IPSec デッド ピア検出定期メッセージ オプション

IPsec デッド ピア検出定期メッセージ オプション機能を使用すれば、ルータを、その Internet Key Exchange（IKE; インターネット キー エクスチェンジ）ピアの活性を定期的に照会するように設定できます。このオプションを使用すると、デフォルトのオンデマンド デッド ピア検出機能を使用した場合に比べ、停止しているピアをより早期に検出できます。

機能情報の入手

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IPSec デッド ピア検出定期メッセージ オプションの機能情報」（P.14）を参照してください。

プラットフォームのサポートと Cisco IOS および Catalyst OS ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

IPSec デッド ピア検出定期メッセージ オプションの前提条件

IPSec デッド ピア検出定期メッセージ オプション機能を設定するには、次のことが必要です。

- IP Security（IPsec; IP セキュリティ）の設定についての知識。
- DPD（Dead Peer Detection）がサポートされている IKE ピア。Cisco VPN 3000 コンセントレータ、Cisco PIX ファイアウォール、Cisco VPN クライアント、すべてのモードの動作（サイト間）における Cisco IOS ソフトウェア、Easy VPN Remote、および Easy VPN サーバなどの DPD がサポートされている実装。

IPSec デッド ピア検出定期メッセージ オプションの制約事項

定期的な DPD を使用すると、ルータによって、オンデマンドの DPD と比較してより速い応答時間で無応答の IKE ピアを検知できる可能性があります。ただし、定期的な DPD では、余分なオーバーヘッドが発生します。大量の IKE ピアと通信する場合は、オンデマンドの DPD の方を検討してください。

IPSec デッド ピア検出定期メッセージ オプションに関する情報

IPSec デッド ピア検出定期メッセージ オプションを設定するには、次の概念を理解しておく必要があります。

- 「DPD および Cisco IOS キープアライブ機能の動作」（P.2）
- 「IPSec デッド ピア検出定期メッセージ オプションの使用」（P.3）
- 「クリプト マップ内の複数のピアとの DPD および Cisco IOS キープアライブ機能の使用」（P.3）
- 「Easy VPN Remote コンフィギュレーション内での DPD の使用」（P.3）

DPD および Cisco IOS キープアライブ機能の動作

DPD and Cisco IOS キープアライブは、タイマーを基に機能します。タイマーが 10 秒に設定されている場合、10 秒毎に「hello」メッセージが送信されます（もちろん、ルータによってピアからの「hello」メッセージが受信された場合は除きます）。IOS キープアライブおよび定期的な DPD の利点は、デッド ピアの検知が早くなることです。しかし、IOS キープアライブおよび定期的な DPD では、かなりの頻度でメッセージを定期的に送信する必要があります。頻繁にメッセージを送信する結果、通信を行うピアによって暗号化および復号化しなければならないパケット数が増加します。

DPD にはオンデマンド方式もあります。対称的なこのオンデマンド方式がデフォルトです。オンデマンド DPD では、トラフィック パターンに基づいてメッセージが送信されます。たとえば、ルータによって発信トラフィックが送信される必要があり、ピアの活性に疑問がある場合、ルータによって DPD メッセージが送信され、ピアのステータスが照会されます。ルータに送信するトラフィックがない場合、DPD メッセージは送信されません。ピアが停止しており、ピアに送信するトラフィックがルータにない場合、IKE または IPsec Security Association（SA; セキュリティ アソシエーション）のキー再生成が必要でないかぎり、ルータによる検知は行われません（ルータによるピアとの通信が行わ

れない場合、ピアの活性は重要ではありません）。一方、ピアに送信するトラフィックがルータにあり、ピアの応答がない場合は、ピアのステートを判断するために、ルータによって DPD メッセージが開始されます。

IPSec デッド ピア検出定期メッセージ オプションの使用

IPSec デッド ピア検出定期メッセージ オプション機能では、DPD メッセージが定期的に「強制される」ように、ルータを設定できます。この強制方式の結果、デッド ピアが早期に検知されます。たとえば、送信するトラフィックがルータにない場合でも、DPD メッセージが定期的に送信され、ピアが停止していた場合、IKE SA による検知がタイムアウトになるまでルータが待機する必要はありません。

DPD Periodic Message Option を設定する場合、**crypto isakmp keepalive** コマンドを **periodic** キーワードを指定して使用する必要があります。**periodic** キーワードを指定しない場合、ルータはデフォルトでオンデマンド方式になります。

（注） **crypto isakmp keepalive** コマンドを設定すると、Cisco IOS ソフトウェアよって、Cisco IOS キープアライブまたは DPD（ピアでサポートされているプロトコルによります）の使用についてネゴシエーションが行われます。

クリプト マップ内の複数のピアとの DPD および Cisco IOS キープアライブ機能の使用

DPD および IOS キープアライブ機能をクリプト マップ内の複数のピアと組み合せて使用し、ステートレス フェールオーバーを実現できます。DPD により、ルータによる停止 IKE ピアの検知が可能となり、ルータによって停止状態が検知されると、ルータによってピアに対する IPsec と IKE SA が削除されます。複数のピアを設定している場合、ルータによって、次にリストされているピアへの切り替えが行われ、ステートレス フェールオーバーが実現します。

Easy VPN Remote コンフィギュレーション内での DPD の使用

Easy VPN Remote コンフィギュレーション内で DPD を使用できます。「Easy VPN Remote の DPD の設定」（P.6）を参照してください。

IPSec デッド ピア検出定期メッセージ オプションの設定方法

ここでは、次の作業について説明します。

定期的な DPD メッセージの設定

定期的な DPD メッセージを設定するには、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**crypto isakmp keepalive** *seconds* [*retry-seconds*] [**periodic** | **on-demand**] **例**： `Router (config)# crypto isakmp keepalive 10 periodic`	ゲートウェイによるピアへの DPD メッセージの送信を許可します。 • *seconds*：**periodic** キーワードを使用する場合、この引数には DPD メッセージの間隔を秒数で指定します。範囲は 10 ～ 3600 秒です。 **on-demand** キーワードを使用する場合、この引数には、送信するデータ（IPSec）トラフィックがあるときに、DPD リトライ メッセージを送信するまでにピアからトラフィックを受信しない間待機する秒数を指定します。範囲は 10 ～ 3600 秒です。 **（注）** 間隔を指定しない場合、エラー メッセージが表示されます。 • *retry-seconds*：（任意）ピアによって DPD リトライ メッセージが失われた場合の DPD リトライ メッセージの送信間隔を秒数で指定します。範囲は 2 ～ 60 秒です。 1 つの DPD メッセージがピアで失われると、ルータはよりアグレッシブな状態に移行し、より短いリトライ間隔で DPD リトライ メッセージを送信します。ピアによって DPD リトライ メッセージが失われた場合のこの間隔は、DPD リトライ間の秒数です。デフォルトの DPD リトライ メッセージは 2 秒間隔で送信されます。アグレッシブな 5 回の DPD リトライ メッセージが失われると、トンネルがダウンした状態としてマークされます。 **（注）** IPsec High Availability（HA; ハイ アベイラビリティ）を使用して DPD を設定するには、デフォルト（2 秒）以外の値を使用することを推奨します。HA には、キープアライブ時間を 10 秒、試行を 5 回に設定するのが適しています。その時間が、ルータがアクティブ モードになるためにかかる時間であるからです。 • **periodic**：（任意）DPD メッセージが定期的に送信されます。 • **on-demand**：（任意）デフォルトの動作です。DPD リトライがオンデマンドで送信されます。 **（注）** このオプションはデフォルトであるため、**on-demand** キーワードは設定の出力に表示されません。

クリプト マップ内の複数のピアとの DPD および Cisco IOS キープアライブの設定

DPD および IOS キープアライブを、クリプト マップと組み合せて使用するように設定し、ステートレス フェールオーバーを実現するには、次の手順を実行します。この設定により、最初のピアが停止していることが検知されると、ルータによってピア リストが循環されます。

手順の概要

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*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name seq-num* **ipsec-isakmp** **例：** `Router (config)# crypto map green 1 ipsec-isakmp`	クリプト マップ コンフィギュレーション モードを開始して、クリプト マップ エントリを作成または変更します。 • **ipsec-isakmp** キーワードは、このクリプト マップ エントリによって指定されたトラフィックを保護するための IPsec SA を確立するために、IKE が使用されることを示します。
ステップ 4	**set peer** {*host-name* [**dynamic**]	*ip-address*} **例：** `Router (config-crypto-map)# set peer 10.12.12.12`	クリプト マップ内の IPsec ピアを指定します。 • このコマンドを繰り返すことによって、複数のピアを指定できます。
ステップ 5	**set transform-set** *transform-set-name* **例：** `Router (config-crypto-map)# set transform-set txfm`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。 • このコマンドを繰り返すことによって、複数のトランスフォーム セットを指定できます。
ステップ 6	**match address** [*access-list-id*	*name*] **例：** `Router (config-crypto-map)# match address 101`	クリプト マップ エントリの拡張アクセス リストを指定します。

Easy VPN Remote の DPD の設定

Easy VPN Remote コンフィギュレーション内で DPD を設定するには、次の手順を実行します。また、この設定により、最初のピアが停止していることがルータで検知されると、ルータによってピア リストが循環されます。

（注） Easy VPN Remote コンフィギュレーション用の IOS キープアライブはサポートされていません。

手順の概要

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*}

手順の詳細

ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec client ezvpn** *name* **例：** `Router (config)# crypto ipsec client ezvpn ezvpn-config1`	Cisco Easy VPN Remote コンフィギュレーションを作成し、Cisco Easy VPN Remote コンフィギュレーション モードを開始します。
ステップ 4	**connect** {**auto** | **manual**} **例：** `Router (config-crypto-ezvpn)# connect manual`	要求に応じて、IPsec VPN トンネルを手動で確立および終了します。 • **auto** キーワード オプションはデフォルト設定です。
ステップ 5	**group** *group-name* **key** *group-key* **例：** `Router (config-crypto-ezvpn)# group unity key preshared`	Virtual Private Network（VPN; バーチャル プライベート ネットワーク）接続用のグループ名およびキー値を指定します。
ステップ 6	**mode** {**client** | **network-extension**} **例：** `Router (config-crypto-ezvpn)# mode client`	ルータの動作の VPN モードを指定します。
ステップ 7	**peer** {*ipaddress* | *hostname*} **例：** `Router (config-crypto-ezvpn)# peer 10.10.10.10`	VPN 接続に対して、ピアの IP アドレスまたはホスト名を設定します。 • ホスト名を指定できるのは、ルータから DNS サーバを介してホスト名解決を行える場合に限りにます。 • このコマンドは複数回繰り返して実行できます。

DPD がイネーブルになっていることの確認

DPD を使用すれば、ピアが到達不能になった時に、ルータによる IKE ステートのクリアが可能になります。DPD がイネーブルになっており、ピアがしばらくの間到達不能になった場合、**clear crypto session** コマンドを使用して、手動で IKE と IPsec SA をクリアできます。

debug crypto isakmp コマンドを使用して、DPD がイネーブルになっていることを確認できます。

手順の概要

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

手順の詳細

ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clear crypto session** [**local** *ip-address* [**port** *local-port*]] [**remote** *ip-address* [**port** *remote-port*]]	[**fvrf** *vrf-name*] [**ivrf** *vrf-name*] **例：** `Router# clear crypto session`	暗号セッション（IPsec および IKE SA）を削除します。
ステップ 3	**debug crypto isakmp** **例：** `Router# debug crypto isakmp`	IKE イベントに関するメッセージを表示します。

IPSec デッド ピア検出定期メッセージ オプションの設定例

ここでは、次の設定例について説明します。

定期的な DPD をイネーブルにしたサイト間設定

次の設定は、定期的な DPD をイネーブルにしていないサイト間設定用です。設定は、IKE フェーズ 1 ポリシー用と IKE 事前共有キー用です。

IKE フェーズ 1 ポリシー

```
crypto isakmp policy 1
  encryption 3des
  authentication pre-share
  group 2
!
```

IKE 事前共有キー

```
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
!
```

DPD をイネーブルにした Easy VPN Remote：例

次の設定は、ルータに対して、30 秒毎に定期的な DPD メッセージを送信するように指示するものです。ピアによる DPD R_U_THERE メッセージに対する応答が失敗した場合、ルータによって、20 秒毎にメッセージが再送信されます（全部で 4 回の転送）。

```
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
```

debug crypto isakmp コマンドを使用した DPD 設定の確認：例

次の **debug crypto isakmp** コマンドの出力例では、IKE DPD がイネーブルになっていることを確認しています。

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

IKE DPD がイネーブルになっていること（および、ピアによって DPD がサポートされていること）を確認するには、定期的な DPD をイネーブルにする時に、コマンドによって指定された間隔で次のデバッグ メッセージが出力されることを確認する必要があります。

```
*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_MESG_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
```

上記のメッセージは、DPD R_U_THERE メッセージの送信に対応しています。

```
*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_MESG_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
```

上記のメッセージは、ピアからの確認応答（ACK）メッセージに対応しています。

```
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_MESG_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_MESG_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_MESG_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_MESG_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
```

上記のメッセージは、リモート ピアが到達不能なっている時に何が発生しているのかを示しています。ルータによって、最終的に IPsec および SA が削除される前に、1 つの DPD R_U_THERE メッセージおよび 4 つの転送が送信されます。

クリプト マップ内の複数のピアとの組み合せで使用される DPD および Cisco IOS キープアライブ

次に、SA を確立するために IKE が使用される場合、DPD および Cisco IOS キープアライブがクリプト マップ設定内の複数のピアとの組み合せで使用される例を示します。この例では、SA が、10.0.0.1、10.0.0.2、または 10.0.0.3 の IPsec ピアに設定される可能性があります。

```
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
```

Easy VPN Remote の複数のピアとの組み合せで使用される DPD：例

次に、DPD が Easy VPN Remote コンフィギュレーション内の複数のピアとの組み合せで使用される例を示します。この例では、SA が、10.10.10.10、10.2.2.2、または 10.3.3.3 の IPsec ピアに設定される可能性があります。

```
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
```

その他の参考資料

次の項では、IPSec デッド ピア検出定期メッセージ オプション機能の関連資料を示します。

関連資料

内容	参照先
IPsec の設定	「*Configuring Security for VPNs with IPsec*」
IPsec コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
DPD は、インターネット ドラフト「draft-ietf-ipsec-dpd-04.txt」に準拠しています。このドラフトは、Informational RFC（番号はまだ割り当てられていません）として公表の検討中です。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

IPSec デッド ピア検出定期メッセージ オプションの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連の Cisco IOS ソフトウェア リリースでもサポートされます。

表 1　IPSec デッド ピア検出定期メッセージ オプションの機能情報

機能名	リリース	機能情報
IPsec Dead Peer Detection Periodic Message Option	12.3(7)T 12.2(33)SRA 12.2(33)SXH	IPsec デッド ピア検出定期メッセージ オプション機能を使用すれば、ルータを、その IKE ピアの活性を定期的に照会するように設定できます。このオプションを使用すると、デフォルトのオンデマンド デッド ピア検出機能を使用した場合に比べ、停止しているピアをより早期に検出できます。 この機能は、Cisco IOS Release 12.3(7)T で導入されました。 この機能は、Cisco IOS Release 12.2(33)SRA に統合されました。 この機能は、Cisco IOS Release 12.2(33)SXH に統合されました。 次のコマンドが導入または変更されました。 **crypto isakmp keepalive**