Unicast Reverse Path Forwarding ACL Support

The Unicast Reverse Path Forwarding feature helps to mitigate problems that are caused by malformed or forged IP source addresses that pass through a device. The Unicast Reverse Path Forwarding ACL Support feature adds the access control list (ACL) support to the Unicast Reverse Path Forwarding feature. With the ACL support, Unicast Reverse Path Forwarding (RPF) can determine whether to drop or to forward data packets that have malformed or forged IP source addresses.

This module describes the ACL support for Unicast RPF.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Unicast Reverse Path Forwarding ACL Support

- Unicast RPF requires Cisco Express Forwarding to function properly on a device.

- Prior to configuring Unicast RPF, you must configure the following ACLs:
  - Configure standard or extended ACLs to mitigate the transmission of invalid IP addresses (by performing egress filtering). Configuring standard or extended ACLS, permit only valid source addresses to leave your network and enter the Internet.
  - Configure standard or extended ACL entries to drop (deny) packets that have invalid source IP addresses (by performing ingress filtering). Invalid source IP addresses include the following types:
    - Broadcast addresses (including multicast addresses)
    - Loopback addresses
    - Private addresses (RFC 1918, *Address Allocation for Private Internets*)
    - Reserved addresses
    - Source addresses that fall outside the range of valid addresses associated with a protected network
  - Configure standard or extended ACL entries to forward (permit) packets that fail the Unicast RPF checks and allow specific traffic from known asymmetric routed sources.
- Configure ACLs to track Unicast RPF events to provide additional information about network attacks.

Restrictions for Unicast Reverse Path Forwarding ACL Support

ACL templates are not supported.

Information About Unicast Reverse Path Forwarding ACL Support

Unicast RPF Operation

When Unicast RPF is enabled on an interface of a device, the device examines all packets received as input on that interface to ensure that the source address and source interface information appears in the routing table and matches the interface on which packets are received. This ability to "look backwards" is available only when Cisco Express Forwarding is enabled on a device because the lookup relies on the presence of a Forwarding Information Base (FIB). Cisco Express Forwarding generates a FIB as part of its operation.

Note Unicast RPF is an input function and is applied only on the input interface of a device at the upstream end of a connection.

Unicast RPF does a reverse lookup in the Cisco Express Forwarding table to check if any packet received at the interface of a device arrives on the best return path (or return route) to the source of the packet. If the packet was received from one of the best reverse path routes, the packet is forwarded as normal. No reverse path route on the interface from which the packet was received can mean that the source address was modified.

Note With Unicast RPF, all equal-cost "best" return paths are considered valid. Unicast RPF supports multiple return paths, provided that each path is equal to the others in terms of the routing cost (such as number of hops, weights, and so on) and the route is available in the FIB. Unicast RPF also functions where Enhanced Interior Gateway Routing Protocol (EIGRP) variants are used.

Before forwarding a packet that is received at the interface on which Unicast RPF and ACLs have been configured, Unicast RPF does the following checks:

1. If input ACLs are configured on the inbound interface.
2. If the packet has arrived on the best return path to the source by doing a reverse lookup in the FIB table.
3. Does a lookup of the Cisco Express Forwarding table for packet forwarding.
4. Checks output ACLs on the outbound interface.
5. Forwards the packet.

Access Control Lists and Logging

When you configure an access control list (ACL) and a packet fails the Unicast RPF check, the Unicast RPF checks the ACL to see if the packet should be dropped (by using a deny statement in the ACL) or forwarded (by using a permit statement in the ACL). Regardless of whether the packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is configured, the device drops the forged or malformed packet immediately, and no ACL logging occurs. The device and the interface Unicast RPF logging counters are updated.

To log Unicast RPF events, specify the logging option for ACL entries. Using the log information, administrators can view source addresses that are used in an attack, the time at which packets arrived at an interface, and so on.

Caution Logging requires CPU and memory resources. Logging Unicast RPF events for attacks that have a high rate of forged packets can degrade the performance of a device.

Per-Interface Statistics

Each time a packet is dropped or forwarded at an interface, that information is counted two ways: globally on the router and at each interface where you have applied Unicast RPF. Global statistics on dropped packets provide information about potential attacks on the network; however, these global statistics do not help to specify which interface is the source of the attack.

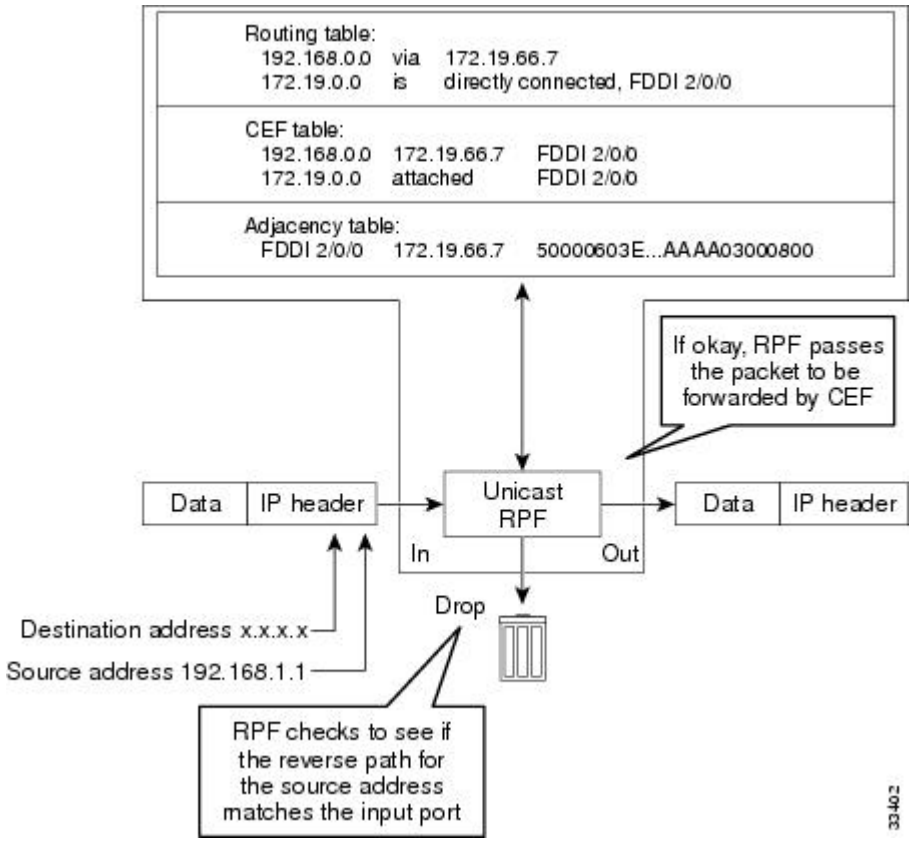
Per-interface statistics allow network administrators to track two types of information about malformed packets: Unicast RPF drops and Unicast RPF suppressed drops. Statistics on the number of packets that Unicast RPF drops help to identify the interface that is the entry point of the attack. The Unicast RPF drop count tracks the number of drops at the interface. The Unicast RPF suppressed drop count tracks the number of packets that failed the Unicast RPF check but were forwarded because of the permit permission set up in the ACL.

Using the drop count and suppressed drop count statistics, a network administrator can takes steps to isolate the attack at a specific interface.

Note Judicious use of ACL logging can further identify the address or addresses that are being dropped by Unicast RPF.

The figure below illustrates how Unicast RPF and CEF work together to validate IP source addresses by verifying packet return paths. In this example, a customer has sent a packet having a source address of 192.168.1.1 from interface FDDI 2/0/0. Unicast RPF checks the FIB to see if 192.168.1.1 has a path to FDDI 2/0/0. If there is a matching path, the packet is forwarded. If there is no matching path, the packet is dropped.

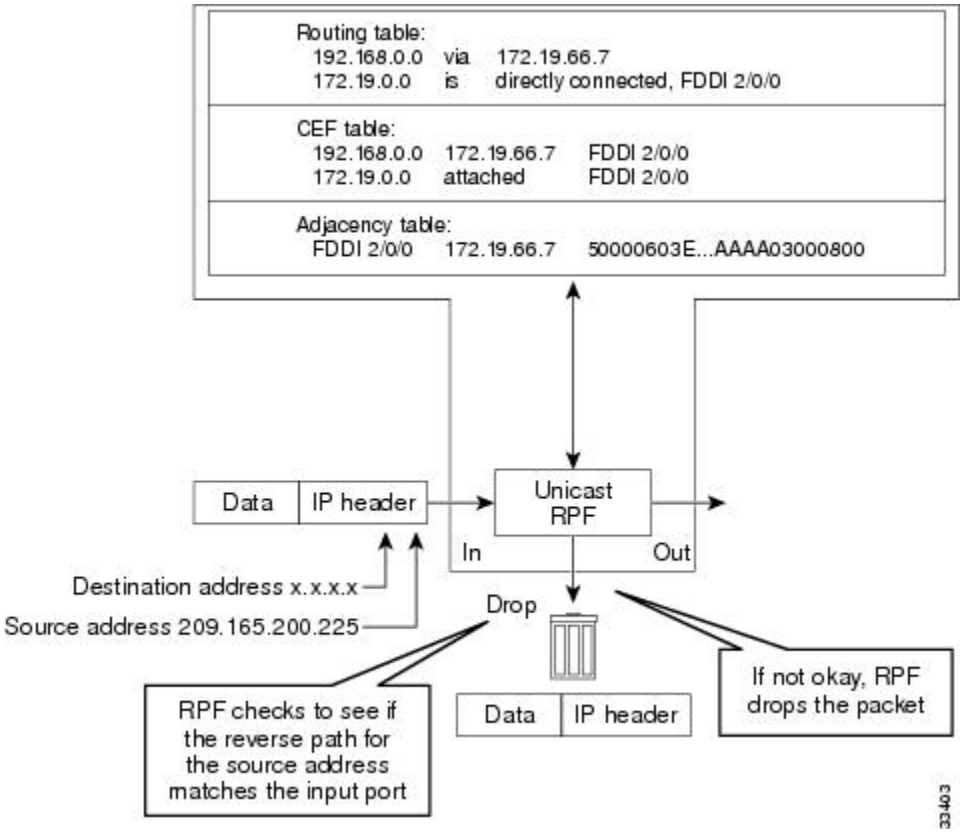
Figure 1: Unicast RPF Validating IP Source Addresses



The figure below illustrates how Unicast RPF drops packets that fail validation. In this example, a customer has sent a packet having a source address of 209.165.200.225, which is received at interface FDDI 2/0/0. Unicast RPF checks the FIB to see if 209.165.200.225 has a return path to FDDI 2/0/0. If there is a matching

path, the packet is forwarded. In this case, there is no reverse entry in the routing table that routes the customer packet back to source address 209.165.200.225 on interface FDDI 2/0/0, and so the packet is dropped.

Figure 2: Unicast RPF Dropping Packets That Fail Verification



How to Configure Unicast Reverse Path Forwarding ACL Support

Configuring Unicast RPF with ACL Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** *ipv6-address/prefix-length*
5. **ipv6 verify unicast source reachable-via** {**rx** | **any**} [*access-list*]
6. **end**
7. **show cef interface** [*type number*]
8. **show ipv6 traffic**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/1`	Configures an interface and enters interface configuration mode.
Step 4	**ipv6 address** *ipv6-address*/*prefix-length* **Example:** `Device(config-if)# ipv6 address 2001:DB8:1::1/96`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 5	**ipv6 verify unicast source reachable-via** {**rx** | **any**} [*access-list*] **Example:** `Device(config-if)# ipv6 verify unicast source reachable-via any acl1`	Verifies that a source address exists in the FIB table and enables Unicast RPF.
Step 6	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.
Step 7	**show cef interface** [*type number*] **Example:** `Device# show cef interface gigabitethernet 0/0/1`	Displays detailed Cisco Express Forwarding information for a specified interface or for all interfaces.
Step 8	**show ipv6 traffic** **Example:** `Device# show ipv6 traffic`	Displays statistics about IPv6 traffic.

Example:

The following is sample output from the **show cef interface gigabitethernet 0/0/1** command:

```
Device# show cef interface gigabitethernet 0/0/1

 GigabitEthernet0/0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C67D:4FFF:FEB6:E410
  No Virtual link-local address(es):
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FFB6:E410
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  Input features: Verify Unicast Reverse-Path
 IPv6 verify source reachable-via rx, ACL test
   0 verification drop(s) (process), 0 (CEF)
   0 suppressed verification drop(s) (process), 0 (CEF)
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

The following is sample output from the **show ipv6 traffic** command:

```
Device# show ipv6 traffic

 IPv6 statistics:
        Rcvd:  6 total, 0 local destination
               0 source-routed, 0 truncated
               0 format errors, 0 hop count exceeded
               0 bad header, 0 unknown option, 0 bad source
               0 unknown protocol, 0 not a router
               0 fragments, 0 total reassembled
               0 reassembly timeouts, 0 reassembly failures
        Sent:  34 generated, 28 forwarded
               0 fragmented into 0 fragments, 0 failed
               0 encapsulation failed, 0 no route, 0 too big
               0 RPF drops, 0 RPF suppressed drops
        Mcast: 6 received, 34 sent

ICMP statistics:
        Rcvd: 6 input, 0 checksum errors, 0 too short
              0 unknown info type, 0 unknown error type
              unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
                       0 sa policy, 0 reject route
              parameter: 0 error, 0 header, 0 option
              0 hopcount expired, 0 reassembly timeout,0 too big
              0 echo request, 0 echo reply
              0 group query, 0 group report, 0 group reduce
              0 router solicit, 0 router advert, 0 redirects
              0 neighbor solicit, 0 neighbor advert
        Sent: 34 output, 0 rate-limited
              unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
                       0 sa policy, 0 reject route
              parameter: 0 error, 0 header, 0 option
              0 hopcount expired, 0 reassembly timeout,0 too big
              0 echo request, 0 echo reply
              0 group query, 0 group report, 0 group reduce
              0 router solicit, 18 router advert, 0 redirects
              2 neighbor solicit, 2 neighbor advert
```

Configuration Examples for Unicast Reverse Path Forwarding ACL Support

Example: Configuring Unicast RPF with ACL Support

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# ipv6 address 2001:DB8:1::1/96
Device(config-if)# ipv6 verify unicast source reachable-via any acl1
Device(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Unicast RPF command descriptions	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
Cisco Express Forwarding commands	Cisco IOS IP Switching Command Reference

Standards & RFCs

Standard/RFC	Title
RFC 1918	*Address Allocation for Private Internets*
RFC 2267	*Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Unicast Reverse Path Forwarding ACL Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Unicast Reverse Path Forwarding ACL Support

Feature Name	Releases	Feature Information
Unicast Reverse Path Forwarding ACL Support	Cisco IOS XE Release 3.7S	The Unicast Reverse Path Forwarding feature helps to mitigate problems that are caused by malformed or forged IP source addresses that pass through a device. The Unicast Reverse Path Forwarding ACL support feature adds the ACL support to the Unicast Reverse Path Forwarding feature. With the ACL support, Unicast RPF can determine whether to drop or to forward data packets that have malformed or forged IP source addresses. The following commands were introduced or modified: **ip verify unicast source reachable-via** and **ipv6 verify unicast source reachable-via**.