Configuring TrustSec DMVPN Inline Tagging Support

The TrustSec DMVPN Inline Tagging Support feature enables IPsec to carry the Cisco TrustSec (CTS) Security Group Tag (SGT) between IPsec peers.

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.

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 Configuring TrustSec DMVPN Inline Tagging Support

Internet Key Exchange Version 2 (IKEv2) and IPsec must be configured on the router. For more information, see the "*Configuring Internet Key Exchange Version 2 and FlexVPN Site-to-Site*" and "*Configuring Security for VPNs with IPsec*" modules.

Restrictions for Configuring TrustSec DMVPN Inline Tagging Support

The TrustSec DMVPN Inline Tagging Support feature via IKEv2 supports the following:

- Dynamic Virtual Tunnel Interface (dVTI)
- GRE with Tunnel Protection
- Site-to-site VPNs
- Static crypto maps
- Static Virtual Tunnel Interface (sVTI)

The TrustSec DMVPN Inline Tagging Support feature does not support the following:

- Cisco AnyConnect
- Cisco VPNClient
- DMVPN with IKEv1
- EasyVPN
- FlexVPN
- GetVPN
- IKEv1 IPsec methods
- SSLVPN

crypto ikev2 cts sgt and **cts sgt inline** commands on tunnel are two different features. Do not configure these two features together as it causes the packets getting tagged twice.

cts sgt inline command does not rely on crypto or IKEv2. It can be configured statically or by NHRP. **cts sgt inline** command works with DMVPN IPSEC tunnel and also in transport mode.

The TrustSec DMVPN Inline Tagging Support feature via the **cts sgt inline** command is supported on all combinations of DMVPN (IKEv1, IKEv2, non-crypto, crypto accelerators such as ISM-VPN, point-to-point, multipoint) except when running MPLS (as an MPLS cloud extension or as MPLS L3VPN) over DMVPN.

Information About Configuring TrustSec DMVPN Inline Tagging Support

Cisco TrustSec

The Cisco TrustSec (CTS) architecture helps to build secure networks by establishing a domain of trusted network devices by combining identity, trust, and policy to protect user transactions and enforce role-based policies. CTS uses the user and the device identification information acquired during the authentication phase

to classify packets as they enter the network. CTS maintains a classification of each packet by tagging packets on ingress to the CTS network so that they can be properly identified for applying security and other policy criteria along the data path. The packets or frames are tagged using the Security Group Tag (SGT), which allows network intermediaries such as switches and firewalls, to enforce an access control policy based on the classification.

The IPsec Inline Tagging for TrustSec feature is used to propagate the SGT to other network devices.

Note If this feature is not supported, you can use the SGT Exchange Protocol over TCP (SXP) feature.

For more information on CTS and SXP, see the *Cisco TrustSec Switch Configuration Guide*.

SGT and IPsec

IPsec uses the IKE protocol for negotiating algorithms, keys, and capabilities. IKEv2 is used to negotiate and inform IPsec about the SGT capability. Once the peers acknowledge the SGT tagging capability, an SGT tag number (a 16-bit) is added as the SGT Cisco Meta Data (CMD) payload into IPsec and sent to the receiving peer.

The access layer device authenticates the incoming packets. The access layer device receives an SGT from the authentication server and assigns the SGT along with an IP address to the incoming packets. In other words, an IP address is bound to an SGT. This IP address/SGT binding is propagated to upstream devices to enforce SGT-based policy and inline tagging.

If IKEv2 is configured to negotiate the SGT capability in the initiator, the initiator proposes the SGT capability information in the SA_INIT request. If IKEv2 is configured to negotiate the SGT capability in the responder, the responder acknowledges in the SA_INIT response and the initiator and the responder inform IPsec to use inline tagging for all packets to the peer.

During egress, IPsec adds the SGT capability and prefixes to the IPsec payload if the peer supports inline tagging; otherwise the packet is not tagged.

During ingress, IPsec inspects the packet for the SGT capability. If a tag is available, IPsec extracts the tag information and passes the information to the device only if inline tagging is negotiated. If there is no tag, IPsec processes the packet as a normal packet.

The tables below describe how IPsec behaves during egress and ingress.

Table 1: IPsec Behavior on the Egress Path

Inline Tagging Negotiated	CTS Provides SGT	IPsec Behavior
Yes	Yes	An SGT CMD is added to the packet.
Yes	No	The packet is sent without the SGT CMD.
No	Yes or no	The packet is sent without the SGT CMD.

Table 2: IPsec Behavior on the Ingress Path

Packet Is Tagged	Inline Tagging Negotiated	IPsec Behavior
Yes	Yes	The SGT CMD in the packet is processed.

Packet Is Tagged	Inline Tagging Negotiated	IPsec Behavior
Yes	No	The SGT CMD in the packet is not processed.
No	Yes or no	The packet is processed as a normal IPsec packet.

SGT on the IKEv2 Initiator and Responder

To enable SGT on an IKEv2 session, the SGT capability support must be sent to the peers using the **crypto ikev2 cts** command. SGT is a Cisco proprietary capability; hence, it is sent as a Vendor ID (VID) payload in the SA_INIT exchange.

The table below explains the scenarios when SGT capability is configured on the initiator and the responder:

Table 3: SGT Capability on IKEv2 Initiator and Responder

SGT Enabled on Initiator	SGT Enabled on Responder	What Happens . . .
Yes	Yes	The VID is exchanged between the initiator and the responder, and IPsec SA is enabled with the SGT inline tagging capability.
Yes	No	The initiator proposes the VID, but the responder ignores the VID. IPsec SA is not enabled with the SGT inline tagging capability.
No	Yes	The initiator does not propose the VID, and the responder does not send the VID payload. IPsec SA is not enabled with the SGT inline tagging capability.
No	No	The initiator does not propose the VID, and responder also does not send the VID payload. IPsec SA is not enabled with the SGT inline tagging capability.

Handling Fragmentation

Fragmentation is handled in the following two ways:

- Fragmentation before IPsec—If IPsec receives fragmented packets, each fragment is tagged.
- Fragmentation after IPsec—If IPsec packets are fragmented after encryption, the first fragment will be tagged.

How to Configure TrustSec DMVPN Inline Tagging Support

Enabling IPsec Inline Tagging

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel id*
4. **cts sgt inline**
5. **exit**

DETAILED STEPS

	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	**interface tunnel** *tunnel id* **Example:** `Device(config)# interface tunnel 1`	Specifies a tunnel interface number, and enters interface configuration mode.
Step 4	**cts sgt inline** **Example:** `Device(config-if)# cts sgt inline`	Enables TrustSec on DMVPN. This command is valid for generic routing encapsulation (GRE) and to tunnel interfaces modes only.
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Monitoring and Verifying TrustSec DMVPN Inline Tagging Support

To monitor and verify the TrustSec DMVPN Inline Tagging Support configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show dmvpn**

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

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Step 2 **show dmvpn**

Example:

```
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
```

Use this command to display Dynamic Multipoint VPN (DMVPN)-specific session information.

Step 3 **show ip nhrp nhs detail**

Example:

```
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
```

Use this command to display Next Hop Resolution Protocol (NHRP) next hop server (NHS) information.

Step 4 **show tunnel endpoints**

Example:

```
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
```

Use this command to display the contents of the tunnel endpoint database that is used for tunnel endpoint address resolution, when running a tunnel in multipoint generic routing encapsulation (mGRE) mode.

Step 5 **show adjacency** *interface-type interface-number* **detail**

Example:

```
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:
.
.
.
```

Use this command to display information about the protocol.

Enabling IPsec Inline Tagging on IKEv2 Networks

Configuring the **cts sgt inline** and **crypto ikev2 cts sgt** commands results in the packets getting tagged twice - once each by each command.

Before you begin

IKEv2 and IPsec must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ikev2 cts sgt**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**crypto ikev2 cts sgt** **Example:** `Device(config)# crypto ikev2 cts sgt`	Enables TrustSec on DMVPN on IKEv2 networks. This command is valid for generic routing encapsulation (GRE) and to tunnel interfaces modes only.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Configuration Examples for TrustSec DMVPN Inline Tagging Support

Example: Enabling IPsec Inline Tagging on IKEv2 Networks

Static VTI Initiator Configuration

The following example shows how to enable IPsec inline tagging on a static VTI initiator. You can use this configuration for configuring crypto maps and VTIs.

```
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
```

Dynamic VTI Responder Configuration

The following example shows how to enable IPsec inline tagging on a dynamic VTI responder. You can use this configuration for configuring crypto maps and VTIs.

```
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
```

Additional References for TrustSec DMVPN Inline Tagging Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
Security commands	• *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 and SXP configuration	*Cisco TrustSec Switch Configuration Guide*
IPsec configuration	*Configuring Security for VPNs with IPsec*
IKEv2 configuration	*Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site*
Cisco Secure Access Control Server	Configuration Guide for the Cisco Secure ACS

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 TrustSec DMVPN Inline Tagging Support

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 4: Feature Information for Configuring TrustSec DMVPN Inline Tagging Support

Feature Name	Releases	Feature Information
TrustSec DMVPN Inline Tagging Support	Cisco IOS XE Release 3.13S	The TrustSec DMVPN Inline Tagging Support feature enables IPsec to carry Cisco Trust Sec (CTS) Security Group Tag (SGT) between IPsec peers. The following commands were introduced or modified: **cts sgt inline**, **show dmvpn**, **show ip nhrp nhs**, **show tunnel endpoints**, **show adjacency**.