Filtering 802.1X Supplicants Using RADIUS Server Attributes

There are two ways to configure the RADIUS server with port firewall filters:

- Include a match statement and corresponding action in the Juniper-Firewall-Filter attribute. The Juniper-Firewall-Filter attribute is a vendor-specific attribute (VSA) in the Juniper dictionary on the RADIUS server. Use this attribute to configure simple filter conditions for authenticated users. Nothing needs to be configured on the switch; all of the configuration is on the RADIUS server.
- Apply a local firewall filter to users authenticated through the RADIUS server. Use this method for more complex filters. The firewall filter must be configured on each switch.

This example describes using FreeRADIUS software 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:

1. Configuring Match Statements on the RADIUS Server on page 1
2. Applying a Port Firewall Filter from the RADIUS Server on page 4

Configuring Match Statements on the RADIUS Server

You can configure simple filter conditions using the Juniper-Switching-Filter attribute in the Juniper dictionary on the RADIUS server. These filters are then sent to a switch whenever a new user is authenticated successfully. The filters are created and applied on all EX Series switches that authenticate users through that RADIUS server without the need to configure anything on each individual switch.

To configure the Juniper-Switching-Filter attribute, enter one or more match conditions and a resulting action using the CLI for the RADIUS server. Enter the match statement plus an action statement enclosed within quotes (" ") using the following syntax:

```
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)>
}
```

See VSA Match Conditions and Actions for EX Series Switches for definitions of match statement options.

To configure match conditions on the RADIUS server:

1. Verify that the Juniper dictionary is loaded on your RADIUS server and includes the filtering attribute Juniper-Switching-Filter, attribute ID 48:

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

```
#  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-Switching-Filter                48      string
<-
```

2. Enter the match conditions and actions. For example:

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

     ```
     [root@freeradius]#
     cd /usr/local/etc/raddb
     vi users
     ```

     For each relevant user, add the Juniper-Switching-Filter attribute:

     ```
     Juniper-Switching-Filter = "match source-dot1q-tag 10 action deny"
     ```

   - To deny access based on a destination IP address:

     ```
     [root@freeradius]# cd /usr/local/etc/raddb
     vi users
     ```

     For each relevant user, add the Juniper-Switching-Filter attribute:

     ```
     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/etc/raddb
     vi users
     ```

     For each relevant user, add the Juniper-Switching-Filter attribute:

     ```
     Juniper-Switching-Filter = "match destination-mac 00:04:0f:fd:ac:fe,
     ip-protocol 2, forwarding-class high, action loss-priority high"
     ```

NOTE: 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.

3. Stop and restart the RADIUS process to activate the configuration.

Applying a Port Firewall Filter from the RADIUS Server

You can apply a firewall filter to user policies on the RADIUS server. The RADIUS server can then specify the firewall filters that are to be applied to each user that requests to authenticate. Use this method when the firewall filter has more extensive conditions or you want to use different conditions for the same filter on different switches. The firewall filters must be configured on each switch.

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:

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.

1. Create the firewall filter on the local switch. In this example, the filter is called filter1.
2. Open the users file on the RADIUS server:

```
[root@freeradius]#
cd /usr/local/pool/raddb
vi users
```

3. For each relevant user, add the filter (here, the filter ID is filter1):

```
Filter-Id = "filter1"
```

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.

4. Stop and restart the RADIUS process to activate the configuration.

Related Topics

- Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on an EX Series Switch
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches
- Configuring 802.1X Interface Settings (CLI Procedure)
- Understanding 802.1X and VSAs on EX Series Switches

Published: 2009-07-21