CHAPTER 31

IPSec VPN SPA のトラブルシューティング

この章では、Cisco 7600 シリーズ ルータ上の IPSec VPN SPA のトラブルシューティングに関するさまざまな技法について説明します。

具体的な内容は次のとおりです。

一般的なトラブルシューティングの方法

ここでは、IPSec VPN SPA および Cisco 7600 SSC-400 のトラブルシューティングに関する一般的な情報を示します。具体的な内容は次のとおりです。

コンソールのエラー メッセージの解釈

Cisco 7600 シリーズ ルータには、注意を要するイベントをオペレータに通知するため、エラー メッセージなどのシステム メッセージを生成する機能があります。これらのメッセージは、コンソールに表示される場合もありますし、System Logging（Syslog プロトコルまたは SNMP［簡易ネットワーク管理プロトコル］）を使用してロギング ホストに送信される場合もあります。

マニュアルでは、一連のシステム エラー メッセージが、生成元のシステム ファシリティ別に記載されています。IPSec VPN SPA および Cisco 7600 SSC-400 のエラー メッセージには、次のファシリティ名が使用されます。

- IPSec VPN SPA — SPA_IPSEC
- Cisco 7600 SSC-400 — C7600_SSC400

Cisco 7600 シリーズ ルータ SIP および SPA に関連するメッセージなど、Cisco 7600 シリーズ ルータのエラー メッセージの説明および推奨される処置については、以下のマニュアルを参照してください。

- 『*Cisco 7600 Series Cisco IOS System Message Guide*』
- 『*Cisco IOS System Error Messages*』

debug コマンドの使用

Cisco 7600 シリーズ ルータに搭載されている SIP および SPA 固有のデバッグ情報を取得するには、Cisco 7600 シリーズ ルータでサポートされるその他の **debug** コマンドのほかに、**debug hw-module subslot** 特権 EXEC コマンドを使用できます。

debug hw-module subslot コマンドは、シスコシステムズのテクニカル サポート担当者による使用を前提としています。

注意　デバッグ出力には CPU プロセス内で高いプライオリティを割り当てられており、これによってシステムが使用不可能になる場合があります。そのため、**debug** コマンドは、特定の問題のトラブルシューティングを行う目的に限って使用するか、またはシスコ社のテクニカル サポート スタッフとのトラブルシューティング セッションの際に使用してください。また、**debug** コマンドは、ネットワーク トラフィックやユーザが少ない時間帯に使用することを推奨します。こうした時間帯のデバッグの実行は、**debug** コマンド処理によるオーバーヘッドの増加がシステム利用へ影響を与える可能性を減らすことができます。

使用できる暗号 debug コマンドについての詳細は、「暗号条件別デバッグの使用」（p.31-34）を参照してください。

Cisco 7600 シリーズ ルータでサポートされるその他の **debug** コマンドについての詳細は、『*Cisco IOS Debug Command Reference*』を参照してください。

show コマンドの使用

いくつかの **show** コマンドを使用して、Cisco 7600 シリーズ ルータに搭載されている IPSec VPN SPA のモニタリングおよびトラブルシューティングを行うことができます。

IPSec VPN SPA を検証し、モニタする **show** コマンドの詳細については、『*Cisco IOS Software Releases 12.2SR Command Reference*s』および『*Cisco IOS Software Releases 12.2SX Command References*』を参照してください。

セキュリティ関連の **show** コマンドについての詳細は、『*Cisco IOS Security Command Reference*』を参照してください。

IPSec VPN SPA のモニタリング

ここでは、IPSec VPN SPA のハードウェアおよび設定に関する情報を表示するための、各種コマンドについて説明します。具体的な内容は次のとおりです。

IPSec VPN SPA のハードウェアおよびシステム情報の表示

ハードウェアおよびシステム情報を表示するには、次のコマンドを使用します。

- **show diagbus** —「IPSec VPN SPA ポートに関する情報の表示」（p.31-4）を参照してください。
- **show crypto engine accelerator statistic slot** —「IPSec VPN SPA のプラットフォームおよびネットワーク インターフェイス コントローラ統計情報の表示」（p.31-4）を参照してください。
- **show hw-module slot fpd** —「ハードウェア リビジョン レベルに関する情報の表示」（p.31-6）を参照してください。

IPSec VPN SPA ポートに関する情報の表示

ルータに搭載されている SPA のタイプについての情報を表示するには、**show diagbus** コマンドを使用します。

以下に、Cisco 7600 シリーズ ルータのスロット 5 に搭載された Cisco 7600 SSC-400 のサブスロット 1 にある IPSec VPN SPA について、**show diagbus** コマンドの出力例を示します。

```
Router# show diagbus

Slot 5: Logical_index 10
        2-subslot Services SPA Carrier-400 controller
        Board is analyzed ipc ready
        HW rev 0.3, board revision A01
        Serial Number: abc Part number: 73-6348-01

        Slot database information:
        Flags: 0x2004   Insertion time: 0x3DB5F4BC (4d20h ago)

        Controller Memory Size:
                248 MBytes CPU Memory
                8 MBytes Packet Memory
                256 MBytes Total on Board SDRAM
   Cisco IOS Software, cwlc Software (smsc-DWDBG-M), Version 12.2(nightly.SRA060615)
   NIGHTLY BUILD, synched to rainier RAINER_BASE

        SPA Information:
        subslot 5/1: SPA-IPSEC-2G (0x3D7), status: ok
```

IPSec VPN SPA のプラットフォームおよびネットワーク インターフェイス コントローラ統計情報の表示

プラットフォームの統計情報を表示し、オプションとしてネットワーク インターフェイス コントローラの統計情報を表示するには、**show crypto engine accelerator statistic slot** コマンドを使用します。

次に、スロット 1、サブスロット 0 に搭載された IPSec VPN SPA のプラットフォーム統計情報、およびネットワーク インターフェイス コントローラの統計情報を表示する例を示します。

```
Router# show crypto engine accelerator statistic slot 1/0 detail

VPN module in slot 1/0


Decryption Side Data Path Statistics
====================================
Packets RX..............: 454260
Packets TX..............: 452480

IPSec Transport Mode.....: 0
IPSec Tunnel Mode........: 452470
AH Packets..............: 0
ESP Packets.............: 452470
GRE Decapsulations.......: 0
NAT-T Decapsulations.....: 0
Clear....................: 8
ICMP.....................: 0

Packets Drop.............: 193
Authentication Errors....: 0
Decryption Errors........: 0
Replay Check Failed......: 0
Policy Check Failed......: 0
Illegal CLear Packet.....: 0
GRE Errors..............: 0
SPD Errors..............: 0
HA Standby Drop..........: 0

Hard Life Drop...........: 0
Invalid SA..............: 191
SPI No Match............: 0
Destination No Match.....: 0
Protocol No Match........: 0

Reassembly Frag RX.......: 0
IPSec Fragments..........: 0
IPSec Reasm Done.........: 0
Clear Fragments..........: 0
Clear Reasm Done.........: 0
Datagrams Drop...........: 0
Fragments Drop...........: 0


Decryption Side Controller Statistics

====================================
Frames RX...............: 756088
Bytes RX................: 63535848
Mcast/Bcast Frames RX....: 2341
RX Less 128Bytes.........: 756025
RX Less 512Bytes.........: 58
RX Less 1KBytes..........: 2
RX Less 9KBytes..........: 3
RX Frames Drop...........: 0

Frames TX...............: 452365
Bytes TX................: 38001544
Mcast/Bcast Frames TX....: 9
TX Less 128Bytes.........: 452343
TX Less 512Bytes.........: 22
TX Less 1KBytes..........: 0
TX Less 9KBytes..........: 0


Encryption Side Data Path Statistics
```

```
====================================
Packets RX..............: 756344
Packets TX..............: 753880
IPSec Transport Mode.....: 0
IPSec Tunnel Mode........: 753869
GRE Encapsulations.......: 0
NAT-T Encapsulations.....: 0
LAF prefragmented........: 0

Fragmented..............: 0
Clear...................: 753904
ICMP....................: 0

Packets Drop............: 123
IKE/TED Drop............: 27
Authentication Errors....: 0
Encryption Errors........: 0
HA Standby Drop.........: 0

Hard Life Drop..........: 0
Invalid SA..............: 191

Reassembly Frag RX.......: 0
Clear Fragments.........: 0
Clear Reasm Done........: 0
Datagrams Drop..........: 0
Fragments Drop..........: 0


Encryption Side Controller Statistics
====================================
Frames RX...............: 454065
Bytes RX................: 6168274/
Mcast/Bcast Frames RX....: 1586
RX Less 128Bytes........: 1562
RX Less 512Bytes........: 452503
RX Less 1KBytes.........: 0
RX Less 9KBytes.........: 0
RX Frames Drop..........: 0

Frames TX...............: 753558
Bytes TX................: 100977246
Mcast/Bcast Frames TX....: 2
TX Less 128Bytes........: 3
TX Less 512Bytes........: 753555
TX Less 1KBytes.........: 0
TX Less 9KBytes.........: 0
```

ハードウェア リビジョン レベルに関する情報の表示

Cisco 7600 SSC-400 および IPSec VPN SPA のハードウェア リビジョンと、キャリア カードおよび SPA 上の Field-Programmable Device（FPD）のバージョンについて情報を表示するには、**show hw-module slot fpd** コマンドを使用します。シスコのテクニカル サポート担当者によって、SPA のインストレーションに関する問題をデバッグまたはトラブルシューティングする際に、この情報が必要になる場合があります。

以下に、Cisco 7600 シリーズ ルータのスロット 6 に搭載された Cisco 7600 SSC-400 のサブスロット 0 にある IPSec VPN SPA について、**show hw-module slot fpd** コマンドの出力例を示します。

```
Router# show hw-module slot 6 fpd
==== ============ ==== ==================================================
     H/WField ProgrammableCurrentMin. Required
SlotCard TypeVer.Device: "ID-Name"VersionVersion
===== ============ ==== ==================== ================ ================
6    7600-SSC-4000.51-I/O FPGA1.01.0
---- ------------ ---- ------------------- ---------------- ---------------
6/0 SPA-IPSEC-2G0.31-PROM1.11.1
==== ============ ===== ==================================================
```

IPSec VPN SPA の設定情報の表示

IPSec VPN SPA の設定に関する情報を表示するには、以下のコマンドを使用します。

- **show crypto vlan** —「接続されているアクセス ポートおよびルーテッド ポートに関する情報の表示」（p.31-8）、「VPN の動作状態の表示」（p.31-8）、および「GRE トンネルを介した IP マルチキャストの情報表示」（p.31-12）を参照
- **show interfaces trunk** —「トランク ポートで許可される VLAN に関する情報の表示」（p.31-8）を参照
- **show ip route** —「ルーティング テーブルの表示」（p.31-9）を参照
- **show interfaces tunnel** —「トンネル インターフェイス情報の表示」（p.31-9）を参照
- **show ip mroute** —「GRE トンネルを介した IP マルチキャストの情報表示」（p.31-12）を参照
- **show crypto map** —「暗号マップに関する情報の表示」（p.31-13）を参照
- **show crypto ipsec sa** —「IPSec SA に関する情報の表示」（p.31-14）を参照
- **show crypto isakmp sa** —「ピアの SA 情報の表示」（p.31-15）を参照
- **show crypto session** —「暗号化セッションに関する情報の表示」（p.31-15）を参照
- **show crypto isakmp policy** —「IKE ポリシーに関する情報の表示」（p.31-16）を参照
- **show crypto ipsec transform-set** —「IPSec トランスフォーム セットに関する情報の表示」（p.31-17）を参照
- **show call admission statistics** —「CAC 情報の表示」（p.31-17）を参照
- **show crypto call admission statistics** —「CAC 情報の表示」（p.31-17）を参照
- **show crypto key mypubkey rsa** —「RSA 公開鍵に関する情報の表示」（p.31-18）を参照
- **show crypto key pubkey-chain rsa** —「RSA 公開鍵に関する情報の表示」（p.31-18）を参照
- **show crypto pki trustpoints** —「トラストポイントに関する情報の表示」（p.31-19）を参照
- **show crypto pki certificates storage** —「証明書ストレージ場所の表示」（p.31-19）を参照
- **show crypto pki certificates** —「証明書に関する情報の表示」（p.31-20）を参照
- **show crypto pki server** —「証明書サーバに関する情報の表示」（p.31-21）を参照
- **show ip nhrp** —「NHRP キャッシュに関する情報の表示」（p.31-21）を参照
- **show crypto isakmp ha standby** —「HSRP 情報の表示」（p.31-22）を参照
- **show crypto ipsec ha** —「HSRP 情報の表示」（p.31-22）を参照
- **show crypto ipsec sa** —「HSRP 情報の表示」（p.31-22）を参照
- **show crypto ipsec sa standby** —「HSRP 情報の表示」（p.31-22）を参照
- **show ssp client** —「SSP 情報の表示」（p.31-25）を参照
- **show ssp packet** —「SSP 情報の表示」（p.31-25）を参照
- **show ssp peers** —「SSP 情報の表示」（p.31-25）を参照
- **show ssp redundancy** —「SSP 情報の表示」（p.31-25）を参照

- **show redundancy linecard-group** — 「BFG 設定に関する情報の表示」（p.31-26）を参照
- **show crypto ace redundancy** — 「BFG 設定に関する情報の表示」（p.31-26）を参照

show コマンドで表示される情報についての詳しい説明は、『*Cisco IOS Security Command Reference*』の「IP Security and Encryption」の章を参照してください。

接続されているアクセス ポートおよびルーテッド ポートに関する情報の表示

アクセス ポートまたはルーテッド ポートが接続されていることを確認するには、**show crypto vlan** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show crypto vlan

Interface VLAN 100 on IPSec Service Module port Gi5/0/1 connected to VLAN 2022 with
crypto map set coral2

Router# show crypto vlan

Interface VLAN 100 on IPSec Service Module port Gi5/0/1 connected to Gi2/8 with crypto
mark set M10K
```

トランク ポートで許可される VLAN に関する情報の表示

トランク ポートで許可されている VLAN（仮想 LAN）について情報を表示するには、**show interfaces trunk** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show interfaces GigabitEthernet 2/0/1 trunk

Port      Mode         Encapsulation  Status        Native vlan
Gi2/1     on           802.1q         trunking      1

Port      Vlans allowed on trunk
Gi2/1     1-4094

Port      Vlans allowed and active in management domain
Gi2/1     1-4,7-8,513,1002-1005

Port      Vlans in spanning tree forwarding state and not pruned
Gi2/1     1-4,7-8,513,1002-1005
```

VPN の動作状態の表示

VPN の動作状態を表示するには、**show crypto vlan** コマンドを使用します。以下に、このコマンドの出力例を示します。

次の例では、インターフェイス VLAN は IPSec VPN SPA の内部ポートに属しています。

```
Router# show crypto vlan

  Interface VLAN 2 on IPSec Service Module port 7/0/1 connected to Fa8/3
```

次の例では、VLAN 2 がインターフェイス VLAN で、VLAN 2022 が非表示 VLAN です。

```
Router# show crypto vlan

Interface VLAN 2 on IPSec Service Module port 3/0/1 connected to VLAN 2022 with crypto
map set coral2
```

次の例では、インターフェイス VLAN が IPSec VPN SPA の内部ポートに存在しないか、シャーシから IPSec VPN SPA が取り外されているか、または IPSec VPN SPA が別のサブスロットに移動されていることを示しています。

```
Router# show crypto vlan

  Interface VLAN 2 connected to VLAN 3 (no IPSec Service Module attached)
```

ルーティング テーブルの表示

ルーティング テーブルの現在の状態を表示するには、**show ip route** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router1# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.0.35.0/24 is directly connected, Ethernet3/3
S 10.0.36.0/24 is directly connected, Tunnel0
C 10.0.51.0/24 is directly connected, Tunnel0
C 10.0.149.0/24 is directly connected, Ethernet3/0
```

トンネル インターフェイス情報の表示

トンネル インターフェイス情報を表示するには、**show interfaces tunnel** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show interfaces tunnel 1

Tunnel4 is up, line protocol is down
Hardware is Routing Tunnel
Internet address is 10.1.1.1/24
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
Encapsulation TUNNEL, loopback not set
Keepalive set (10 sec)
Tunnel source 9.2.2.1, destination 6.6.6.2
Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
Tunnel TOS 0xF, Tunnel TTL 128
Checksumming of packets disabled, fast tunneling enabled
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy, fifo
Output queue 0/0, 1 drops; input queue 0/75, 0 drops
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets, 0 restarts
```

表 31-1 に、この出力で表示される重要なフィールドの説明を示します。

表 31-1　show interfaces tunnel のフィールドの説明

フィールド	説明
Tunnel is {up | down}	現在インターフェイスはアクティブであり、リングに挿入されています（up）。または、非アクティブであり、挿入されていません（down）。
line protocol is {up | down | administratively down}	トンネルの宛先への有効なルートが使用可能な場合、line protocol up と表示されます。使用可能なルートがない場合、または再帰ルートが使用されている場合は、line protocol down と表示されます。
Hardware	ハードウェアのタイプを指定します。
MTU	インターフェイスの最大伝送ユニット（maximum transmission unit; MTU）
BW	インターフェイスの帯域幅（kbps）
DLY	インターフェイスの遅延（マイクロ秒）
rely	255 を分母とする分数で表したインターフェイスの信頼性（255/255 は 100% の信頼性）。5 分間の幾何平均から算出されます。
load	インターフェイスの負荷を表す、255 を分母とする分数（255/255 は完全な飽和状態を表します）。5 分間の幾何平均から算出されています。
Encapsulation	トンネルの場合、カプセル化方式は常に TUNNEL です。
loopback	ループバックが設定されているかどうかを示します。
Keepalive	キープアライブが設定されているかどうかを表します。
Tunnel source	トンネル パケットの送信元アドレスとして使用されている IP アドレス
destination	トンネルの宛先 IP アドレス
Tunnel protocol	トンネルのトランスポート プロトコル（トンネルが使用しているプロトコル）。**tunnel mode** コマンドに基づいており、デフォルトは GRE（総称ルーティング カプセル化）です。
key	（任意）トンネル インターフェイスの ID キー
sequencing	（任意）トンネル インターフェイスで、順序が不正なデータグラムをドロップするかどうかを表します。
Last input	最後にパケットがインターフェイスによって正常に受信され、ルータ上でローカルに処理されてから経過した時間、分、秒（または never）。この情報は、デッド インターフェイスでいつ障害が発生したかを把握する場合に役立ちます。 このフィールドは、ファースト スイッチングされたトラフィックでは更新されません。
output	最後にパケットがインターフェイスによって正常に送信されてから経過した時、分、秒（または never）
output hang	送信に時間がかかりすぎたためにインターフェイスが最後にリセットされてから経過した時間、分、秒（または never）。「last」フィールドの時間数が 24 時間を超える場合、日数および時間数が表示されます。そのフィールドがオーバーフローした場合、アスタリスクが表示されます。

表 31-1　show interfaces tunnel のフィールドの説明 （続き）

フィールド	説明
Last clearing	このレポートで表示される統計情報（送受信バイト数など）を累積しているカウンタが前回ゼロにリセットされた時刻。このカウンタをクリアしても、ルーティングに影響する可能性のある変数（load や reliability など）はクリアされません。 3 つのアスタリスク（***）は、経過時間が長すぎて表示できないことを意味します。 0:00:00 は、カウンタがクリアされてからの経過時間が 231 ms より長い（および 232 ms 未満であること）を示します。
Output queue, drops Input queue, drops	出力および入力キューのパケット数。各数値の後ろに、スラッシュ、キューの最大サイズ、およびキューが満杯になったためにドロップされたパケット数が表示されます。
30 second input rate, 30 second output rate	最近 30 秒間における、1 秒あたりの伝送ビット数および伝送パケット数の平均。 この、30 秒間の送受信レートは、あくまでも所定の 30 秒間における 1 秒あたりのトラフィックの予想値です。これらの速度は、30 秒を時間定数とし、指数関数的に重み付けを行った平均値です。この平均値が該当期間中の均一なトラフィック ストリームについて瞬間速度の 2% 以内に収まるまでに、この時間定数の 4 倍の期間が経過する必要があります。
packets input	システムが受信したエラーのないパケットの総数
bytes	システムが受信したエラーのないパケットの合計バイト数（データおよび MAC［メディア アクセス制御］カプセル化など）
no buffer	メイン システムにバッファ スペースがないためにドロップされた受信パケット数。ignored カウントと比較します。イーサネット ネットワークのブロードキャスト ストームおよびシリアル回線のノイズのバーストが、ほとんどの場合 no input buffer イベントの原因になります。
broadcasts	インターフェイスが受信したブロードキャストまたはマルチキャスト パケットの総数
runts	メディアの最小パケット サイズに満たないためにドロップされたパケット数
giants	メディアの最大パケット サイズを超過したためにドロップされたパケット数
CRC	送信元の LAN ステーションまたは遠端デバイスで生成された Cyclic Redundancy Check（CRC; 巡回冗長検査）が、受信データから算出されたチェックサムと一致しません。LAN の場合は通常、LAN インターフェイスまたは LAN バス自体にノイズまたは伝送上の問題があります。CRC の値が大きい場合は通常、ステーションで不正なデータが伝送されています。
frame	CRC エラーおよび整数以外のオクテット数を含む、不正な受信パケット数
overrun	入力速度がレシーバーのデータ処理能力を超えたために、シリアル レシーバー ハードウェアが受信したデータをハードウェア バッファに格納できなかった回数

表 31-1　show interfaces tunnel のフィールドの説明 （続き）

フィールド	説明
ignored	インターフェイス ハードウェアの内部バッファの容量が少ないために、インターフェイスによって無視された受信パケット数。no buffer カウントと比較します。これらのバッファは、no buffer の説明で述べたシステム バッファとは異なります。ブロードキャスト ストームやノイズのバーストによって、ignored の値は大きくなります。
abort	シリアル インターフェイスの 1 ビットの不正なシーケンス。一般に、シリアル インターフェイスとデータ リンク機器間で、クロッキングの問題があることを表します。
packets output	システムが送信したメッセージの総数
bytes	データおよび MAC カプセル化など、システムが送信したバイトの総数
underruns	遠端トランスミッタが近端ルータのレシーバーの処理速度よりも速く動作した回数一部のインターフェイスでは、この値が報告されない場合があります。
output errors	検査するインターフェイスに関し、発信されるデータグラムの最終的な送信を妨げたエラーの総数。複数のエラーがあるデータグラムや、特定のカテゴリに分類されないエラーのあるデータグラムもあるため、この値は列挙される出力エラーの総数とは必ずしも一致しません。
collisions	イーサネット コリジョンが発生したために再送信されたメッセージ数。この原因は通常、LAN の過剰な延長（イーサネット ケーブルまたはトランシーバ ケーブルが長すぎる、ステーション間にリピータが 3 台以上設置されている、またはカスケードされたマルチポート トランシーバが多すぎるなど）です。ある程度のコリジョンは正常です。ただし、コリジョンの発生率が 4 ～ 5% に増えている場合は、障害のある機器がセグメントにないかどうかを確認し、既存の一部のステーションを新しいセグメントに移動することを検討する必要があります。コリジョンを発生させたパケットは、出力パケット内で 1 回のみカウントされます。
interface resets	インターフェイスがリセットされた回数。管理者がインターフェイスをリセットする場合や、内部エラーが発生した際に自動的にリセットされる場合もあります。
restarts	エラーのためコントローラが再起動された回数

GRE トンネルを介した IP マルチキャストの情報表示

GRE トンネルを介した IP マルチキャストの設定に関する情報を表示するには、**show crypto vlan** および **show ip mroute** コマンドを入力します。

トンネルが IPSec VPN SPA に引き継がれたことを確認するには、**show crypto vlan** コマンドを入力します。以下に、このコマンドの出力例を示します。

```
Router(config)# show crypto vlan

Interface VLAN 100 on IPSec Service Module port Gi7/0/1 connected to Po1 with crypto
map set map_t3
Tunnel15 is accelerated via IPSec SM in subslot 7/0
```

IP マルチキャスト トラフィックがハードウェアでスイッチングされることを確認するには、**show ip mroute** コマンドを入力して、「H」フラグを検索します。以下に、このコマンドの出力例を示します。

```
Router# show ip mroute 230.1.1.5

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
T - SPT-bit set, J - Join SPT, M - MSDP created entry,
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 230.1.1.5), 01:23:45/00:03:16, RP 15.15.1.1, flags: SJC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Tunnel15, Forward/Sparse-Dense, 00:25:47/00:03:16
(120.1.0.3, 230.1.1.5), 01:23:46/00:03:25, flags: T
Incoming interface: GigabitEthernet8/1, RPF nbr 0.0.0.0, RPF-MFD
Outgoing interface list:
Tunnel15, Forward/Sparse-Dense, 00:25:47/00:03:16, H
```

暗号マップに関する情報の表示

暗号マップの設定について情報を表示するには、**show crypto map** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show crypto map

Crypto Map: "router-alice" idb: Ethernet0 local address: 172.21.114.123
Crypto Map "router-alice" 10 ipsec-isakmp
Peer = 172.21.114.67
Extended IP access list 141
access-list 141 permit ip
source: addr = 172.21.114.123/0.0.0.0
dest:   addr = 172.21.114.67/0.0.0.0
Current peer: 172.21.114.67
Security-association lifetime: 4608000 kilobytes/120 seconds
PFS (Y/N): N
Transform sets={t1,}
```

IPSec SA に関する情報の表示

IPSec SA（セキュリティ アソシエーション）について情報を表示するには、**show crypto ipsec sa** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show crypto ipsec sa

interface: Ethernet0

    Crypto map tag: router-alice, local addr. 172.21.114.123
    local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
    remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
    current_peer: 172.21.114.67
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0

    local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
    path mtu 1500, media mtu 1500
    current outbound spi: 20890A6F

    inbound esp sas:
    spi: 0x257A1039(628756537)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 26, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y

    inbound ah sas:

    outbound esp sas:
    spi: 0x20890A6F(545852015)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 27, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:

interface: Tunnel0

    Crypto map tag: router-alice, local addr. 172.21.114.123
    local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
    remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
    current_peer: 172.21.114.67
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0
    local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
    path mtu 1500, media mtu 1500
    current outbound spi: 20890A6F

    inbound esp sas:
    spi: 0x257A1039(628756537)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 26, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y

    inbound ah sas:

    outbound esp sas:
```

```
spi: 0x20890A6F(545852015)
    transform: esp-des esp-md5-hmac,
    in use settings ={Tunnel,}
    slot: 0, conn id: 27, crypto map: router-alice
    sa timing: remaining key lifetime (k/sec): (4607999/90)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:
```

ピアの SA 情報の表示

ピアに関する現在のすべての Internet Key Exchange（IKE; インターネット キー エクスチェンジ）SA 情報を表示するには、**show crypto isakmp sa** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show crypto isakmp sa

f_vrf/i_vrf     dst             src           state        conn-id     slot
```

暗号化セッションに関する情報の表示

アクティブな暗号化セッションのステータス情報を表示するには、**show crypto session** コマンドを使用します。出力には、以下のような情報が表示されます。

- インターフェイス
- IKE ピアの記述（ある場合）
- IPSec SA を作成したピアに対応付けられている IKE SA
- セッションのフローを処理している IPSec SA

以下に、このコマンドの出力例を示します。

```
Router# show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication

Interface: Ethernet1/0
Session status: UP-NO-IKE
Peer: 10.2.80.179/500 fvrf: (none) ivrf: (none)
Desc: My-manual-keyed-peer
Phase1_id: 10.2.80.179
IPSEC FLOW: permit ip host 10.2.80.190 host 10.2.80.179
Active SAs: 4, origin: manual-keyed crypto map
Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

Interface: Ethernet1/2
Session status: DOWN
Peer: 10.1.1.1/500 fvrf: (none) ivrf: (none)
Desc: SJC24-2-VPN-Gateway
Phase1_id: 10.1.1.1
IPSEC FLOW: permit ip host 10.2.2.3 host 10.2.2.2
Active SAs: 0, origin: crypto map
Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
IPSEC FLOW: permit ip 10.2.0.0/255.255.0.0 10.4.0.0/255.255.0.0
Active SAs: 0, origin: crypto map
Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

Interface: Serial2/0.17
Session status: UP-ACTIVE
Peer: 10.1.1.5/500 fvrf: (none) ivrf: (none)
Desc: (none)
Phase1_id: 10.1.1.5
IKE SA: local 10.1.1.5/500 remote 10.1.1.5/500 Active
Capabilities:(none) connid:1 lifetime:00:59:51
IPSEC FLOW: permit ip host 10.1.1.5 host 10.1.2.5
Active SAs: 2, origin: dynamic crypto map
Inbound: #pkts dec'ed 4 drop 0 life (KB/Sec) 20085/171
Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 20086/171
```

IKE ポリシーに関する情報の表示

IKE ポリシーについて情報を表示するには、**show crypto isakmp policy** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show crypto isakmp policy 1

    encr 3des
    authentication pre-share
    group 2
    crypto isakmp key cisco address 192.168.3.1
```

（注）　ハードウェアでサポートされていない IKE 暗号方式をユーザが入力すると、**show crypto isakmp policy** コマンドの出力に次の警告メッセージが表示されます。

```
WARNING:encryption hardware does not support the configured encryption method for ISAKMP
policy value
```

IPSec トランスフォーム セットに関する情報の表示

トランスフォーム セットの設定について情報を表示するには、**show crypto ipsec transform-set** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show crypto ipsec transform-set

Transform set combined-des-md5: {esp-des esp-md5-hmac}
will negotiate = {Tunnel,},
Transform set t1: {esp-des esp-md5-hmac}
will negotiate = {Tunnel,},
Transform set t100: {ah-sha-hmac}
will negotiate = {Transport,},
Transform set t2: {ah-sha-hmac}
will negotiate = {Tunnel,},
{esp-des}
will negotiate = {Tunnel,},
```

（注）　ハードウェア（IPSec ピア）でサポートされていない IPSec トランスフォーム セットをユーザが入力すると、**show crypto ipsec transform-set** コマンドの出力に次の警告メッセージが表示されます。

```
WARNING:encryption hardware does not support transform.
```

CAC 情報の表示

CAC（コール アドミッション制御）設定情報を表示するには、**show call admission statistics** および **show crypto call admission statistics** コマンドを使用します。

show call admission statistics コマンドは、グローバルな CAC 設定パラメータおよび CAC の動作をモニタします。以下に、このコマンドの出力例を示します。

```
Router# show call admission statistics
Total Call admission charges: 0, limit 25
Total calls rejected 12, accepted 51
Load metric: charge 0, unscaled 0
```

show crypto call admission statistics コマンドは、暗号 CAC 統計情報をモニタします。以下に、このコマンドの出力例を示します。

```
Router# show crypto call admission statistics
------------------------------------------------------------
               Crypto Call Admission Control Statistics
------------------------------------------------------------
System Resource Limit: 0    Max IKE SAs 0
Total IKE SA Count:    0    active:     0   negotiating: 0
Incoming IKE Requests: 0    accepted:   0   rejected:    0
Outgoing IKE Requests: 0    accepted:   0   rejected:    0
Rejected IKE Requests: 0    rsrc low:   0   SA limit:    0
```

RSA 公開鍵に関する情報の表示

ルータに設定されている RSA 公開鍵について情報を表示するには、**show crypto key mypubkey rsa** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show crypto key mypubkey rsa

% Key pair was generated at: 06:07:50 UTC Jan 13 1996

Key name: myrouter.example.com

 Usage: Encryption Key

 Key Data:

  00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5

  18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB

  07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

ルータに保存されているすべての RSA 公開鍵（IPSec のピア認証時にルータに証明書を送信したピアの公開鍵など）を一覧表示するか、またはルータに保存されている特定の RSA 公開鍵の詳細情報を表示するには、**show crypto key pubkey-chain rsa** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show crypto key pubkey-chain rsa

Codes: M - Manually Configured, C - Extracted from certificate

Code  Usage        IP-address     Name

M     Signature    10.0.0.1       myrouter.example.com

M     Encryption   10.0.0.1       myrouter.example.com

C     Signature    172.16.0.1     routerA.example.com

C     Encryption   172.16.0.1     routerA.example.com

C     General      192.168.10.3   routerB.domain1.com
```

トラストポイントに関する情報の表示

ルータに設定されているトラストポイントを表示するには、**show crypto pki trustpoints** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show crypto pki trustpoints

Trustpoint bo:

    Subject Name:

    CN = bomborra Certificate Manager

     O = cisco.com

     C = US

          Serial Number:01

    Certificate configured.

    CEP URL:http://bomborra

    CRL query url:ldap://bomborra
```

証明書ストレージ場所の表示

PKI 証明書ストレージ場所の現在の設定を表示するには、**show crypto pki certificates storage** コマンドを使用します。

以下に、このコマンドの出力例を示します。

```
Router# show crypto pki certificates storage

Certificates will be stored in disk0:/certs/
```

証明書に関する情報の表示

証明書、CA の証明書、および RA 証明書について情報を表示するには、**show crypto pki certificates** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show crypto pki certificates

CA Certificate

Status: Available
    Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
    Certificate Usage: Signature

    Issuer:
        CN = new-user
        OU = pki new-user
        O = cisco
        L = santa cruz2
        ST = CA
        C = US
        EA = user@cysco.net

    Subject:
        CN = new-user
        OU = pki new-user
        O = cisco
        L = santa cruz2
        ST = CA
        C = US
        EA = user@cysco.net

    CRL Distribution Point:
        http://new-user.cysco.net/CertEnroll/new-user.crl

    Validity Date:
        start date: 14:19:29 PST Oct 31 2002
        end date: 14:27:27 PST Oct 31 2017

    Associated Trustpoints: MS

Certificate

Status: Available
    Certificate Serial Number: 193E28D20000000009F7
    Certificate Usage: Signature

    Issuer:
        CN = new-user
        OU = pki new-user
        O = cisco
        L = santa cruz2
        ST = CA
        C = US
        EA = user@cysco.net

    Subject:
        Name: User1.Cysco.Net

    CRL Distribution Point:
        http://new-user.cysco.net/CertEnroll/new-user.crl

    Validity Date:
        start date: 12:40:14 PST Feb 26 2003
        end   date: 12:50:14 PST Mar 5 2003
        renew date: 16:00:00 PST Dec 31 1969

    Associated Trustpoints: MS
```

証明書サーバに関する情報の表示

証明書サーバの現在のステートおよび設定を表示するには、**show crypto pki server** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show crypto pki server

Certificate Server status: disabled, storage configuration incomplete

    Granting mode is: manual

    Last certificate issued serial number: 0

    CA certificate expiration timer: 21:29:38 GMT Jun 5 2006

    CRL NextUpdate timer: 21:31:39 GMT Jun 6 2003

    Current storage dir: ftp://myftpserver

    Database Level: Minimum - no cert data written to storage
```

NHRP キャッシュに関する情報の表示

Next Hop Resolution Protocol（NHRP）キャッシュについて情報を表示するには、**show ip nhrp** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router# show ip nhrp

10.10.1.75/32 via 10.10.1.75, Tunnel5 created 00:32:11, expire 00:01:46

  Type: dynamic, Flags: authoritative unique registered

  NBMA address: 172.16.175.75

10.10.1.76/32 via 10.10.1.76, Tunnel5 created 00:26:41, expire 00:01:37

  Type: dynamic, Flags: authoritative unique registered

  NBMA address: 172.16.175.76

10.10.1.77/32 via 10.10.1.77, Tunnel5 created 00:31:26, expire 00:01:33

  Type: dynamic, Flags: authoritative unique registered

  NBMA address: 172.17.63.20
```

HSRP 情報の表示

HSRP の設定について情報を表示するには、**show crypto isakmp ha standby**、**show crypto ipsec ha**、**show ipsec sa**、および **show crypto ipsec sa standby** コマンドを使用します。

ISAKMP スタンバイ SA またはアクティブ SA を表示するには、**show crypto isakmp ha standby** コマンドを入力します。以下に、このコマンドの出力例を示します。

```
Router# show crypto isakmp ha standby

dst             src             state       I-Cookie           R-Cookie

172.16.31.100   20.3.113.1      QM_IDLE     796885F3 62C3295E  FFAFBACD

EED41AFF

172.16.31.100   20.2.148.1      QM_IDLE     5B78D70F 3D80ED01  FFA03C6D

09FC50BE

172.16.31.100   20.4.124.1      QM_IDLE     B077D0A1 0C8EB3A0  FF5B152C

D233A1E0

172.16.31.100   20.3.88.1       QM_IDLE     55A9F85E 48CC14DE  FF20F9AE

DE37B913

172.16.31.100   20.1.95.1       QM_IDLE     3881DE75 3CF384AE  FF192CAB
```

IPSec High Availability HA Manager ステートを表示するには、**show crypto ipsec ha** コマンドを入力します。以下に、このコマンドの出力例を示します。

```
Router# show crypto ipsec ha

Interface           VIP                SAs   IPSec HA State

FastEthernet0/0     172.16.31.100     1800   Active since 13:00:16 EDT Tue Oct 1 2002
```

IPSec SA の HA ステータス（スタンバイまたはアクティブ）を表示するには、**show crypto ipsec sa** コマンドを入力します。以下に、このコマンドの出力例を示します。

```
Router# show crypto ipsec sa

interface: FastEthernet0/0

    Crypto map tag: mymap, local addr. 172.168.3.100
    local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (5.6.0.0/255.255.0.0/0/0)
    current_peer: 172.168.3.1
    PERMIT, flags={}
    #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 decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 172.168.3.100, remote crypto endpt.: 172.168.3.1
    path mtu 1500, media mtu 1500
    current outbound spi: 132ED6AB

    inbound esp sas:
    spi: 0xD8C8635F(3637011295)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2006, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
        HA Status: STANDBY

    inbound ah sas:
    spi: 0xAAF10A60(2867923552)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2004, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        replay detection support: Y
        HA Status: STANDBY

    inbound pcp sas:

    outbound esp sas:
    spi: 0x132ED6AB(321836715)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2007, flow_id: 4, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
        HA Status: STANDBY

    outbound ah sas:
    spi: 0x1951D78(26549624)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2005, flow_id: 4, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        replay detection support: Y
        HA Status: STANDBY

    outbound pcp sas:
```

スタンバイ SA を表示するには、**show crypto ipsec sa standby** コマンドを入力します。以下に、このコマンドの出力例を示します。

```
Router# show crypto ipsec sa standby

interface: FastEthernet0/0
    Crypto map tag: mymap, local addr. 172.168.3.100
    local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (5.6.0.0/255.255.0.0/0/0)
    current_peer: 172.168.3.1
    PERMIT, flags={}
    #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 decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 172.168.3.100, remote crypto endpt.: 172.168.3.1
    path mtu 1500, media mtu 1500
    current outbound spi: 132ED6AB

    inbound esp sas:
    spi: 0xD8C8635F(3637011295)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2006, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
        HA Status: STANDBY

    inbound ah sas:
    spi: 0xAAF10A60(2867923552)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2004, flow_id: 3, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        replay detection support: Y
        HA Status: STANDBY

    inbound pcp sas:

    outbound esp sas:
    spi: 0x132ED6AB(321836715)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2007, flow_id: 4, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        IV size: 8 bytes
        replay detection support: Y
        HA Status: STANDBY

    outbound ah sas:
    spi: 0x1951D78(26549624)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2005, flow_id: 4, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4499/59957)
        replay detection support: Y
        HA Status: STANDBY

    outbound pcp sas:
```

SSP 情報の表示

SSP の設定についての情報を表示するには、**show ssp client**、**show ssp packet**、**show ssp peers**、および **show ssp redundancy** コマンドを使用します。

SSP に登録されている各クライアントの domain of interpretation（DOI; ドメイン オブ インタープリテーション）、名前、実行バージョンおよび使用可能バージョンを表示するには、**show ssp client** コマンドを入力します。以下に、このコマンドの出力例を示します。

```
Router# show ssp client

SSP Client Information

    DOI   Client Name                       Version   Running Ver

      1   IPSec HA Manager                   1.0       1.0

      2   IKE HA Manager                     1.0       1.0
```

現在のソケットのバイト カウントおよびパケット カウント、ソケットの作成時刻、サーバ ポート番号、および SSP 通信に使用されるポート番号を表示するには、**show ssp packet** コマンドを入力します。以下に、このコマンドの出力例を示します。

```
Router# show ssp packet

SSP packet Information

    Socket creation time: 01:01:06

    Local port: 3249      Server port: 3249

    Packets Sent = 38559, Bytes Sent = 2285020

    Packets Received = 910, Bytes Received = 61472
```

リモート ピアの IP アドレス、使用するインターフェイス、および接続ステートを表示するには、**show ssp peers** コマンドを入力します。以下に、このコマンドの出力例を示します。

```
Router# show ssp peers

SSP Peer Information

    IP Address      Connection State   Local Interface

    40.0.0.1        Connected          FastEthernet0/1
```

現在の SSP ステート、HSRP グループ名、使用されるインターフェイス、および最後にステートが変化してからの経過時間を表示するには、**show ssp redundancy** コマンドを入力します。以下に、このコマンドの出力例を示します。

```
Router# show ssp redundancy

SSP Redundancy Information

  Device has been ACTIVE for 02:55:34

    Virtual IP      Redundancy Name             Interface

    172.16.31.100   KNIGHTSOFNI                 FastEthernet0/0
```

BFG 設定に関する情報の表示

Blade Failure Group（BFG）設定について情報を表示するには、**show redundancy linecard-group** および **show crypto ace redundancy** コマンドを使用します。以下に、これらのコマンドの出力例を示します。

```
Router# show redundancy linecard-group 1

Line Card Redundancy Group:1 Mode:feature-card
Class:load-sharing
Cards:
Slot:3 Subslot:0
Slot:5 Subslot:0

Router# show crypto ace redundancy
-------------------------------------
LC Redundancy Group ID            :1
Pending Configuration Transactions:0
Current State                     :OPERATIONAL
Number of blades in the group     :2
Slots
-------------------------------------
Slot:3 Subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 22 times
Initialization Timer not running
Slot:5 Subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 24 times
Initialization Timer not running

ACE B2B Group State:OPERATIONAL Event:BULK DONE
ACE B2B Group State:CREATED Event:CONFIG_DOWNLOAD_DONE
ACE B2B Group State:DELETED Event:CONFIG_DELETE
ACE B2B Group State:OPERATIONAL Event:BULK DONE
ACE B2B Group State:CREATED Event:CONFIG_DOWNLOAD_DONE
ACE B2B Group State:DELETED Event:CONFIG_DELETE
ACE B2B Group State:OPERATIONAL Event:CONFIG_DOWNLOAD_DONE
ACE B2B Group State:DELETED Event:CONFIG_ADD
ACE B2B Group State:CREATED Event:UNDEFINED B2B HA EVENT
ACE B2B Group State:CREATED Event:CONFIG_DOWNLOAD_DONE
```

IPSec VPN SPA 固有の問題のトラブルシューティング

ここでは、IPSec VPN SPA 固有の問題のトラブルシューティングについて詳しく説明します。具体的な内容は次のとおりです。

トランク ポート設定のトラブルシューティング

注意　イーサネット ポートをトランク ポートとして設定すると、デフォルトではすべての VLAN がトランク ポート上で許可されます。このデフォルト設定では IPSec VPN SPA はうまく動作せず、ネットワーク ループが発生します。

VRF 対応 IPSec のトラブルシューティング

VRF 対応 IPSec のトラブルシューティングを行うには、**debug crypto ipsec** および **debug crypto isakmp** コマンドを使用します。**debug crypto ipsec** コマンドでは、IP セキュリティ イベントが表示されます。**debug crypto isakmp** コマンドでは、IKE イベントに関するメッセージが表示されます。

VRF 対応 IPSec のデバッグの例

以下に、VRF 対応 IPSec の設定に関するデバッグ出力例を示します。

```
Router# debug crypto ipsec

Crypto IPSEC debugging is on
IPSEC-PE# debug crypto isakmp
Crypto ISAKMP debugging is on
IPSEC-PE# debug crypto isakmp d
04:31:28: ISAKMP (0:12): purging SA., sa=6482B354, delme=6482B354
04:31:28: ISAKMP: Unlocking IKE struct 0x63C142F8 for declare_sa_dead(), count 0
IPSEC-PE# debug crypto isakmp detail
Crypto ISAKMP internals debugging is on
IPSEC-PE#
IPSEC-PE#
IPSEC-PE#
04:32:07: ISAKMP: Deleting peer node by peer_reap for 10.1.1.1: 63C142F8
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B DC887D4E
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.68.1.1
04:32:55: ISAKMP cookie AA8F7B41 49A60E88
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B DBC8E125
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 B4BDB5B7
04:32:55: ISAKMP (0:0): received packet from 10.1.1.1 dport 500 sport 500 Global (N)
NEW
SA
04:32:55: ISAKMP: local port 500, remote port 500
04:32:55: ISAKMP: hash from 729FA94 for 619 bytes
04:32:55: ISAKMP: Packet hash:
64218CC0:                    B91E2C70 095A1346          9.,p.Z.F
64218CD0: 0EDB4CA6 8A46784F B314FD3B 00        .[L&.FxO.};.
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:32:55: ISAKMP cookie AA8F7B41 F7ACF384
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:32:55: ISAKMP cookie AA8F7B41 0C07C670
04:32:55: ISAKMP: insert sa successfully sa = 6482B354
04:32:55: ISAKMP (0:13): processing SA payload. message ID = 0
04:32:55: ISAKMP (0:13): processing ID payload. message ID = 0
04:32:55: ISAKMP (0:13): peer matches vpn2-ra profile
04:32:55: ISAKMP: Looking for a matching key for 10.1.1.1 in default
04:32:55: ISAKMP: Created a peer struct for 10.1.1.1, peer port 500
04:32:55: ISAKMP: Locking peer struct 0x640BBB18, IKE refcount 1 for
crypto_ikmp_config_initialize_sa
04:32:55: ISAKMP (0:13): Setting client config settings 648252B0
04:32:55: ISAKMP (0:13): (Re)Setting client xauth list  and state
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 157 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 123 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v2
04:32:55: ISAKMP (0:13) Authentication by xauth preshared
04:32:55: ISAKMP (0:13): Checking ISAKMP transform 1 against priority 1 policy
04:32:55: ISAKMP:      encryption 3DES-CBC
04:32:55: ISAKMP:      hash SHA
04:32:55: ISAKMP:      default group 2
04:32:55: ISAKMP:      auth XAUTHInitPreShared
04:32:55: ISAKMP:      life type in seconds
04:32:55: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
04:32:55: ISAKMP (0:13): atts are acceptable. Next payload is 3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 157 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 123 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v2
```

```
04:32:55: ISAKMP (0:13): processing KE payload. message ID = 0
04:32:55: ISAKMP (0:13): processing NONCE payload. message ID = 0
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID is DPD
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 175 mismatch
04:32:55: ISAKMP (0:13): vendor ID is XAUTH
```

GRE トンネリングのトラブルシューティング

次の例のように、回線プロトコルがダウンした場合には、再帰ルートが原因であると考えられます。

```
%TUN-RECURDOWN Interface Tunnel 0 temporarily disabled due to recursive routing
```

再帰ルーティングの問題を防ぐには、次の技法を使用して、パッセンジャーおよびトランスポートネットワークのルーティング情報を分離します。

- 異なる AS 番号またはタグの使用
- 異なるルーティング プロトコルの使用
- スタティック ルートによるファースト ホップの上書き（ただし、ルーティング ループに注意すること）

IPSec SA のリセット（および再初期化）

IPSec SA をリセット（および再初期化）するには、**clear crypto sa** コマンドを使用します。

パラメータを指定せずに **clear crypto sa** コマンドを使用すると、SA データベース全体がリセットされ、アクティブなセキュリティ セッションが削除されます。そのほかに、***peer***、***map***、または ***entry*** キーワードを指定して、SA データベースの一部だけをリセットすることもできます。詳細については、『*Cisco IOS Security Command Reference*』の **clear crypto sa** コマンドの説明を参照してください。

IKE ポリシーおよびトランスフォーム セットのトラブルシューティング

現時点でハードウェアがサポートしていない IPSec トランスフォームまたは IKE 暗号化方式は、ディセーブルにする必要があります。ピアとのネゴシエーションを行おうとすると、これらは無条件に無視されます。

ハードウェアでサポートされていない IPSec トランスフォーム セットまたは IKE 暗号化方式をユーザが入力すると、警告メッセージが表示されます。これらの警告メッセージは、起動時にも表示されます。暗号化カードを取り付けると、現在の設定がスキャンされます。ハードウェアでサポートされていない IPSec トランスフォームまたは IKE 暗号化方式が検出されると、警告メッセージが表示されます。

ISAKMP キーリングおよびピア フィルタリングのトラブルシューティング

ISAKMP プロファイルまたは ISAKMP キーリングの選択が失敗する場合、ISAKMP プロファイルまたは ISAKMP キーリングの設定でローカル アドレスのバインディングを確認し、IKE デバッグの出力を調べて、そのアドレスでピアが正しく終端されているかどうかを確認します。ローカル アドレス バインディングを削除し（それによってプロファイルまたはキーリングの適用範囲をグローバルにする）、プロファイルまたはキーリングが選択されるかどうかをチェックして、状況を確認してください。

設定を確認するには、**debug crypto ipsec** および **debug crypto isakmp** コマンドを使用します。

証明書 /ISAKMP プロファイル マッピングのトラブルシューティング

証明書 /ISAKMP プロファイル マッピングを監視および保守するには、特権 EXEC モードで **debug crypto isakmp** コマンドを使用します。

Router# **debug crypto isakmp**

debug crypto isakmp コマンドは、証明書に証明書マップ照合が実行され、証明書が ISAKMP プロファイルに一致したことを示す出力を表示します。

（注）　また、**debug crypto isakmp** コマンドは、ピアがグループに割り当てられているかどうかを確認するためにも使用されます。

IKE アグレッシブ モードの開始のトラブルシューティング

IKE アグレッシブ モードの開始についてトラブルシューティングを行うには、以下のように特権 EXEC モードで debug コマンドを使用します。

Router# **debug aaa authorization**

debug aaa authorization コマンドは、AAA 認証の情報を表示します。

Router# **debug crypto isakmp**

debug crypto isakmp コマンドでは、IKE イベントに関するメッセージが表示されます。

Router# **debug radius**

debug radius コマンドは、RADIUS ホストに関連する情報を表示します。

RRI のトラブルシューティング

Reverse Route Injection（RRI; 逆ルート注入）の動作、および IPSec SA の作成や削除との関係を調べるには、**debug crypto ipsec** コマンドを使用します。

IPSec アンチリプレイ ウィンドウ サイズのトラブルシューティング

アンチリプレイ ウィンドウ サイズが、受信パケット数に対応できる値に設定されていない場合は、次のようなシステム メッセージが表示されます。

```
*Nov 17 19:27:32.279:%CRYPTO-4-PKT_REPLAY_ERR:decrypt:replay check failed
connection id=1
```

上記のメッセージは、受信パケットがアンチリプレイ ウィンドウの範囲にないと判断された場合に生成されます。

暗号マップ ベースの DN 設定のトラブルシューティング

暗号化ピアが接続を試みた際に、Distinguished Name（DN; 識別名）ベースの暗号マップの設定によって接続がブロックされる場合は、次のエラー メッセージがログに書き込まれます。

```
time:%CRYPTO-4-IKE_QUICKMODE_BAD_CERT:encrypted connection attempted with a
peer without the configured certificate attributes
```

PKI AAA 許可のトラブルシューティング

PKI AAA 許可設定が正常に機能していない場合、ルータが使用している AAA ユーザ名が AAA サーバ上のユーザ名と一致しているかどうかを確認する必要があります。ルータが使用しているユーザ名を確認するには、以下のように **debug crypto pki transactions** コマンドを使用します。

```
Router# debug crypto pki transactions

Jul  9 18:11:28.462: CRYPTO_PKI: Found a issuer match
Jul  9 18:11:28.658: CRYPTO_PKI: Certificate validated
Jul  9 18:11:28.686: CRYPTO_PKI_AAA: checking AAA authorization (tac-e,
cn=jack,ou=PKI,o=Cisco Systems,c=US, <all>)
Jul  9 18:11:29.126: CRYPTO_PKI_AAA: authorization declined by AAA, or AAA server not
found.
Jul  9 18:11:29.126: CRYPTO_PKI_AAA: No cert-application attribute found. Failing.
Jul  9 18:11:29.126: CRYPTO_PKI_AAA: authorization failed
Jul  9 18:11:29.126: CRYPTO_PKI: AAA authorization for list 'tac-e', and user
'cn=jack,ou=PKI,o=Cisco Systems,c=US' failed.
Jul  9 18:11:29.126: CRYPTO_PKI: chain cert was anchored to trustpoint root, and chain
validation result was: CRYPTO_INVALID_CERT
```

送信元インターフェイスの選択のトラブルシューティング

送信元インターフェイスの選択設定が正しく機能していない場合、以下の点を確認してください。

- コマンドで指定されているインターフェイスのアドレスが有効かどうかを確認します。指定されているインターフェイスのアドレスを使用して、他のデバイス（CRL を処理している HTTP サーバまたは LDAP サーバなど）からルータに ping を実行します。また、外部デバイスからルータへのトレース ルートを使用しても、同様の確認ができます。
- Cisco IOS の CLI（コマンドライン インターフェイス）を使用して、ルータと CA または LDAP サーバ間の接続をテストすることもできます。**ping ip** コマンドを入力し、プロンプトに応答します。「**Extended commands [n]**:」プロンプトに「yes」で応答すると、送信元アドレスまたはインターフェイスを指定できます。
- さらに、Cisco IOS の CLI を使用して **traceroute** コマンドを使用できます。**traceroute ip** コマンドを（ユーザまたは特権 EXEC モードで）入力すると、宛先および送信元アドレスを要求するプロンプトが表示されます。宛先として CA または LDAP サーバを、送信元アドレスとして「source interface」に指定したインターフェイスのアドレスを指定する必要があります。

Easy VPN Remote RSA シグニチャのトラブルシューティング

Easy VPN Remote RSA シグニチャ設定のトラブルシューティングを行うには、次の debug コマンドを使用します。debug コマンドは任意の順番で使用したり、個別に使用することができます。

Router# **debug crypto ipsec client ezvpn**

debug crypto ipsec client ezvpn コマンドは、Easy VPN リモート コンフィギュレーションに関連する VPN トンネルについての情報を表示します。

Router# **debug crypto isakmp**

debug crypto isakmp コマンドでは、IKE イベントに関するメッセージが表示されます。

HSRP および SSP を使用する IPSec ステートフル フェールオーバー（VPN ハイ アベイラビリティ）のトラブルシューティング

アクティブまたはスタンバイのいずれかの IPSec ステートフル フェールオーバー（VPN ハイ アベイラビリティ）処理に機能障害が発生していることを発見した場合、次の確認を行なってください。

- SSP 処理が実行されていることを確認するには、**show ssp** コマンドを使用します。
- いずれのルータも同じ IPSec コンフィギュレーションを共有していることを確認します。この確認は重要です。ルータが異なる設定になっていると、IPSec ステートフル フェールオーバー（VPN ハイ アベイラビリティ）は動作しません。
- IPSec 接続が、既存のマップ、トランスフォーム、およびアクセス リストで形成されていることを確認します。
- インターフェイスの内側および外側で HSRP を設定し、HSRP グループが互いに追跡するようにします。インターフェイスのそれぞれの側で **shut** コマンドを実行して正しく設定されていることを確認し、さらに HSRP スタンバイ ルータがアクティブ ルータからアクティブ コントロールを取得しているかどうかを観察します。
- アクティブ ルータとスタンバイ ルータの両方で **show ssp peer** コマンドを実行し、SSP ピアが互いを見られることを確認します。
- IKE および IPSec を SSP にバインドし、トンネルでトラフィックを送信します。アクティブとスタンバイ両方のルータが同期されていれば、ハイ アベイラビリティ（HA）メッセージがスタンバイ ルータに表示されます。
- HSRP 設定には、ファスト イーサネットまたはギガビット イーサネットなど、配置されているインターフェイスによって調整が必要なことがあります。

HSRP 設定の確認

HSRP 設定を確認するには、次の手順を実行します。

	コマンド	説明
ステップ 1	Router # **show standby brief**	インターフェイスが同期化されていることを確認します。
ステップ 2	Router# **no standby delay timer**	遅延タイマーをデフォルト設定のままにします。
ステップ 3	Router # **show standby brief**	他のルータがオンラインになったら、**show standby brief** コマンドを再度発行します。出力でスタンバイのインターフェイスが表示された場合、スタンバイ ルータの遅延タイマーを設定する必要があります。

スタンバイ ルータでの休止 SA のクリア

関連付けられた SA エントリをクリアするには、次のコマンドを実行します。

	コマンド	説明
ステップ 1	Router# **clear crypto isakmp ha** [***standby***][***resync***]	デバイスから休止（standby）エントリをすべてクリアします。**resync** キーワードを使用するとすべてのスタンバイ IKE SA が削除され、ステートの再同期化が行われます。
ステップ 2	Router# **clear crypto sa ha standby** [***peer*** *ip address* | ***resync***]	**peer** を指定すると、デバイスのすべてのスタンバイ SA がクリアされます。

HA のデバッグのイネーブル化

HA のデバッグをイネーブルにするには、次のコマンドを実行します。

	コマンド	説明
ステップ 1	Router# **debug crypto isakmp ha** [***detail*** | ***fsm*** | ***update***]	IKE HA Manager に関連する基本的なデバッグ メッセージをイネーブルにします。
ステップ 2	Router# **debug crypto ipsec ha** [***detail*** | ***fsm*** | ***update***]	IPSec HA のデバッグをイネーブルにします。
ステップ 3	Router# **debug ssp** [***fsm*** | ***socket*** | ***packet*** | ***peers*** | ***redundancy*** | ***config***]	SSP のデバッグをイネーブルにします。

バッファ ログのイネーブル化

コンソールからのデバッグ メッセージのフラッディングを避けるには、次のようにコンソール ログをディセーブルにし、バッファ ログをイネーブルにします。

	コマンド	説明
ステップ 1	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 2	Router(config)# **logging buffered**	バッファ ログをイネーブルにします。
ステップ 3	Router(config)# **no logging console**	コンソール ログをディセーブルにします。

BFG のトラブルシューティング

BFG に関する IPSec VPN SPA のデバッグをイネーブルにするには、**debug crypto ace b2b** コマンドを入力します。

```
Router# debug crypto ace b2b

ACE B2B Failover debugging is on
```

Cisco VRF 対応 IPSec の IPSec および IKE MIB サポート機能のトラブルシューティング

次の **debug crypto mib** コマンドを使用すると、Cisco VRF 対応 IPSec に関連する IPsec 情報および IKE MIB 情報を表示できます。

Router# **debug crypto mib** {**detail | error**}

このコマンドで、**detail** キーワードは IPSec MIB サブシステムで発生したのとは異なるイベントを表示し、**error** キーワードは MIB エージェントで発生したエラー イベントを表示します。

（注）　**detail** キーワードを指定すると、出力が非常に長くなることがあるため、**debug crypto mib detail** をイネーブルにする場合は注意する必要があります。

暗号条件別デバッグの使用

暗号条件別デバッグ機能では、事前に定義した暗号条件（ピアの IP アドレス、暗号エンジンの接続 ID、Security Parameter Index [SPI] など）に基づいて IPSec トンネルをデバッグできる、3 種類の CLI が提供されます。特定の IPSec 処理に限定してデバッグ メッセージを表示し、デバッグ出力の量を減らすことで、多数のトンネルを使用するルータを効率よくトラブルシューティングできます。

暗号条件別 debug コマンド（**debug crypto condition**、**debug crypto condition unmatched**、および **show crypto debug-condition**）では、条件（フィルタ値）を指定し、指定した条件に関連するデバッグ メッセージだけを生成および表示します。

表 31-2 に、サポートされる条件タイプを示します。

表 31-2　暗号条件別 debug コマンドでサポートされる条件タイプ

条件タイプ（キーワード）	説明
connid	1 ～ 32,766 の整数。現在の IPSec 処理で、この値が暗号エンジンのあるインターフェイスへの接続 ID として使用されている場合、関連するデバッグ メッセージが表示されます。
flowid	1 ～ 32,766 の整数。現在の IPSec 処理で、この値が暗号エンジンのあるインターフェイスへのフロー ID として使用されている場合、関連するデバッグ メッセージが表示されます。
fvrf	VPN Routing/Forwarding instance（VRF; VPN ルーティング / 転送インスタンス）インスタンスの名前を表すストリング。この VRF インスタンスが、現在の IPSec 処理で前面扉 VRF（FVRF）として使用されている場合、関連するデバッグ メッセージが表示されます。
ivrf	VRF インスタンスの名前を表すストリング。この VRF インスタンスが、現在の IPSec 処理で Inside VRF（IVRF）として使用されている場合、関連するデバッグ メッセージが表示されます。
peer group	Unity グループ名を表すストリング。このグループ名をピアがアイデンティティとして使用している場合、関連するデバッグ メッセージが表示されます。
peer hostname	Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を表すストリング。このストリングをピアがアイデンティティとして使用している場合、関連するデバッグ メッセージが表示されます。
peer ipv4	1 つの IP アドレス。現在の IPSec 処理が、このピアの IP アドレスに関係している場合、関連するデバッグ メッセージが表示されます。
peer subnet	ピアの IP アドレスの範囲を表すサブネットおよびサブネット マスク。現在の IPSec ピアの IP アドレスが、指定したサブネット範囲に属する場合、関連するデバッグ メッセージが表示されます。
peer username	ユーザ名を表すストリング。このユーザ名をピアがアイデンティティとして使用している場合、関連するデバッグ メッセージが表示されます。
spi	32 ビットの符号なし整数。現在の IPSec 処理がこの値を SPI として使用している場合、関連するデバッグ メッセージが表示されます。

（注）　***connid***、***flowid***、または **spi** をデバッグ条件として使用する場合、関連する IPSec フローのデバッグ メッセージが生成されます。1 つの IPSec フローには接続 ID、フロー ID、および SPI 値が 2 つずつ（インバウンド側およびアウトバウンド側にそれぞれ 1 つ）があります。2 つの接続 ID、フロー ID、および SPI 値のどちらか 1 つをデバッグ条件として使用し、該当する IPSec フローに関するデバッグ メッセージのトリガーとして使用できます。

暗号条件別デバッグの設定時の注意事項および制約事項

暗号条件別デバッグを設定する場合は、次の注意事項および制約事項に従ってください。

- この機能では、ハードウェア暗号エンジンに関するデバッグ メッセージのフィルタリングはサポートされません。
- 条件別デバッグは、特定のピアまたは機能について IKE および IPSec の問題のトラブルシューティングを行うのに役立ちますが、多数のデバッグ条件を定義してチェックすることはできない場合があります。
- デバッグ条件の値を保存するために余分にスペースが必要になるため、CPU の処理のオーバーヘッドが増え、メモリ使用量が増加します。したがって、扱うトラフィック量の大きいルータで暗号条件別デバッグをイネーブルにする場合は、注意が必要です。
- ルータによって条件別デバッグが実行されるのは、最低 1 つのグローバルな暗号 debug コマンド（**debug crypto isakmp**、**debug crypto ipsec**、または **debug crypto engine**）がイネーブルに設定されている場合に限られます。この要件により、条件別デバッグを使用しなければ、ルータのパフォーマンスには影響が出ないようになっています。

暗号条件別デバッグ フィルタリングのイネーブル化

暗号条件別デバッグ フィルタリングをイネーブルにするには、次の作業を行います。

	コマンド	説明
ステップ 1	Router# **enable**	特権 EXEC モードをイネーブルにします。
ステップ 2	Router# **debug crypto condition** [***connid*** *integer* ***engine-id*** *integer*] [***flowid*** *integer* ***engine-id*** *integer*] [***fvrf*** *string*] [***ivrf*** *string*] [***peer*** [***group*** *string*] [***hostname*** *string*] [***ipv4*** ipaddress] [***subnet*** *subnet mask*] [***username*** *string*]] [**spi** *integer*] [**reset**]	条件別デバッグ フィルタを定義します。それぞれの値についての説明は、表 31-2 を参照してください。
ステップ 3	Router# **show crypto debug-condition** {[***peer***] [***connid***] [***spi***] [***fvrf***] [***ivrf***] [***unmatched***]}	ルータ上ですでにイネーブルに設定されている暗号デバッグ条件を表示します。
ステップ 4	Router# **debug crypto isakmp**	グローバルな IKE デバッグをイネーブルにします。
ステップ 5	Router# **debug crypto ipsec**	グローバルな IPSec デバッグをイネーブルにします。
ステップ 6	Router# **debug crypto engine**	グローバルな暗号エンジン デバッグをイネーブルにします。
ステップ 7	Router# ***debug crypto condition unmatched*** [***isakmp*** | ***ipsec*** | ***engine***]	（任意）デバッグ条件をチェックするためのコンテキスト情報がない場合に、暗号条件別デバッグ メッセージを表示します。オプションのキーワードを指定しない場合、暗号関連のすべての情報が表示されます。

暗号条件別デバッグのディセーブル化

暗号条件別デバッグをディセーブルにするには、発行済みのグローバルな暗号デバッグ CLI を事前にディセーブルにする必要があります。そのあとで、暗号条件別デバッグをディセーブルに設定できます。暗号条件別デバッグをディセーブルにするには、次のコマンドを入力します。

```
Router# debug crypto condition reset
```

crypto error debug メッセージのイネーブル化

debug crypto error コマンドをイネーブルにすると、エラーに関連するデバッグ メッセージだけが表示されます。これにより、システムで IKE ネゴシエーションなどの暗号処理が失敗した理由を簡単に判別できます。crypto error debug メッセージをイネーブルにするには、特権 EXEC モードから次のコマンドを入力します。

```
Router# debug crypto {isakmp | ipsec | engine} error
```

（注）　このコマンドをイネーブルにする場合は、グローバルな暗号 debug コマンドがイネーブルに設定されていないことを確認してください。設定されていると、グローバル コマンドによってエラー関連のデバッグ メッセージが上書きされます。

暗号条件別デバッグ サポートに関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gt_dbcry.htm

SPA の活性挿抜の準備

Cisco 7600 シリーズ ルータは、各 SPA および SIP の活性挿抜をサポートしています。したがって、SPA を取り付けたまま SIP を取り外すことや、SIP をルータに搭載したまま SIP から特定の SPA だけを取り外すことができます。

つまり、SIP のいずれかのサブスロットから片方の SPA を取り外しても、別のアクティブな SPA のある SIP はルータに搭載したままで、もう 1 つの SPA をアクティブにしておくことができます。すぐに代わりの SPA を SIP に取り付ける予定がない場合は、該当するサブスロットにブランク フィラー プレートを必ず取り付けてください。SIP のすべてのサブスロットには、動作中の SPA またはブランク フィラー プレートのどちらかを常に取り付けておく必要があります。

活性挿抜の準備のために SPA をアクティブにするか、または非アクティブにする方法については、このマニュアルの「SIP のトラブルシューティング」の章にある「SIP および SPA の活性挿抜の準備」を参照してください。