Filtering 802.1X Supplicants Using Vendor-Specific Attributes (CLI Procedure)

EX-series switches support a set of port filtering attributes called vendor-specific attributes (VSAs). Through VSAs, you can configure port-filtering attributes on the RADIUS server. VSAs are clear text fields sent from the RADIUS server to the switch as a result of 802.1X authentication success or failure. (The 802.1X authentication prevents unauthorized user access by blocking a supplicant at the port until the supplicant is authenticated by the RADIUS server.) The VSAs are interpreted by the switch, and the switch takes appropriate actions.

The following procedure uses FreeRADIUS to configure VSAs. For specifics on configuring your server, consult the AAA documentation that was included with your server.

This topic includes the following tasks:

Load the Juniper Dictionary

Load the Juniper Dictionary, which includes the set of filtering attributes called Juniper-Switching-Filter, attribute ID 48.

1. Load the Juniper Dictionary:

```
[root@freeradius]# cd usr/share/freeradius/dictionary.juniper
```

The output shows the dictionary file's content:

```
#  dictionary.juniper
#
# Version:      $Id: dictionary.juniper,v 1.2.6.1 2005/11/30 22:17:25
aland Exp
$
#  VENDOR          Juniper                         2636
BEGIN-VENDOR    Juniper
ATTRIBUTE       Juniper-Local-User-Name              1       string
ATTRIBUTE       Juniper-Allow-Commands               2       string
ATTRIBUTE       Juniper-Deny-Commands                3       string
ATTRIBUTE       Juniper-Allow-Configuration          4       string
ATTRIBUTE       Juniper-Deny-Configuration           5       string
ATTRIBUTE       Juniper-Firewall-Filter              44      string
ATTRIBUTE       Juniper-Switching-Filter             48      string
<—
```

2. If the attribute Juniper-Switching-Filter is not displayed in the dictionary, you can copy the string shown at the bottom of step 1, and paste the string at the end of the list in the dictionary file.

   The output shows where to paste the string:

```
#  dictionary.juniper
#
# Version:      $Id: dictionary.juniper,v 1.2.6.1 2005/11/30 22:17:25
aland Exp
$
#  VENDOR          Juniper                         2636
BEGIN-VENDOR    Juniper
ATTRIBUTE       Juniper-Local-User-Name                 1       string
ATTRIBUTE       Juniper-Allow-Commands                  2       string
ATTRIBUTE       Juniper-Deny-Commands                   3       string
ATTRIBUTE       Juniper-Allow-Configuration             4       string
ATTRIBUTE       Juniper-Deny-Configuration              5       string
ATTRIBUTE       Juniper-Firewall-Filter                 44      string
copy and paste the entire string here
  <-
```

3. Close the dictionary file:

```
[root@freeradius]# cd usr/share/freeradius/dictionary.juniper
```

Configure a Match Statement

To configure VSAs, enter one or more match conditions and a resulting action through the RADIUS server CLI. The syntax for the match statement is shown below. Enter the match statement plus an action statement enclosed within quotes (" "). See VSA Match Conditions and Actions for EX-series Switches for definitions of match statement options.

match <destination-mac *mac-address*> <source-vlan *vlan-name*> <source-dot1q-tag *tag*> <destination-ip *ip-address*> <ip-protocol *protocol-id*> <source-port *port*> <destination-port *port*>
}
action [allow | deny] <forwarding-class *class-of-service*> <loss-priority (*low* | *medium* | *high*)>
}

To configure basic match conditions using the RADIUS server CLI:

- To deny authentication based on the 802.1Q tag (here, the 802.1Q tag is 10):

```
[root@freeradius]#
cd /usr/local/pool/raddbvi users
Juniper-Switching-Filter = "match source-dot1q-tag 10 action deny"
```

- To deny access based on a destination IP address:

```
[root@freeradius]# cd /usr/local/pool/raddbvi users
Juniper-Switching-Filter = “match destination-ip 192.168.1.0/31 action
deny”
```

- To set the packet loss priority (PLP) to high based on a destination MAC address and the IP protocol:

```
[root@freeradius]# cd /usr/local/pool/raddbvi users
Juniper-Switching-Filter = "match destination-mac 00:04:0f:fd:ac:fe,
ip-protocol 2, forwarding-class high, action loss-priority high"
```

NOTE: In order for the forwarding-class option to be applied, the forwarding class must be configured on the switch. If it is not configured on the switch, this option is ignored. You must specify both the forwarding class and the packet loss priority.

NOTE: After you configure a match statement, stop and restart the RADIUS process to activate the configuration.

Apply a Port Firewall Filter Directly to the RADIUS Server Configuration (Optional)

Port (Layer 2) firewall filters apply to Layer 2 switch ports. When the 802.1X configuration on an interface is set to multiple supplicant mode, you can specify a single port firewall filter configured on the EX-series switch through the JUNOS CLI to be applied to any number of supplicants (users) that are connected to the switch on one interface by adding the filter centrally to the RADIUS server.

For more information about firewall filters, see Firewall Filters for EX-series Switches Overview.

To apply a port firewall filter centrally from the RADIUS server:

- To apply a port firewall filter (here, the filter ID is 23):

```
[root@freeradius]#
cd /usr/local/pool/raddbvi usersFilter-Id = "23"
```

NOTE: Multiple filters are not supported on a single interface. However, you can support multiple filters for multiple users that are connected to the switch on the same interface by configuring a single filter with policies for each of those users.

NOTE: If port firewall filters are also configured locally for the interface, then VSAs take precedence if they conflict with the filters. If the VSAs and the local port firewall filters do not conflict, they are merged.

Related Topics

- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX-series Switches
- Configuring 802.1X Authentication (CLI Procedure)
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX-series Switch
- Understanding 802.1X and VSAs on EX-series Switches