



IPsec Dead Peer Detection Periodic Message Option

The IPsec Dead Peer Detection Periodic Message Option feature is used to configure the router to query the liveness of its Internet Key Exchange (IKE) peer at regular intervals. The benefit of this approach over the default approach (on-demand dead peer detection) is earlier detection of dead peers.



Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the [Next Generation Encryption \(NGE\)](#) white paper.

- [Prerequisites for IPsec Dead Peer Detection PeriodicMessage Option, on page 1](#)
- [Restrictions for IPsec Dead Peer Detection PeriodicMessage Option, on page 1](#)
- [How to Configure IPsec Dead Peer Detection PeriodicMessage Option, on page 2](#)
- [Configuration Examples for IPsec Dead Peer Detection Periodic Message Option, on page 4](#)
- [Additional References, on page 4](#)

Prerequisites for IPsec Dead Peer Detection PeriodicMessage Option

Before configuring the IPsec Dead Peer Detection Periodic Message Option feature, you should have the following:

- Familiarity with configuring IP Security (IPsec).

Restrictions for IPsec Dead Peer Detection PeriodicMessage Option

Using periodic DPD potentially allows the router to detect an unresponsive IKE peer with better response time when compared to on-demand DPD. However, use of periodic DPD incurs extra overhead. When communicating to large numbers of IKE peers, you should consider using on-demand DPD instead.

How to Configure IPsec Dead Peer Detection PeriodicMessage Option

Configuring a Periodic DPD Message

To configure a periodic DPD message, perform the following steps.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	crypto isakmp keepalive <i>seconds</i> <i>[retry-seconds]</i> [periodic on-demand] Example: <pre>Router (config)# crypto isakmp keepalive 10 periodic</pre>	Allows the gateway to send DPD messages to the peer. <ul style="list-style-type: none"> • <i>seconds</i> --When the periodic keyword is used, this argument is the number of seconds between DPD messages; the range is from 10 to 3600 seconds. <p>When the on-demand keyword is used, this argument is the number of seconds during which traffic is not received from the peer before DPD retry messages are sent if there is data (IPSec) traffic to send; the range is from 10 to 3600 seconds.</p> <p>Note If you do not specify a time interval, an error message appears.</p> <ul style="list-style-type: none"> • <i>retry-seconds</i> --(Optional) Number of seconds between DPD retry messages if the DPD retry message is missed by the peer; the range is from 2 to 60 seconds. <p>Once 1 DPD message is missed by the peer, the router moves to a more aggressive state and sends the DPD retry message at the faster retry interval, which is the number of seconds</p>

	Command or Action	Purpose
		<p>between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five aggressive DPD retry messages can be missed before the tunnel is marked as down.</p> <p>Note To configure DPD with IPsec High Availability (HA), the recommendation is to use a value other than the default (which is 2 seconds). A keepalive timer of 10 seconds with 5 retries seems to work well with HA because of the time that it takes for the router to get into active mode.</p> <ul style="list-style-type: none"> • periodic --(Optional) DPD messages are sent at regular intervals. • on-demand --(Optional) The default behavior. DPD retries are sent on demand. <p>Note Because this option is the default, the on-demand keyword does not appear in configuration output.</p>

Verifying That DPD Is Enabled

DPD allows the router to clear the IKE state when a peer becomes unreachable. If DPD is enabled and the peer is unreachable for some time, you can use the **clear crypto session** command to manually clear IKE and IPsec SAs.

The **debug crypto isakmp** command can be used to verify that DPD is enabled.

Procedure

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>clear crypto session [<i>local ip-address</i> [<i>port local-port</i>]] [<i>remote ip-address</i> [<i>port remote-port</i>]] [<i>fvr</i> <i>vrf-name</i>] [<i>ivrf vrf-name</i>]</p> <p>Example:</p> <pre>Router# clear crypto session</pre>	<p>Deletes crypto sessions (IPsec and IKE SAs).</p>

	Command or Action	Purpose
Step 3	debug crypto isakmp Example: Router# debug crypto isakmp	Displays messages about IKE events.

Configuration Examples for IPsec Dead Peer Detection Periodic Message Option

Site-to-Site Setup with Periodic DPD Enabled Example

The following configurations are for a site-to-site setup with periodic DPD enabled. The configurations are for the IKE Phase 1 policy and for the IKE preshared key.

IKE Phase 1 Policy

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 14
!
```

IKE Preshared Key

```
crypto isakmp key kd94j1ksldz address 10.2.80.209 255.255.255.0
crypto isakmp keepalive 10 periodic
crypto ipsec transform-set Trans1 esp-aes esp-sha-hmac
!
!
interface GigabitEthernet 0/0
  ip address 10.1.32.14 255.255.255.0
  speed auto
!
```

Additional References

Related Documents

Related Topic	Document Title
Configuring IPsec	Configuring Security for VPNs with IPsec
IPsec commands	Cisco IOS Security Command Reference

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
DPD conforms to the Internet draft “draft-ietf-ipsec-dpd-04.txt,” which is pending publication as an Informational RFC (a number has not yet been assigned).	--

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

