GETVPN GDOI Bypass

The GETVPN GDOI Bypass feature supports enabling and disabling the default Group Domain of Interpretation (GDOI) bypass crypto policy. It also supports hardening of the default GDOI bypass crypto policy once it is enabled.

Restrictions for GETVPN GDOI Bypass

When a key server (KS) is placed behind a group member (GM), the local deny Access Control List (ACL) must be configured explicitly to allow traffic using UDP as the transport protocol and port 848 as either the source or destination (UDP 848 traffic) to pass through.

Information About GETVPN GDOI Bypass

GDOI Bypass Crypto Policy

The Cisco IOS Group Encrypted Transport VPN (GETVPN) uses Group Domain of Interpretation (GDOI) as the key management protocol.

A group member (GM) is a device responsible for encryption and decryption, that is, a device responsible for handling the GET VPN data plane.

A key server (KS) is a device responsible for creating and maintaining the GET VPN control plane. All encryption policies, such as traffic, encryption protocols, security association, rekey timers, and so on, are centrally defined on the KS and are pushed down to all GMs at registration time.

Enabling and Disabling the Default GDOI Bypass Crypto Policy

A new group member (GM) configuration allows users to disable the Group Domain of Interpretation (GDOI) bypass crypto policy and to control traffic exceptions by explicitly configuring the GM local access control list (ACL).

Hardening of the Default GDOI Bypass Crypto Policy

To improve security, the following changes have been enforced while applying the default Group Domain of Interpretation (GDOI) bypass crypto policy:

- The default GDOI bypass crypto policy is installed only on Group Encrypted Transport VPN (GETVPN)-protected interfaces (interfaces at which GDOI crypto map is applied). Only UDP848 traffic that is destined for the group member's (GM) address used for registration or rekey is allowed.
- If the GM VRF-aware feature is used to specify that the GDOI data plane and control plane are in different VRFs, auto-insertion of the default GDOI bypass crypto policy is not applied to the GDOI-protected interface.
- If traffic using UDP as the transport protocol and port 848 as either the source or destination (UDP 848 traffic) is expected to arrive at other non-GDOI-protected interfaces (but with other crypto maps applied), exceptions for the non-GDOI crypto map must be explicitly configured.
- If a crypto map set with multiple groups is configured, the overall GDOI bypass crypto policy installed is the union of all the GDOI bypass crypto policies for each group within the security association database (SADB).

Any of the conditions mentioned below triggers a recompute of the default GDOI bypass crypto policy applied to a GETVPN-protected interface:

- Removing **client bypass-policy** configuration using the **no client bypass-policy** command.
- Applying or removing the GDOI bypass crypto map from an interface.
- Applying or removing the GDOI bypass crypto map from crypto map sets.
- Changing the IP address of the GDOI-protected interface (if **no client registration interface** is used)
    - If **client registration interface** is used, the following cases trigger a recompute of the default GDOI bypass crypto policy applied to a GETVPN-protected interface:
        - Changes from **no client registration interface** to **client registration interface**
        - Changes to the client registration interface (for example, from loopback 0 to loopback 1)
        - Changes to the client registration interface address

How to Configure GETVPN GDOI Bypass

Enabling the Default GDOI Bypass Crypto Policy

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **client bypass-policy**
5. **end**

DETAILED STEPS

Procedure

	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 GETVPN`	Identifies a GDOI group and enters GDOI group configuration mode.
Step 4	**client bypass-policy** **Example:** `Device(config-gdoi-group)# client bypass-policy`	Enables the default GDOI bypass crypto policy.
Step 5	**end** **Example:** `Device(config-gdoi-group)# end`	Exits GDOI group configuration mode and returns to privileged EXEC mode.

Disabling the Default GDOI Bypass Crypto Policy

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **no client bypass-policy**
5. **end**

DETAILED STEPS

Procedure

	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 GETVPN`	Identifies a GDOI group and enters GDOI group configuration mode.
Step 4	**no client bypass-policy** **Example:** `Device(config-gdoi-group)# no client bypass-policy`	Disables the default GDOI bypass crypto policy.
Step 5	**end** **Example:** `Device(config-gdoi-group)# end`	Exits GDOI group configuration mode and returns to privileged EXEC mode.

Verifying Enablement and Disablement of the Default GDOI Bypass Crypto Policy

SUMMARY STEPS

1. **enable**
2. **show crypto gdoi gm acl**
3. **show crypto gdoi gm acl**

DETAILED STEPS

Procedure

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **show crypto gdoi gm acl**

Verifies the enablement of the default GDOI bypass crypto policy.

Note VRF will be displayed only if it is non-global.

Example:

```
Device# show crypto gdoi gm acl

Group Name: GETVPN
 ACL Downloaded From KS 10.0.0.2:
   access-list   deny eigrp any any
   access-list   permit ip any any
 ACL Configured Locally:
 ACL of default GDOI bypass policy:
   Ethernet1/0: deny udp host 10.0.0.9 eq 848 any eq 848 vrf RED*
```

Step 3 **show crypto gdoi gm acl**

Verifies the disablement of the default GDOI bypass crypto policy.

Example:

```
Device# show crypto gdoi gm acl

Group Name: GETVPN
 ACL Downloaded From KS 10.0.0.2:
   access-list   deny eigrp any any
   access-list   permit ip any any
 ACL Configured Locally:
 ACL of default GDOI bypass policy: Disabled
```

Configuration Examples for GETVPN GDOI Bypass

Example: Enabling the Default GDOI Bypass Crypto Policy

```
Device> enable
Device# configure terminal
```

```
Device(config)# crypto gdoi group getvpn
Device(config-gdoi-group)# client bypass-policy
Device(config-gdoi-group)# end
```

Example: Disabling the Default GDOI Bypass Crypto Policy

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group getvpn
Device(config-gdoi-group)# no client bypass-policy
Device(config-gdoi-group)# end
```

Additional References for GETVPN GDOI Bypass

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*
Designing and implementing a GET VPN network	*Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide*

Standards and RFCs

Standard/RFC	Title
RFC 6407	*The Group Domain of Interpretation*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for GETVPN GDOI Bypass

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 GETVPN GDOI Bypass

Feature Name	Releases	Feature Information
GETVPN GDOI Bypass		The following commands were introduced: **client bypass-policy** and **show crypto gdoi gm acl**.