Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on an EX-series Switch

You can use RADIUS server attributes and a port-based firewall filter to centrally apply terms to multiple supplicants connected to an EX-series switch in your enterprise. Terms are applied following a supplicant's successful authentication through 802.1X.

EX-series switches support port-based firewall filters. Port firewall filters are configured on a single EX-series switch, but in order for them to operate throughout an enterprise, they have to be configured on multiple switches. To reduce the need to configure the same port firewall filter on multiple switches, you can instead apply the filter centrally on the RADIUS server using RADIUS server attributes.

The following example uses FreeRADIUS to apply a port firewall filter on a RADIUS server. For specifics on configuring your server, consult the AAA documentation that was included with your server.

This example describes how to configure a port firewall filter with terms, create counters to count packets for the supplicants, apply the filter to user profiles on the RADIUS server, and display the counters to verify the configuration:

Requirements

This example uses the following hardware and software components:

- JUNOS Release 9.3 or later for EX-series switches
- One EX 4200 switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Set up a connection between the switch and the RADIUS server. See Example: Connecting a RADIUS Server for 802.1X to an EX-series Switch.
- Configured 802.1X authentication on the switch, with the authentication mode for interface ge-0/0/2 set to multiple. See Configuring 802.1X Authentication (CLI Procedure) and Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX-series Switch.

- Configured users on the RADIUS authentication server (in this example, the user profiles for Supplicant 1 and Supplicant 2 in the topology are modified on the RADIUS server).

Overview and Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, you can apply a single port firewall filter configured through the JUNOS CLI on the EX-series switch to any number of users (supplicants) on one interface by adding the filter centrally to the RADIUS server. Only a single filter can be applied to an interface; however, the filter can contain multiple terms for separate supplicants.

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

RADIUS server attributes are applied to supplicants after the supplicants are successfully authenticated using 802.1X. To authenticate the supplicants, the switch forwards a supplicant's credentials to the RADIUS server. The RADIUS server matches the credentials forwarded by the switch against preconfigured information about the supplicant located in the supplicant's user profile on the RADIUS server. If a match is made, the RADIUS server instructs the switch to open an interface to the supplicant. Traffic then flows from and to the supplicant on the LAN. Further instructions configured in the port firewall filter and added to the supplicant's user profile using a RADIUS server attribute further define the access that the supplicant is granted. Filtering terms configured in the port firewall filter are applied to the supplicant after 802.1X authentication is complete.

Figure 1 on page 3 shows the topology used for this example. The RADIUS server is connected to the EX 4200 switch on access port ge-0/0/10. Two supplicants are accessing the LAN on interface ge-0/0/2. Supplicant 1 has a MAC address of 00:50:8b:6f:60:3a. Supplicant 2 has a MAC address of 00:50:8b:6f:60:3b.

Figure 1: Topology for Firewall Filter and RADIUS Server Attributes Configuration

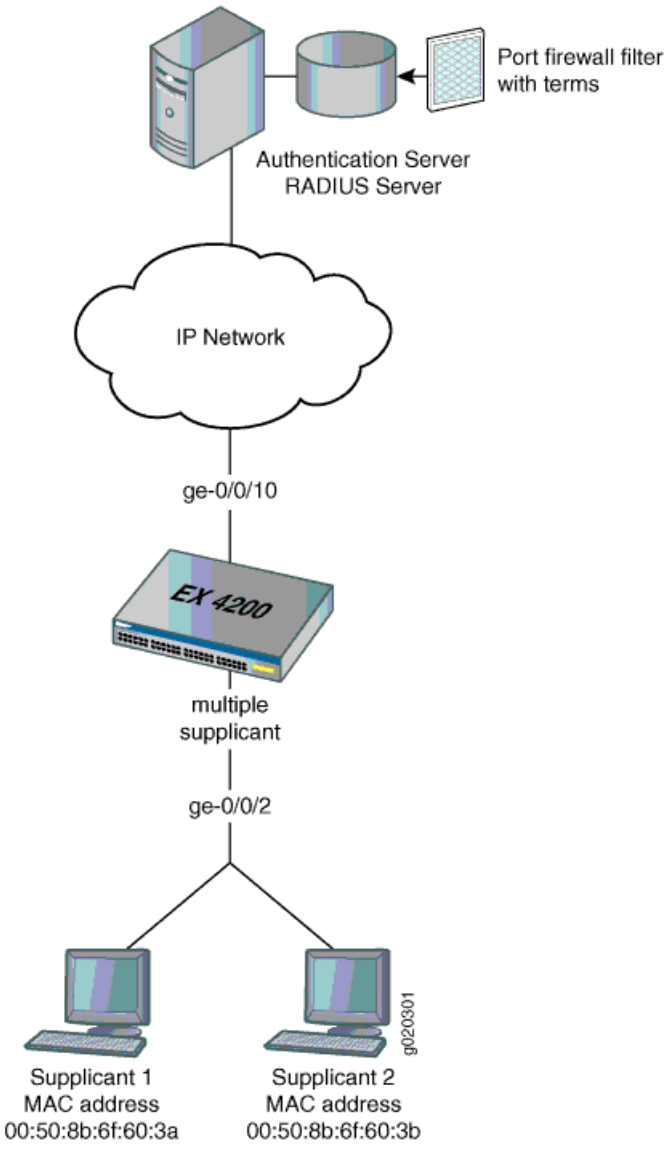

Table 1 on page 3 describes the components in this topology.

Table 1: Components of the Firewall Filter and RADIUS Server Attributes Topology

Property	Settings
Switch hardware	EX 4200 access switch, 24 Gigabit Ethernet ports, 8 PoE ports.
One RADIUS server	Backend database with an address of 10.0.0.100 connected to the switch at port ge-0/0/10.
802.1X supplicants connected to the switch on interface ge-0/0/2	■ Supplicant 1 has MAC address 00:50:8b:6f:60:3a. ■ Supplicant 2 has MAC address 00:50:8b:6f:60:3b.

Table 1: Components of the Firewall Filter and RADIUS Server Attributes Topology *(continued)*

Port firewall filter to be applied on the RADIUS server	filter1
Counters	counter1 counts packets from Supplicant 1, and counter2 counts packets from Supplicant 2.
User profiles on the RADIUS server	■ Supplicant 1 has the user profile supplicant1. ■ Supplicant 2 has the user profile supplicant2.

In this example, you configure a port firewall filter named filter1. The filter contains terms that will be applied to the supplicants based on the MAC addresses of the supplicants. When you configure the filter, you also configure the counters called counter1 and counter2. Packets from each supplicant will be counted, helping you verify that the configuration is working. Then, you check to see that the RADIUS server attribute is available on the RADIUS server and apply the filter to the user profiles of each supplicant on the RADIUS server. Finally, you verify the configuration by displaying output for the two counters.

NOTE: For more information about authentication, authorization, and accounting (AAA) services, see the *JUNOS Software System Basics Configuration Guide* at http://www.juniper.net/techpubs/software/junos/junos93/index.html.

Configuring the Port Firewall Filter and Counters

Configure a port firewall filter and counters:

CLI Quick Configuration

To quickly configure a port firewall filter with terms for Supplicant 1 and Supplicant 2 and create parallel counters for each supplicant, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter filter1 term supplicant1 from
source-mac-address 00:50:8b:6f:60:3a
set firewall family ethernet-switching filter filter1 term supplicant2 from
source-mac-address 00:50:8b:6f:60:3b
set firewall family ethernet-switching filter filter1 term supplicant1 then count
counter1
set firewall family ethernet-switching filter filter1 term supplicant2 then count
counter2
```

Step-by-Step Procedure

To configure a port firewall filter and counters on the switch:

1. Configure a port firewall filter (here, filter1) with terms for each supplicant based upon the MAC address of each supplicant:

```
[edit firewall family ethernet-switching]

user@switch# set filter filter1 term supplicant1 from source-mac-address
00:50:8b:6f:60:3a
```

```
user@switch# set filter filter1 term supplicant2 from source-mac-address
00:50:8b:6f:60:3b
```

2. Create two counters that will count packets for each supplicant:

```
[edit firewall family ethernet-switching]

user@switch# set filter filter1 term supplicant1 then count counter1
user@switch# set filter filter1 term supplicant2 then count counter2
```

Results Display the results of the configuration:

```
user@switch> show configuration
  firewall {
    family ethernet-switching {
      filter filter1 {
        term supplicant1 {
          from {
            source-mac-address {
              00:50:8b:6f:60:3a;
            }
          }
          then count counter1;
        }
        term supplicant2 {
          from {
            source-mac-address {
              00:50:8b:6f:60:3b;
            }
          }
          then count counter2;
        }
      }
    }
  }
```

Applying the Port Firewall Filter to the Supplicant User Profiles on the RADIUS Server

Verify that the RADIUS server attribute needed to apply a filter on the RADIUS server is on the server and apply the port firewall filter to each supplicant's user profile on the RADIUS server:

Step-by-Step Procedure To verify that the RADIUS server attribute Filter-ID is on the RADIUS server and to apply the filter to the user profiles:

1. Display the dictionary dictionary.rfc2865 on the RADIUS server, and verify that the attribute Filter-ID is in the dictionary:

```
[root@freeradius]# cd usr/share/freeradius/dictionary.rfc2865
```

2. Close the dictionary file:

```
[root@freeradius]# cd usr/share/freeradius/dictionary.rfc2865
```

3. Display the local user profiles of the supplicants to which you want to apply the filter (here, the user profiles are called supplicant1 and supplicant2):

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

The output shows:

```
supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = "1005"

supplicant2 Auth-Type := EAP, User-Password == "supplicant2"
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = "1005"
```

4. Apply the filter to both user profiles by adding the line Filter-Id = “filter1” to each profile, and then close the file:

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

After you paste the line into the files, the files look like this:

```
supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = "1005",
        Filter-Id = "filter1"

supplicant2 Auth-Type := EAP, User-Password == "supplicant2"
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = "1005",
        Filter-Id = "filter1"
```

Verification

Verify that the filter has been applied to the supplicants:

■ Verifying That the Filter Has Been Applied to the Supplicants on page 6

Verifying That the Filter Has Been Applied to the Supplicants

Purpose After supplicants are authenticated, verify that the filter configured on the switch and added to each supplicant’s user profile on the RADIUS server has been applied:

Action Display information about firewall filter filter1:

```
user@switch> show firewall filter filter1
Filter: filter1
Counters:
Name                                                Bytes              Packets
counter1                                              128                    2
counter2                                               64                    1
```

Meaning The output of the command show firewall filter filter1 displays counter1 and counter2. Packets from Supplicant 1 are counted using counter1, and packets from Supplicant 2 are counted using counter2. The output from the command displays packets incrementing for both counters. The filter has been applied to both supplicants.

Related Topics

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