Inbound Policy Marking for dVTI

This document provides conceptual information and tasks for using the Inbound Policy Marking for Dynamic Virtual Tunnel Interface feature, which allows you to attach a policy map to a dVTI so that marking instructions are applied to inbound packets.

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 at the end of this module.

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 Inbound Policy Marking for dVTI

- Policy map

Restrictions for Inbound Policy Marking for dVTI

The following are not supported:

- Policing
- Network Based Application Recognition (NBAR)-based classification
- Queuing
- Outbound policy marking

Only input QoS policy is supported. Only the marking feature is supported on the input policy. Other QoS configurations may not be blocked but will not be supported.

Information About Inbound Policy Marking for dVTI

Inbound Policy Marking

Marking is the setting of QoS information related to a packet. For the Inbound Policy Marking for dVTI feature, you can attach a policy map to a dVTI so that marking instructions are applied to inbound packets.

Dynamic Virtual Tunnel Interfaces Overview

DVTIs can provide highly secure and scalable connectivity for remote-access VPNs. The dVTI technology replaces dynamic crypto maps and the dynamic hub-and-spoke method for establishing tunnels.

DVTIs can be used for both the server and remote configuration. The tunnels provide an on-demand separate virtual access interface for each VPN session. The configuration of the virtual access interfaces is cloned from a virtual template configuration, which includes the IPsec configuration and any Cisco IOS XE software feature configured on the virtual template interface, such as QoS, NetFlow, or ACLs.

DVTIs function like any other real interface so that you can apply QoS, firewall, other security services as soon as the tunnel is active. QoS features can be used to improve the performance of various applications across the network. Any combination of QoS features offered in Cisco IOS XE software can be used to support voice, video, or data applications.

DVTIs provide efficiency in the use of IP addresses and provide secure connectivity. DVTIs allow dynamically downloadable per-group and per-user policies to be configured on a RADIUS server. The per-group or per-user definition can be created using extended authentication (Xauth) User or Unity group, or it can be derived from a certificate. DVTIs are standards based, so interoperability in a multiple-vendor environment is supported. IPsec dVTIs allow you to create highly secure connectivity for remote access VPNs and can be combined with Cisco Architecture for Voice, Video, and Integrated Data (AVVID) to deliver converged voice, video, and data over IP networks. The dVTI simplifies VPN routing and forwarding (VRF)-aware IPsec deployment. The VRF is configured on the interface.

A dVTI requires minimal configuration on the router. A single virtual template can be configured and cloned.

The dVTI creates an interface for IPsec sessions and uses the virtual template infrastructure for dynamic instantiation and management of dynamic IPsec VTIs. The virtual template infrastructure is extended to create dynamic virtual-access tunnel interfaces. DVTIs are used in hub-and-spoke configurations.

In Cisco IOS XE Release 3.4S, support for the following was added:

- Maximum of 2000 dynamic tunnels with QoS applied
- Maximum of 4000 dynamic tunnels (2000 with QoS, 2000 without QoS)
- dVTI QoS LLQ for high-speed access egress shaping with overhead accounting and queuing

Security Associations and dVTI

Security Associations (SAs) are security policy instances and keying material applied to a data flow. IPSec SAs are unidirectional and unique in each security protocol. You need multi SAs for a protected data pipe, one per direction per protocol. The Inbound Policy Marking for dVTI feature uses multi SAs. It enables multiple specific-to-specific SAs to link to one dVTI tunnel.

How to Use Inbound Policy Marking for dVTI

To use the Inbound Policy Marking for dVTI feature, first create a policy map. After creating the policy map, attach it to an interface.

Creating a Policy Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class {class-name | class-default}**
5. **set ip dscp** *ip-dscp-value*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map p-map`	Enters QoS policy-map configuration mode and creates a policy map that can be attached to one or more interfaces to specify a service policy,
Step 4	**class {class-name | class-default}** **Example:** `Router(config-pmap)# class class-default`	Specifies the default class so that you can configure or modify its policy.
Step 5	**set ip dscp** *ip-dscp-value* **Example:** `Router(config-pmap-c)# set ip dscp af21`	Marks a packet by setting the IP differentiated services code point (DSCP) value in the type of service (ToS) byte.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Returns to privileged EXEC mode.

Attaching a Policy Map to a dVTI

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **policy-map** [**type** {**control** | **service**}] *policy-map-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1 type tunnel`	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 4	**policy-map** [**type** {**control** | **service**}] *policy-map-name* **Example:** `Router(config)# policy-map input policy1`	Enters QoS policy-map configuration mode and attaches this policy map to the interface.
Step 5	**end** **Example:** `Router(config-pmap-c)# end`	Returns to privileged EXEC mode.

Configuration Example for Inbound Policy Marking for dVTI

Example 1

```
class-map match-any RT
  match ip dscp cs5  ef
!
class-map match-any DATA
  match ip dscp cs1 cs2 af21 af22
!
policy-map CHILD
  class RT
    priority
    police 200000
      conform-action transmit exceed-action drop violate-action drop
```

```
  class DATA
    bandwidth remaining percent 100
!
policy-map PARENT
  class class-default
   shape average 1000000 account user-defined xx
   service-policy CHILD
!
interface Virtual-Template 1 type tunnel
  ip vrf forwarding Customer1
  service-policy output PARENT
```

Example 2 Configuring Inbound Policy Marking

This shows an example configuration of the hub side of dVTI:

```
aaa new-model
!
aaa authentication login default local
aaa authorization network default local
!
aaa session-id common
!
policy-map pm1
class class-default
  shape average 1280000
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
!
crypto isakmp key cisco123 address 192.0.2.1
crypto isakmp keepalive 10
!
crypto isakmp client configuration group cisco
  key cisco
  dns 198.51.100.1
  wins 203.0.113.1
  domain cisco.com
  pool dpool
  acl 101
!
crypto isakmp profile vi
   match identity group cisco
   isakmp authorization list default
   client configuration address respond
   virtual-template 1
!
crypto ipsec transform-set trans-set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
  set transform-set trans-set
  set isakmp-profile vi
!
interface FastEthernet0/0
  ip address 203.0.113.254 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 203.0.113.255 255.255.255.0
  duplex auto
  speed 100
!
interface Virtual-Template1 type tunnel
  ip unnumbered FastEthernet0/0
  tunnel source FastEthernet0/0
  tunnel mode ipsec ipv4
```

```
  tunnel protection ipsec profile vi
  service-policy output pm1
!
router eigrp 1
  network 192.168.1.0
  network 1.0.0.0
  no auto-summary
!
ip local pool dpool 192.0.2.1 192.0.2.254
ip route 198.51.100.1 198.51.100.254
!
access-list 101 permit ip 192.168.1.0 255.255.255.0 any
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping
Classifying Network Traffic	"Classifying Network Traffic" module
Marking Network Traffic	"Marking Network Traffic" module

Standards and RFCs

Standard/RFC	Title
RFC 2474	*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
RFC 2475	*An Architecture for Differentiated Services Framework*
RFC 2597	*Assured Forwarding PHB*
RFC 2598	*An Expedited Forwarding PHB*
RFC 2697	*A Single Rate Three Color Marker*
RFC 2698	*A Two Rate Three Color Marker*

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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 Using Inbound Policy Marking for dVTI

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 Inbound Policy Marking for dVTI

Feature Name	Releases	Feature Information
Inbound Policy Marking for dVTI	Cisco IOS XE Release 3.2S	The Inbound Policy Marking for dVTI feature allows you to attach a policy map to a dVTI so that marking instructions are applied to inbound packets. In Cisco IOS XE Release 3.2S, support was added for the Cisco ASR 10000. In Cisco IOS XE Release 3.4S, support for the following was added: • Maximum of 2000 dynamic tunnels with QoS applied • Maximum of 4000 dynamic tunnels (2000 with QoS, 2000 without QoS) • dVTI QoS LLQ for high-speed access egress shaping with overhead accounting and queuing The following sections provide information about this feature: