TrustSec DMVPN インライン タギング サポートの設定

TrustSec DMVPN インライン タギング サポート機能により、IPsec は Cisco TrustSec（CTS）セキュリティ グループ タグ（SGT）を IPsec ピア間で伝送できます。

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、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、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。

TrustSec DMVPN インライン タギング サポートの設定の前提条件

インターネット キー交換バージョン 2（IKEv2）および IPsec をルータで設定する必要があります。詳細については、「Configuring Internet Key Exchange Version 2 and FlexVPN Site-to-Site」および「Configuring Security for VPNs with IPsec」の章を参照してください。

この機能は、Cisco ISR G2 890、1900、2900、3900、および 3900E ルータでのみサポートされています。

TrustSec DMVPN インライン タギング サポートの設定に関する制約事項

TrustSec DMVPN インライン タギング サポート機能は IKEv2 でのみネゴシエート可能で、IKEv2 を使用して次をサポートします。

- DMVPN
- ダイナミック仮想トンネル インターフェイス（dVTI）
- トンネル保護を使用した GRE
- サイト間 VPN
- スタティック クリプト マップ
- スタティック仮想トンネル インターフェイス（sVTI）

TrustSec DMVPN インライン タギング サポート機能は、次をサポートしません。

- Cisco AnyConnect
- Cisco VPNClient
- IKEv1 を使用した DMVPN
- EasyVPN
- FlexVPN
- GetVPN
- IKEv1 IPsec メソッド
- SSLVPN

TrustSec DMVPN インライン タギング サポートの設定について

Cisco TrustSec

Cisco TrustSec（CTS）アーキテクチャでは、ID、信頼性、およびポリシーを組み合わせ、ユーザトランザクションを保護してロールベースのポリシーを適用することで、信頼できるネットワーク デバイスのドメインを確立し、セキュアなネットワークを構築できます。CTS は認証時に取得したユーザとデバイスの ID 情報を使用して、ネットワークに進入するパケットを分類します。CTS では、CTS ネットワークへの進入時にパケットにタグを付けることで各パケットの分類が維持されます。これにより、パケットはデータ パス全体を通じて正しく識別され、セキュリティおよびその他のポリシー基準が適用されます。パケットまたはフレームは、スイッチやファイアウォールなどのネットワーク中継を可能にするセキュリティ グループ タグ（SGT）を使用してタグ付けされ、分類に基づいてアクセス コントロール ポリシーが適用されます。

TrustSec の IPsec インライン タギング機能は、SGT を他のネットワーク デバイスに伝播する際に使用します。

（注） この機能がサポートされていない場合は、SGT Exchange Protocol over TCP（SXP）機能を使用できます。

CTS および SXP の詳細については、『Cisco TrustSec Switch Configuration Guide』を参照してください。

SGT および IPsec

IPsec はアルゴリズム、キー、および機能のネゴシエーションに IKE プロトコルを使用します。IKEv2 は、IPSec のネゴシエーションと SGT 機能に関する通知に使用されます。ピアで SGT タギング機能が認識されると、SGT タグ番号（16 ビット）が SGT Cisco メタデータ（CMD）ペイロードとして IPsec に追加され、受信側のピアに送信されます。

アクセス レイヤ デバイスが着信パケットを認証します。アクセス レイヤ デバイスは認証サーバから SGT を受信し、IP アドレスと SGT を着信パケットに割り当てます。つまり、IP アドレスを SGT にバインドします。この IP アドレスと SGT のバインディングがアップストリーム デバイスに伝搬され、SGT ベースのポリシーとインライン タギングが適用されます。

発信側で IKEv2 が SGT 機能をネゴシエートするように設定されている場合、発信側は SA_INIT 要求で SGT 機能情報を提示します。応答側で IKEv2 が SGT 機能をネゴシエートするように設定されている場合、応答側が SA_INIT 応答で確認応答し、発信側と応答側はピアへのすべてのパケットに対してインライン タギングを使用することを IPsec に通知します。

ピアでインライン タギングがサポートされている場合、出力時に IPsec は SGT 機能とプレフィクスを IPsec ペイロードに追加します。サポートされていない場合、パケットはタグ付けされません。

入力時に、IPsec は SGT 機能についてパケットを検査します。タグが使用可能な場合、IPsec はタグ情報を取得してデバイスに情報を渡します（インライン タギングがネゴシエートされる場合のみ）。タグがないパケットは、IPsec によって通常のパケットとして処理されます。

次の表で、出力および入力時の IPsec の動作について説明します。

表 *1*：出力パスでの *IPsec* の動作

インライン タギングのネゴシエーション	CTS による SGT の提供	IPsec の動作
Yes	Yes	SGT CMD をパケットに追加します。
Yes	No	SGT CMD を追加せずにパケットを送信します。
No	Yes または No	SGT CMD を追加せずにパケットを送信します。

表 *2*：入力パスでの *IPsec* の動作

パケットのタグ付け	インライン タギングのネゴシエーション	IPsec の動作
Yes	Yes	パケットの SGT CMD を処理します。
Yes	No	パケットの SGT CMD を処理しません。
No	Yes または No	パケットを通常の IPsec パケットとして処理します。

IKEv2 の発信側と応答側での SGT

IKEv2 セッションで SGT をイネーブルにするには、**crypto ikev2 cts** コマンドを使用して SGT 機能サポートをピアに送信する必要があります。SGT はシスコ独自の機能です。したがって、SA_INIT 交換ではベンダー ID（VID）ペイロードとして送信されます。

次の表で、SGT 機能が発信側と応答側で設定されているシナリオについて説明します。

表 *3* : *IKEv2* の発信側と応答側の *SGT* 機能

SGT が発信側でイネーブル	SGT が応答側でイネーブル	動作..
Yes	Yes	発信側と応答側の間で VID が交換され、SGT インライン タギング機能で IPsec SA がイネーブルになります。
Yes	No	発信側は VID を提示しますが、応答側は VID を無視します。IPsec SA は SGT インライン タギング機能でイネーブルになりません。
No	Yes	発信側は VID を提示せず、応答側は VID ペイロードを送信しません。IPsec SA は SGT インラインタギング機能でイネーブルになりません。
No	No	発信側は VID を提示せず、応答側も VID ペイロードを送信しません。IPsec SA は SGT インラインタギング機能でイネーブルになりません。

フラグメンテーションの処理

フラグメンテーションは、次の 2 つの方法で処理されます。

- IPsec 前のフラグメンテーション：IPsec がフラグメント化されたパケットを受信すると、各フラグメントがタグ付けされます。
- IPsec 後のフラグメンテーション：IPsec パケットが暗号化後にフラグメント化された場合、最初のフラグメントがタグ付けされます。

TrustSec DMVPN インライン タギング サポートの設定方法

IPsec インライン タギングのイネーブル化

はじめる前に

IKEv2 および IPsec を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sgt inline**
4. **exit**

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** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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** 例： `Device# 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	**cts sgt inline** 例： `Device(config)# cts sgt inline`	DMVPN の TrustSec をイネーブルにします。このコマンドは、総称ルーティング カプセル化（GRE）とトンネル インターフェイス モードに対してのみ有効です。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

TrustSec DMVPN インライン タギング サポートのモニタリングと確認

TrustSec DMVPN インライン タギング サポート設定をモニタおよび確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show dmvpn**
3. **show ip nhrp nhs detail**
4. **show tunnel endpoints**
5. **show adjacency***interface-type interface-number* **detail**

手順の詳細

ステップ 1 enable

例：
```
Device> enable
```
特権 EXEC モードをイネーブルにします。

ステップ 2 show dmvpn

例：
```
Device# show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 1.1.1.99              10.1.1.99    UP 00:00:01    SC
```
Dynamic Multipoint VPN（DMVPN）固有のセッション情報を表示するには、このコマンドを使用します。

ステップ 3 show ip nhrp nhs detail

例：
```
Device# show ip nhrp nhs detail

Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
10.1.1.99  RE NBMA Address: 1.1.1.99 priority = 0 cluster = 0  req-sent 44  req-failed 0  repl-recv
 43 (00:01:37 ago)
 TrustSec Enabled
```

Next Hop Resolution Protocol（NHRP）ネクスト ホップ サーバ（NHS）情報を表示するには、このコマンドを使用します。

ステップ 4 **show tunnel endpoints**

例：

```
Device# show tunnel endpoints

 Tunnel0 running in multi-GRE/IP mode

 Endpoint transport 1.1.1.99 Refcount 3 Base 0xF3FB79B4 Create Time 00:03:15
   overlay 10.1.1.99 Refcount 2 Parent 0xF3FB79B4 Create Time 00:03:15
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 1 entries; TrustSec enabled
```

マルチポイント総称ルーティング カプセル化（mGRE）モードでトンネルを実行している場合に、トンネル エンドポイントのアドレス解決に使用されるトンネル エンドポイント データベースの内容を表示するには、このコマンドを使用します。

ステップ 5 **show adjacency***interface-type interface-number* **detail**

例：

```
Device# show adjaceny tunnel0 detail

Protocol Interface                 Address
IP       Tunnel0                   10.1.1.99(2)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 1
                                   Encap length 32
                                   4500000000000000FF2FB76901010101
                                   0101016300008909080001010001000 0
                                   Tun endpt
                                   Next chain element:
.
.
.
```

プロトコルに関する情報を表示するには、このコマンドを使用します。

TrustSec DMVPN インライン タギング サポートの設定例

例：IPsec インライン タギングのイネーブル化

次の例では、スタティック VTI の発信側とダイナミック VTI の応答側で IPsec インライン タギングをイネーブルにする方法を示します。この設定を使用してクリプト マップおよび VTI を設定できます。

スタティック VTI の発信側の設定

```
crypto ikev2 proposal p1
 encryption 3des
 integrity md5
```

```
 group 2
!
crypto ikev2 policy policy1
 proposal p1
!
crypto ikev2 keyring key
 peer peer
  address ::/0
  pre-shared-key cisco
 !
 peer v4
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !
!
!
crypto ikev2 profile prof3
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring key
!
crypto ikev2 cts sgt
!
crypto ipsec transform-set trans esp-3des esp-sha-hmac
!
crypto map cmap 1 ipsec-isakmp
 set peer 10.1.1.2
 set transform-set trans
 set ikev2-profile prof3
 match address ipv4acl
!
!
interface Loopback1
 ip address 209.165.201.1 255.255.255.224
 ipv6 address 2001::4:1/112
!
interface Loopback2
 ip address 209.165.200.1 255.255.255.224
 ipv6 address 2001::40:1/112
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.210.74 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.0.1 255.240.0.0
 duplex auto
 speed auto
 ipv6 address 2001::5:1/112
 ipv6 enable
 crypto map cmap
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 172.16.0.2
ip route 10.12.255.200 255.0.0.0 172.31.255.254
!
ip access-list extended ipv4acl
 permit ip host 209.165.201.1host 192.168.12.125
 permit ip host 209.165.200.1 host 172.18.0.1
 permit ip host 172.28.0.1 host 10.10.10.1
 permit ip host 10.12.255.200 host 192.168.14.1
!
logging esm config
```

```
ipv6 route ::/0 2001::5:2
!
!
!
!
!!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
```

ダイナミック VTI の応答側の設定

```
crypto ikev2 proposal p1
 encryption 3des
 integrity md5
 group 2
!
crypto ikev2 policy policy1
 proposal p1
!
crypto ikev2 keyring key
 peer peer
  address 172.160.1.1 255.240.0.0
  pre-shared-key cisco
 !
 peer v4_p2
  address 172.31.255.1 255.240.0.0
  pre-shared-key cisco
 !
crypto ikev2 profile prof
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring key
 virtual-template 25
!
crypto ikev2 cts sgt
!
crypto ipsec transform-set trans esp-null esp-sha-hmac
!
crypto ipsec profile prof_ipv4
 set transform-set trans
 set ikev2-profile prof1_ipv4
!
!
interface Loopback0
 ip address 192.168.12.1 255.255.0.0
!
interface Loopback1
 no ip address
!
interface Loopback2
 ip address 172.18.0.1 255.240.0.0
!
```

```
interface Loopback10
 no ip address
 ipv6 address 2001::8:1/112
!
interface Loopback11
 no ip address
 ipv6 address 2001::80:1/112
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 10.1.1.2 255.0.0.0
 duplex auto
 speed auto
 ipv6 address 2001::7:1/112
 ipv6 enable
!
interface GigabitEthernet0/1
 ip address 10.10.10.2 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 192.168.210.144 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/0/0
 no ip address
 shutdown
!
interface FastEthernet0/0/1
 no ip address
!
interface FastEthernet0/0/2
 no ip address
!
interface FastEthernet0/0/3
 no ip address
!
!
interface Virtual-Template25 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile prof_ipv4
!
interface Vlan1
 no ip address
!
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 172.17.0.0 255.240.0.0 10.10.10.1
!
logging esm config
ipv6 route ::/0 2001::7:2
!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line 2
 no activation-character
 no exec
```

```
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

TrustSec DMVPN インライン タギング サポートの参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『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 TrustSec および SXP の設定	『Cisco TrustSec Switch Configuration Guide』
IPsec の設定	*IPsec* を使用した *VPN* のセキュリティの設定
IKEv2 の設定	『*Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site*』
Cisco Secure Access Control Server	Cisco Secure ACS のコンフィギュレーション ガイド

シスコのテクニカル 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

TrustSec DMVPN インライン タギング サポートの機能情報

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、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 リリースだけを示しています。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 *4*：*TrustSec DMVPN* インライン タギング サポートの設定に関する機能情報

機能名	リリース	機能情報
TrustSec DMVPN インライン タギング サポート	Cisco IOS XE Release 3.13S	TrustSec DMVPN インライン タギング サポート機能により、IPsec は Cisco TrustSec（CTS）セキュリティ グループ タグ（SGT）を IPsec ピア間で伝送できます。 次のコマンドが導入または変更されました。**cts sgt inline**、**show dmvpn**、**show ip nhrp nhs**、**show tunnel endpoints**、**show adjacency**