Device Access Policy

Table 1: Feature History

Feature Name	Release Information	Description
Device Access Policy on SNMP and SSH	Cisco SD-WAN Release 20.1.1	This feature defines the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. The control plane of Cisco SD-WAN processes the data traffic for local services (like SSH and SNMP) from a set of sources in a VPN. Routing packets are required to form the overlay.
Device Access Policy on SNMP and SSH	Cisco SD-WAN Release 19.3.x	This feature defines the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic on Cisco vEdge devices, they are applied to the traffic before any other policies are applied.

Device Access Policy Overview

Starting from Cisco SD-WAN Release 19.3, the Cisco vManage user interface is enhanced to configure device access policy on all the Cisco SD-WAN devices.

The control plane of Cisco vEdge devices process the data traffic for local services like, SSH and SNMP from a set of sources in a VPN. It is important to protect the CPU from device access traffic by applying the filter to avoid malicious traffic.

Access policies define the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. You can use access policies, in routed and transparent firewall mode to control IP traffic. An access rule permits or denies traffic based on the protocol used, the source and destination IP address or network, and optionally, the users and user groups. Each incoming packet at an interface is analyzed to determine if it must be forwarded or dropped based on criteria you specify. If you define access rules for the outgoing traffic, packets are also analyzed

before they are allowed to leave an interface. Access policies are applied in order. That is, when the device compares a packet to the rules, it searches from top to bottom in the access policies list, and applies the policy for the first matched rule, ignoring all subsequent rules (even if a later rule is a better match). Thus, you should place specific rules above more general rules to ensure the specific rules are not skipped.

Configure Device Access Policy Using Cisco vManage

Cisco vEdge devices support device access policy configuration to handle SNMP and SSH traffic directed towards the control plane. Use Cisco vManage to configure destination ports based on the device access policy.

Note In order to allow connections to devices from **Tools** > **SSH Terminal** in Cisco vManage, create a rule to accept **Device Access Protocol** as SSH and **Source Data Prefix** as 192.168.1.5/32.

Cisco vEdge devices receive the device access policy configuration and triggers Forwarding Policy Manager (FPM). FPM compiles the policy filters in the device memory and binds it to the device as a global policy. FPM receives the local services packets and applies the device access policy filter as per the configuration and either forwards the packets or drops the packets.

To configure localized device access control policies, use the Cisco vManage policy configuration wizard.

Configure specific or all components depending on the specific policy you are creating. To skip a component, click the **Next** button. To return to a component, click the **Back** button at the bottom of the screen.

To configure Device Access Policy:

1. In Cisco vManage, select the **Configuration** > **Policies** screen.
2. Select the **Localized Policy** tab.
3. From the **Custom Options** > **Localized Policy** pane, select **Access Control Lists.**
4. Click the **Add Device Access Policy** drop-down list to add a device. The options are **Add IPv4 Device Access Policy** and **Add IPv6 Device Access Policy**.
5. Select **Add IPv4 Device Access Policy** from the drop-down list to add an IPv4 ACL Policy. The Edit Device IPv4 ACL Policy page displays.
6. Enter the name and the description for the new policy.
7. Click **Add ACL Sequence** to add a sequence. The Device Access Control List page displays.
8. Click **Sequence Rule**. Match and Actions options display.
9. From the **Match** pane, select and configure the following conditions for your ACL policy:

Match Condition	Description
Device Access Protocol (required)	Select a carrier from the drop-down list. For example SNMP, SSH.
Source Data Prefix	Enter the source IP address. For example, 10.0.0.0/12.
Source Port	Enter the list of source ports. The range is 0-65535.

Match Condition	Description
Destination Data Prefix	Enter the destination IP address. For example, 10.0.0.0/12.
Destination VPN	Enter a VPN ID.

10. From the **Actions** tab, configure the following conditions for your ACL policy:

Action Condition	Description
Accept	
Counter Name	Enter the counter name to be accepted. The maximum length can be 20 characters.
Drop	
Counter Name	Enter the counter name to drop. The maximum length can be 20 characters.

11. Click **Save Match And Actions** to save all the conditions for the ACL policy.
12. Click **Save Device Access Control List Policy** to apply the selected match conditions to an action.
13. If no packets match any of the route policy sequence rules, the **Default Action** in the left pane is to drop the packets.

Note IPv6 prefix match is not supported on Cisco vEdge devices. When you try to configure IPv6 prefix matches on these devices, Cisco vManage fails to generate device configuration.

Configure Device Access Policy Using CLIs

To configure a device access policy:

```
Device(config)# system
Device(config-system) device-access-policy ipv4 <pol-name>
```

Configuration:

```
Device(config)# policy
Device(config-policy) policy device-access-policy <name>
    sequence 1
        match
            destination-data-prefix-list    Destination prefix list
            destination-ip                  List of destination addresses
            destination-port                List of destination ports
            dscp                            List of DSCP values
            packet-length                   Packet length
            protocol                        List of protocols
            source-data-prefix-list         Source prefix list
            source-ip                       List of source addresses
```

```
            source-port                     List of source ports
            destination-vpn                 List of VPN-ID
        action
            accept
            count                           Number of packets/bytes matching this rule
            drop
    default-action       Accept or drop

system
    device-access-policy ipv4 <pol-name>
```

Note IPv6 prefix match is not supported on Cisco SD-WANs.

The following example shows the sample configuration for device access policy:

```
policy device-access-policy dev_pol
  sequence 1
   match
    destination-port 22
   !
   action drop
    count ssh_packs
   !
  !
  default-action drop
 !
 device-access-policy snmp_policy
  sequence 2
   match
    destination-port 161
   !
   action drop
    count snmp_packs
   !
  !
  default-action accept
 !
!
system
 device-access-policy ipv4 snmp_policy
!
```

Verifying Device Access Policy Configuration

Cisco SD-WANs support the following operational commands to provide information for device-access-policy. These commands provide a visual for the counters and the names of the configured device-access-policy. The two commands and the respective yang models are shown in the following sections.

Yang model for the command **device-access-policy-counters**:

```
list device-access-policy-counters {
        tailf:info "IPv6 Device Access Policy counters";
        when "/viptela-system:system/viptela-system:personality = 'vedge'";
        tailf:callpoint device-access-policy-counters-v6; // _nfvis_exclude_line_
        key "name";
        tailf:hidden cli;

        leaf name {
```

```
        tailf:info "Device Access Policy name";
        type viptela:named-type-127;
      }
      config false;
      list device-access-policy-counter-list {
        tailf:info "Device access policy counter list";
        tailf:callpoint device-access-policy-counter-list-v6; // _nfvis_exclude_line_
        tailf:cli-no-key-completion;
        tailf:cli-suppress-show-match;
        key "counter-name";
        tailf:hidden cli;

        leaf counter-name {
          tailf:info "Counter name";
          tailf:cli-suppress-show-match;
          type viptela:named-type;
        }
        leaf packets {
          type yang:counter64;
          tailf:cli-suppress-show-match;
        }
        leaf bytes {
          type yang:counter64;
          tailf:cli-suppress-show-match;
        }
      }
```

The following example shows the policy details of a counter.

show policy device-access-policy-counters

```
                  COUNTER
NAME          NAME         PACKETS   BYTES
-------------------------------------------------------------
dev_pol       ssh_packs      -       -
snmp_policy   snmp_packs     0       0
```

Yang model for the command **device-access-policy-names**:

```
list device-access-policy-names {
        tailf:info "IPv6 device access policy names";
        when "/viptela-system:system/viptela-system:personality = 'vedge'";
        tailf:callpoint device-access-policy-names-v6; // _nfvis_exclude_line_
        tailf:cli-no-key-completion;
        key "name";
        tailf:hidden cli;

        leaf name {
          tailf:info "Device Access Policy name";
          type viptela:named-type-127;
        }
        config false;
      }
```

The following example shows the list of configured policies:

show policy device-access-policy-names

```
NAME
-------------
dev_pol
snmp_policy
```