

Example: Configuring IP Source Guard with Other EX-series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces

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.

You can use IP source guard in combination with other EX-series switch features to mitigate address-spoofing attacks on untrusted access interfaces. This example shows two configuration scenarios:

- Requirements on page 1
- Overview and Topology on page 1
- Configuring IP Source Guard with 802.1X Authentication, DHCP Snooping, and Dynamic ARP Inspection on page 2
- Configuring IP Source Guard on a Guest VLAN on page 5
- Verification on page 7

Requirements

This example uses the following hardware and software components:

- JUNOS Release 9.2 or later for EX-series switches
- An EX 4200-24P switch
- 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 these scenarios, be sure you have:

- Connected the DHCP server to the switch.
- Connected the RADIUS server and configured user authentication on the RADIUS server. See Example: Connecting a RADIUS Server for 802.1X to an EX-series Switch.
- Configured the VLANs on the switch. 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 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 an EX-4200-24P switch, 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.

In the first example configuration, two clients (network devices) are connected to an access switch. You configure IP source guard and 802.1X user authentication, in combination with access port security features DHCP snooping and dynamic ARP inspection (DAI). This setup is designed to protect the switch from IP attacks such as “ping of death” attacks, DHCP starvation, and ARP spoofing.

In the second example configuration, the switch is configured for 802.1X user authentication. If the client fails authentication, the switch redirects the client to a guest VLAN that allows this client to access a set of restricted network features. You configure IP source guard on the guest VLAN to mitigate effects of source IP spoofing.



NOTE: Control-plane rate limiting is achieved by restricting CPU control-plane protection. It can be used in conjunction with storm control (see Understanding Storm Control on EX-series Switches) to limit data-plane activity.



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

Configuring IP Source Guard with 802.1X Authentication, DHCP Snooping, and Dynamic ARP Inspection

CLI Quick Configuration To quickly configure IP source guard with 802.1X authentication and with other access port security features, copy the following commands and paste them into the switch terminal window:

```
set ethernet-switching-options secure-access-port interface ge-0/0/24 dhcp-trusted  
set ethernet-switching-options secure-access-port vlan data examine-dhcp
```

```

set ethernet-switching-options secure-access-port vlan data arp-inspection
set ethernet-switching-options secure-access-port vlan data ip-source-guard
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members data
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members data
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members data
set protocols lldp-med interface ge-0/0/0.0
set protocols dot1x authenticator authentication-profile-name profile52
set protocols dot1x authenticator interface ge-0/0/0.0 supplicant single
set protocols lldp-med interface ge-0/0/1.0
set protocols dot1x authenticator interface ge-0/0/1.0 supplicant single

```

Step-by-Step Procedure

To configure IP source guard with 802.1X authentication and various port security features:

1. 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 dhcp-trusted
user@switch# set set ge-0/0/24 unit 0 family ethernet-switching vlan
members data

```

2. Associate two interfaces with the data VLAN:

```

[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching vlan members
data
user@switch# set ge-0/0/1 unit 0 family ethernet-switching vlan members
data

```

3. Configure 802.1X user authentication and LLDP-MED on the two interfaces that you associated with the data VLAN:

```

[edit protocols]
user@switch# set lldp-med interface ge-0/0/0.0
user@switch# set dot1x authenticator authentication-profile-name profile52
user@switch# set dot1x authenticator interface ge-0/0/0.0 supplicant
single
user@switch# set lldp-med interface ge-0/0/1.0
user@switch# set dot1x authenticator interface ge-0/0/1.0 supplicant single

```

4. Configure access port security features DHCP snooping, dynamic ARP inspection (DAI), 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 arp-inspection
user@switch# set secure-access-port vlan data ip-source-guard

```

Results Check the results of the configuration:

```

[edit ethernet-switching-options]
secure-access-port {
  interface ge-0/0/24.0 {
    dhcp-trusted;
  }
  vlan data {
    arp-inspection;
    examine-dhcp;
    ip-source-guard;
  }
}

[edit interfaces]
ge-0/0/0 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members data;
      }
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members data;
      }
    }
  }
}
ge-0/0/24 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members data;
      }
    }
  }
}

[edit protocols]
lldp-med {
  interface ge-0/0/14.0;
  interface ge-0/0/0.0;
  interface ge-0/0/1.0;
}
dot1x {
  authenticator {
    authentication-profile-name profile52;
  }
  interface {
    ge-0/0/0.0 {
      supplicant single;
    }
    ge-0/0/1.0 {

```

```

        supplicant single;
    }
    ge-0/0/14.0 {
        supplicant single;
    }
}
}

```

Configuring IP Source Guard on a Guest VLAN

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

```

set ethernet-switching-options secure-access-port interface ge-0/0/24 dhcp-trusted
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members employee
set ethernet-switching-options secure-access-port vlan employee examine-dhcp
set ethernet-switching-options secure-access-port vlan employee ip-source-guard
set ethernet-switching-options secure-access-port interface ge-0/0/0 static-ip
11.1.1.1 mac 00:11:11:11:11:11 vlan employee
set ethernet-switching-options secure-access-port interface ge-0/0/1 static-ip
11.1.1.2 mac 00:22:22:22:22:22 vlan employee
set interfaces ge-0/0/0 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/1 unit 0 family ethernet-switching port-mode access
set protocols dot1x authenticator authentication-profile-name profile52
set protocols dot1x authenticator interface ge-0/0/0 supplicant single
set protocols dot1x authenticator interface ge-0/0/0 guest-vlan employee
set protocols dot1x authenticator interface ge-0/0/0 supplicant-timeout 2
set protocols dot1x authenticator interface ge-0/0/1 supplicant single
set protocols dot1x authenticator interface ge-0/0/1 guest-vlan employee
set protocols dot1x authenticator interface ge-0/0/1 supplicant-timeout 2
set vlans employee vlan-id 300

```

Step-by-Step Procedure To configure IP source guard on a guest VLAN:

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

```

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

```

2. Configure two interfaces for the access port mode:

```

[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching port-mode
access
user@switch# set ge-0/0/1 unit 0 family ethernet-switching port-mode access

```

3. Configure DHCP snooping and IP source guard on the employee VLAN:

```

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

```

4. Configure a static IP address on each of two interfaces on the employee VLAN (optional):

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

```
[edit ethernet-switching-options]
user@switch# set secure-access-port interface ge-0/0/1 static-ip 11.1.1.2
mac 00:22:22:22:22:22 vlan employee
```

5. Configure 802.1X user authentication:

```
[edit protocols]
user@switch# set dot1x authenticator authentication-profile-name profile52
user@switch# set dot1x authenticator interface ge-0/0/0 supplicant single
user@switch# set dot1x authenticator interface ge-0/0/1 supplicant single
user@switch# set dot1x authenticator interface ge-0/0/0 supplicant-timeout
2
user@switch# set dot1x authenticator interface ge-0/0/1 supplicant-timeout
2
```

6. Set the VLAN ID for the employee VLAN:

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

Results Check the results of the configuration:

```
[edit protocols]
dot1x {
  authenticator {
    authentication-profile-name profile52;
  }
  interface {
    ge-0/0/0.0 {
      guest-vlan employee;
      supplicant single;
      supplicant-timeout 2;
    }
    ge-0/0/1.0 {
      guest-vlan employee;
      supplicant single;
      supplicant-timeout 2;
    }
  }
}
}
```

```
[edit vlans]
```

```

employee {
  vlan-id 100;
}

[edit interfaces]
ge-0/0/0 {
  unit 0 {
    family ethernet-switching {
      port-mode access;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family ethernet-switching {
      port-mode access;
    }
  }
}
ge-0/0/24 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members employee;
      }
    }
  }
}

[edit ethernet-switching-options]
secure-access-port {
  interface ge-0/0/0.0 {
    static-ip 11.1.1.1 vlan employee mac 00:11:11:11:11:11;
  }
  interface ge-0/0/1.0 {
    static-ip 11.1.1.2 vlan employee mac 00:22:22:22:22:22;
  }
  interface ge-0/0/24.0 {
    dhcp-trusted;
  }
  vlan employee {
    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 8
- Verifying the VLAN Association with the Interface on page 8
- Verifying That DHCP Snooping and IP Source Guard Are Working on the VLAN on page 8

Verifying That 802.1X User Authentication Is Working on the Interface

Purpose Verify that the 802.1X configuration is working on the interface.

Action Use the `show dot1x interface` command to view the 802.1X details.

Meaning The `Supplicant mode` output field displays the configured administrative mode for each interface.

Verifying the VLAN Association with the Interface

Purpose Verify interface states and VLAN memberships.

Action Use the `show ethernet-switching interfaces` command to view the Ethernet switching table entries.

Meaning The field `VLAN members` shows the associations between VLANs and interfaces. The `State` field shows whether the interfaces are up or down.

For the guest VLAN configuration, the interface is associated with the guest VLAN if and when the supplicant fails 802.1X user authentication.

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

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

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

Use the `show dhcp snooping binding` command to display the DHCP snooping information when the interface on which the DHCP server connects to the switch is trusted. View the MAC addresses from which requests were sent and the IP addresses and leases provided by the server.

Use the `show ip-source-guard` command to view IP source guard information for the VLAN.

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output 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.

- Related Topics**
- 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
 - Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN
 - Configuring IP Source Guard (CLI Procedure)

