

8K GM Scale Improvement

The 8K GM Scale Improvement feature supports optimization of the Cooperative Protocol (COOP) announcement messages by increasing the number of Group Members (GM) to 8000.

- Prerequisites for 8K GM Scale Improvement, on page 1
- Information About 8K GM Scale Improvement, on page 1
- How to Configure 8K GM Scale Improvement, on page 2
- Configuration Examples for 8K GM Scale Improvement, on page 3
- IPSEC Encryption and Decryption in GETVPN, on page 3
- Additional References for 8K GM Scale Improvement, on page 4
- Feature Information, on page 5

Prerequisites for 8K GM Scale Improvement

To upgrade or downgrade a particular protocol version, maintain the same policies, keys, and group member (GM) database to ensure uninterrupted communication between GMs.

Information About 8K GM Scale Improvement

8K GM Scale Improvement

A Cooperative Protocol Announcement (COOP ANN) message has several clients and each client is associated with a protocol version. The COOP ANN message has been optimized to hold up to 8000 Group Members (GM), subsequently increasing the protocol version of the GM header.

This feature also supports upgrade and downgrade of a GM header protocol version.

How to Configure 8K GM Scale Improvement

Upgrading and Downgrading the Group Member Header Protocol Version

Before you begin

- Ensure that all Key Servers (KS) are upgraded to the “optimize” protocol version before scaling the network to more than 4000 GMs
- Ensure that all upgraded KSs must be downgraded to the “base” protocol version before scaling down to a network that supports only up to 4000 GMs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **server local**
5. **redundancy**
6. **protocol version** {**base** | **optimize**}
7. **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	**server local** **Example:** `Device(config-gdoi-group)# server local`	Identifies a group server defined locally and enters GDOI local server configuration mode.

	Command or Action	Purpose
Step 5	**redundancy** **Example:** `Device(gdoi-local-server)# redundancy`	Enters GDOI COOP KS configuration mode. **Note** Ensure that the local server source address is defined.
Step 6	**protocol version** {**base** | **optimize**} **Example:** `Device(gdoi-coop-ks-config)# protocol version optimize`	Upgrades or downgrades the protocol version of the GM header. • **base**—COOP ANN message supports up to 4000 GMs. • **optimize**—COOP ANN message supports up to 8000 GMs.
Step 7	**end** **Example:** `Device(gdoi-coop-ks-config)# end`	Exits COOP KS configuration mode and returns to privileged EXEC mode.

Configuration Examples for 8K GM Scale Improvement

Example: Upgrading the Group Member Header Protocol Version

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group getvpn
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# redundancy
Device(gdoi-coop-ks-config)# protocol version optimize
Device(gdoi-coop-ks-config)# end
```

Example: Downgrading the Group Member Header Protocol Version

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group getvpn
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# redundancy
Device(gdoi-coop-ks-config)# protocol version base
Device(gdoi-coop-ks-config)# end
```

IPSEC Encryption and Decryption in GETVPN

In GETVPN IPsec flow, inbound traffic decryption might not happen in the expected IPsec flow recorder. The decrypted traffic can be recorded in any IPsec SA, if available. The decryption might happen in a random IPsec flow recorder. The following is an example:

```
Device# ping vrf cust1 48.1.1.1 so 38.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 48.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 38.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Device# show crypto session ivrf cust1  detail | sec permit ip 38.0.0.0
  IPSEC FLOW: permit ip 38.0.0.0/255.0.0.0 48.0.0.0/255.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1 hours, 16
mins
        Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1 hours, 16
mins

Device# show crypto session ivrf cust1  detail | sec permit ip 48.0.0.0
  IPSEC FLOW: permit ip 48.0.0.0/255.0.0.0 38.0.0.0/255.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1 hours, 16
mins
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1 hours, 16
mins

Device# show crypto session ivrf cust1  detail | sec permit ip 45.0.0.0
  IPSEC FLOW: permit ip 45.0.0.0/255.0.0.0 35.0.0.0/255.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 5 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1 hours, 15
mins
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1 hours, 15
mins
```

In the above example, flow inbound traffic is not decrypted in the expected IPsec flow.

To overcome this issue and view the number of encrypted and decrypted packets, you can use the following **show** command. Here's a sample output of the **show** command.

```
Device# show crypto gdoi group v6-cust-gdoi1 gm dataplane counters

Data-plane statistics for group v6-cust-gdoi1:
   #pkts encrypt            : 1912   #pkts decrypt            : 1914
    #pkts tagged (send)      : 1841     #pkts untagged (rcv)     : 1834
    #pkts no sa (send)       : 0        #pkts invalid sa (rcv)   : 0
    #pkts encaps fail (send) : 0        #pkts decap fail (rcv)   : 0
    #pkts invalid prot (rcv) : 0        #pkts verify fail (rcv)  : 0
    #pkts not tagged (send)  : 0        #pkts not untagged (rcv) : 0
    #pkts internal err (send): 0        #pkts internal err (rcv) : 0
```

Additional References for 8K GM Scale Improvement

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*

Related Topic	Document Title
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

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

Feature Name	Releases	Feature Information
8K GM Scale Improvement		The 8K GM Scale Improvement feature supports optimization of the Cooperative Protocol (COOP) announcement messages by increasing the number of Group Members (GM) to 8000. The following command was modified: **protocol**.