



Inbound Policy Marking for dVTI

Last Updated: July 11, 2012

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, page 1](#)
- [Prerequisites for Inbound Policy Marking for dVTI, page 1](#)
- [Restrictions for Inbound Policy Marking for dVTI, page 1](#)
- [Information About Inbound Policy Marking for dVTI, page 2](#)
- [How to Use Inbound Policy Marking for dVTI, page 3](#)
- [Configuration Example for Inbound Policy Marking for dVTI, page 5](#)
- [Additional References, page 7](#)
- [Feature Information for Using Inbound Policy Marking for dVTI, page 8](#)

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:



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- 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, page 2](#)
- [Dynamic Virtual Tunnel Interfaces Overview, page 2](#)
- [Security Associations and dVTI, page 3](#)

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, page 3](#)
- [Attaching a Policy Map to a dVTI, page 4](#)

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. <ul style="list-style-type: none">• Enter your password if prompted. |
| Step 2 configure terminal Example: Router# configure terminal | Enters global configuration mode. |

| Command or Action | Purpose |
|---|---|
| Step 3 <code>policy-map <i>policy-map-name</i></code> Example: <code>Router(config)# policy-map p-map</code> | 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 <code>class {class-name class-default}</code> Example: <code>Router(config-pmap)# class class-default</code> | Specifies the default class so that you can configure or modify its policy. |
| Step 5 <code>set ip dscp <i>ip-dscp-value</i></code> Example: <code>Router(config-pmap-c)# set ip dscp af21</code> | Marks a packet by setting the IP differentiated services code point (DSCP) value in the type of service (ToS) byte. |
| Step 6 <code>end</code> Example: <code>Router(config-pmap-c)# end</code> | 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 <code>enable</code> Example: <code>Router> enable</code> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |

| Command or Action | Purpose |
|--|--|
| Step 2 <code>configure terminal</code> Example: Router# <code>configure terminal</code> | Enters global configuration mode. |
| Step 3 <code>interface virtual-template number</code> Example: Router(config)# <code>interface virtual-template 1 type tunnel</code> | Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces. |
| Step 4 <code>policy-map [type {control service}] policy-map-name</code> Example: Router(config)# <code>policy-map input policy1</code> | Enters QoS policy-map configuration mode and attaches this policy map to the interface. |
| Step 5 <code>end</code> Example: Router(config-pmap-c)# <code>end</code> | 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 pml
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 pml
!
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 |
|--------------------|--|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| QoS commands | <i>Cisco IOS QoS Command Reference</i> |

Standards

| Standard | Title |
|---|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

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 XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

RFCs

| RFC | Title |
|---|-------|
| No RFCs were created or modified to support this feature. | -- |

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 | <p>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.</p> <p>In Cisco IOS XE Release 3.2S, support was added for the Cisco ASR 10000.</p> <p>In Cisco IOS XE Release 3.4S, support for the following was added:</p> <ul style="list-style-type: none"> • 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 <p>The following sections provide information about this feature:</p> |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.