GET VPN Support of IPsec Inline Tagging for Cisco TrustSec

The Cisco TrustSec (CTS) architecture secures networks by establishing domains of trusted network devices. Once a network device authenticates with the network, the communication on the links between devices in the cloud is secured with a combination of encryption, message integrity checks, and replay protection mechanisms.

CTS uses the user and device identification information acquired during the authentication phase to classify packets as they enter the network. CTS maintains classification of each packet or frame by tagging it with a security group tag (SGT) on ingress to the network so that it can be identified for applying security and other policy criteria along the data path. The tags allow network intermediaries such as switches and firewalls to enforce access control policy based on the classification.

The GET VPN Support of IPsec Inline Tagging for Cisco TrustSec feature uses GET VPN inline tagging to carry the SGT information across the private WAN.

Prerequisites for GET VPN Support of IPsec Inline Tagging for Cisco TrustSec

All key servers (KSs) and group members (GMs) on which you want to enable this feature must be running GET VPN software version 1.0.5 or higher. You should use this feature only after all devices in the GET VPN network are upgraded to GET VPN software versions that support it.

This feature provides a command that you use on the KS (or primary KS) to check whether all devices in the network are running versions that support IPsec inline tagging for Cisco TrustSec. For more information, see the "Ensuring That GMs Are Running Software Versions That Support IPsec Inline Tagging for Cisco TrustSec" section.

Restrictions for GET VPN Support of IPsec Inline Tagging for Cisco TrustSec

- This feature does not support IPv6 traffic.
- This feature does not support transport mode on the Cisco ASR 1000 Series Aggregation Services Routers or on the Cisco VPN Internal Service Module for Cisco Integrated Services Routers Generation 2 (ISR G2).

Information About GET VPN Support of IPsec Inline Tagging for Cisco TrustSec

Group Member Registration of Security Group Tagging Capability

When a KS receives a security association (SA) registration request from a group member (GM) or receives a connection establishment request from a cooperative KS, it checks whether any group SA has SGT inline tagging enabled. If so, all GMs and cooperative KSs must register using GET VPN software version 1.0.5 or higher to be accepted. Otherwise, the registration request or establishment request is rejected, and the KS generates a syslog message to notify the network administrator.

Creation of SAs with Security Group Tagging Enabled

After you enable GET VPN support of IPsec inline tagging (using the **tag cts sgt** command) in a group SA and then trigger a rekey (using the **crypto gdoi ks rekey** command), the KS checks for GMs and cooperative KSs in the group not using a compatible software version. If found, a warning message appears:

```
WARNING for group GETVPN: some devices cannot support SGT inline tagging. Rekey can cause
traffic disruption and GM registration failures. Please check 'show crypto gdoi feature
sgt'.
Are you sure you want to proceed ? [yes/no]:
```

Handling of Security Group Tags in the Group Member Data Plane

Egress traffic is traffic sent out from a GDOI-protected interface of a GM. The following table specifies GM behavior for the egress path:

Table 1: Egress Handling of Security Group Tags

Security group tagging is enabled on SA	CTS provides SGTs	GM data plane behavior
Yes	Yes	Adds SGTs to Cisco metadata and encrypts
Yes	No	Encrypts without SGTs

Security group tagging is enabled on SA	CTS provides SGTs	GM data plane behavior
No	Yes	Encrypts without SGTs
No	No	Encrypts without SGTs

Ingress traffic is traffic received by a GDOI-protected interface of a GM. The table below specifies GM behavior for the ingress path:

Table 2: Ingress Handling of Security Group Tags

Security group tagging is enabled on SA	CTS provides SGTs	GM data plane behavior
Yes	Yes	Decrypts and extracts SGTs for CTS
Yes	No	Decrypts without SGT processing
No	Yes	Decrypts and ignores SGTs
No	No	Decrypts without SGT processing

Packet Overhead and Fragmentation When Using Security Group Tagging

Because it adds Cisco metadata containing the SGT information to each GDOI packet, SGT inline tagging increases packet overhead by eight bytes (or 16 bytes with time-based antireplay enabled).

If a packet is fragmented before GDOI encryption, each fragment is inline tagged with SGT information accordingly. If packet is fragmented after GDOI encryption, only the first fragment is inline tagged with SGT information.

You can use two methods to handle fragmentation. The first method is to use the **ip mtu** command on the interface that is handling encryption to accommodate the extra bytes used to carry the SGT information via Cisco metadata. The second method is to use the **ip tcp adjst-mss 1352** command on the GM's LAN interface. This command ensures that the resulting IP packet on the LAN segment is less than 1392 bytes, thereby providing 108 bytes for any overhead plus the Cisco metadata to carry the SGTs.

For more information about designing around MTU issues, refer to the “Designing Around MTU Issues” section of the Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide

How to Configure GET VPN Support of IPsec Inline Tagging for Cisco TrustSec

Ensuring That GMs Are Running Software Versions That Support IPsec Inline Tagging for Cisco TrustSec

You should use the IPsec Inline Tagging for Cisco TrustSec feature only after all devices in the GET VPN network are upgraded to GET VPN software versions that support this feature.

Perform this task on the KS (or primary KS) to ensure that all devices in the network support IPsec inline tagging for Cisco TrustSec.

SUMMARY STEPS

1. **enable**
2. **show crypto gdoi feature cts-sgt**
3. **show crypto gdoi feature cts-sgt | include No**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show crypto gdoi feature cts-sgt** **Example:** `Device# show crypto gdoi feature cts-sgt`	Displays the version of the GET VPN software running on each KS and GM in the GET VPN network and displays whether that device supports IPsec inline tagging for Cisco TrustSec.
Step 3	**show crypto gdoi feature cts-sgt | include No** **Example:** `Device# show crypto gdoi feature cts-sgt | include No`	(Optional) Displays only those devices that do not support IPsec inline tagging for Cisco TrustSec.

Configuring IPsec Inline Tagging for Cisco TrustSec

To configure IPsec inline tagging for Cisco TrustSec, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto gdoi group** *group-name*
4. Enter one of the following commands:
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server local**
6. **sa ipsec** *sequence-number*
7. **tag cts sgt**
8. **end**

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	**crypto gdoi group** *group-name* **Example:** `Device(config)# crypto gdoi group GET-SGT`	Identifies a GDOI group and enters GDOI group configuration mode.

Step 4	Enter one of the following commands:
	• **identity number** *number*
	• **identity address ipv4** *address*
	Example:
	`Device(config-gdoi-group)# identity number 3333`
	Example:
	`Device(config-gdoi-group)# identity address ipv4 10.2.2.2`
		Identifies a GDOI group number or address.

Step 5	**server local** **Example:** `Device(config-gdoi-group)# server local`	Designates a device as a GDOI KS and enters GDOI local server configuration mode.

	Command or Action	Purpose
Step 6	**sa ipsec** *sequence-number* **Example:** `Device(gdoi-local-server)# sa ipsec 1`	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.
Step 7	**tag cts sgt** **Example:** `Device(gdoi-sa-ipsec)# tag cts sgt`	Enables IPsec inline tagging for Cisco TrustSec.
Step 8	**end** **Example:** `Device(gdoi-sa-ipsec)# end`	Exits GDOI SA IPsec configuration mode and returns to privileged EXEC mode.

After enabling IPsec inline tagging, you must trigger a rekey. For more information, see the "Triggering a Rekey" section.

Triggering a Rekey

If you change the security policy (for example, from DES to AES) on the KS (or primary KS) and exit from global configuration mode, a syslog message appears on the KS indicating that the policy has changed and a rekey is needed. You enter the rekey triggering command as described below to send a rekey based on the latest policy in the running configuration.

Perform this task on the KS (or primary KS) to trigger a rekey.

SUMMARY STEPS

1. **enable**
2. **crypto gdoi ks** [**group** *group-name*] **rekey** [**replace-now**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**crypto gdoi ks** [**group** *group-name*] **rekey** [**replace-now**] **Example:** `Device# crypto gdoi ks group mygroup rekey`	Triggers a rekey on all GMs. The optional **replace-now** keyword immediately replaces the old TEKs and KEK on each GM to enable the new policy before the SAs expire. **Note** Using the **replace-now** keyword could cause a temporary traffic discontinuity.

Examples

A message appears on the KS as follows:

```
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

After the policy change, when each GM receives this triggered rekey, it installs the new SAs (for example, for AES) and shortens the lifetimes of the old SAs (for example, for DES). Each GM continues to encrypt and decrypt traffic using the old SA until its shortened lifetime expires.

If you try to trigger a rekey on the secondary KS, it rejects the command as shown below:

```
Device# crypto gdoi ks rekey
ERROR for group GET: This command must be executed on Pri-KS
```

Verifying and Troubleshooting GET VPN Support of IPsec Inline Tagging for Cisco TrustSec

To view the configuration that is running on a GM, use the **show running-config** command.

To display the number of packets that are tagged with SGTs, enter the following command.

```
Device# show crypto ipsec sa detail

interface: Ethernet0/0
   Crypto map tag: GET, local addr 5.0.0.2
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   Group: GET-SGT
.
.
.
#pkts tagged (send): 0, #pkts untagged (rcv): 5
```

The pkts tagged (send) field displays packets tagged with an SGT in the outbound direction. The pkts untagged (rcv) field displays packets not tagged with an SGT in the inbound direction.

Configuration Examples for GET VPN Support of IPsec Inline Tagging for Cisco TrustSec

Example: Ensuring That GMs Are Running Software Versions That Support IPsec Inline Tagging for Cisco TrustSec

The following example shows how to use the GET VPN software versioning command on the KS (or primary KS) to check whether all the devices in each group support IPsec inline tagging for Cisco TrustSec:

```
Device# show crypto gdoi feature cts-sgt

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.5          Yes
        10.0.6.2         1.0.5          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No

    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
        10.0.3.1         1.0.5          Yes
        10.0.3.2         1.0.5          Yes
```

You can also enter the above command on a GM (which will display the information for the GM but not for the KS or other GMs).

The following example shows how to enter the command on the KS (or primary KS) find only those devices in the GET VPN network that do *not* support IPsec inline tagging for Cisco TrustSec:

```
Device# show crypto gdoi feature cts-sgt | include No

        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
```

Example: Configuring IPsec Inline Tagging for Cisco TrustSec

The following example shows how to configure CTS SGT inline tagging in an IPsec SA for a KS serving a single GDOI group:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended ACL-SGT
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# crypto gdoi group GET-SGT
```

```
Device(config-gdoi-group)# identity number 1
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# tag cts sgt
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL-SGT
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# end
```

The following example shows how to configure two groups: A group with GMs that are upgraded to GET VPN version 1.0.5 or higher (and therefore supports CTS SGT inline tagging) and a group with GMs that are not yet upgraded. The upgraded GMs will register to group number 1111 (a lower crypto map sequence number) and with group number 2222 (a higher crypto-map sequence number). Non-upgraded GMs will register only to group number 2222.

This example configures SGT tagging for traffic between two sites. The **permit ip** commands add access control entries (ACEs) to the access control list (ACL) that permit communication between the two sites:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended ACL_NET_AB
Device(config-ext-nacl)# permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
Device(config-ext-nacl)# permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
Device(config-ext-nacl)# exit
Device(config)# ip access-list extended ACL_ALL
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# crypto gdoi group GET1
Device(config-gdoi-group)# identity number 1111
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey authentication mypubkey rsa mykey
Device(gdoi-local-server)# rekey transport unicast
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# tag cts sgt
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL_NET_AB
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# exit
Device(gdoi-local-server)# exit
Device(config-gdoi-group)# exit
Device(config)# crypto gdoi group GET2
Device(config-gdoi-group)# crypto gdoi group GET2
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey authentication mypubkey rsa mykey
Device(gdoi-local-server)# rekey transport unicast
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL_ALL
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# end
```

Note GET VPN supports a maximum of 100 ACEs per ACL.

Example: Triggering Rekeys on Group Members

Ensuring That GMs Are Running Software Versions That Support Rekey Triggering

The following example shows how to use the GET VPN software versioning command on the KS (or primary KS) to display the version of software on devices in the GET VPN network and display whether they support rekey triggering after a policy change:

```
Device# show crypto gdoi feature policy-replace

Key Server ID       Version  Feature Supported
  10.0.8.1         1.0.2          Yes
  10.0.9.1         1.0.2          Yes
  10.0.10.1        1.0.2          Yes
  10.0.11.1        1.0.2          Yes
 Group Member ID     Version  Feature Supported
  5.0.0.2          1.0.2          Yes
  9.0.0.2          1.0.1          No
```

The following example shows how to find only those devices that do not support rekey triggering after policy replacement:

```
Device# show crypto gdoi feature policy-replace  | include No

       9.0.0.2          1.0.1          No
```

For these devices, the primary KS sends only the triggered rekey without instructions for policy replacement. Therefore, when a GM receives the rekey, it installs the new SAs but does not shorten the lifetimes of the old SAs.

Triggering a Rekey

The following example shows how to trigger a rekey after you have performed a policy change. In this example, an IPsec policy change (for example, DES to AES) occurs with the **profile gdoi-p2** command:

```
Device# configure terminal
Device(config)# crypto gdoi group GET
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# no profile gdoi-p
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# end
Device#

*Jan 28 09:15:15.527: %SYS-5-CONFIG_I: Configured from console by console
*Jan 28 09:15:15.527: %GDOI-5-POLICY_CHANGE: GDOI group GET policy has changed. Use
'crypto gdoi ks rekey' to send a rekey, or the changes will be send in the next scheduled
rekey
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

The following example shows the error message that appears if you try to trigger a rekey on the secondary KS:

```
Device# crypto gdoi ks rekey

ERROR for group GET: This command must be executed on Pri-KS
```

Note If time-based antireplay (TBAR) is set, the key server periodically sends a rekey to the group members every 2 hours (7200 sec). In the following example, even though the lifetime is set to 8 hours (28800 sec), the rekey timer is set to 2 hours.

```
Device(config)# crypto ipsec profile atm-profile
Device(ipsec-profile)# set security-association lifetime seconds 28800
!
Device(ipsec-profile)# exit
Device(config)# crypto gdoi group ATM-DSL
Device(config-gdoi-group)# server local
Device(gdoi-sa-ipsec)# sa ipsec 1
!
Device(gdoi-sa-ipsec)# replay time window-size 100
```

The commands **show crypto gdoi gm replay** and **show crypto gdoi ks replay** displays TBAR information.

Additional References for GET VPN Support of IPsec Inline Tagging for Cisco TrustSec

Related Documents

Related Topic	Document Title
Cisco IOS security commands	*Cisco IOS Security Command References*
Basic deployment guidelines for enabling GET VPN in an enterprise network	Cisco IOS GET VPN Solutions Deployment Guide
Configuring Cisco TrustSec	Cisco TrustSec Configuration Guide, Cisco IOS Release 15M&T
Designing around MTU issues	Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide

Standards and RFCs

Standard/RFC	Title
RFC 2401	Security Architecture for the Internet Protocol
RFC 6407	The Group Domain of Interpretation

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 GET VPN Support of IPsec Inline Tagging for Cisco TrustSec

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 3: Feature Information for GET VPN Support of IPsec Inline Tagging for Cisco TrustSec

Feature Name	Releases	Feature Information
GET VPN Support of IPsec Inline Tagging for Cisco TrustSec		The Cisco TrustSec (CTS) architecture secures networks by establishing domains of trusted network devices. Once a network device authenticates with the network, the communication on the links between devices in the cloud is secured with a combination of encryption, message integrity checks, and replay protection mechanisms. CTS uses the user and device identification information acquired during the authentication phase to classify packets as they enter the network. CTS maintains classification of each packet or frame by tagging it with a security group tag (SGT) on ingress to the network so that it can be identified for applying security and other policy criteria along the data path. The tags allow network intermediaries such as switches and firewalls to enforce access control policy based on the classification. The GET VPN Support of IPsec Inline Tagging for Cisco TrustSec feature uses GET VPN inline tagging to carry the SGT information across the private WAN. The following commands were introduced or modified: **show crypto gdoi, show crypto ipsec sa, tag cts sgt.**