Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches

This example shows how to configure and apply firewall filters to control traffic that is entering or exiting a port on the switch, a VLAN on the network, and a Layer 3 interface on the switch. Firewall filters define the rules that determine whether to forward or deny packets at specific processing points in the packet flow.

Requirements

This example uses the following software and hardware components:

- JUNOS Release 9.0 or later for EX Series switches.
- Two Juniper Networks EX3200-48T switches: one to be used as an access switch, the other to be used as a distribution switch
- One Juniper Networks EX-UM-4SFP uplink module
- One Juniper Networks J-series router

Before you configure and apply the firewall filters in this example, be sure you have:

- An understanding of firewall filter concepts, policers, and CoS
- Installed the uplink module in the distribution switch. See Installing an Uplink Module in an EX3200 or EX4200 Switch.

Overview

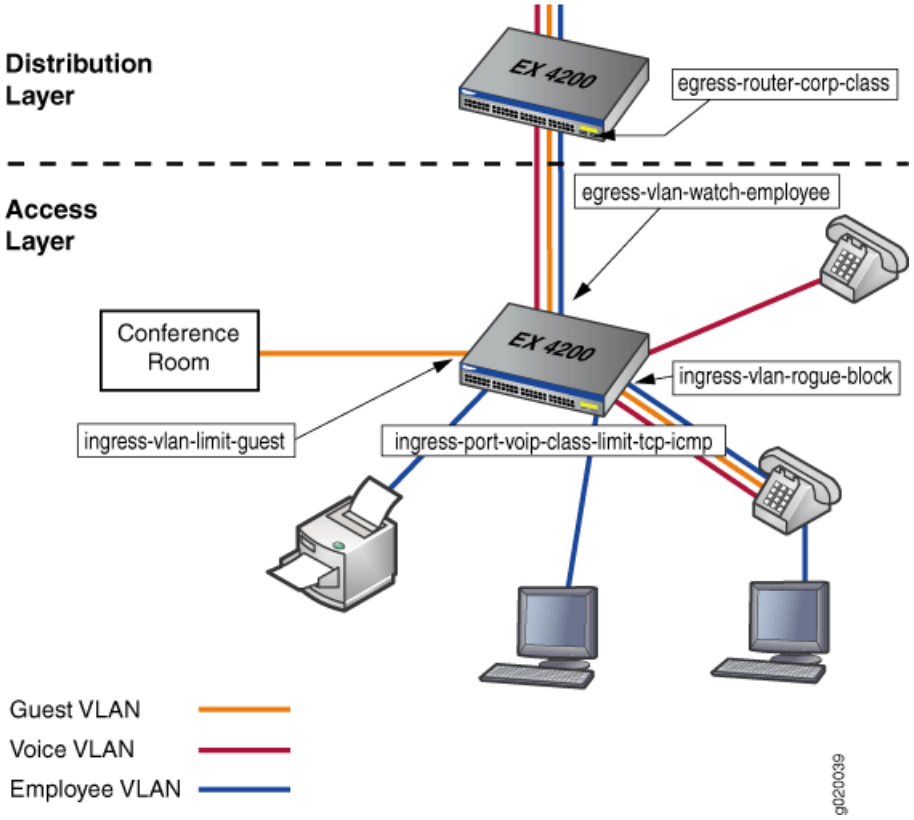
This configuration example show how to configure and apply firewall filters to provide rules to evaluate the contents of packets and determine when to discard, forward, classify, count, and analyze packets that are destined for or originating from the EX Series switches that handle all voice-vlan, employee-vlan, and guest-vlan traffic. Table 1 shows the firewall filters that are configured for the EX Series switches in this example.

Table 1: Configuration Components: Firewall Filters

Component	Purpose/Description
Port firewall filter, ingress-port-voip-class-limit-tcp-icmp	This firewall filter performs two functions: ■ Assigns priority queueing to packets with a source MAC address that matches the phone MAC addresses. The forwarding class expedited-forwarding provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service for all voice-vlan traffic. ■ Performs rate limiting on packets that enter the ports for employee-vlan. The traffic rate for TCP and ICMP packets is limited to 1 Mbps with a burst size up to 30,000 bytes. This firewall filter is applied to port interfaces on the access switch.
VLAN firewall filter, ingress-vlan-rogue-block	Prevents rogue devices from using HTTP sessions to mimic the gatekeeper device that manages call registration, admission, and call status for VoIP calls. Only TCP or UDP ports should be used; and only the gatekeeper uses HTTP. That is, all voice-vlan traffic on TCP ports should be destined for the gatekeeper device. This firewall filter applies to all phones on voice-vlan, including communication between any two phones on the VLAN and all communication between the gatekeeper device and VLAN phones. This firewall filter is applied to VLAN interfaces on the access switch.
VLAN firewall filter, egress-vlan-watch-employee	Accepts employee-vlan traffic destined for the corporate subnet, but does not monitor this traffic. Employee traffic destined for the Web is counted and analyzed. This firewall filter is applied to vlan interfaces on the access switch.
VLAN firewall filter, ingress-vlan-limit-guest	Prevents guests (non-employees) from talking with employees or employee hosts on employee-vlan. Also prevents guests from using peer-to-peer applications on guest-vlan, but allows guests to access the Web. This firewall filter is applied to VLAN interfaces on the access switch.
Router firewall filter, egress-router-corp-class	Prioritizes employee-vlan traffic, giving highest forwarding-class priority to employee traffic destined for the corporate subnet. This firewall filter is applied to a routed port (Layer 3 uplink module) on the distribution switch.

Figure 1 shows the application of port, VLAN, and Layer 3 routed firewall filters on the switch.

Figure 1: Application of Port, VLAN, and Layer 3 Routed Firewall Filters



Network Topology

The topology for this configuration example consists of one EX-3200-48T switch at the access layer, and one EX-3200-48T switch at the distribution layer. The distribution switch's uplink module is configured to support a Layer 3 connection to a J-series router.

The EX Series switches are configured to support VLAN membership. Table 2 shows the VLAN configuration components for the VLANs.

Table 2: Configuration Components: VLANs

VLAN Name	VLAN ID	VLAN Subnet and Available IP Addresses	VLAN Description
voice-vlan	10	192.0.2.0/28 192.0.2.1 through 192.0.2.14 192.0.2.15 is subnet's broadcast address	Voice VLAN used for employee VoIP traffic

Table 2: Configuration Components: VLANs *(continued)*

VLAN Name	VLAN ID	VLAN Subnet and Available IP Addresses	VLAN Description
employee-vlan	20	192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is subnet's broadcast address	VLAN standalone PCs, PCs connected to the network through the hub in VoIP telephones, wireless access points, and printers. This VLAN completely includes the voice VLAN. Two VLANs (voice-vlan and employee-vlan) must be configured on the ports that connect to the telephones.
guest-vlan	30	192.0.2.32/28 192.0.2.33 through 192.0.2.46 192.0.2.47 is subnet's broadcast address	VLAN for guests' data devices (PCs). The scenario assumes that the corporation has an area open to visitors, either in the lobby or in a conference room, that has a hub to which visitors can plug in their PCs to connect to the Web and to their company's VPN.
camera-vlan	40	192.0.2.48/28 192.0.2.49 through 192.0.2.62 192.0.2.63 is subnet's broadcast address	VLAN for the corporate security cameras.

Ports on the EX Series switches support Power over Ethernet (PoE) to provide both network connectivity and power for VoIP telephones connecting to the ports. Table 3 shows the switch ports that are assigned to the VLANs and the IP and MAC addresses for devices connected to the switch ports:

Table 3: Configuration Components: Switch Ports on a 48-Port All-PoE Switch

Switch and Port Number	VLAN Membership	IP and MAC Addresses	Port Devices
ge-0/0/0, ge-0/0/1	voice-vlan, employee-vlan	IP addresses: 192.0.2.1 through 192.0.2.2 MAC addresses: 00.05.85.00.00.01, 00.05.85.00–00.02	Two VoIP telephones, each connected to one PC.
ge-0/0/2, ge-0/0/3	employee-vlan	192.0.2.17 through 192.0.2.18	Printer, wireless access points

Table 3: Configuration Components: Switch Ports on a 48-Port All-PoE Switch *(continued)*

Switch and Port Number	VLAN Membership	IP and MAC Addresses	Port Devices
ge-0/0/4, ge-0/0/5	guest-vlan	192.0.2.34 through 192.0.2.35	Two hubs into which visitors can plug in their PCs. Hubs are located in an area open to visitors, such as a lobby or conference room
ge-0/0/6, ge-0/0/7	camera-vlan	192.0.2.49 through 192.0.2.50	Two security cameras
ge-0/0/9	voice-vlan	IP address: 192.0.2.14 MAC address:00.05.85.00.00.0E	Gatekeeper device. The gatekeeper manages call registration, admission, and call status for VoIP phones.
ge-0/1/0		IP address: 192.0.2.65	Layer 3 connection to a router; note that this is a port on the switch's uplink module

Configuring an Ingress Port Firewall Filter to Prioritize Voice Traffic and Rate-Limit TCP and ICMP Traffic

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

CLI Quick Configuration

To quickly configure and apply a port firewall filter to prioritize voice traffic and rate-limit packets that are destined for the employee-vlan subnet, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall policer tcp-connection-policer if-exceeding burst-size-limit 30k
bandwidth-limit 1m
set firewall policer tcp-connection-policer then discard
set firewall policer icmp-connection-policer if-exceeding burst-size-limit 30k
bandwidth-limit 1m
set firewall policer icmp-connection-policer then discard
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term voip-high from source-mac-address
00.05.85.00.00.01
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term voip-high from source-mac-address
00.05.85.00.00.02
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term voip-high from protocol udp
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term voip-high then forwarding-class
expedited-forwarding
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term voip-high then loss-priority low
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term network-control from precedence
net-control
```

```
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term network-control then forwarding-class
network-control
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term network-control then loss-priority
low
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term tcp-connection from destination-address
192.0.2.16/28
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term tcp-connection from protocol tcp
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term tcp-connection then policer
tcp-connection-policer
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term tcp-connection then count tcp-counter
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term tcp-connection then forwarding-class
best-effort
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term tcp-connection then loss-priority
high
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term icmp-connection from
destination-address 192.0.2.16/28
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term icmp-connection from protocol icmp
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term icmp-connection then policer
icmp-connection-policer
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term icmp-connection then count icmp-counter
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term icmp-connection then forwarding-class
best-effort
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term icmp-connection then loss-priority
high
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term best-effort then forwarding-class
best-effort
set firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp term best-effort then loss-priority high
set interfaces ge-0/0/0 description "voice priority and tcp and icmp traffic
rate-limiting filter at ingress port"
set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input
ingress-port-voip-class-limit-tcp-icmp
set interfaces ge-0/0/1 description "voice priority and tcp and icmp traffic
rate-limiting filter at ingress port"
set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input
ingress-port-voip-class-limit-tcp-icmp
set class-of-service schedulers voice-high buffer-size percent 15
set class-of-service schedulers voice-high priority high
set class-of-service schedulers net-control buffer-size percent 10
set class-of-service schedulers net-control priority high
set class-of-service schedulers best-effort buffer-size percent 75
set class-of-service schedulers best-effort priority low
set class-of-service scheduler-maps ethernet-diffsrv-cos-map forwarding-class
expedited-forwarding scheduler voice-high
set class-of-service scheduler-maps ethernet-diffsrv-cos-map forwarding-class
network-control scheduler net-control
```

```
set class-of-service scheduler-maps ethernet-diffsrv-cos-map forwarding-class
best-effort scheduler best-effort
```

Step-by-Step Procedure To configure and apply a port firewall filter to prioritize voice traffic and rate-limit packets that are destined for the employee-vlan subnet:

1. Define the policers tcp-connection-policer and icmp-connection-policer:

```
[edit]
user@switch# set firewall policer tcp-connection-policer if-exceeding
burst-size-limit 30k bandwidth-limit 1m
user@switch# set firewall policer tcp-connection-policer then discard
user@switch# set firewall policer icmp-connection-policer if-exceeding
burst-size-limit 30k bandwidth-limit 1m
user@switch# set firewall policer icmp-connection-policer then discard
```

2. Define the firewall filter ingress-port-voip-class-limit-tcp-icmp:

```
[edit firewall]
user@switch# set family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp
```

3. Define the term voip-high:

```
[edit firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp ]
user@switch# set term voip-high from source-mac-address 00.05.85.00.00.01
user@switch# set term voip-high from source-mac-address 00.05.85.00.00.02
user@switch# set term voip-high from protocol udp
user@switch# set term voip-high then forwarding-class expedited-forwarding
user@switch# set term voip-high then loss-priority low
```

4. Define the term network-control:

```
[edit firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp ]
user@switch# set term network-control from precedence net-control
user@switch# set term network-control then forwarding-class network-control
user@switch# set term network-control then loss-priority low
```

5. Define the term tcp-connection to configure rate limits for TCP traffic:

```
[edit firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp]
user@switch# set term tcp-connection from destination-address 192.0.2.16/28
user@switch# set term tcp-connection from protocol tcp
user@switch# set term tcp-connection then policer tcp-connection-policer
user@switch# set term tcp-connection then count tcp-counter
user@switch# set term tcp-connection then forwarding-class best-effort
user@switch# set term tcp-connection then loss-priority high
```

6. Define the term icmp-connection to configure rate limits for ICMP traffic:

```
[edit firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp]
```

```
user@switch# set term icmp-connection from destination-address
192.0.2.16/28
user@switch# set term icmp-connection from protocol icmp
user@switch# set term icmp-connection then policer icmp-policer
user@switch# set term icmp-connection then count icmp-counter
user@switch# set term icmp-connection then forwarding-class best-effort
user@switch# set term icmp-connection then loss-priority high
```

7. Define the term best-effort with no match conditions for an implicit match on all packets that did not match any other term in the firewall filter:

```
[edit firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp]
user@switch# set term best-effort then forwarding-class best-effort
user@switch# set term best-effort then loss-priority high
```

8. Apply the firewall filter ingress-port-voip-class-limit-tcp-icmp as an input filter to the port interfaces for employee-vlan :

```
[edit interfaces]
user@switch# set ge-0/0/0 description "voice priority and tcp and icmp
traffic rate-limiting filter at ingress port"
user@switch# set ge-0/0/0 unit 0 family ethernet-switching filter input
ingress-port-voip-class-limit-tcp-icmp
user@switch# set ge-0/0/1 description "voice priority and tcp and icmp
traffic rate-limiting filter at ingress port"
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input
ingress-port-voip-class-limit-tcp-icmp
```

9. Configure the parameters that are desired for the different schedulers.

NOTE: When you configure parameters for the schedulers, define the numbers to match your network traffic patterns.

```
[edit class-of-service]
user@switch# set schedulers voice-high buffer-size percent 15
user@switch# set schedulers voice-high priority high
user@switch# set schedulers network-control buffer-size percent 10
user@switch# set schedulers network-control priority high
user@switch# set schedulers best-effort buffer-size percent 75
user@switch# set schedulers best-effort priority low
```

10. Assign the forwarding-classes to schedulers with a scheduler map:

```
[edit class-of-service]
user@switch# set scheduler-maps ethernet-diffsrv-cos-map
user@switch# set scheduler-maps ethernet-diffsrv-cos-map forwarding-class
expedited-forwarding scheduler voice-high
user@switch# set scheduler-maps ethernet-diffsrv-cos-map forwarding-class
network-control scheduler net-control
```

```
user@switch# set scheduler-maps ethernet-diffsrv-cos-map forwarding-class
best-effort scheduler best-effort
```

11. Associate the scheduler map with the outgoing interface:

```
edit class-of-service
user@switch# set interfaces ge-0/1/0 scheduler-map ethernet-diffsrv-cos-map
```

Results Display the results of the configuration:

```
user@switch# show
  firewall {
    policer tcp-connection-policer {
      if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 30k;
      }
      then {
        discard;
      }
    }
    policer icmp-connection-policer {
      if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 30k;
      }
      then {
        discard;
      }
    }
    family ethernet-switching {
      filter ingress-port-voip-class-limit-tcp-icmp {
        term voip-high {
          from {
            destination-mac-address 00.05.85.00.00.01;
              destination-mac-address 00.05.85.00.00.02;
            protocol udp;
          }
          then {
            forwarding-class expedited-forwarding;
            loss-priority low;
          }
        }
        term network-control {
          from {
            precedence net-control ;
          }
          then {
            forwarding-class network-control;
            loss-priority low;
          }
        }
        term tcp-connection {
```

```
            from {
                destination-address 192.0.2.16/28;
                protocol tcp;
            }
            then {
                policer tcp-connection-policer;
                    count tcp-counter;
                    forwarding-class best-effort;
                loss-priority high;
            }
        }
        term icmp-connection
            from {
                protocol icmp;
            }
            then {
                policer icmp-connection-policer;
                    count icmp-counter;
                    forwarding-class best-effort;
                loss-priority high;
            }
        }
        term best-effort {
            then {
                forwarding-class best-effort;
                loss-priority high;
            }
        }
    }
  }
}
interfaces {
    ge-0/0/0 {
        description "voice priority and tcp and icmp traffic rate-limiting filter at ingress
            port";
        unit 0 {
            family ethernet-switching {
                filter {
                    input ingress-port-voip-class-limit-tcp-icmp;
                }
            }
        }
    }
    ge-0/0/1 {
        description "voice priority and tcp and icmp traffic rate-limiting filter at ingress
            port";
            unit 0 {
            family ethernet-switching {
                filter {
                    input ingress-port-voip-class-limit-tcp-icmp;
                }
            }
        }
    }
}
scheduler-maps {
```

```
    ethernet-diffsrv-cos-map {
        forwarding-class expedited-forwarding scheduler voice-high;
            forwarding-class network-control scheduler net-control;
        forwarding-class best-effort scheduler best-effort;
    }
}
interfaces {
    ge/0/1/0 {
        scheduler-map ethernet-diffsrv-cos-map;
    }
}
```

Configuring a VLAN Ingress Firewall Filter to Prevent Rogue Devices from Disrupting VoIP Traffic

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

CLI Quick Configuration

To quickly configure a VLAN firewall filter on voice-vlan to prevent rogue devices from using HTTP sessions to mimic the gatekeeper device that manages VoIP traffic, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter ingress-vlan-rogue-block term
to-gatekeeper from destination-address 192.0.2.14
set firewall family ethernet-switching filter ingress-vlan-rogue-block term
to-gatekeeper from destination-port 80
set firewall family ethernet-switching filter ingress-vlan-rogue-block term
to-gatekeeper then accept
set firewall family ethernet-switching filter ingress-vlan-rogue-block term
from-gatekeeper from source-address 192.0.2.14
set firewall family ethernet-switching filter ingress-vlan-rogue-block term
from-gatekeeper from source-port 80
set firewall family ethernet-switching filter ingress-vlan-rogue-block term
from-gatekeeper then accept
set firewall family ethernet-switching filter ingress-vlan-rogue-block term
not-gatekeeper from destination-port 80
set firewall family ethernet-switching filter ingress-vlan-rogue-block term
not-gatekeeper then count rogue-counter
set firewall family ethernet-switching filter ingress-vlan-rogue-block term
not-gatekeeper then discard
set vlans voice-vlan description "block rogue devices on voice-vlan"
set vlans voice-vlan filter input ingress-vlan-rogue-block
```

Step-by-Step Procedure

To configure and apply a VLAN firewall filter on voice-vlan to prevent rogue devices from using HTTP to mimic the gatekeeper device that manages VoIP traffic:

1. Define the firewall filter ingress-vlan-rogue-block to specify filter matching on the traffic you want to permit and restrict:

```
[edit firewall]
user@switch# set family ethernet-switching filter ingress-vlan-rogue-block
```

2. Define the term to-gatekeeper to accept packets that match the destination IP address of the gatekeeper:

```
[edit firewall family ethernet-switching filter ingress-vlan-rogue-block]
user@switch# set term to-gatekeeper from destination-address 192.0.2.14
user@switch# set term to-gatekeeper from destination-port 80
user@switch# set term to-gatekeeper then accept
```

3. Define the term from-gatekeeper to accept packets that match the source IP address of the gatekeeper:

```
[edit firewall family ethernet-switching filter ingress-vlan-rogue-block]
user@switch# set term from-gatekeeper from source-address 192.0.2.14
user@switch# set term from-gatekeeper from source-port 80
user@switch# set term from-gatekeeper then accept
```

4. Define the term not-gatekeeper to ensure all voice-vlan traffic on TCP ports is destined for the gatekeeper device:

```
[edit firewall family ethernet-switching filter ingress-vlan-rogue-block]
user@switch# set term not-gatekeeper from destination-port 80
user@switch# set term not-gatekeeper then count rogue-counter
user@switch# set term not-gatekeeper then discard
```

5. Apply the firewall filter ingress-vlan-rogue-block as an input filter to the VLAN interface for the VoIP telephones:

```
[edit interfaces]
user@switch# set vlans voice–vlan description "block rogue devices on
voice-vlan"
user@switch# set vlans voice–vlan filter input ingress-vlan-rogue-block
```

Results Display the results of the configuration:

```
user@switch# show
  firewall {
    family ethernet-switching {
      filter ingress-vlan-rogue-block {
        term to-gatekeeper {
          from {
            destination-address 192.0.2.14/32
            destination-port 80;
          }
          then {
            accept;
          }
        }
        term from-gatekeeper {
          from {
            source-address 192.0.2.14/32
            source-port 80;
          }
          then {
            accept;
          }
```

```
        }
        term not-gatekeeper {
            from {
                destination-port 80;
            }
            then {
                count rogue-counter;
                discard;
            }
        }
    }
vlans {
    voice-vlan {
        description "block rogue devices on voice-vlan";
        filter {
            input ingress-vlan-rogue-block;
        }
    }
}
```

Configuring a VLAN Firewall Filter to Count, Monitor, and Analyze Egress Traffic on the Employee VLAN

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

CLI Quick Configuration

A firewall filter is configured and applied to VLAN interfaces to filter employee-vlan egress traffic. Employee traffic destined for the corporate subnet is accepted but not monitored. Employee traffic destined for the Web is counted and analyzed.

To quickly configure and apply a VLAN firewall filter, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter egress-vlan-watch-employee term
employee-to-corp from destination-address 192.0.2.16/28
set firewall family ethernet-switching filter egress-vlan-watch-employee term
employee-to-corp then accept
set firewall family ethernet-switching filter egress-vlan-watch-employee term
employee-to-web from destination-port 80
set firewall family ethernet-switching filter egress-vlan-watch-employee term
employee-to-web then count employee-web-counter
set firewall family ethernet-switching filter egress-vlan-watch-employee term
employee-to-web then analyzer employee-monitor
set vlans employee-vlan description "filter at egress VLAN to count and analyze
employee to Web traffic"
set vlans employee-vlan filter output egress-vlan-watch-employee
```

Step-by-Step Procedure To configure and apply an egress port firewall filter to count and analyze employee-vlan traffic that is destined for the Web:

1. Define the firewall filter egress-vlan-watch-employee:

```
[edit firewall]
user@switch# set family ethernet-switching filter
egress-vlan-watch-employee
```

2. Define the term employee-to-corp to accept but not monitor all employee-vlan traffic destined for the corporate subnet:

```
[edit firewall family ethernet-switching filter egress-vlan-watch-employee]
user@switch# set term employee-to-corp from destination-address
192.0.2.16/28
user@switch# set term employee-to-corp then accept
```

3. Define the term employee-to-web to count and monitor all employee-vlan traffic destined for the Web:

```
[edit firewall family ethernet-switching filter egress-vlan-watch-employee]
user@switch# set term employee-to-web from destination-port 80
user@switch# set term employee-to-web then count employee-web-counter
user@switch# set term employee-to-web then analyzer employee-monitor
```

NOTE: See Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches for information about configuring the employee-monitor analyzer.

4. Apply the firewall filter egress-vlan-watch-employee as an output filter to the port interfaces for the VoIP telephones:

```
[edit]
user@switch# set vlans employee-vlan description "filter at egress VLAN
to count and analyze employee to Web traffic"
user@switch# set vlans employee-vlan filter output
egress-vlan-watch-employee
```

Results Display the results of the configuration:

```
user@switch# show
  firewall {
    family ethernet-switching {
      filter egress-vlan-watch-employee {
        term employee-to-corp {
          from {
            destination-address 192.0.2.16/28
          }
          then {
            accept;
```

```
            }
        }
        term employee-to-web {
            from {
                destination-port 80;
            }
            then {
                count employee-web-counter:
                analyzer employee-monitor;
            }
        }
    }
  }
}
vlans {
    employee-vlan {
        description "filter at egress VLAN to count and analyze employee to Web traffic";
        filter {
            output egress-vlan-watch-employee;
        }
    }
}
```

Configuring a VLAN Firewall Filter to Restrict Guest-to-Employee Traffic and Peer-to-Peer Applications on the Guest VLAN

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

CLI Quick Configuration

In the following example, the first filter term permits guests to talk with other guests but not employees on employee-vlan. The second filter term allows guests Web access but prevents them from using peer-to-peer applications on guest-vlan.

To quickly configure a VLAN firewall filter to restrict guest-to-employee traffic, blocking guests from talking with employees or employee hosts on employee-vlan or attempting to use peer-to-peer applications on guest-vlan, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter ingress-vlan-limit-guest term
guest-to-guest from destination-address 192.0.2.33/28
set firewall family ethernet-switching filter ingress-vlan-limit-guest term
guest-to-guest then accept
set firewall family ethernet-switching filter ingress-vlan-limit-guest term
no-guest-employee-no-peer-to-peer from destination-mac-address 00.05.85.00.00.DF
set firewall family ethernet-switching filter ingress-vlan-limit-guest term
no-guest-employee-no-peer-to-peer then accept
set vlans guest-vlan description "restrict guest-to-employee traffic and
peer-to-peer applications on guest VLAN"
set vlans guest-vlan filter input ingress-vlan-limit-guest
```

Step-by-Step Procedure To configure and apply a VLAN firewall filter to restrict guest-to-employee traffic and peer-to-peer applications on guest-vlan:

1. Define the firewall filter ingress-vlan-limit-guest:

```
[edit firewall]
set firewall family ethernet-switching filter ingress-vlan-limit-guest
```

2. Define the term guest-to-guest to permit guests on the guest-vlan to talk with other guests but not employees on the employee-vlan:

```
[edit firewall family ethernet-switching filter ingress-vlan-limit-guest]
user@switch# set term guest-to-guest from destination-address 192.0.2.33/28
user@switch# set term guest-to-guest then accept
```

3. Define the term no-guest-employee-no-peer-to-peer to allow guests on guest-vlan Web access but prevent them from using peer-to-peer applications on the guest-vlan.

NOTE: The destination-mac-address is the default gateway, which for any host in a VLAN is the next-hop router.

```
[edit firewall family ethernet-switching filter ingress-vlan-limit-guest]
user@switch# set term no-guest-employee-no-peer-to-peer from
destination-mac-address 00.05.85.00.00.DF
user@switch# set term no-guest-employee-no-peer-to-peer then accept
```

4. Apply the firewall filter ingress-vlan-limit-guest as an input filter to the interface for guest-vlan :

```
[edit]
user@switch# set vlans guest-vlan description "restrict guest-to-employee
traffic and peer-to-peer applications on guest VLAN"
user@switch# set vlans guest-vlan filter input ingress-vlan-limit-guest
```

Results Display the results of the configuration:

```
user@switch# show
  firewall {
    family ethernet-switching {
      filter ingress-vlan-limit-guest {
        term guest-to-guest {
          from {
            destination-address 192.0.2.33/28;
          }
          then {
            accept;
          }
        }
        term no-guest-employee-no-peer-to-peer {
```

```
            from {
               destination-mac-address 00.05.85.00.00.DF;
            }
            then {
               accept;
            }
         }
      }
   }
}
vlans {
   guest-vlan {
      description "restrict guest-to-employee traffic and peer-to-peer applications on
         guest VLAN";
      filter {
         input ingress-vlan-limit-guest;
      }
   }
}
```

Configuring a Router Firewall Filter to Give Priority to Egress Traffic Destined for the Corporate Subnet

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

CLI Quick Configuration

To quickly configure a firewall filter for a routed port (Layer 3 uplink module) to filter employee-vlan traffic, giving highest forwarding-class priority to traffic destined for the corporate subnet, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family inet filter egress-router-corp-class term corp-expedite from
destination-address 192.0.2.16/28
set firewall family inet filter egress-router-corp-class term corp-expedite then
forwarding-class expedited-forwarding
set firewall family inet filter egress-router-corp-class term corp-expedite then
loss-priority low
set firewall family inet filter egress-router-corp-class term not-to-corp then
accept
set interfaces ge-0/1/0 description "filter at egress router to expedite destined
for corporate network"
set ge-0/1/0 unit 0 family inet address 103.104.105.1
set interfaces ge-0/1/0 unit 0 family inet filter output egress-router-corp-class
```

Step-by-Step Procedure

To configure and apply a firewall filter to a routed port (Layer 3 uplink module) to give highest priority to employee-vlan traffic destined for the corporate subnet:

1. Define the firewall filter egress-router-corp-class:

```
[edit]
user@switch# set firewall family inet filter egress-router-corp-class
```

2. Define the term corp-expedite:

```
[edit firewall]
user@switch# set family inet filter egress-router-corp-class term
corp-expedite from destination-address 192.0.2.16/28
user@switch# set family inet filter egress-router-corp-class term
corp-expedite then forwarding-class expedited-forwarding
user@switch# set family inet filter egress-router-corp-class term
corp-expedite then loss-priority low
```

3. Define the term not-to-corp:

```
[edit firewall]
user@switch# set family inet filter egress-router-corp-class term
not-to-corp then accept
```

4. Apply the firewall filter egress-router-corp-class as an output filter for the port on the switch's uplink module, which provides a Layer 3 connection to a router:

```
[edit interfaces]
user@switch# set ge-0/1/0 description "filter at egress router to expedite
employee traffic destined for corporate network"
user@switch# set ge-0/1/0 unit 0 family inet address 103.104.105.1
user@switch# set ge-0/1/0 unit 0 family inet filter output
egress-router-corp-class
```

Results Display the results of the configuration:

```
user@switch# show
  firewall {
    family inet {
      filter egress-router-corp-class {
        term corp-expedite {
          from {
            destination-address 192.0.2.16/28;
          }
          then {
            forwarding-class expedited-forwarding;
            loss-priority low;
          }
        }
        term not-to-corp {
          then {
            accept;
          }
        }
      }
    }
  }
  interfaces {
    ge-0/1/0 {
      unit 0 {
        description "filter at egress router interface to expedite employee traffic
          destined for corporate network";
        family inet {
```

```
            source-address 103.104.105.1
            filter {
               output egress-router-corp-class;
            }
         }
      }
   }
}
```

Verification

To confirm that the firewall filters are working properly, perform the following tasks:

- Verifying that Firewall Filters and Policers are Operational on page 19
- Verifying that Schedulers and Scheduler-Maps are Operational on page 19

Verifying that Firewall Filters and Policers are Operational

Purpose Verify the operational state of the firewall filters and policers that are configured on the switch.

Action Use the operational mode command:

```
user@switch>  show firewall
Filter: ingress-port-voip-class-limit-tcp-icmp
Counters:
Name                                                Packets
icmp-counter                                              0
tcp-counter                                               0
Policers:
Name                                                Packets
icmp-connection-policer                                   0
tcp-connection-policer                                    0

Filter: ingress-vlan-rogue-block

Filter: egress-vlan-watch-employee
Counters:
Name                                                Packets
employee-web-counter                                      0
```

Meaning The show firewall command displays the names of the firewall filters, policers, and counters that are configured on the switch. The output fields show byte and packet counts for all configured counters and the packet count for all policers.

Verifying that Schedulers and Scheduler-Maps are Operational

Purpose Verify that schedulers and scheduler-maps are operational on the switch.

Action Use the operational mode command:

```
user@switch>  show class-of-service scheduler-map

Scheduler map: default, Index: 2
```

```
  Scheduler: default-be, Forwarding class: best-effort, Index: 20
    Transmit rate: 95 percent, Rate Limit: none, Buffer size: 95 percent,
    Priority: low
    Drop profiles:
      Loss priority   Protocol    Index    Name
      Low             non-TCP         1    default-drop-profile
      Low             TCP             1    default-drop-profile
      High            non-TCP         1    default-drop-profile
      High            TCP             1    default-drop-profile

  Scheduler: default-nc, Forwarding class: network-control, Index: 22
    Transmit rate: 5 percent, Rate Limit: none, Buffer size: 5 percent,
    Priority: low
    Drop profiles:
      Loss priority   Protocol    Index    Name
      Low             non-TCP         1    default-drop-profile
      Low             TCP             1    default-drop-profile
      High            non-TCP         1    default-drop-profile
      High            TCP             1    default-drop-profileScheduler map:
ethernet-diffsrv-cos-map, Index: 21657

  Scheduler: best-effort, Forwarding class: best-effort, Index: 61257
    Transmit rate: remainder, Rate Limit: none, Buffer size: 75 percent,
    Priority: low
    Drop profiles:
      Loss priority   Protocol    Index    Name
      Low             non-TCP         1    <default-drop-profile>
      Low             TCP             1    <default-drop-profile>
      High            non-TCP         1    <default-drop-profile>
      High            TCP             1    <default-drop-profile>

  Scheduler: voice-high, Forwarding class: expedited-forwarding, Index: 3123
    Transmit rate: remainder, Rate Limit: none, Buffer size: 15 percent,
    Priority: high
    Drop profiles:
      Loss priority   Protocol    Index    Name
      Low             non-TCP         1    <default-drop-profile>
      Low             TCP             1    <default-drop-profile>
      High            non-TCP         1    <default-drop-profile>
      High            TCP             1    <default-drop-profile>

  Scheduler: net-control, Forwarding class: network-control, Index: 2451
    Transmit rate: remainder, Rate Limit: none, Buffer size: 10 percent,
    Priority: high
    Drop profiles:
      Loss priority   Protocol    Index    Name
      Low             non-TCP         1    <default-drop-profile>
      Low             TCP             1    <default-drop-profile>
      High            non-TCP         1    <default-drop-profile>
      High            TCP             1    <default-drop-profile>
```

Meaning Displays statistics about the configured schedulers and schedulers-maps.

Related Topics

- Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches
- Example: Configuring CoS on EX Series Switches
- Configuring Firewall Filters (CLI Procedure)
- Configuring Firewall Filters (J-Web Procedure)

- Configuring Policers to Control Traffic Rates (CLI Procedure)
- Firewall Filter Match Conditions and Actions for EX Series Switches
- [edit firewall] Configuration Statement Hierarchy

Published: 2009-07-28