

Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches

Administrators can configure filter-based forwarding on an EX Series switch by using a firewall filter to forward matched traffic to a specific virtual routing instance.

This example describes how to set up filter-based forwarding:

- Requirements on page 1
- Overview and Topology on page 1
- Configuration on page 1
- Verification on page 3

Requirements

This example uses the following software and hardware components:

- One EX Series switch
- JUNOS Release 9.4 or later for EX Series switches

Overview and Topology

In this example, traffic from one application server that is destined for a different application server is matched by a firewall filter based on the IP address. Any matching packets are routed to a particular virtual routing instance that first sends all traffic to a security device, then forwards it to the designated destination address.

Configuration

To configure filter-based forwarding:

CLI Quick Configuration To quickly create and configure filter-based forwarding, copy the following commands and paste them into the switch terminal window:

```
[edit]
set interfaces ge-0/0/0 unit 0 family inet address 10.1.0.1/24
set interfaces ge-0/0/3 unit 0 family inet address 10.1.3.1/24
set firewall family inet filter fil term t1 from source-address 1.1.1.1/32
set firewall family inet filter fil term t1 from protocol tcp
set interfaces ge-0/0/0 unit 0 family inet filter input fil
set routing-instances vrf01 instance-type virtual-router
set routing-instances vrf01 interface ge-0/0/1.0
set routing-instances vrf01 interface ge-0/0/3.0
set routing-instances vrf01 routing-options static route 12.34.56.0/24 next-hop 10.1.3.254
set firewall family inet filter fil term t1 then routing-instance vrf01
```

Step-by-Step Procedure To configure filter-based forwarding:

1. Create interfaces to the application servers:

```
[edit]
user@switch# set interfaces ge-0/0/0 unit 0 family inet address 10.1.0.1/24
user@switch# set interfaces ge-0/0/3 unit 0 family inet address 10.1.3.1/24
```

2. Create a firewall filter that matches the correct source address:

```
[edit]
user@switch# set firewall family inet filter fil term t1 from
source-address 1.1.1.1/32
user@switch# set firewall family inet filter fil term t1 from protocol
tcp
```

3. Associate the filter with the source application server's interface:

```
[edit]
user@switch# set interfaces ge-0/0/0 unit 0 family inet filter input fil
```

4. Create a virtual router:

```
[edit]
user@switch# set routing-instances vrf01 instance-type virtual-router
```

5. Associate the interfaces with the virtual router:

```
[edit]
user@switch# set routing-instances vrf01 interface ge-0/0/1.0
user@switch# set routing-instances vrf01 interface ge-0/0/3.0
```

6. Configure the routing information for the virtual routing instance:

```
[edit]
user@switch# set routing-instances vrf01 routing-options static route
12.34.56.0/24 next-hop 10.1.3.254
```

7. Set the filter to forward packets to the virtual router you created:

```
[edit]
user@switch# set firewall family inet filter fil term t1 then
routing-instance vrf01
```

Results Check the results of the configuration:

```
user@switch> show configuration
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        filter {
```

```

        input fil;
    }
    address 10.1.0.1/24;
}
}
}
ge-0/0/3 {
    unit 0 {
        family inet {
            address 10.1.3.1/24;
        }
    }
}
}
}
firewall {
    family inet {
        filter fil {
            term t1 {
                from {
                    source-address {
                        1.1.1.1/32;
                    }
                    protocol tcp;
                }
                then {
                    routing-instance vrf01;
                }
            }
        }
    }
}
}
routing-instances {
    vrf01 {
        instance-type virtual-router;
        interface ge-0/0/1.0;
        interface ge-0/0/3.0;
        routing-options {
            static {
                route 12.34.56.0/24 next-hop 10.1.3.254;
            }
        }
    }
}
}

```

Verification

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

- Verifying That Filter-Based Forwarding Was Configured on page 3

Verifying That Filter-Based Forwarding Was Configured

Purpose Verify that filter-based forwarding was properly enabled on the switch.

Action 1. Use the show interfaces filters command:

```
user@switch> show interfaces filters ge-0/0/0.0
```

Interface	Admin	Link	Proto	Input Filter	Output Filter
ge-0/0/0.0	up	down	inet	fil	

2. Use the show route forwarding-table command:

```
user@switch> show route forwarding-table
```

Routing table: default.inet

Internet:

Destination	Type	RtRef	Next hop	Type	Index	NhRef	Netif
default	user	1	0:12:f2:21:cf:0	ucst	331	4	me0.0
default	perm	0		rjct	36	3	
0.0.0.0/32	perm	0		dscd	34	1	
10.1.0.0/24	ifdn	0		rslv	613	1	
ge-0/0/0.0							
10.1.0.0/32	iddn	0	10.1.0.0	recv	611	1	
ge-0/0/0.0							
10.1.0.1/32	user	0		rjct	36	3	
10.1.0.1/32	intf	0	10.1.0.1	loc1	612	2	
10.1.0.1/32	iddn	0	10.1.0.1	loc1	612	2	
10.1.0.255/32	iddn	0	10.1.0.255	bcst	610	1	
ge-0/0/0.0							
10.1.1.0/26	ifdn	0		rslv	583	1	vlan.0
10.1.1.0/32	iddn	0	10.1.1.0	recv	581	1	vlan.0
10.1.1.1/32	user	0		rjct	36	3	
10.1.1.1/32	intf	0	10.1.1.1	loc1	582	2	
10.1.1.1/32	iddn	0	10.1.1.1	loc1	582	2	
10.1.1.63/32	iddn	0	10.1.1.63	bcst	580	1	vlan.0
255.255.255.255/32	perm	0		bcst	32	1	

Routing table: vrf01.inet

Internet:

Destination	Type	RtRef	Next hop	Type	Index	NhRef	Netif
default	perm	0		rjct	559	2	
0.0.0.0/32	perm	0		dscd	545	1	
10.1.3.0/24	ifdn	0		rslv	617	1	
ge-0/0/3.0							
10.1.3.0/32	iddn	0	10.1.3.0	recv	615	1	
ge-0/0/3.0							
10.1.3.1/32	user	0		rjct	559	2	
10.1.3.1/32	intf	0	10.1.3.1	loc1	616	2	
10.1.3.1/32	iddn	0	10.1.3.1	loc1	616	2	
10.1.3.255/32	iddn	0	10.1.3.255	bcst	614	1	
ge-0/0/3.0							
224.0.0.0/4	perm	0		mdsc	546	1	
224.0.0.1/32	perm	0	224.0.0.1	mcst	529	1	
255.255.255.255/32	perm	0		bcst	543	1	

Routing table: default.iso

ISO:

Destination	Type	RtRef	Next hop	Type	Index	NhRef	Netif
default	perm	0		rjct	60	1	

Routing table: vrf01.iso

ISO:									
Destination	Type	RtRef	Next	hop	Type	Index	NhRef	Netif	
default	perm	0			rjct	600	1		

Meaning The output indicates that the filter was created on the interface and that the virtual routing instance is forwarding matching traffic to the correct IP address.

- Related Topics**
- Configuring Firewall Filters (CLI Procedure)
 - Configuring Static Routing (CLI Procedure)
 - Configuring Static Routing (J-Web Procedure)
 - Understanding Filter-Based Forwarding for EX Series Switches

Published: 2009-07-28