



IPSec Dead Peer Detection Periodic Message Option

First Published: May 1, 2004
Last Updated: August 21, 2007

The IPSec Dead Peer Detection Periodic Message Option feature allows you to configure your 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.

History for IPSec Dead Peer Detection Periodic Message Option Feature

| Release | Modification |
|-------------|---|
| 12.3(7)T | This feature was introduced. |
| 12.2(33)SRA | This feature was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This feature was integrated into Cisco IOS Release 12.2(33)SXH. |

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for IPSec Dead Peer Detection Periodic Message Option, page 2](#)
- [Restrictions for IPSec Dead Peer Detection Periodic Message Option, page 2](#)
- [Information About IPSec Dead Peer Detection Periodic Message Option, page 2](#)
- [How to Configure IPSec Dead Peer Detection Periodic Message Option, page 3](#)
- [Configuration Examples for IPSec Dead Peer Detection Periodic Message Option, page 7](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2004–2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 12](#)
- [Command Reference, page 13](#)

Prerequisites for IPSec Dead Peer Detection Periodic Message Option

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

- Familiarity with configuring IP Security (IPSec).
- An IKE peer that supports DPD (dead peer detection). Implementations that support DPD include the Cisco VPN 3000 concentrator, Cisco PIX Firewall, Cisco VPN Client, and Cisco IOS software in all modes of operation—site-to-site, Easy VPN remote, and Easy VPN server.

Restrictions for IPSec Dead Peer Detection Periodic Message 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.

Information About IPSec Dead Peer Detection Periodic Message Option

To configure IPSec Dead Peer Detection Periodic Message Option, you should understand the following concepts:

- [How DPD and Cisco IOS Keepalive Features Work, page 2](#)
- [Using the IPSec Dead Peer Detection Periodic Message Option, page 3](#)
- [Using DPD and Cisco IOS Keepalive Features with Multiple Peers in the Crypto Map, page 3](#)
- [Using DPD in an Easy VPN Remote Configuration, page 3](#)

How DPD and Cisco IOS Keepalive Features Work

DPD and Cisco IOS keepalives function on the basis of the timer. If the timer is set for 10 seconds, the router will send a “hello” message every 10 seconds (unless, of course, the router receives a “hello” message from the peer). The benefit of IOS keepalives and periodic DPD is earlier detection of dead peers. However, IOS keepalives and periodic DPD rely on periodic messages that have to be sent with considerable frequency. The result of sending frequent messages is that the communicating peers must encrypt and decrypt more packets.

DPD also has an on-demand approach. The contrasting on-demand approach is the default. With on-demand DPD, messages are sent on the basis of traffic patterns. For example, if a router has to send outbound traffic and the liveliness of the peer is questionable, the router sends a DPD message to query the status of the peer. If a router has no traffic to send, it never sends a DPD message. If a peer is dead, and the router never has any traffic to send to the peer, the router will not find out until the IKE or IPSec security association (SA) has to be rekeyed (the liveliness of the peer is unimportant if the router is not trying to communicate with the peer). On the other hand, if the router has traffic to send to the peer, and the peer does not respond, the router will initiate a DPD message to determine the state of the peer.

Using the IPSec Dead Peer Detection Periodic Message Option

With the IPSec Dead Peer Detection Periodic Message Option feature, you can configure your router so that DPD messages are “forced” at regular intervals. This forced approach results in earlier detection of dead peers. For example, if a router has no traffic to send, a DPD message is still sent at regular intervals, and if a peer is dead, the router does not have to wait until the IKE SA times out to find out.

If you want to configure the DPD periodic message option, you should use the **crypto isakmp keepalive** command with the **periodic** keyword. If you do not configure the **periodic** keyword, the router defaults to the on-demand approach.



Note

When the **crypto isakmp keepalive** command is configured, the Cisco IOS software negotiates the use of Cisco IOS keepalives or DPD, depending on which protocol the peer supports.

Using DPD and Cisco IOS Keepalive Features with Multiple Peers in the Crypto Map

DPD and IOS keepalive features can be used in conjunction with multiple peers in the crypto map to allow for stateless failover. DPD allows the router to detect a dead IKE peer, and when the router detects the dead state, the router deletes the IPSec and IKE SAs to the peer. If you configure multiple peers, the router will switch over to the next listed peer for a stateless failover.

Using DPD in an Easy VPN Remote Configuration

DPD can be used in an Easy VPN remote configuration. See the section [“Configuring DPD for an Easy VPN Remote”](#) section on page 5.

How to Configure IPSec Dead Peer Detection Periodic Message Option

This section contains the following procedures:

- [Configuring a Periodic DPD Message](#), page 4
- [Configuring DPD and Cisco IOS Keepalives with Multiple Peers in the Crypto Map](#), page 4
- [Configuring DPD for an Easy VPN Remote](#), page 5
- [Verifying That DPD Is Enabled](#), page 6

Configuring a Periodic DPD Message

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp keepalive *seconds* [*retries*] [**periodic** | **on-demand**]**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | crypto isakmp keepalive <i>seconds</i> [<i>retries</i>] [periodic on-demand] Example: Router (config)# crypto isakmp keepalive 10 periodic | Allows the gateway to send DPD messages to the peer. <ul style="list-style-type: none"> • <i>seconds</i>—Number of seconds between DPD messages. • <i>retries</i>—(Optional) Number of seconds between DPD retries if the DPD message fails. • periodic—(Optional) DPD messages are sent at regular intervals. • on-demand—(Optional) DPD retries are sent on demand. This is the default behavior. |

Configuring DPD and Cisco IOS Keepalives with Multiple Peers in the Crypto Map

To configure DPD and IOS keepalives to be used in conjunction with the crypto map to allow for stateless failover, perform the following steps. This configuration will cause a router to cycle through the peer list when it detects that the first peer is dead.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map *map-name seq-num ipsec-isakmp***
4. **set peer {*host-name* [**dynamic**] | *ip-address*}**

5. **set transform-set** *transform-set-name*
6. **match address** [*access-list-id* | *name*]

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | crypto map <i>map-name</i> <i>seq-num</i> ipsec-isakmp Example: Router (config)# crypto map green 1 ipsec-isakmp | Enters crypto map configuration mode and creates or modifies a crypto map entry. <ul style="list-style-type: none">The ipsec-isakmp keyword indicates that IKE will be used to establish the IPSec SAs for protecting the traffic specified by this crypto map entry. |
| Step 4 | set peer { <i>host-name</i> [dynamic] <i>ip-address</i> } Example: Router (config-crypto-map)# set peer 10.12.12.12 | Specifies an IPSec peer in a crypto map entry. <ul style="list-style-type: none">You can specify multiple peers by repeating this command. |
| Step 5 | set transform-set <i>transform-set-name</i> Example: Router (config-crypto-map)# set transform-set txfm | Specifies which transform sets can be used with the crypto map entry. <ul style="list-style-type: none">You can specify more than one transform set name by repeating this command. |
| Step 6 | match address [<i>access-list-id</i> <i>name</i>] Example: Router (config-crypto-map)# match address 101 | Specifies an extended access list for a crypto map entry. |

Configuring DPD for an Easy VPN Remote

To configure DPD in an Easy VPN remote configuration, perform the following steps. This configuration also will cause a router to cycle through the peer list when it detects that the first peer is dead.



Note

IOS keepalives are not supported for Easy VPN remote configurations.

SUMMARY STEPS

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

3. **crypto ipsec client ezvpn** *name*
4. **connect** { **auto** | **manual** }
5. **group** *group-name* **key** *group-key*
6. **mode** { **client** | **network-extension** }
7. **peer** { *ipaddress* | *hostname* }

DETAILED STEPS

| | | |
|--------|---|---|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | crypto ipsec client ezvpn <i>name</i> Example: Router (config)# crypto ipsec client ezvpn ezvpn-config1 | Creates a Cisco Easy VPN remote configuration and enters the Cisco Easy VPN Remote configuration mode. |
| Step 4 | connect { auto manual } Example: Router (config-crypto-ezvpn)# connect manual | Manually establishes and terminates an IPSec VPN tunnel on demand. <ul style="list-style-type: none">The auto keyword option is the default setting. |
| Step 5 | group <i>group-name</i> key <i>group-key</i> Example: Router (config-crypto-ezvpn)# group unity key preshared | Specifies the group name and key value for the Virtual Private Network (VPN) connection. |
| Step 6 | mode { client network-extension } Example: Router (config-crypto-ezvpn)# mode client | Specifies the VPN mode of operation of the router. |
| Step 7 | peer { <i>ipaddress</i> <i>hostname</i> } Example: Router (config-crypto-ezvpn)# peer 10.10.10.10 | Sets the peer IP address or host name for the VPN connection. <ul style="list-style-type: none">A hostname can be specified only when the router has a DNS server available for host-name resolution.This command can be repeated multiple times. |

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.

SUMMARY STEPS

1. **enable**
2. **clear crypto session** [**local** *ip-address* [**port** *local-port*]] [**remote** *ip-address* [**port** *remote-port*]] | [**fvr** *vrf-name*] [**ivrf** *vrf-name*]
3. **debug crypto isakmp**

DETAILED STEPS

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

This section provides the following configuration examples:

- [Site-to-Site Setup with Periodic DPD Enabled: Example, page 7](#)
- [Easy VPN Remote with DPD Enabled: Example, page 8](#)
- [Verifying DPD Configuration Using the debug crypto isakmp Command: Example, page 8](#)
- [DPD and Cisco IOS Keepalives Used in Conjunction with Multiple Peers in a Crypto Map: Example, page 11](#)
- [DPD Used in Conjunction with Multiple Peers for an Easy VPN Remote: Example, page 11](#)

Site-to-Site Setup with Periodic DPD Enabled: Example

The following configurations are for a site-to-site setup with no 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 3des
```

```

    authentication pre-share
    group 2
!

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 esp-3des-sha esp-3des esp-sha-hmac
crypto map test 1 ipsec-isakmp
    set peer 10.2.80.209
    set transform-set esp-3des-sha
    match address 101
!
!
interface FastEthernet0
    ip address 10.1.32.14 255.255.255.0
    speed auto
    crypto map test
!

```

Easy VPN Remote with DPD Enabled: Example

The following configuration tells the router to send a periodic DPD message every 30 seconds. If the peer fails to respond to the DPD R_U_THERE message, the router will resend the message every 20 seconds (four transmissions altogether).

```

crypto isakmp keepalive 30 20 periodic
crypto ipsec client ezvpn ezvpn-config
    connect auto
    group unity key preshared
    mode client
    peer 10.2.80.209
!
!
interface Ethernet0
    ip address 10.2.3.4 255.255.255.0
    half-duplex
    crypto ipsec client ezvpn ezvpn-config inside
!
interface FastEthernet0
    ip address 10.1.32.14 255.255.255.0
    speed auto
    crypto ipsec client ezvpn ezvpn-config outside

```

Verifying DPD Configuration Using the debug crypto isakmp Command: Example

The following sample output from the **debug crypto isakmp** command verifies that IKE DPD is enabled:

```
*Mar 25 15:17:14.131: ISAKMP:(0:1:HW:2):IKE_DPD is enabled, initializing timers
```

To see that IKE DPD is enabled (and that the peer supports DPD): when periodic DPD is enabled, you should see the following debug messages at the interval specified by the command:

```
*Mar 25 15:18:52.107: ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:18:52.107: ISAKMP:(0:1:HW:2):purging node 899852982 *Mar 25 15:18:52.111:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_IM_ALIVE
*Mar 25 15:18:52.111: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

The above message corresponds to sending the DPD R_U_THERE message.

```
*Mar 25 15:18:52.123: ISAKMP (0:268435457): received packet from 10.2.80.209
dport 500 sport 500 Global (I) QM_IDLE
*Mar 25 15:18:52.123: ISAKMP: set new node -443923643 to QM_IDLE *Mar 25 15:18:52.131:
ISAKMP:(0:1:HW:2): processing HASH payload. message ID =
-443923643
*Mar 25 15:18:52.131: ISAKMP:(0:1:HW:2): processing NOTIFY R_U_THERE_ACK protocol 1
spi 0, message ID = -443923643, sa = 81BA4DD4
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2): DPD/R_U_THERE_ACK received from peer
10.2.80.209, sequence 0x9
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2):deleting node -443923643 error FALSE
reason "informational (in) state 1"
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_PEER, IKE_INFO_NOTIFY *Mar
25 15:18:52.135: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

The above message corresponds to receiving the acknowledge (ACK) message from the peer.

```
Router#
*Mar 25 15:47:35.335: ISAKMP: set new node -90798077 to QM_IDLE *Mar 25 15:47:35.343:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:35.343: ISAKMP:(0:1:HW:2):purging node -90798077 *Mar 25 15:47:35.347:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_IM_ALIVE
*Mar 25 15:47:35.347: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:36.611: ISAKMP:(0:1:HW:2):purging node 1515050537 *Mar 25 15:47:37.343:
ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:37.343: ISAKMP: set new node -1592471565 to QM_IDLE *Mar 25 15:47:37.351:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:37.351: ISAKMP:(0:1:HW:2):purging node -1592471565 *Mar 25 15:47:37.355:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:37.355: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:39.355: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:39.355: ISAKMP: set new node 1758739401 to QM_IDLE *Mar 25 15:47:39.363:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:39.363: ISAKMP:(0:1:HW:2):purging node 1758739401 *Mar 25 15:47:39.367:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:39.367: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

```

*Mar 25 15:47:41.367: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:41.367: ISAKMP: set new node 320258858 to QM_IDLE *Mar 25 15:47:41.375:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:41.379: ISAKMP:(0:1:HW:2):purging node 320258858 *Mar 25 15:47:41.379:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:41.379: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:43.379: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:43.379: ISAKMP: set new node -744493014 to QM_IDLE *Mar 25 15:47:43.387:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:43.387: ISAKMP:(0:1:HW:2):purging node -744493014 *Mar 25 15:47:43.391:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:43.391: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):peer 10.2.80.209 not responding! *Mar 25
15:47:45.391: ISAKMP:(0:1:HW:2):peer does not do paranoid keepalives.

*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):deleting SA reason "peers alive" state
(I) QM_IDLE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.395: ISAKMP: Unlocking IPSEC struct 0x81E5C4E8 from
delete_siblings, count 0
*Mar 25 15:47:45.395: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN. Peer
10.2.80.209:500 Id: 10.2.80.209
*Mar 25 15:47:45.399: ISAKMP: set new node -2061951065 to QM_IDLE *Mar 25 15:47:45.411:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:45.411: ISAKMP:(0:1:HW:2):purging node -2061951065 *Mar 25 15:47:45.411:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:45.411: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_DEST_SA

*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting SA reason "peers alive" state
(I) QM_IDLE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.415: ISAKMP: Unlocking IKE struct 0x81E5C4E8 for
isadb_mark_sa_deleted(), count 0
*Mar 25 15:47:45.415: ISAKMP: Deleting peer node by peer_reap for 10.2.80.209:
81E5C4E8
*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting node -1067612752 error TRUE
reason "peers alive"
*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting node -114443536 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):deleting node 2116015069 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):deleting node -1981865558 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):Input = IKE_MESG_INTERNAL, IKE_PHASE1_DEL *Mar 25
15:47:45.419: ISAKMP:(0:1:HW:2):Old State = IKE_DEST_SA New State =
IKE_DEST_SA

*Mar 25 15:47:45.419: ISAKMP: received ke message (4/1)
*Mar 25 15:47:45.419: ISAKMP: received ke message (3/1)
*Mar 25 15:47:45.423: ISAKMP: ignoring request to send delete notify (no ISAKMP
sa) src 10.1.32.14 dst 10.2.80.209 for SPI 0x3A7B69BF

```

```

*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting SA reason "" state (I)
MM_NO_STATE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node -1067612752 error FALSE
reason ""
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node -114443536 error FALSE
reason ""
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node 2116015069 error FALSE
reason ""
*Mar 25 15:47:45.427: ISAKMP:(0:1:HW:2):deleting node -1981865558 error FALSE
reason ""
*Mar 25 15:47:45.427: ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH *Mar 25
15:47:45.427: ISAKMP:(0:1:HW:2):Old State = IKE_DEST_SA New State =
IKE_DEST_SA

```

The above message shows what happens when the remote peer is unreachable. The router sends one DPD R_U_THERE message and four retransmissions before it finally deletes the IPSec and IKE SAs.

DPD and Cisco IOS Keepalives Used in Conjunction with Multiple Peers in a Crypto Map: Example

The following example shows that DPD and Cisco IOS keepalives are used in conjunction with multiple peers in a crypto map configuration when IKE will be used to establish the security associations (SAs). In this example, an SA could be set up to the IPSec peer at 10.0.0.1, 10.0.0.2, or 10.0.0.3.

```

crypto map green 1 ipsec-isakmp
  set peer 10.0.0.1
  set peer 10.0.0.2
  set peer 10.0.0.3
  set transform-set txfm
  match address 101

```

DPD Used in Conjunction with Multiple Peers for an Easy VPN Remote: Example

The following example shows that DPD is used in conjunction with multiple peers in an Easy VPN remote configuration. In this example, an SA could be set up to the IPSec peer at 10.10.10.10, 10.2.2.2, or 10.3.3.3.

```

crypto ipsec client ezvpn ezvpn-config
  connect auto
  group unity key preshared
  mode client
  peer 10.10.10.10
  peer 10.2.2.2
  peer 10.3.3.3

```

Additional References

The following sections provide references related to IPSec Dead Peer Detection Periodic Message Option.

Related Documents

| Related Topic | Document Title |
|-------------------|---|
| Configuring IPSec | “IP Security and Encryption” section of <i>Cisco IOS Security Configuration Guide</i> |
| IPSec commands | <i>Cisco IOS Security Command Reference</i> , Release 12.4 T |

Standards

| Standards | Title |
|---|-------|
| No new or modified standards are supported by this feature. | — |

MIBs

| MIBs | MIBs Link |
|--|--|
| No new or modified MIBs are supported by this feature. | To locate and download MIBs for selected platforms, Cisco IOS 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 |
|---|--|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p>http://www.cisco.com/techsupport</p> |

Command Reference

This section documents only commands that are new or modified.

- [crypto isakmp keepalive](#)

crypto isakmp keepalive

To allow the gateway to send dead peer detection (DPD) messages to the peer, use the **crypto isakmp keepalive** command in global configuration mode. To disable keepalives, use the **no** form of this command.

crypto isakmp keepalive *seconds* [*retries*] [**periodic** | **on-demand**]

no crypto isakmp keepalive *seconds* [*retries*] [**periodic** | **on-demand**]

Syntax Description

| | |
|------------------|---|
| <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. When the on-demand keyword is used, this argument is the number of seconds during which traffic is not received from the peer before DPDs are sent if there is data (IPSec) traffic to send; the range is from 10 to 3600 seconds. Note If you do not specify a time interval, an error message appears. |
| <i>retries</i> | (Optional) Number of seconds between DPD retries if the DPD message fails; the range is from 2 to 60 seconds. If unspecified, the default is 2 seconds. |
| periodic | (Optional) DPD messages are sent at regular intervals. |
| on-demand | (Optional) The default behavior. DPD retries are sent on demand. Note Because this option is the default, the on-demand keyword does not appear in configuration output. |

Command Default

No DPD messages are sent.

Command Modes

Global configuration (config)

Command History

| Release | Modification |
|-------------|--|
| 12.2(8)T | This command was introduced. |
| 12.3(7)T | The periodic and on-demand keywords were added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco 12.2SX family of releases. Support in a 12.2SX release is dependent on your feature set, platform, and platform hardware. |

Usage Guidelines

Use the **crypto isakmp keepalive** command to enable the gateway to send DPD messages to the peer. DPD is a keepalives scheme that allows the router to query the liveness of its Internet Key Exchange (IKE) peer.

Use the **periodic** keyword to configure your router so that DPD messages are “forced” at regular intervals. This forced approach results in earlier detection of dead peers than with the on-demand approach. If you do not configure the periodic option, the router defaults to the on-demand approach.

**Note**

When the **crypto isakmp keepalive** command is configured, the Cisco IOS software negotiates the use of Cisco IOS keepalives or DPD, depending on which protocol the peer supports.

Examples

The following example shows how to configure DPD messages to be sent every 60 seconds and every 5 seconds between retries if the peer does not respond:

```
crypto isakmp keepalive 60 5
```

The following example shows that periodic DPD messages are to be sent at intervals of 10 seconds:

```
crypto isakmp keepalive 10 periodic
```

The following example shows that the above periodic behavior is being disabled:

```
crypto isakmp keepalive 10 on-demand
```

Related Commands

| Command | Description |
|------------|-----------------------------|
| acl | Configures split tunneling. |

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2004–2007 Cisco Systems, Inc. All rights reserved.

■ `crypto isakmp keepalive`