# dVTI 用インバウンド ポリシー マーキング

このマニュアルでは、ダイナミック仮想トンネル インターフェイス用インバウンド ポリシー マーキング機能の使用に関する概念情報と作業について説明します。この機能を使用すれば、マーキング指示が受信パケットに適用されるようにポリシー マップを dVTI に適用できます。



## 機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

# dVTI 用インバウンド ポリシー マーキングの前提条件

- ポリシー マップ

# dVTI 用インバウンド ポリシー マーキングの制約事項

次はサポートされていません。

- ポリシング
- Network Based Application Recognition（NBAR）ベースの分類
- Queuing
- アウトバウンド ポリシー マーキング

入力 QoS ポリシーだけがサポートされます。 入力ポリシーに対して、マーキング機能だけがサポートされます。 他の QoS 設定はブロックされない可能性もありますが、サポートがされることはありません。

# dVTI 用インバウンド ポリシー マーキングに関する情報

## インバウンド ポリシー マーキング

マーキングとは、パケットに関連した QoS 情報の設定です。 dVTI 用インバウンド ポリシー マーキング機能では、マーキング指示が受信パケットに適用されるようにポリシー マップを dVTI に適用できます。

## ダイナミック仮想トンネル インターフェイスの概要

DVTI によって、リモートアクセス VPN 用接続のセキュリティ保護とスケーラビリティが向上します。 dVTI テクノロジーは、ダイナミック クリプト マップとトンネルを確立するためのダイナミック ハブアンドスポーク方式にとって代わるものです。

DVTI は、サーバと、リモート設定の両方に対して使用可能です。 トンネルにより、各 VPN セッションに対して、仮想アクセスインターフェイスがオンデマンドで個別に提供されます。 仮想アクセス インターフェイス設定は、仮想テンプレート設定からコピーされます。このコピーには、IPsec 設定と、QoS、NetFlow、ACL といった、仮想テンプレート インターフェイス上で設定されたすべての Cisco IOS XE ソフトウェア機能が含まれています。

DVTI は、他の現実のインターフェイスと同様に機能するので、トンネルがアクティブになるのと同時に、QoS、ファイアウォール、およびその他セキュリティ サービスを適用できます。 QoS 機能を使用して、ネットワーク上の各種アプリケーションのパフォーマンスを向上させることが可

能です。 Cisco IOS XE ソフトウェア内で提供される各種 QoS 機能の組み合わせを使用して、音声、ビデオ、またはデータ アプリケーションをサポートできます。

DVTI によって、IP アドレスを効率的に使用できるようになり、また、セキュアな接続を実現できます。 DVTIによって、動的にダウンロード可能な、グループごとおよびユーザごとのポリシーをRADIUSサーバ上で設定できます。 グループごとまたはユーザごとの定義を、拡張認証（Xauth）UserまたはUnityグループを使用して作成するか、証明書から取得できます。 DVTIは、標準ベースです。そのため、複数のベンダー環境における相互運用性がサポートされます。 IPsec dVTI を使用すれば、リモート アクセス VPN 用のセキュリティ保護が強化された接続を作成できます。また、Cisco Architecture for Voice, Video, and Integrated Data（AVVID）と組み合わせて、IP ネットワーク経由で集約された音声、ビデオ、およびデータを転送できます。 dVTI は VPN ルーティングおよび転送（VRF）対応 IPsec の導入を容易にします。 VRF は、インターフェイス上で設定されます。

dVTIには、ルータ上での最小限の設定が必要です。 単一の仮想テンプレートを設定およびコピーできます。

dVTI によって、IPsec セッション用のインターフェイスが作成され、ダイナミック IPsec VTI の動的なインスタンス化および管理のための仮想テンプレート インフラストラクチャが使用されます。 仮想テンプレート インフラストラクチャは、ダイナミック仮想アクセス トンネル インターフェイスを作成するために拡張されます。 DVTI は、ハブアンドスポーク設定で使用されます。

Cisco IOS XE Release 3.4S で、次のサポートが追加されました。

- QoS が適用された最大 2000 のダイナミック トンネル
- 最大 4000 のダイナミック トンネル（QoS ありの 2000 と QoS なしの 2000）
- オーバーヘッドアカウンティングとキューイングを使用した高速アクセス出力シェーピング用 dVTI LLQ QoS

## セキュリティ アソシエーションと dVTI

セキュリティ アソシエーション（SA）は、セキュリティ ポリシー インスタンスであり、データフローに適用される鍵素材です。 IPsec SA は単方向で、セキュリティ プロトコルごとに一意です。 保護されたデータ パイプには、複数のSAが必要です（プロトコルと方向ごとに1つずつ）。 dVTI 用インバウンド ポリシー マーキング機能はマルチ SA を使用します。 この機能を使用すると、複数の個別 SA が 1 つの dVTI トンネルにリンクできます。

# dVTI 用インバウンド ポリシー マーキングの使用方法

dVTI 用インバウンド ポリシー マーキング機能を使用するには、先にポリシー マップを作成します。 ポリシー マップを作成したら、それをインターフェイスに適用します。

# ポリシー マップの作成

## 手順の概要

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**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br><br>例：<br>`Router# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **policy-map** *policy-map-name*<br><br>例：<br>`Router(config)# policy-map p-map` | QoS ポリシーマップ コンフィギュレーション モードを開始し、サービス ポリシーを指定するために 1 つ以上のインターフェイスに適用可能なポリシーマップを作成します。 |
| ステップ 4 | **class {class-name \| class-default}**<br><br>例：<br>`Router(config-pmap)# class class-default` | ポリシーを設定または変更できるようデフォルト クラスを指定します。 |
| ステップ 5 | **set ip dscp** *ip-dscp-value*<br><br>例：<br>`Router(config-pmap-c)# set ip dscp af21` | タイプ オブ サービス（ToS）バイトに IP DiffServ コードポイント（DSCP）値を設定することによってパケットをマーキングします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **end**<br><br>例：<br>`Router(config-pmap-c)# end` | 特権 EXEC モードに戻ります。 |

# ポリシー マップの dVTI への適用

## 手順の概要

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

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br><br>例：<br>`Router# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface virtual-template** *number*<br><br>例：<br>`Router(config)# interface virtual-template 1 type tunnel` | 仮想アクセスインターフェイスの作成時にダイナミックに設定および適用される仮想テンプレートインターフェイスを作成します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 4 | **policy-map** [**type** {**control** \| **service**}] *policy-map-name*<br><br>例：<br><br>`Router(config)# policy-map input policy1` | QoS ポリシーマップ コンフィギュレーション モードを開始して、このポリシーマップをインターフェイスに適用します。 |
| ステップ 5 | **end**<br><br>例：<br><br>`Router(config-pmap-c)# end` | 特権 EXEC モードに戻ります。 |

# dVTI 用インバウンド ポリシー マーキングの設定例

## 例 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
```

## 例 2：入力ポリシー マーキングの設定

dVTI のハブ側の設定例を示します。

```
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
```

# その他の関連資料

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| IPv6 アドレッシングと接続 | 『*IPv6 Configuration Guide*』 |
| Cisco IOS コマンド | 『Cisco IOS Master Commands List, All Releases』 |
| IPv6 コマンド | 『Cisco IOS IPv6 Command Reference』 |
| Cisco IOS IPv6 機能 | 『Cisco IOS IPv6 Feature Mapping』 |
| ネットワーク トラフィックの分類 | 「Classifying Network Traffic」モジュール |
| ネットワーク トラフィックのマーキング | 「Marking Network Traffic」モジュール |

### 規格および RFC

| 規格/RFC | タイトル |
|---|---|
| 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*』 |
| IPv6 に関する RFC | IPv6 RFCs |

### MIB

| MIB | MIB のリンク |
|---|---|
| この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。 | 選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。<br>http://www.cisco.com/go/mibs |

### テクニカル サポート

| 説明 | リンク |
|---|---|
| 右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。 | http://www.cisco.com/cisco/web/support/index.html |

# dVTI用インバウンドポリシーマーキングの使用に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *1*：*dVTI* 用インバウンド ポリシー マーキングの機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| dVTI 用インバウンド ポリシー マーキング | Cisco IOS XE Release 3.2S | dVTI 用インバウンド ポリシー マーキング機能を使用すれば、マーキング指示が受信パケットに適用されるようにポリシー マップを dVTI に適用できます。<br>Cisco IOS XE Release 3.2S で、Cisco ASR 10000 のサポートが追加されました。<br>Cisco IOS XE Release 3.4S で、次のサポートが追加されました。<br>• QoS が適用された最大 2000 のダイナミック トンネル<br>• 最大 4000 のダイナミック トンネル（QoS ありの 2000 と QoS なしの 2000）<br>• オーバーヘッド アカウンティングとキューイングを使用した高速アクセス出力シェーピング用 dVTI LLQ QoS<br>この機能に関する詳細については、次の各項を参照してください。 |