GETVPN Resiliency GM - Error Detection

The GETVPN Resiliency - GM Error Detection feature detects erroneous packets in the data plane for each Group Domain of Interpretation (GDOI) group such as invalid stateful packet inspections (SPIs) or Time-Based Anti-Replay (TBAR) errors. These errors are tracked, and the outer source IP address of the packet is recorded.

Information About GETVPN Resiliency - GM Error Detection

Error Handling

The GETVPN Resiliency - GM Error Detection feature should be enabled on both the GM and KS for error handling to work. The KS encodes the group information in the SPI (Security Parameter Index) and then it downloads it via the TEK policy to the GM.

When a failure is detected by the GETVPN Resiliency - GM Error Detection feature, a syslog message is generated to show the source IP address of the erroneous packet:

```
 *Feb 10 21:01:56.043:
%GDOI-4-TIMEBASED_REPLAY_FAILED: An anti replay check has failed in
group GETVPN from sourceip-address
100.0.0.9.
 my_pseudotime is 600006.78 secs,
peer_pseudotime is 500033.34 secs, replay_window is 100
(second)
 *Feb 10 21:01:56.043:
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
 connection id=29, sequence
number=11
```

The **show crypto gdoi gm** command displays the history of the last 50 Time-Based Anti-Replay (TBAR) errors. You can use these source IP address records to track down the sender group members (GMs) and investigate any existing hardware or software problems. The following statistical information is also available in the command:

- GM recovery feature ON/OFF

- Interval between recoveries
- Number of GM recovery reregistration enforced

When errors occur, the GM reregisters to the next available key server (KS) to retrieve the latest policy and keys and maintains all previously downloaded group policies and keys until the registration is complete.

For instance, when a cooperative key server (COOP KS) split occurs, each promoted KS generates its own Key Encryption Key (KEK) and Traffic Encryption Key (TEK). When a GM receives invalid SPI packets, it will decode it (the KS encodes the group information in the SPI and then it downloads it via the TEK policy to the GM) and if it finds that it belongs to the current getvpn group then it will start the recovery registration.

An invalid SPIs can belong to one of the following two categories:

- Positive invalid SPI: An invalid SPI that belong to the current group and require GM recovery registration.
- Negative invalid SPI: An invalid SPI that does not require recovery registration.

In the case of a positive invalid SPI, a recovery registration to the next key server (KS) on its list is performed. This recovery registration is repeated for each invalid stateful packet inspection (SPI) packet or TBAR error in each client recovery interval to the next KS on the list. When all the KSs in the list are recovered and no longer contain the invalid SPI, that SPI is marked as a false positive and no more recovery registrations are performed. The KSs will always do the recovery registration for TBAR errors. However, once the GM recovers to all the KSs in the list because of an invalid SPI and none of the KSs has that SPI, it will mark that SPI as a false positive and will not do more recovery registrations due to that SPI.

A syslog message is generated to notify you that this GM recovery reregistration feature is triggered. For instance, if you configure the GM to monitor for control-plane errors every 300 seconds, when the recovery registration occurs the following syslog is generated:

```
*Feb 23 19:06:28.600: %GDOI-5-GM_RECOVERY_REGISTER: received invalid GDOI packets; register
 to KS to refresh policy, keys, and PST.
```

How to Configure GETVPN Resiliency - GM Error Detection

Configuring GETVPN Resiliency - GM Error Detection

SUMMARY STEPS

1. **crypto gdoi group** *group-name*
2. **identity number** *number*
3. **server address ipv4** *address*
4. **client recovery-check interval** *interval*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**crypto gdoi group** *group-name* **Example:**	Creates a Group Domain of Interpretation (GDOI) group and enters GDOI group configuration mode.

	Command or Action	Purpose
	`Device(config)# crypto gdoi group GETVPN`	
Step 2	**identity number** *number* **Example:** `Device(config-gdoi-group)# identity number 1111`	Identifies a GDOI group number.
Step 3	**server address ipv4** *address* **Example:** `Device(config-gdoi-group)# server address ipv4 1.0.0.2`	Specifies the IP address of the server that the GDOI group is trying to reach.
Step 4	**client recovery-check interval** *interval* **Example:** `Device(config-gdoi-group)# client recovery-check interval 300`	Sets the interval of time for the client group member (GM) to monitor for control-plane errors.
Step 5	**exit** **Example:** `Device(config-gdoi-group)# exit`	Exits GDOI group configuration mode and returns to global configuration mode.

Configuration Examples for GETVPN Resiliency - GM Error Detection

Example: Configuring GETVPN Resiliency - GM Error Detection

The following example shows how to enable the group member (GM) to monitor for control-plane errors every 300 seconds.

```
crypto gdoi group GETVPN
 identity number 1111
 server address ipv4 1.0.0.2
 client recovery-check interval 300
```

Additional References for GETVPN Resiliency - GM Error Detection

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 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 GETVPN Resiliency - GM Error Detection

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 Resiliency - GM Error Detection

Feature Name	Releases	Feature Information
GETVPN Resiliency - GM Error Detection		Detects erroneous packets in the data plane for each GDOI group. The following command was introduced: **client recovery-check interval.**