

IPv6 Destination Guard

The IPv6 Destination Guard feature works with IPv6 neighbor discovery to ensure that the device performs address resolution only for those addresses that are known to be active on the link. It relies on the address glean functionality to populate all destinations active on the link into the binding table and then blocks resolutions before they happen when the destination is not found in the binding table.

- Prerequisites for IPv6 Destination Guard, on page 1
- Information About IPv6 Destination Guard, on page 1
- How to Configure the IPv6 Destination Guard, on page 2
- Configuration Examples for IPv6 Destination Guard, on page 3
- Additional References, on page 4
- Feature Information for Overview of Cisco TrustSec, on page 4

Prerequisites for IPv6 Destination Guard

- You should be familiar with the IPv6 Neighbor Discovery feature. For information about IPv6 neighbor discovery, see the “Implementing IPv6 Addressing and Basic Connectivity” module.
- You should be familiar with the IPv6 First-Hop Security Binding Table feature. For information, see the “IPv6 First-Hop Security Binding Table” module.

Information About IPv6 Destination Guard

IPv6 Destination Guard Overview

The IPv6 Destination Guard feature works with IPv6 neighbor discovery to ensure that the device performs address resolution only for those addresses that are known to be active on the link. It relies on the address glean functionality to populate all destinations active on the link into the binding table and then blocks resolutions before they happen when the destination is not found in the binding table.

Prior to filtering incoming routed traffic, the device gleans addresses on the link, by snooping Neighbor Discovery Protocol (NDP) and DHCP messages. When a packet reaches the device and there is not yet an adjacency for the destination or for the next hop, the NDP consults the device binding table to verify that the destination on link or the next-hop have been previously gleaned. If the destination is not found in the binding table, the packet is dropped. Otherwise, neighbor discovery resolution is performed.

How to Configure the IPv6 Destination Guard

Configuring IPv6 Destination Guard

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 destination-guard policy** *policy-name*
4. **enforcement** {**always** | **stressed**}
5. **exit**
6. **interface** *type number*
7. **ipv6 destination-guard attach-policy** [*policy-name*]
8. **exit**
9. **show ipv6 destination-guard policy** [*policy-name*]

DETAILED STEPS

Procedure

	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	**ipv6 destination-guard policy** *policy-name* **Example:** `Device(config)# ipv6 destination-guard policy pol1`	Defines the destination guard policy name and enters destination-guard configuration mode.
Step 4	**enforcement** {**always**	**stressed**} **Example:** `Device(config-destguard)# enforcement always`	Sets the enforcement level for the target address.
Step 5	**exit** **Example:**	Exits destination-guard configuration mode and returns to global configuration mode.

	Command or Action	Purpose
	`Device(config-destguard)# exit`	
Step 6	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/1`	Enters interface configuration mode.
Step 7	**ipv6 destination-guard attach-policy** [*policy-name*] **Example:** `Device(config-if)# ipv6 destination-guard attach-policy pol1`	Attaches a destination guard policy to an interface.
Step 8	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to privileged EXEC configuration mode.
Step 9	**show ipv6 destination-guard policy** [*policy-name*] **Example:** `Device# show ipv6 destination-guard policy pol1`	(Optional) Displays the policy configuration and all interfaces where the policy is applied.

Configuration Examples for IPv6 Destination Guard

Example: Configuring an IPv6 Destination Guard Policy

The following example shows how to configure a destination guard policy:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# ipv6 destination-guard attach-policy destination

Router# show ipv6 destination-guard policy destination
Destination guard policy Destination:
  enforcement always
        Target: Gi0/0/1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*

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 Overview of Cisco TrustSec

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 Overview of Cisco TrustSec

Feature Name	Releases	Feature Information
IPv6 enablement - Inline Tagging	Cisco IOS XE Fuji 16.8.1	The support for IPv6 is introduced.