Implementing URPF

This section describes the implementation of URPF.

Understanding URPF

It has become a commonplace practice for hackers planning a DoS attack to use forged IP addresses (the practice is known as IP address spoofing) and constantly change the source IP address to avoid detection by service providers.

Unicast Reverse Path Forwarding (URPF) is a mechanism for validating the source IP address of packets received on a router. A router configured with URPF performs a reverse path lookup in the FIB table to validate the presence of the source IP address. If the source IP address is listed in the table, then it indicates that the source is reachable and valid. If source IP address cannot be located in the FIB table, the packet is treated as malicious by the router and discarded.

The router supports the use of URPF in both strict and loose modes. URPF loose mode is enabled when the router is configured to validate only the prefix of the source IP address in the FIB and not the interface used by the packet to reach the router. By configuring loose mode, legitimate traffic that uses an alternate interface to reach the router is not mistaken to be malicious. URPF loose mode is very useful in multi-homed provider edge networks.

When URPF strict mode is enabled, the source address of the packet is checked in the FIB. If the packet is received on the same interface that would be used to forward the traffic to the source of the packet, the packet passes the check and is further processed; otherwise, it is dropped. Strict uRPF should only be applied where there is natural or configured symmetry. Because internal interfaces are likely to have routing asymmetry, that is, multiple routes to the source of a packet, URPF strict mode should not be implemented on interfaces that are internal to the network.

Note The behavior of URPF strict mode varies slightly by platform, number of recursion levels, and number of paths in Equal-Cost Multipath (ECMP) scenarios. A platform may switch to loose RPF check for some or all prefixes, even though strict RPF is configured.

The URPF loose and strict modes support both **allow self-ping** and **self-ping** options. The **self-ping** option allows the source of the packet to ping itself.

Configuring URPF Loose Mode

This section explains how you can configure URPF loose mode on the router for both IPv4 and IPv6 networks.

Before You Begin

Before you can configure URPF loose mode on a router, you must disable the default scale on the Cisco NCS 5500 series line card, as described in this section.

Note The **hw-module fib ipv4 scale internet-optimized** command and **hw-module fib ipv6 scale internet-optimized** command are deprecated from Cisco IOS XR Software Release 7.3.1 and Release 7.4.1, respectively. Hence, if you are upgrading a router (where these configurations are already existing) to Release 7.3.1 or Release 7.4.1 or later, you might see a corresponding warning message stating so.

Note Cisco NCS 5500 series line cards must be reloaded after disabling the default scale. This is done to ensure that the **hw-module** command configuration takes immediate effect. Line card reload is not required for NCS 5700 Series line card.

Note On NCS55Ax systems with external TCAM (eTCAM), the dual capacity mode need not be disabled to enable uRPF.

Note If you have configured `hw-module fib ipv4 scale host-optimized-disable`, you cannot configure `hw-module profile segment-routing srv6 mode micro-segment format f3216`, as these profiles are mutually exclusive.

For all types of line cards with TCAM:

```
RP/0/RP0/CPU0:router(config)# hw-module tcam fib ipv4 scaledisable

RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# end
RP/0/RP0/CPU0:router# reload location all
Proceed with reload? [confirm]
```

For all types of line cards without TCAM:

```
RP/0/RP0/CPU0:router(config)# hw-module fib ipv4 scale host-optimized-disable

RP/0/RP0/CPU0:router(config)# commit
```

```
RP/0/RP0/CPU0:router(config)# end
RP/0/RP0/CPU0:router# reload location all
Proceed with reload? [confirm]
```

Configuration

Use the following configuration to configure URPF loose mode on the router.

Note You must configure both IPv4 and IPv6 commands (as described in this section) for URPF to work.

```
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether1
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.0.0.1 255.255.255.0
RP/0/RP0/CPU0:router(config-if)# ipv4 verify unicast source reachable-via any
RP/0/RP0/CPU0:router(config-if)# ipv6 address 2001::1/64
RP/0/RP0/CPU0:router(config-if)# ipv6 verify unicast source reachable-via any
RP/0/RP0/CPU0:router(config-if)# commit
```

Running Configuration

Confirm your configuration as shown:

```
RP/0/RP0/CPU0:router(config-if)# show running-config
Thu Jul 27 14:40:38.167 IST
...
!
interface Bundle-Ether1
 ipv4 address 10.0.0.1 255.255.255.0
 ipv4 verify unicast source reachable-via any
ipv6 address 2001::1/64
 ipv6 verify unicast source reachable-via any
!
```

You have successfully configured URPF loose mode on the router.

Configure uRPF strict mode

Use this procedure to configure uRPF strict mode on a router.

uRPF strict mode discards packets if the device cannot verify that the source address of each packet is reachable through the receiving interface. uRPF helps prevent attacks that rely on spoofing source addresses.

Before you begin

- Configure both IPv4 and IPv6 commands as described in Configuring URPF Loose Mode, on page 2.

Procedure

Step 1 Enter interface configuration mode for the required interface.

Example:

```
Router(config)#interface GigabitEthernet 0/1/0/0
```

Step 2   Assign the IPv4 address to the interface.

Example:

```
Router(config-if)#ipv4 address 10.0.0.1 255.255.255.0
```

Step 3   Enable uRPF strict mode for IPv4.

Example:

```
Router(config-if)#ipv4 verify unicast source reachable-via rx
```

Step 4   Assign the IPv6 address to the interface.

Example:

```
Router(config-if)#ipv6 address  2001:DB8::1/64
```

Step 5   Enable uRPF strict mode for IPv6.

Example:

```
Router(config-if)#ipv6 verify unicast source reachable-via rx
Router(config-if)#commit
```

Step 6   Verify your configuration.

Example:

```
Router#show running-config
...
!
interface GigabitEthernet 0/1/0/0
 ipv4 address 10.0.0.1 255.255.255.0
 ipv4 verify unicast source reachable-via rx
ipv6 address  2001:DB8::1/64
 ipv6 verify unicast source reachable-via rx
!
```