydWUiIGNhcHR1cmUtZ3JvdXA9IlwwIiBwYXR0ZXJuLWlkPSJFdmVudE5hbWUtUGF0dGVybi05IiBmaWVsZD0iRXZlbnROYW1lIi8+CiAgICAgICAgP
G1hdGNoZXIgb3JkZXI9IjEiIGVuYWJsZS1zdWJzdGl0dXRpb25zPSJ0cnVlIiBjYXB0dXJlLWdyb3VwPSJcMSIgcGF0dGVybi1pZD0iRGVzdGluYXRpb25JcHY2LVBhdHRlcm4tMSIgZmllbGQ9IkRlc3Rpb
mF0aW9uSXB2NiIvPgogICAgICAgIDxtYXRjaGVyIG9yZGVyPSIxIiBlbmFibGUtc3Vic3RpdHV0aW9ucz0idHJ1ZSIgY2FwdHVyZS1ncm91cD0iXDEiIHBhdHRlcm4taWQ9IlNvdXJjZUlwdjYtUGF0dGVyb
i0xIiBmaWVsZD0iU291cmNlSXB2NiIvPgogICAgICAgIDxtYXRjaGVyIG9yZGVyPSIxIiBlbmFibGUtc3Vic3RpdHV0aW9ucz0idHJ1ZSIgY2FwdHVyZS1ncm91cD0iXDEiIHBhdHRlcm4taWQ9IlByb3RvY
29sLVBhdHRlcm4tMSIgZmllbGQ9IlByb3RvY29sIi8+CiAgICAgICAgPG1hdGNoZXIgb3JkZXI9IjEiIGVuYWJsZS1zdWJzdGl0dXRpb25zPSJ0cnVlIiBjYXB0dXJlLWdyb3VwPSJcMSIgcGF0dGVybi1pZ
D0iU291cmNlSXAtUGF0dGVybi0xIiBmaWVsZD0iU291cmNlSXAiLz4KICAgICAgICA8bWF0Y2hlciBvcmRlcj0iMSIgZW5hYmxlLXN1YnN0aXR1dGlvbnM9InRydWUiIGNhcHR1cmUtZ3JvdXA9IlwxIiBwY
XR0ZXJuLWlkPSJTb3VyY2VQb3J0LVBhdHRlcm4tMSIgZmllbGQ9IlNvdXJjZVBvcnQiLz4KICAgICAgICA8ZXZlbnQtbWF0Y2gtbXVsdGlwbGUgZm9yY2UtcWlkbWFwLWxvb2t1cC1vbi1maXh1cD0idHJ1Z
SIgc2VuZC1pZGVudGl0eT0iVXNlRFNNUmVzdWx0cyIgcGF0dGVybi1pZD0iQWxsRXZlbnRzIi8+CiAgICA8L21hdGNoLWdyb3VwPgo8L25zMjpkZXZpY2UtZXh0ZW5zaW9uPgo=</xml>
  <use_condition>0</use_condition>
  <name>VMwareSDWANEdgeCustom_ext</name>
  <description></description>
  <id>1</id>
  <uuid>51efd5f4-d904-43ea-a621-2322dc36db1f</uuid>
  <enabled>true</enabled>
 </device_ext>
 <ariel_property_expression>
  <ap_id>321d358d-1203-4a8f-b46e-74d818d7f761</ap_id>
  <creationdate>1688547602909</creationdate>
  <deviceid>-1</deviceid>
  <sequenceid>752</sequenceid>
  <qid>-1</qid>
  <enabled>true</enabled>
  <devicetypeid>4001</devicetypeid>
  <capturegroup>1</capturegroup>
  <regex>SID=(.*?)\s</regex>
  <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
  <rank>1</rank>
  <id>f32c06e5-e8b5-478c-ba67-cfc7dac57e72</id>
  <editdate>1692467164748</editdate>
  <category>-1</category>
  <username>admin</username>
 </ariel_property_expression>
 <ariel_property_expression>
  <ap_id>62c9297f-15c4-4ab9-bfbc-6b6bb5567305</ap_id>
  <creationdate>1688550878540</creationdate>
  <deviceid>-1</deviceid>
  <sequenceid>753</sequenceid>
  <qid>-1</qid>
  <enabled>true</enabled>
  <devicetypeid>4001</devicetypeid>
  <capturegroup>1</capturegroup>
  <regex>SIG_ID=(.*?)\s</regex>
  <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
  <rank>1</rank>
  <id>db836e50-80f4-4bf8-b314-2757d9fd01a8</id>
  <editdate>1692467165072</editdate>
  <category>-1</category>
  <username>admin</username>
 </ariel_property_expression>
 <ariel_property_expression>
  <ap_id>207a1188-f381-4c6d-8a2a-6766e337a51b</ap_id>
  <creationdate>1688549297879</creationdate>
  <deviceid>-1</deviceid>
  <sequenceid>754</sequenceid>
  <qid>-1</qid>
  <enabled>true</enabled>
  <devicetypeid>4001</devicetypeid>
  <capturegroup>1</capturegroup>
  <regex>DURATION_SECS=(.*?)\s</regex>
  <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
  <rank>1</rank>
  <id>762610a0-76d9-41e0-9215-2e04b4a4f30e</id>
  <editdate>1692467164518</editdate>
  <category>-1</category>
  <username>admin</username>
 </ariel_property_expression>
 <ariel_property_expression>
  <ap_id>bb14e276-15a7-42e8-afc6-e75ccb491a14</ap_id>
  <creationdate>1688550878598</creationdate>
  <deviceid>-1</deviceid>
  <sequenceid>755</sequenceid>
  <qid>-1</qid>
  <enabled>true</enabled>
  <devicetypeid>4001</devicetypeid>
  <capturegroup>1</capturegroup>
  <regex>SIGNATURE=(.*?)\s[A-Z]*CAT</regex>
  <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
  <rank>1</rank>
  <id>7db8a580-70ae-4176-9027-a94ebd1e8c40</id>
  <editdate>1692467164809</editdate>
  <category>-1</category>
  <username>admin</username>
 </ariel_property_expression>
 <ariel_property_expression>
  <ap_id>b412ed65-0448-4897-98c0-80bbcc65ea24</ap_id>
  <creationdate>1688549632349</creationdate>
  <deviceid>-1</deviceid>
  <sequenceid>756</sequenceid>
  <qid>-1</qid>
  <enabled>true</enabled>
  <devicetypeid>4001</devicetypeid>
  <capturegroup>1</capturegroup>
  <regex>APPLICATION=(.*?)\s[A-Z]*(_|=)</regex>
  <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
  <rank>1</rank>
  <id>0b757648-8cfa-4c71-93e3-2ddb6dd1d681</id>
  <editdate>1692467164409</editdate>
  <category>-1</category>
  <username>admin</username>
 </ariel_property_expression>
 <ariel_property_expression>
  <ap_id>c2e9607f-057b-46b7-a4d1-01816d6b583c</ap_id>
  <creationdate>1688546129939</creationdate>
```

```
   <deviceid>162</deviceid>
   <sequenceid>758</sequenceid>
   <qid>-1</qid>
   <enabled>true</enabled>
   <devicetypeid>4001</devicetypeid>
   <capturegroup>1</capturegroup>
   <regex>SEGMENT=(.*?)\s</regex>
   <payload></payload>
   <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
   <rank>-1</rank>
   <id>3696a6b5-d742-4079-93c5-f76657992d71</id>
   <editdate>1692467164990</editdate>
   <category>-1</category>
   <username>admin</username>
  </ariel_property_expression>
  <ariel_property_expression>
   <ap_id>8999aa82-29d4-44c2-b9f9-e2829ff7bb39</ap_id>
   <creationdate>1688544444793</creationdate>
   <deviceid>-1</deviceid>
   <sequenceid>757</sequenceid>
   <qid>-1</qid>
   <enabled>true</enabled>
   <devicetypeid>4001</devicetypeid>
   <capturegroup>1</capturegroup>
   <regex>PROTO=(.*?)\s</regex>
   <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
   <rank>1</rank>
   <id>15c115fd-7013-4ced-8bc3-32e06516f1ad</id>
   <editdate>1692467164449</editdate>
   <category>-1</category>
   <username>admin</username>
  </ariel_property_expression>
  <ariel_property_expression>
   <ap_id>fa70435d-0389-4dd9-9f75-270b65263c23</ap_id>
   <creationdate>1688549446788</creationdate>
   <deviceid>-1</deviceid>
   <sequenceid>759</sequenceid>
   <qid>-1</qid>
   <enabled>true</enabled>
   <devicetypeid>4001</devicetypeid>
   <capturegroup>1</capturegroup>
   <regex>BYTES_RECEIVED=([0-9]*?)\s</regex>
   <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
   <rank>1</rank>
   <id>48cff8e7-d7b0-4bbf-b699-e71cb75ea6f4</id>
   <editdate>1692467164469</editdate>
   <category>-1</category>
   <username>admin</username>
  </ariel_property_expression>
  <ariel_property_expression>
   <ap_id>8c107314-a062-43ad-8409-b78d99cc6b2f</ap_id>
   <creationdate>1688549188837</creationdate>
   <deviceid>-1</deviceid>
   <sequenceid>760</sequenceid>
   <qid>-1</qid>
   <enabled>true</enabled>
   <devicetypeid>4001</devicetypeid>
   <capturegroup>1</capturegroup>
   <regex>DEST_NAME=(.*?)\s[A-Z]</regex>
   <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
   <rank>1</rank>
   <id>3da34978-358e-4a62-9a46-20efb708b2bb</id>
   <editdate>1692467164430</editdate>
   <category>-1</category>
   <username>admin</username>
  </ariel_property_expression>
  <ariel_property_expression>
   <ap_id>7b5d7aba-e249-4fa0-8f63-49d81c8f7abf</ap_id>
   <creationdate>1688549188854</creationdate>
   <deviceid>-1</deviceid>
   <sequenceid>761</sequenceid>
   <qid>-1</qid>
   <enabled>true</enabled>
   <devicetypeid>4001</devicetypeid>
   <capturegroup>1</capturegroup>
   <regex>IN=(.*?)\s</regex>
   <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
   <rank>1</rank>
   <id>3a8f01dd-4bd7-4cb3-9299-ffff5e9f6791</id>
   <editdate>1692467164927</editdate>
   <category>-1</category>
   <username>admin</username>
  </ariel_property_expression>
  <ariel_property_expression>
   <ap_id>485023e9-452b-4897-b518-7e40a3a05288</ap_id>
   <creationdate>1690838511581</creationdate>
   <deviceid>-1</deviceid>
   <sequenceid>763</sequenceid>
   <qid>-1</qid>
   <enabled>true</enabled>
   <devicetypeid>4001</devicetypeid>
   <capturegroup>1</capturegroup>
   <regex>ACTION=VCF\s(.*?)\s</regex>
   <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
   <rank>1</rank>
   <id>526ea3b7-e2b1-41da-bb5d-0369461d5234</id>
   <editdate>1692467164569</editdate>
   <category>-1</category>
   <username>admin</username>
  </ariel_property_expression>
  <ariel_property_expression>
   <ap_id>873812fd-18aa-43e7-a10c-bcad77f5a662</ap_id>
   <creationdate>1688549188828</creationdate>
   <deviceid>-1</deviceid>
   <sequenceid>762</sequenceid>
   <qid>-1</qid>
   <enabled>true</enabled>
   <devicetypeid>4001</devicetypeid>
   <capturegroup>1</capturegroup>
   <regex>FW_POLICY_NAME=(.*?)\s[A-Z]*(_|=)</regex>
   <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
   <rank>1</rank>
   <id>08b0ae51-27d6-4957-869a-8516bf3e62e2</id>
   <editdate>1692467164639</editdate>
   <category>-1</category>
   <username>admin</username>
  </ariel_property_expression>
  <ariel_property_expression>
   <ap_id>bd029346-adaf-422f-a17d-5a82a1e203d9</ap_id>
   <creationdate>1688549188756</creationdate>
   <deviceid>-1</deviceid>
   <sequenceid>764</sequenceid>
   <qid>-1</qid>
   <enabled>true</enabled>
   <devicetypeid>4001</devicetypeid>
   <capturegroup>1</capturegroup>
   <regex>DEST_DOMAIN=(.*)\sFW</regex>
   <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
```

```
  <rank>1</rank>
  <id>8c6a35f3-2f90-439c-a341-64045ca77802</id>
  <editdate>1692467164369</editdate>
  <category>-1</category>
  <username>admin</username>
</ariel_property_expression>
<ariel_property_expression>
  <ap_id>e2b48f1b-f8a6-4422-9aae-0d0e38cd4e66</ap_id>
  <creationdate>1688549446815</creationdate>
  <deviceid>-1</deviceid>
  <sequenceid>765</sequenceid>
  <qid>-1</qid>
  <enabled>true</enabled>
  <devicetypeid>4001</devicetypeid>
  <capturegroup>1</capturegroup>
  <regex>BYTES_SENT=([0-9]*?)\s</regex>
  <propertybase>com.q1labs.core.types.event.NormalizedEventProperties$Payload</propertybase>
  <rank>1</rank>
  <id>43c120ba-313d-47c6-b719-71aa24a6ab39</id>
  <editdate>1692467164679</editdate>
  <category>-1</category>
  <username>admin</username>
</ariel_property_expression>
<sensordeviceprotocols>
  <sensorprotocolid>41</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>4374</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>76</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>4991</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>31</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2551</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>30</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2550</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>20</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2548</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>7</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2547</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>6</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2546</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>5</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2545</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>4</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2544</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>3</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2543</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>2</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2542</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>1</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2541</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>78</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>3894</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>10</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2529</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>9</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2528</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>8</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2527</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>21</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
  <documented>false</documented>
  <id>2549</id>
</sensordeviceprotocols>
<sensordeviceprotocols>
  <sensorprotocolid>62</sensorprotocolid>
  <sensordevicetypeid>4001</sensordevicetypeid>
```

```
   <documented>false</documented>
   <id>5372</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>23</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>5213</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>0</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2540</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>80</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>3156</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>42</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2537</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>22</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>4815</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>19</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2536</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>18</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2535</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>37</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2557</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>51</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>3525</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>17</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2534</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>36</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2556</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>16</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2533</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>35</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2555</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>15</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2532</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>34</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2554</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>12</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2531</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>33</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2553</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>11</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2530</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>32</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2552</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>85</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>5920</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>24</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>4834</id>
```

```
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>63</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2539</id>
  </sensordeviceprotocols>
  <sensordeviceprotocols>
   <sensorprotocolid>50</sensorprotocolid>
   <sensordevicetypeid>4001</sensordevicetypeid>
   <documented>false</documented>
   <id>2538</id>
  </sensordeviceprotocols></content>
```

A.2 Related Documents

The following documentation is available for ***Arista VeloCloud SD-WAN***:

- *Arista VeloCloud SD-WAN Operator Guide*
- *Arista VeloCloud SD-WAN Administration Guide*
- *Arista VeloCloud SD-WAN Gateway Monitoring Guide*
- *Arista VeloCloud SD-WAN Orchestrator Deployment and Monitoring Guide*
- *Arista VeloCloud SD-WAN Partner Guide*
- *Arista VeloCloud SASE Global Settings Guide*
- *Arista VeloCloud SD-WAN Troubleshooting Guide*
- *Arista VeloCloud SD-WAN Design Guide for Enhanced Firewall Services*
- *Arista VeloCloud SD-WAN 6.4 API*
- *Arista VeloCloud Portal API 6.4*
- *Arista AliCloud Virtual Edge Deployment Guide*
- *Arista AWD Virtual Edge Deployment Guide*
- *Arista Azure Virtual Edge Deployment Guide*
- *Arista Google Cloud Platform Virtual Edge Deployment Guide*
- *Arista VeloCloud SASE and QRadar SIEM Integration Guide*
- *Arista VeloCloud SD-WAN and Cloud on AWS Deployment Guide*
- *Arista VeloCloud SD-WAN and Forcepoint SSE Integration Guide*
- *Arista VeloCloud SD-WAN and Google Network Connectivity Center Integration Guide*
- *Arista VeloCloud SD-WAN and Microsoft Route Server Integration Guide*
- *Arista VeloCloud SD-WAN and Netskope SSE Integration Guide*
- *Arista VeloCloud SD-WAN Azure Private Multi-Access Edge Compute Deployment Guide*
- *Arista VeloCloud SD-WAN License Management Guide*