Invalid Security Parameter Index Recovery

IP Security（IPsec; IP セキュリティ）パケットの処理中に無効なセキュリティ パラメータ インデックス エラー（「Invalid SPI」として表示されます）が発生した場合、機能によって、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）Security Association（SA; セキュリティ アソシエーション）を確立できます。「IKE」モジュールによって「Invalid SPI」エラーの通知が、発信側の IPsec ピアに対して送信され、Security Association Database（SADB）の再同期化と、成功したパケット処理のレジュームが可能になります。

この章で紹介する機能情報の入手方法

*ご使用の Cisco IOS 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。*この章に記載されている特定の機能に関する説明へのリンク、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、「Invalid Security Parameter Index Recovery の機能情報」（P.17）を参照してください。

プラットフォーム、Cisco IOS ソフトウェア イメージ、および Catalyst OS ソフトウェア イメージの各サポート情報を検索するには

Cisco Feature Navigator を使用すると、プラットフォーム、Cisco IOS ソフトウェア イメージ、および Cisco Catalyst OS ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

Invalid Security Parameter Index Recovery の前提条件

機能を設定する前に、ルータ上で IKE および IPsec をイネーブルにしておく必要があります。

Invalid Security Parameter Index Recovery の制約事項

IPsec ピアに対して「Invalid SPI」エラーを通知するために IKE SA を開始する場合、Denial-of-Service（DoS; サービス拒絶）攻撃が発生するリスクがあります。機能には、そのようなリスクを最小化するためのメカニズムが内蔵されていますが、リスクが存在するため、機能は、デフォルトではイネーブルになっていません。Command-Line Interface（CLI; コマンドライン インターフェイス）を使用してコマンドをイネーブルにする必要があります。

Invalid Security Parameter Index Recovery に関する情報

機能を使用するには、次の概念を理解しておく必要があります。

- 「機能の動作」（P.2）

機能の動作

ある IPsec ピアが「死ぬ」（たとえば、リブートが発生したり、IPsec ピアが何らかの理由によりリセットされたりした場合にピアが応答しなくなる可能性があります）と、IPsec の「ブラック ホール化」が発生します。ピアの 1 つ（受信側のピア）は完全にリセットされるため、そのピアでは他のピアとの IKE SA が失われます。一般に、IPsec ピアによって、SA を検出できないパケットが受信されると、そのピアによって、そのデータの発信者に対する IKE「INVALID SPI NOTIFY」メッセージの送信が試行されます。この通知は IKE SA を使用して送信されます。IKE SA が使用できない場合、受信側のピアによってパケットが廃棄されます。

（注） 1 つの SA のピアは 2 つだけです。しかし、SADB は複数の SA を持てます。これにより、各 SA は異なるピアとのアソシエーションを持ちます。

無効な Security Parameter Index（SPI; セキュリティ パラメータ インデックス）が発生した場合、Invalid Security Parameter Index 機能によって、データの発信者との IKE SA が設定され、IKE「INVALID SPI NOTIFY」メッセージが送信されます。データを発信したピアによって「INVALID SPI NOTIFY」メッセージが「検出」され、無効な SPI を持つ IPsec SA が削除されます。発信側のピアからトラフィックがさらにある場合、IPsec SA は存在せず、新しい SA が設定されます。トラフィックが再び流れます。デフォルトの動作（つまり、機能が設定されていない状態）では、無効な SPI エラーの原因となったデータ パケットは廃棄されます。発信側のピアによって、無効な SPI を持つ IPsec SA を使用したデータの送信が続けられ、受信側のピアによってトラフィックが廃棄され続けます（その結果、「ブラック ホール」が作成されます）。

IPsec モジュールでは、IKE モジュールが使用されて、他のピアに IKE 「INVALID SPI NOTIFY」メッセージが送信されます。無効な SPI リカバリが行われると、IPsec SA の設定自体によっていくつかのパケットが廃棄されますが、意味のあるパケット廃棄は一切行われません。

機能用にルータを設定するには、**crypto isakmp invalid-spi-recovery** コマンドを使用します。IKE SA は、このコマンドを設定しない限り開始されません。

Invalid Security Parameter Index Recovery の設定方法

ここでは、次の各手順について説明します。

Invalid Security Parameter Index Recovery の設定

Invalid Security Parameter Index Recovery 機能を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp invalid-spi-recovery**

手順の詳細

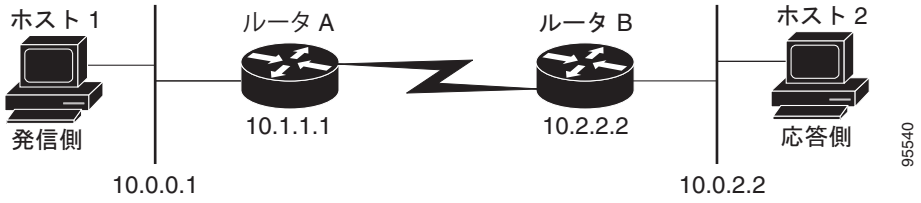
	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp invalid-spi-recovery** **例：** `Router (config)# crypto isakmp invalid-spi-recovery`	IKE モジュール プロセスを開始します。それにより、IKE モジュールによって、受信側ピアに対して「Invalid SPI」エラーが発生したことが通知されます。

設定の確認

2 つのピア間におけるトラフィックに関する IPsec SA のステートを確認するには、**show crypto ipsec sa** コマンドを使用します。IPsec SA が、あるピアでは使用可能で、他のピアでは使用不可の場合、「ブラック ホール化」の状況が発生します。この場合、無効な SPI エラーが受信側のピアのログに記録されます。コンソール ロギングをオンにするか、シスログ サーバを確認すると、これらのエラーもログに記録されていることがわかります。

図 1 に、一般的な事前共有設定を示します。ホスト 1 が発信側のピア（発信側）を開始し、ホスト 2 が受信側のピア（応答側）を開始しています。

図 1　　事前共有設定トポロジ



手順の概要

事前共有設定を確認するには、次の手順を実行します。

1. **ホスト 1 とホスト 2 の間における IKE および IPsec SA を開始します。**
2. **ルータ B 上の IKE および IPsec SA をクリアします。**
3. **ホスト 1 からのトラフィックをホスト 2 に送信し、IKE および IPsec SA が正しく確立されているかどうかを確認します。**
4. **ルータ B に無効な SPI メッセージがないか確認します。**

手順の詳細

ステップ 1　**ホスト 1 とホスト 2 の間における IKE および IPsec SA を開始します。**

ルータ A

```
Router# show crypto isakmp sa

  f_vrf/i_vrf   dst            src             state       conn-id slot
       / 10.2.2.2              10.1.1.1        QM_IDLE               1       0
```

ルータ B

```
Router# show crypto isakmp sa

  f_vrf/i_vrf   dst            src             state       conn-id slot
       /        10.1.1.1       10.2.2.2        QM_IDLE               1       0
```

ルータ A

```
Router# show crypto ipsec sa interface fastethernet0/0

interface: FastEthernet0/0
    Crypto map tag: testtag1, local addr. 10.1.1.1
```

```
protected vrf:
local  ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
current_peer: 10.2.2.2:500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
 #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.2
  path mtu 1500, media mtu 1500
  current outbound spi: 7AA69CB7

  inbound esp sas:
   spi: 0x249C5062(614223970)
     transform: esp-des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 5123, flow_id: 1, crypto map: testtag1
     crypto engine type: Hardware
     sa timing: remaining key lifetime (k/sec): (4537831/3595)
     IV size: 8 bytes
     replay detection support: Y

  inbound ah sas:
   spi: 0xB16D1587(2976716167)
     transform: ah-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 5121, flow_id: 1, crypto map: testtag1
     crypto engine type: Hardware
     sa timing: remaining key lifetime (k/sec): (4537831/3595)
     replay detection support: Y

  inbound pcp sas:

  outbound esp sas:
   spi: 0x7AA69CB7(2057739447)
     transform: esp-des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 5124, flow_id: 2, crypto map: testtag1
     crypto engine type: Hardware
     sa timing: remaining key lifetime (k/sec): (4537835/3595)
     IV size: 8 bytes
     replay detection support: Y

  outbound ah sas:
   spi: 0x1214F0D(18960141)
     transform: ah-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 5122, flow_id: 2, crypto map: testtag1
     crypto engine type: Hardware
     sa timing: remaining key lifetime (k/sec): (4537835/3594)
     replay detection support: Y

  outbound pcp sas:
```

ルータ B

```
Router# show crypto ipsec sa interface ethernet1/0

interface: Ethernet1/0
    Crypto map tag: testtag1, local addr. 10.2.2.2

   protected vrf:
   local  ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
   current_peer: 10.1.1.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0

    #send errors 0, #recv errors 0

     local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: 249C5062

     inbound esp sas:
      spi: 0x7AA69CB7(2057739447)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5123, flow_id: 1, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4421281/3593)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0x1214F0D(18960141)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5121, flow_id: 1, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4421281/3593)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0x249C5062(614223970)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5124, flow_id: 2, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4421285/3593)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
      spi: 0xB16D1587(2976716167)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5122, flow_id: 2, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4421285/3592)
        replay detection support: Y

     outbound pcp sas:
```

ステップ 2 ルータ B 上の IKE および IPsec SA をクリアします。

```
Router# clear crypto isakmp

Router# clear crypto sa

Router# show crypto isakmp sa

  f_vrf/i_vrf   dst            src             state       conn-id slot
       /        10.2.2.2.       10.1.1.1      MM_NO_STATE           1       0 (deleted)

Router# show crypto ipsec sa

interface: Ethernet1/0
    Crypto map tag: testtag1, local addr. 10.2.2.2


   protected vrf:
   local  ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
   current_peer: 10.1.1.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: 0

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:
```

ステップ 3 ホスト 1 からのトラフィックをホスト 2 に送信し、新しい IKE および IPsec SA が正しく確立されているかどうかを確認します。

```
ping
Protocol [ip]: ip
Target IP address: 10.0.2.2
Repeat count [5]: 30
Datagram size [100]: 100
Timeout in seconds [2]:
Extended commands [n]: no
Sweep range of sizes [n]: n
Type escape sequence to abort.
Sending 30, 100-byte ICMP Echos to 10.0.2.2, timeout is 2 seconds:
..!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 93 percent (28/30), round-trip min/avg/max = 1/3/8 ms

RouterB# show crypto isakmp sa
```

```
  f_vrf/i_vrf   dst            src             state       conn-id slot
       /        10.1.1.1       10.2.2.2     QM_IDLE              3       0
       /        10.1.1.1       10.2.2.2      MM_NO_STATE          1       0 (deleted)

RouterB# show crypto ipsec sa

interface: Ethernet1/0
    Crypto map tag: testtag1, local addr. 10.2.2.2

   protected vrf:
   local  ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
   current_peer: 10.1.1.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
    #pkts decaps: 28, #pkts decrypt: 28, #pkts verify: 28
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0

    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: D763771F

     inbound esp sas:
      spi: 0xE7AB4256(3886760534)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5127, flow_id: 3, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4502463/3596)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0xF9205CED(4179647725)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5125, flow_id: 3, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4502463/3596)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0xD763771F(3613619999)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5128, flow_id: 4, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4502468/3596)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
      spi: 0xEB95406F(3952427119)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5126, flow_id: 4, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4502468/3595)
```

```
        replay detection support: Y

     outbound pcp sas:

RouterA# show crypto isakmp sa

  f_vrf/i_vrf   dst            src             state       conn-id slot
       /        10.2.2.2       10.1.1.1      MM_NO_STATE           1       0 (deleted)
       /        10.2.2.2       10.1.1.1      QM_IDLE               2       0


               Check for an invalid SPI message on Router B
Router# show logging


Syslog logging: enabled (10 messages dropped, 13 messages rate-limited, 0 flushes, 0
overruns, xml disabled)
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled
    Buffer logging: level debugging, 43 messages logged, xml disabled
    Logging Exception size (8192 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 72 message lines logged

Log Buffer (8000 bytes):

*Mar 24 20:55:45.739: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid
spi for
        destaddr=10.2.2.2, prot=51, spi=0x1214F0D(18960141), srcaddr=10.1.1.1
*Mar 24 20:55:47.743: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/255.255.255.255/0/0 (type=1),
    remote_proxy= 10.0.0.1/255.255.255.255/0/0 (type=1),
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar 24 20:55:47.743: IPSEC(validate_proposal_request): proposal part #2,
  (key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/255.255.255.255/0/0 (type=1),
    remote_proxy= 10.0.0.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar 24 20:55:47.743: IPSEC(kei_proxy): head = testtag1, map->ivrf = , kei->ivrf =
*Mar 24 20:55:47.743: IPSEC(key_engine): got a queue event with 2 kei messages
*Mar 24 20:55:47.743: IPSEC(spi_response): getting spi 4179647725 for SA
        from 10.2.2.2        to 10.1.1.1     for prot 2
*Mar 24 20:55:47.747: IPSEC(spi_response): getting spi 3886760534 for SA
        from 10.2.2.2     to 10.1.1.1        for prot 3
*Mar 24 20:55:48.071: IPSec: Flow_switching Allocated flow for flow_id 939524099
*Mar 24 20:55:48.071: IPSec: Flow_switching Allocated flow for flow_id 939524100
*Mar 24 20:55:48.135: IPSEC(key_engine): got a queue event with 4 kei messages
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xF9205CED(4179647725), conn_id= 939529221, keysize= 0, flags= 0x2
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
    protocol= AH, transform= ah-sha-hmac ,
```

```
    lifedur= 3600s and 4608000kb,
    spi= 0xEB95406F(3952427119), conn_id= 939529222, keysize= 0, flags= 0xA
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xE7AB4256(3886760534), conn_id= 939529223, keysize= 0, flags= 0x2
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-sha-hmac ,

    lifedur= 3600s and 4608000kb,
    spi= 0xD763771F(3613619999), conn_id= 939529224, keysize= 0, flags= 0xA
*Mar 24 20:55:48.139: IPSEC(kei_proxy): head = testtag1, map->ivrf = , kei->ivrf =
*Mar 24 20:55:48.139: IPSEC(mtree_add_ident): src 10.2.2.2, dest 10.1.1.1, dest_port 0

*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.1.1.1, sa_prot= 51,
    sa_spi= 0xF9205CED(4179647725),
    sa_trans= ah-sha-hmac , sa_conn_id= 939529221
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.2.2.2, sa_prot= 51,
    sa_spi= 0xEB95406F(3952427119),
    sa_trans= ah-sha-hmac , sa_conn_id= 939529222
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.1.1.1, sa_prot= 50,
    sa_spi= 0xE7AB4256(3886760534),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 939529223
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.2.2.2, sa_prot= 50,
    sa_spi= 0xD763771F(3613619999),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 939529224
ipseca-72a#
```

Invalid Security Parameter Index Recovery の設定例

ここでは、次の設定例について説明します。

- 「Invalid Security Parameter Index Recovery：例」（P.10）

Invalid Security Parameter Index Recovery：例

次に、Invalid Security Parameter Index Recovery がルータ A とルータ B に設定されている例を示します。図 1 に、この例で使用されているトポロジを示します。

ルータ A

```
Router# show running-config

Building configuration...

Current configuration : 2048 bytes
!
version 12.3
no service pad
```

```
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service tcp-small-servers
!
hostname ipseca-71a
!
logging queue-limit 100
no logging console
enable secret 5 $1$4GZB$L2YOmnenOCNAu0jgFxebT/
enable password lab
!
clock timezone PST -8

clock summer-time PDT recurring
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
mpls ldp logging neighbor-changes
no ftp-server write-enable
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 180
crypto isakmp key 0 1234 address 10.2.2.2
crypto isakmp invalid-spi-recovery
!
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag1 10 ipsec-isakmp
 set peer 10.2.2.2
 set transform-set auth2
 match address 150
!
!
controller ISA 5/1
!
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.0.0.0
 no ip route-cache cef
 duplex full
 speed 100
 crypto map testtag1
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.0.0.0
 no ip route-cache cef
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
```

```
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
 clockrate 128000
!
interface Serial1/1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
 clockrate 128000
!

interface Serial1/2
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
!
interface Serial1/3
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 no keepalive
 serial restart_delay 0
 clockrate 128000
!
ip classless
ip route 10.3.3.3 255.0.0.0 10.2.0.1
no ip http server
no ip http secure-server
!
!
access-list 150 permit ip host 10.0.0.1 host 10.0.2.2
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
call rsvp-sync
!
!
mgcp profile default
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password lab
 login
!
!
end

ipseca-71a#
```

ルータ B

```
Router# show running-config

Building configuration...

Current configuration : 2849 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname ipseca-72a
!

logging queue-limit 100
no logging console
enable secret 5 $1$kKqL$5Th5Qhw1ubDkkK90KWFxi1
enable password lab
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
mpls ldp logging neighbor-changes
no ftp-server write-enable
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 180
crypto isakmp key 0 1234 address 10.1.1.1
crypto isakmp invalid-spi-recovery
!
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag1 10 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set auth2
 match address 150
!
!
controller ISA 5/1
!
!
interface FastEthernet0/0
```

```
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/0
 ip address 10.2.2.2 255.0.0.0
 no ip route-cache cef
 duplex half
 crypto map testtag1
!
interface Ethernet1/1
 ip address 10.0.2.2 255.0.0.0
 no ip route-cache cef
 duplex half
!
interface Ethernet1/2
 no ip address

 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/3
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/4
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/5
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/6
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/7
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Serial3/0
 no ip address
 no ip route-cache
 no ip mroute-cache
```

```
 shutdown
 serial restart_delay 0
!
interface Serial3/1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
 clockrate 128000
!
interface Serial3/2
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
!
interface Serial3/3
 no ip address

 no ip route-cache
 no ip mroute-cache
 shutdown
 no keepalive
 serial restart_delay 0
 clockrate 128000
!
ip classless
ip route 10.0.0.0 255.0.0.0 10.2.0.1
no ip http server
no ip http secure-server
!
!
access-list 150 permit ip host 10.0.2.2 host 10.0.0.1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password lab
 login
!
!
end
```

その他の参考資料

次の項では、Invalid Security Parameter Index Recovery に関連した参考資料を示します。

関連資料

内容	参照先
IKE の設定	「*Configuring Internet Key Exchange for IPsec VPNs*」
インターフェイス コマンド	『*Cisco IOS Master Command List*』

規格

規格	タイトル
この機能には、新しいまたは変更された規格はありません。	—

MIB

MIB	MIB リンク
この機能には、新しいまたは変更された MIB はありません。	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
この機能には、新しいまたは変更された RFC はありません。	—

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

コマンド リファレンス

次のコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。

- **crypto isakmp invalid-spi-recovery**

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

Cisco IOS の全コマンドを参照する場合は、Command Lookup Tool（http://tools.cisco.com/Support/CLILookup）にアクセスするか、または『Master Command List』を参照してください。

Invalid Security Parameter Index Recovery 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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。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　Invalid Security Parameter Index Recovery の機能情報

機能名	リリース	機能情報
Invalid Security Parameter Index Recovery	12.3(2)T	この機能が追加されました。
	12.2(18)SXE	この機能は、Cisco IOS Release 12.2(18)SXE に統合されました。