Example: Configuring IP Source Guard on a Data VLANThat Shares an Interface with a Voice VLAN

Ethernet LAN switches are vulnerable to attacks that involve spoofing (forging) of source IP addresses or source MAC addresses. These spoofed packets are sent from hosts connected to untrusted access interfaces on the switch. You can enable the IP source guard port security feature on EX-series switches to mitigate the effects of such attacks. If IP source guard determines that a source IP address and a source MAC address in a binding in an incoming packet are not valid, the switch does not forward the packet.

If two VLANs share an interface, you can configure IP source guard on just one of the VLANs; in this example, you configure IP source guard on an untagged data VLAN but not on the tagged voice VLAN. You can use 802.1X user authentication to validate the device connections on the data VLAN.

This example describes how to configure IP source guard with 802.1X user authentication on a data VLAN, with a voice VLAN on the same interface:

Requirements

This example uses the following hardware and software components:

- One EX-series EX 3200-24P switch
- JUNOS Release 9.2 or later for EX-series switches
- A DHCP server to provide IP addresses to network devices on the switch
- A RADIUS server to provide 802.1X authentication

Before you configure IP source guard for the data VLANs, be sure you have:

- Connected the DHCP server to the switch.
- Connected the RADIUS server to the switch and configured user authentication on the server. See Example: Connecting a RADIUS Server for 802.1X to an EX-series Switch.
- Configured the VLANs. See Example: Setting Up Bridging with Multiple VLANs for EX-series Switches for detailed information about configuring VLANs.

Overview and Topology

IP source guard checks the IP source address and MAC source address in a packet sent from a host attached to an untrusted access interface on the switch. If IP source guard determines that the packet header contains an invalid source IP address or

source MAC address, it ensures that the switch does not forward the packet—that is, the packet is discarded.

When you configure IP source guard, you enable on it on one or more VLANs. IP source guard applies its checking rules to untrusted access interfaces on those VLANs. By default, on EX-series switches, access interfaces are untrusted and trunk interfaces are trusted. IP source guard does not check packets that have been sent to the switch by devices connected to either trunk interfaces or trusted access interfaces—that is, interfaces configured with dhcp-trusted so that a DHCP server can be connected to that interface to provide dynamic IP addresses.

IP source guard obtains information about IP-address/MAC-address/VLAN bindings from the DHCP snooping database. It causes the switch to validate incoming IP packets against the entries in that database.

The topology for this example includes one EX-3200-24P switch, a PC and an IP phone connected on the same interface, a connection to a DHCP server, and a connection to a RADIUS server for user authentication.

NOTE: The 802.1X user authentication applied in this example is for single supplicants. Single-secure supplicant mode and multiple supplicant mode do not work with IP source guard. For more information about 802.1X authentication, see Understanding 802.1X Authentication on EX-series Switches.

TIP: You can set the ip-source-guard flag in the traceoptions statement for debugging purposes.

This example shows how to configure a static IP address to be added to the DHCP snooping database.

Configuration

CLI Quick Configuration

To quickly configure IP source guard on a data VLAN, copy the following commands and paste them into the switch terminal window:

```
set ethernet-switching-options voip interface ge-0/0/14.0 vlan voice
set ethernet-switching-options secure-access-port interface ge-0/0/24.0
dhcp-trusted
set ethernet-switching-options secure-access-port interface ge-0/0/14 static-ip
11.1.1.1 mac 00:11:11:11:11:11 vlan data
set ethernet-switching-options secure-access-port vlan data examine-dhcp
set ethernet-switching-options secure-access-port vlan data ip-source-guard
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members data
set vlans voice vlan-id 100
set protocols lldp-med interface ge-0/0/14.0
set protocols dot1x authenticator authentication-profile-name profile52
set protocols dot1x authenticator interface ge-0/0/14.0 supplicant single
```

Step-by-Step Procedure To configure IP source guard on the data VLAN:

1. Configure the VoIP interface:

```
[edit ethernet-switching-options]
user@switch# set voip interface ge-0/0/14.0 vlan voice
```

2. Configure the interface on which the DHCP server is connected to the switch as a trusted interface and add that interface to the data VLAN:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port interface ge-0/0/24.0 dhcp-trusted
[edit interfaces]
user@switch# set ge-0/0/24 unit 0 family ethernet-switching vlan members
data
```

3. Configure a static IP address on an interface on the data VLAN (optional)

```
[edit ethernet-switching-options]
user@switch# set secure-access-port interface ge-0/0/14 static-ip 11.1.1.1
mac 00:11:11:11:11:11 vlan data
```

4. Configure DHCP snooping and IP source guard on the data VLAN:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port vlan data examine-dhcp
user@switch# set secure-access-port vlan data ip-source-guard
```

5. Configure 802.1X user authentication and LLDP-MED on the interface that is shared by the data VLAN and the voice VLAN:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/14.0
user@switch# set dot1x authenticator authentication-profile-name profile52
user@switch# set dot1x authenticator interface ge-0/0/14.0 supplicant
single
```

6. Set the VLAN ID for the voice VLAN:

```
[edit vlans]
user@switch# set voice vlan-id 100
```

Results Check the results of the configuration:

```
[edit ethernet-switching-options]
user@switch# show
voip {
   interface ge-0/0/14.0 {
      vlan voice;
```

```
    }
  }
  secure-access-port {
    interface ge-0/0/14.0 {
      static-ip 11.1.1.1 vlan data mac 00:11:11:11:11:11;
    }
    interface ge-0/0/24.0 {
      dhcp-trusted;
    }
    vlan data {
      examine-dhcp;
      ip-source-guard;
    }
  }

  [edit interfaces]
  ge-0/0/24 {
    unit 0 {
      family ethernet-switching {
        vlan {
          members data;
        }
      }
    }
  }

  [edit vlans]
  voice {
    vlan-id 100;
  }

  [edit protocols]
  lldp-med {
    interface ge-0/0/14.0;
  }
  dot1x {
    authenticator {
      authentication-profile-name profile52;
      interface {
        ge-0/0/14.0 {
          supplicant single;
        }
      }
    }
  }
```

TIP: If you wanted to configure IP source guard on the voice VLAN as well as on the data VLAN, you would configure DHCP snooping and IP source guard exactly as you did for the data VLAN. The configuration result for the voice VLAN under secure-access-port would look like this:

```
  secure-access-port {
    vlan voice {
      examine-dhcp;
```

```
        ip-source-guard;
    }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That 802.1X User Authentication Is Working on the Interface on page 5
- Verifying the VLAN Association with the Interface on page 5
- Verifying That DHCP Snooping and IP Source Guard Are Working on the Data VLAN on page 6

Verifying That 802.1X User Authentication Is Working on the Interface

Purpose Verify the 802.1X configuration on interface ge-0/0/14.

Action Verify the 802.1X configuration with the operational mode command show dot1x interface:

```
user@switch>  show dot1x interface e-0/0/14.0 detail
ge-0/0/14.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Reauthentication: Enabled Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
      Supplicant: user100, 00:00:00:00:22:22
      Operational state: Authenticated
      Reauthentication due in 506 seconds
```

Meaning The Supplicant mode output field displays the configured administrative mode for each interface. Interface ge-0/0/14.0 displays Single supplicant mode.

Verifying the VLAN Association with the Interface

Purpose Display the interface state and VLAN membership.

Action

```
user@switch>  show ethernet-switching interfaces
 Ethernet-switching table: 0 entries, 0 learned

user@switch> show ethernet-switching interfaces
Interface   State    VLAN members         Blocking
ge-0/0/0.0  down     default              unblocked
ge-0/0/1.0  down     employee             unblocked
ge-0/0/2.0  down     employee             unblocked
ge-0/0/12.0 down     default              unblocked
```

```
ge-0/0/13.0 down     default              unblocked
ge-0/0/13.0 down     vlan100              unblocked
ge-0/0/14.0 up       voice                unblocked
                     data                 unblocked
ge-0/0/17.0 down     employee             unblocked
ge-0/0/23.0 down     default              unblocked
ge-0/0/24.0 down     data                 unblocked
                     employee             unblocked
                     vlan100              unblocked
                     voice                unblocked
```

Meaning The field VLAN members shows that the ge-0/0/14.0 interface supports both the data VLAN and the voice VLAN. The State field shows that the interface is up.

Verifying That DHCP Snooping and IP Source Guard Are Working on the Data VLAN

Purpose Verify that DHCP snooping and IP source guard are enabled and working on the data VLAN.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the interface on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

```
user@switch>  show dhcp snooping binding
DHCP Snooping Information:
MAC address        IP address  Lease (seconds) Type     VLAN      Interface

00:05:85:3A:82:77  192.0.2.17  600             dynamic  employee  ge-0/0/1.0
00:05:85:3A:82:79  192.0.2.18  653             dynamic  employee  ge-0/0/1.0
00:05:85:3A:82:80  192.0.2.19  720             dynamic  employee  ge-0/0/2.0
00:05:85:3A:82:81  192.0.2.20  932             dynamic  employee  ge-0/0/2.0

                       00:30:48:92:A5:9D  10.10.10.7  720             dynamic
vlan100   ge-0/0/13.0
00:30:48:8D:01:3D  10.10.10.9  720             dynamic  data      ge-0/0/14.0
00:30:48:8D:01:5D  10.10.10.8  1230            dynamic  voice     ge-0/0/14.0
00:11:11:11:11:11  11.1.1.1    –               static   data      ge-0/0/14.0
00:05:85:27:32:88  192.0.2.22  –               static   employee  ge-0/0/17.0
00:05:85:27:32:89  192.0.2.23  –               static   employee  ge-0/0/17.0
00:05:85:27:32:90  192.0.2.27  –               static   employee  ge-0/0/17.0
```

View the IP source guard information for the data VLAN.

```
user@switch>  show ip-source-guard
IP source guard information:
Interface    Tag  IP Address   MAC Address        VLAN

ge-0/0/13.0  0    10.10.10.7   00:30:48:92:A5:9D  vlan100
```

```
ge-0/0/14.0  0    10.10.10.9   00:30:48:8D:01:3D  data
ge-0/0/14.0  0    11.1.1.1     00:11:11:11:11:11  data

ge-0/0/13.0  100  *            *                  voice
```

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see the preceding sample output for show dhcp snooping binding) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires. Static IP addresses have no assigned lease time. Statically configured entries never expire.

The IP source guard database table contains the VLANs enabled for IP source guard, the untrusted access interfaces on those VLANs, the VLAN 802.1Q tag IDs if there are any, and the IP addresses and MAC addresses that are bound to one another. If a switch interface is associated with multiple VLANs and some of those VLANs are enabled for IP source guard and others are not, the VLANs that are not enabled for IP source guard have a star (*) in the IP Address and MAC Address fields. See the entry for the voice VLAN in the preceding sample output.

Related Topics

- Example: Configuring IP Source Guard with Other EX-series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces
- Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX-series Switch
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX-series Switch
- Configuring IP Source Guard (CLI Procedure)