CHAPTER 26

IPSec VPN SPA を使用した拡張 IPSec 機能の設定

この章では、Cisco 7600 シリーズ ルータ上の IPSec VPN SPA を使用して拡張 IP Security（IPSec）機能を設定する方法について説明します。具体的な内容は次のとおりです。

（注） Cisco IOS の IP Security（IPSec）暗号化処理およびポリシーについての詳細は、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。

システム イメージおよびコンフィギュレーション ファイルの管理については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』および『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

この章で使用する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。また、関連する CiscoIOS Release12.2 ソフトウェア コマンド リファレンスおよびマスター インデックスも参照してください。詳細については、「関連資料」（p.lv）を参照してください。

ヒント IPSec VPN SPA を使用して Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を正しく設定するために、設定の概要および注意事項にすべて目を通してから設定作業を始めてください。

拡張 IPSec 機能の概要

IPSec は Internet Engineering Task Force（IETF）で開発されたオープン規格のフレームワークです。インターネットなど保護されていないネットワークを介して重要な情報を伝達する場合は、IPSec によってセキュリティが確保されます。IPsec はネットワーク レイヤで機能して、シスコ製ルータなど、関与する IPSec デバイス（「ピア」）間の IP パケットを保護し、認証します。

この章では、IPSec VPN のスケーラビリティおよびパフォーマンスを高めるために使用できる高度な IPSec 機能について説明します。

トランスフォーム セットでの AES の設定

Advanced Encryption Standard（AES; 高度暗号化規格）は、Data Encryption Standard（DES; データ暗号規格）の後継として開発された IPSec および IKE のプライバシ トランスフォームです。AES は DES よりも安全度の高い設計となっています。AES ではキーのサイズが従来より大きく、侵入者がメッセージを解読するには、あらゆるキーを試してみるしか方法がありません。AES ではキーの長さは可変であり、128 ビット（デフォルト）、192 ビット、または 256 ビットのキーを指定できます。

トランスフォーム セット内で AES 暗号化アルゴリズムを設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

コマンド	説明
`Router(config)# crypto ipsec transform-set transform-set-name transform1[transform2[transform3]] ...`	トランスフォーム セットおよび IPSec セキュリティ プロファイルおよびアルゴリズムを指定します。

transform-set-name は、トランスフォーム セット名を指定します。

transform1[*transform2*[*transform3*]] は、IPSec セキュリティ プロトコルおよびアルゴリズムを定義します。AES を設定するには、次のいずれかの AES Encapsulating Security Payload（ESP）暗号化トランスフォームを選択する必要があります。

- ***esp-aes*** は、128 ビット AES 暗号化アルゴリズムを使用する ESP を指定します。
- ***esp-aes 192*** は、192 ビット AES 暗号化アルゴリズムを使用する ESP を指定します。
- ***esp-aes 256*** は、256 ビット AES 暗号化アルゴリズムを使用する ESP を指定します。

許容される他の transformx 値、およびトランスフォーム セットの設定についての詳細は、『*Cisco IOS Security Command Reference*』を参照してください。

AES トランスフォーム セットの確認

トランスフォーム セットの設定を確認するには、**show crypto ipsec transform-set** コマンドを入力します。

```
Router# show crypto ipsec transform-set

Transform set transform-1:{esp-256-aes esp-md5-hmac}
will negotiate = {Tunnel, }
```

AES 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/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_aes.html

AES の設定例は、「AES の設定例」（p.26-23）を参照してください。

LAF の設定

パケットのサイズが暗号化ルータのアウトバウンド リンクの最大伝送ユニット（Maximum Transmission Unit; MTU）、サイズとほぼ同じで、そのパケットが IPSec ヘッダーでカプセル化される場合、パケットはアウトバウンド リンクの MTU を超過する可能性があります。その場合、暗号化のあとでパケット フラグメンテーションが行われ、復号化ルータではプロセス パスで再アセンブルを行うことになります。IPSec VPN のプリフラグメンテーションを使用すると、復号化ルータがプロセス パスではなく高性能な CEF パスで動作するようになり、復号化ルータのパフォーマンスが向上します。

Look-Ahead Fragmentation（LAF）機能（別名、IPSec VPN のプリフラグメンテーション機能）により、暗号化ルータは、IPSec SA（セキュリティ アソシエーション）の一部として設定されているトランスフォーム セットで使用可能な情報から、カプセル化パケットのサイズをあらかじめ規定できます。パケットが出力インターフェイスの MTU を超過するように規定された場合、そのパケットはフラグメント化されてから暗号化されます。この機能は、復号化に先立ってプロセス レベルでの再アセンブリを回避し、復号化パフォーマンスおよび IPSec トラフィックの全体的なスループットを向上させます。

LAF 設定時の注意事項

LAF を設定する場合は、次の注意事項に従ってください。

- パケットが大きい場合、IPSec パケット サイズが MTU を超過し、IPSec パケットのフラグメンテーションが発生します。この場合、受信側の IPSec ピアでは、パケットを再アセンブルしてから復号化しなければなりません。この動作によって、多くの VPN ゲートウェイ デバイスには大きな負荷がかかります。この問題を解決するには、IPSec 復号化の前にパケットをフラグメント化し、エンド デバイスに再アセンブルの負荷がかからないようにします。
- IPSec ピアを経由して大容量パケットの送受信を行わない場合には、LAF をオフにしてください（ピアは IPSec パケット内部にあるフラグメントをドロップしている可能性があります）。
- 大容量パケット フローによって IPSec ピアの CPU 利用率が高くなっている場合は、LAF がイネーブルに設定されているかどうかを確認してください（ピアは大容量パケットを再アセンブルしている可能性があります）。
- IPSec VPN の LAF 機能は、IPSec トンネル モードおよび GRE を使用する IPSec トンネル モードで動作しますが、IPSec トランスポート モードでは動作しません。
- 単一方向トラフィックの構成では、暗号化ルータに IPSec VPN の LAF を設定してもパフォーマンスは改善されず、どちらのピアの動作も変更されません。
- IPSec VPN の LAF 機能は、出力インターフェイスの **crypto ipsec df-bit** 設定および着信パケットの「do not fragment」（DF）ビットの状態に依存します。詳細については、次の URL を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftprefrg.html
- GRE フラグメンテーション動作は、ソフトウェア リリースによって次のように異なります。
  - Cisco IOS Release 12.2(18)SXE より前のリリースでは、VPN モジュールの GRE フラグメンテーション動作はトンネル インターフェイスの IP MTU と出力インターフェイスのレイヤ 2 MTU によって決定されます。フラグメンテーションまたはパケット損失を防ぐために、トンネルおよび出力インターフェイス MTU の両方を予測最大 GRE/IPSec パケット サイズ（IP の長さ + GRE オーバーヘッド + IPSec オーバーヘッド）で設定する必要があります。トンネル インターフェイスの IP MTU をデフォルト値のままにする場合、GRE フラグメンテーション動作は出力インターフェイスのレイヤ 2 MTU によって決定されます。
  - Cisco IOS Release 12.2(18)SXE では、IPSec VPN SPA の GRE フラグメンテーション動作は VLAN MTU と出力インターフェイスのレイヤ 2 MTU によって決定されます。フラグメンテーションまたはパケット損失を防ぐために、VLAN MTU を予測最大 GRE パケット サイズ（IP の長さ + GRE オーバーヘッド）で設定し、出力インターフェイス MTU を予測最大 GRE/IPSec パケット サイズ（IP の長さ + GRE オーバーヘッド + IPSec オーバーヘッド）で設定する必要があります。

— Cisco IOS Release 12.2(18)SXF では、IPSec VPN SPA の GRE フラグメンテーション動作はルート プロセッサのフラグメンテーション動作と整合性がとれるように変更されています。VPN モジュールによって GRE カプセル化が実行される場合、アウトバウンド パケットのプリフラグメンテーションはトンネル インターフェイスの IP MTU に基づいて行われます。IPSec VPN SPA によって GRE カプセル化が実行された後、IPSec LAF 設定によってはさらにフラグメンテーションが行われることがあります。IPSec フラグメンテーション動作は Cisco IOS Release 12.2(18)SXE から変更されておらず、出力インターフェイスの IPSec MTU 設定に基づいて行われます。

インターフェイスでの LAF の設定

LAF は、デフォルトではグローバル レベルでイネーブルに設定されています。インターフェイス レベルで IPSec VPN の LAF をイネーブルまたはディセーブルにするには、インターフェイス コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config-if)# crypto ipsec fragmentation before-encryption`	インターフェイスで IPSec VPN のプリフラグメンテーションをイネーブルにします。
ステップ 2	`Router(config-if)# crypto ipsec fragmentation after-encryption`	インターフェイスで IPSec VPN のプリフラグメンテーションをディゼーブルにします。

（注）　この機能を手動でイネーブルまたはディセーブルにすると、グローバルな設定が上書きされます。

グローバル レベルでの LAF の設定

LAF はデフォルトでイネーブルです。グローバル レベルで IPSec VPN のプリフラグメンテーションをイネーブルまたはディセーブルにするには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto ipsec fragmentation before-encryption`	IPSec VPN のプリフラグメンテーションをグローバルでイネーブルにします。
ステップ 2	`Router(config)# crypto ipsec fragmentation after-encryption`	IPSec VPN のプリフラグメンテーションをグローバルでディセーブルにします。

LAF 設定の確認

LAF がイネーブルに設定されているかどうかを確認するには、暗号化ルータおよび復号化ルータのインターフェイス統計情報を調べます。暗号化ルータでフラグメンテーションが発生していて、かつ復号化ルータで再アセンブリが発生していない場合、暗号化の前にフラグメンテーションが実行されており、パケットは再アセンブリされずに復号化されていることになります。つまり、この機能はイネーブルです。

（注）　この確認方法は、復号化ルータを宛先とするパケットには当てはまりません。

この機能がイネーブルに設定されていることを確認するには、暗号化ルータで **show running-configuration** コマンドを入力します。この機能がイネーブルの場合、出力は次のようになります。

```
Router# show running-configuration

crypto isakmp policy 10
authentication pre-share
crypto isakmp key abcd123 address 25.0.0.7
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
crypto map bar 10 ipsec-isakmp
set peer 25.0.0.7
set transform-set fooprime
match address 102
```

この機能がディセーブルの場合、出力は次のようになります。

```
Router# show running-configuration

crypto isakmp policy 10
authentication pre-share
crypto isakmp key abcd123 address 25.0.0.7
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
crypto ipsec fragmentation after-encryption
crypto map bar 10 ipsec-isakmp
set peer 25.0.0.7
set transform-set fooprime
match address 102
```

暗号化ルータの出力インターフェイスの統計情報を表示するには、**show running-configuration interface** コマンドを入力します。この機能がイネーブルの場合、出力は次のようになります。

```
Router# show running-configuration interface gigabitethernet 5/0/1

interface GigabitEthernet5/0/1

ip address 25.0.0.6 255.0.0.0
no ip mroute-cache
load-interval 30
duplex full
speed 100
crypto map bar
```

この機能がディセーブルの場合、出力は次のようになります。

```
Router# show running-configuration interface gigabitethernet 5/0/1

interface GigabitEthernet5/0/1

ip address 25.0.0.6 255.0.0.0
no ip mroute-cache
load-interval 30
duplex full
speed 100
crypto map bar
crypto ipsec fragmentation after-encryption
```

LAF の詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftprefrg.html

MTU 値の設定

Cisco IOS ソフトウェアでは、プロトコル スタックのさまざまなレベルで、いくつかのタイプの設定可能な MTU オプションをサポートしています。パケットの不要な分割を回避するために、すべての MTU 値に一貫性を持たせる必要があります。

MTU 値の設定時の注意事項および制約事項

IPSec VPN SPA の MTU 値を設定する場合には、次の注意事項および制約事項に従ってください。

- 原則として、特に必要がないかぎり MTU 値を変更しないでください。
- IPSec VPN SPA がフラグメンテーションの決定に使用する MTU 値は、以下のセキュア ポートの MTU 値に基づいています。
  - ルーテッド ポート — 自身に対応付けられているセキュア ポートの MTU 値を使用します。
  - アクセス ポート — 自身のインターフェイス VLAN に対応付けられているセキュア ポートの MTU 値を使用します。
  - トランク ポート — 自身のインターフェイス VLAN に対応付けられているセキュア ポートの MTU 値を使用します。
- GRE トンネリングが設定されている場合は、「LAF の設定」（p.26-3）で MTU 値に関する情報を参照してください。

（注）　パケット フラグメンテーションについての詳細は、「LAF の設定」（p.26-3）を参照してください。

MTU の変更

ギガビット イーサネット インターフェイスの MTU 値を変更するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# interface gigabitethernet` *slot/subslot/port*	ギガビット イーサネット インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 • *slot* — SIP が搭載されたシャーシ スロット番号を指定します。 • *subslot* — SPA が搭載されている SIP のセカンダリ スロット番号を指定します。 • *port* — SPA のインターフェイス ポートの番号を指定します。
ステップ 2	`Router(config-if)# mtu` *bytes*	インターフェイスの MTU サイズを設定します。 • *bytes* — 有効な範囲は 1,500 ～ 9,216 です。使用されるデフォルト値は、「MTU 値の設定時の注意事項および制約事項」（p.26-6）に説明されているとおりです。
ステップ 3	`Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MTU サイズの確認

インターフェイスの MTU サイズを確認するには、**show interfaces** コマンドを入力します。

たとえば、セキュア ポートの MTU 値を表示するには、次のコマンドを入力します。

```
Router# show interfaces g1/1/1

GigabitEthernet1/1/1 is up, line protocol is up (connected)
Hardware is C6k 1000Mb 802.3, address is 000a.8ad8.1c4a (bia 000a.8ad8.1c4a)
MTU 9216 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
...
```

GRE トンネルの MTU 値を表示するには、次のコマンドを入力します。

```
Router# show ip interfaces tunnel 2

Tunnel2 is up, line protocol is up
Internet address is 11.1.0.2/16
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1450 bytes
...
```

RRI の設定

Reverse Router Injection（RRI; 逆ルート注入）には、リモート トンネル エンドポイントで保護されたネットワークおよびホストのルーティング プロセスに、スタティック ルートを自動的に挿入する機能があります。保護されたこれらのホストおよびネットワークは、リモート プロキシ アイデンティティとして認識されます。

（注）　RRI は Cisco IOS Release 12.2(33)SRA 以降でのみサポートされます。

各ルートはリモート プロキシ ネットワークおよびマスクに基づいて作成され、このネットワークに対するネクスト ホップがリモート トンネル エンドポイントになります。リモート VPN ルータをネクスト ホップとして使用することにより、トラフィックは強制的に暗号プロセスを通して暗号化されます。

VPN ルータにスタティック ルートを作成すると、この情報がアップストリーム デバイスに伝搬され、IPSec 状態フローを維持するために戻りトラフィックを送信する宛先として適切な VPN ルータを判別できます。適切な VPN ルータの判別機能は、特に、サイトで複数の VPN ルータを使用してロード バランスやフェールオーバーを実現する場合、またはデフォルト ルートを介してリモート VPN デバイスにアクセスできない場合に、便利です。ルートはグローバル ルーティング テーブルまたは適切な Virtual Routing and Forwarding（VRF）テーブルに作成されます。

RRI は、スタティック クリプト マップ テンプレートとダイナミック クリプト マップ テンプレートのいずれを使用するかに関係なく、暗号マップ単位で適用されます。ダイナミック マップとスタティック マップのいずれの場合も、ルートは IPSec SA を作成するときのみ作成されます。SA を削除すると、ルートも削除されます。スタティック クリプト マップのデフォルト動作が必要な場合、つまり、スタティック クリプト マップに適用される暗号 Access Control List（ACL; アクセス コントロール リスト）の内容に基づいてルートを作成する場合は、**reverse-route** コマンドに ***static*** キーワードを追加できます。

RRI 設定時の注意事項および制約事項

RRI 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。

- ダイナミック ルーティング プロトコルを使用して RRI 生成のスタティック ルートを伝播させる場合は、IP ルーティングをイネーブルにし、スタティック ルートを再配信する必要があります。
- インターフェイスまたはアドレスをリモート VPN デバイスの明示的なネクスト ホップとして指定できます。この機能により、デフォルト ルートを上書きして、暗号化された発信パケットを適切に転送できます。
- RRI を使用して作成されるルートには、ルート タグ値を追加できます。このルート タグにより、ルート マップを使用するルートのグループを再配信して、グローバル ルーティング テーブルに格納するルートを選択できます。
- 複数のルータ インターフェイスに適用される同一の暗号マップに、RRI を設定できます。
- ***remote-peer*** [***static***] キーワードを指定すると、2 つのルートが作成されます。1 番めのルートは標準リモート プロキシ ID で、ネクストホップはリモート VPN クライアント トンネル アドレスです。2 番めのルートは、このリモート トンネル エンドポイントへの実際のルートです。再帰検索で、「ネクスト ホップ」経由でリモート エンドポイントに到達できることが必要な場合に、使用されます。VRF では、デフォルト ルートをより明示的なルートで上書きする必要があるため、実際のネクスト ホップに対応する 2 番めのルートを作成することは重要です。

  作成するルート数を削減し、ルート再帰の実現が困難な一部のプラットフォームをサポートするには、***remote-peer*** {*ip-address*} [***static***] キーワードを使用して、ルートを 1 つのみ作成します。

- 仮想 IPSec インターフェイスの場合、リバース ルート オプションを指定すると、ネクスト ホップとして仮想アクセス インターフェイスを表示するルートが作成されます。
- IPSec VPN SPA を使用するデバイスの場合、リバース ルートはインターフェイス、サブインターフェイス、または VLAN（仮想 LAN）となるネクスト ホップを指定し、暗号マップを適用します。

スタティック クリプト マップを使用した RRI の設定

スタティック クリプト マップを使用して RRI を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto map {map-name} {seq-name} ipsec-isakmp`	暗号マップ エントリを作成または修正し、暗号マップ コンフィギュレーション モードを開始します。 • *map-name* — マップ セットの識別名 • *seq-num* — 暗号マップ エントリに割り当てられたシーケンス番号 • ***ipsec-isakmp*** — IKE を使用して IPSec SA を確立し、この暗号マップ エントリで指定されたトラフィックを保護することを表します。
ステップ 2	`Router(config-crypto-map)# reverse-route [[static] | tag {tag-id} [static] | remote-peer [static] | remote-peer {ip-address} [static]]`	暗号マップ エントリに対応する送信元プロキシ情報を作成します。 • ***static*** —（任意）暗号 ACL の有無に従って、ルートを作成します。 • ***tag*** {*tag-id*} — ルート マップによる再配信を制御するための「照合」値として使用できるタグ値 • ***remote-peer*** [***static***] — 2 つのルートが作成されます。1 つはリモート エンドポイント用で、もう 1 つは暗号マップの適用先となるインターフェイスを介してリモート エンドポイントに至るルート再帰用です。***static*** キーワードはオプションです。 • ***remote-peer*** {*ip-address*} [***static***] — ユーザ定義のネクスト ホップを経由してリモート プロキシに至るルートが 1 つ作成されます。このネクスト ホップを使用して、デフォルト ルートを上書きできます。*ip-address* 引数は必須です。***static*** キーワードはオプションです。

ダイナミック クリプト マップを使用した RRI の設定

ダイナミック クリプト マップを使用して RRI を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto dynamic-map {dynamic-map-name} {dynamic-seq-name}`	ダイナミック クリプト マップ エントリを作成し、暗号マップ コンフィギュレーション モードを開始します。 • *dynamic-map-name* — マップ セットの識別名 • *dynamic-seq-num* — 暗号マップ エントリに割り当てられたシーケンス番号
ステップ 2	`Router(config-crypto-map)# reverse-route [tag {tag-id} | remote-peer | remote-peer {ip-address}]`	暗号マップ エントリに対応する送信元プロキシ情報を作成します。 • ***tag*** {*tag-id*} — ルート マップによる再配信を制御するための「照合」値として使用できるタグ値 • ***remote-peer*** — 2 つのルートが作成されます。1 つはリモート エンドポイント用で、もう 1 つは暗号マップの適用先となるインターフェイスを介してリモート エンドポイントに至るルート再帰用です。 • ***remote-peer*** {*ip-address*} — ユーザ定義のネクスト ホップを経由してリモート プロキシに至るルートが 1 つ作成されます。このネクスト ホップを使用して、デフォルト ルートを上書きできます。*ip-address* 引数は必須です。

RRI の詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_rrie.html

RRI の設定例は、「RRI の設定例」（p.26-24）を参照してください。

QoS の設定

IPSec VPN SPA では Cisco 7600 シリーズ ルータ ソフトウェアの QoS 機能を使用して、2 レベルの完全優先 QoS を導入します。IPSec VPN SPA での QoS の設定については、次の URL を参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008014a29f.shtml

Cisco 7600 SSC-400 および IPSec VPN SPA では、インバウンドとアウトバウンドの各方向に 2 つのキューを導入します。パケットは 2 対 1 の比率でデキューされます。すなわち、1 つのパケットがプライオリティが低いキューからデキューされる前に、2 つのパケットがプライオリティが高いキューからデキューされます。パケットはプライオリティ キュー設定に基づいてエンキューされます。IPSec VPN SPA の QoS 機能を活用するには、標準的な QoS コマンドを使用して、パケットの Class of Service（CoS; サービス クラス）が入力側でマークされるようにする必要があります。内部ポートおよび外部ポートに対して CoS マップを設定し、CoS マッピングを承認するように IPSec VPN SPA に対して QoS をグローバルにイネーブル化する必要があります。

QoS 設定時の注意事項および制約事項

IPSec VPN SPA に対して QoS を設定する場合には、次の注意事項および制約事項に従ってください。

- パケットは **mls qos** コマンドとプライオリティ キュー設定に基づいて、次のようにエンキューされます。
  - **mls qos** コマンドが設定されていない場合、すべてのデータ パケットはプライオリティが高いキューにエンキューされます。
  - **mls qos** コマンドが設定されていて、IPSec VPN SPA イーサネット インターフェイスで明示的なプライオリティ キュー設定がない場合、CoS 値が 5 のパケットのみがプライオリティが高いキューにエンキューされ、他のすべてのパケットはプライオリティが低いキューにエンキューされます。
  - **mls qos** コマンドが設定されていて、IPSec VPN SPA イーサネット インターフェイスにプライオリティ キュー設定がある場合、トラフィックはそのプライオリティ キュー設定に基づいてエンキューされます。
- プライオリティが高いキューには、最大 3 つの CoS マップ値を送信できます。CoS 値 5 は高プライオリティとして事前設定されているため、高プライオリティ キューに他の値は 2 つしか選択できません。

（注） CoS 値を 3 つより多く設定しないでください。余分な値は設定されている値を上書きするためです。CoS 値 5 を上書きすると、設定されている他のいずれかの値を上書きすることによって値は復元されます。上書きされた CoS マップ値を復元するには、まず新しい値を削除してから前の値を再設定する必要があります。

- **mls qos** コマンドが設定されている場合、IPSec VPN SPA イーサネット インターフェイスで次の例のように **mls qos trust** コマンドを指定する必要があります。

```
!
Interface GigabitEthernet4/0/1
 mls qos trust dscp
 priority-queue cos-map 1 0 1 5
!
Interface GigabitEthernet4/0/2
 mls qos trust dscp
 priority-queue cos-map 1 0 1 5
!
```

この例では、CoS 値 0、1、5 が高プライオリティ キューに送信されます。

- **mls qos trust** コマンドが設定されていない場合、すべてのトラフィックの QoS フィールドはデフォルト レベルにクリアされます。**mls qos trust** コマンドが設定されている場合、QoS フィールドはそのままになります。

QoS の設定例は、「QoS の設定例」（p.26-25）を参照してください。

IPSec アンチリプレイ ウィンドウ サイズの設定

Cisco IPSec 認証を行うと、アンチリプレイ サービスを利用できます。これにより、暗号化された各パケットに一意のシーケンス番号を割り当てて、暗号化パケットを複製する攻撃者から保護できます（SA アンチリプレイは、受信側がリプレイ攻撃から自身を保護するために、古いパケットまたは重複パケットを拒否できるセキュリティ サービスです）。復号機能によって、以前に認識したシーケンス番号が除外されます。暗号機能によって、シーケンス番号が昇順で割り当てられます。復号機能は、認識済みのシーケンス番号の中の最大値（X）を記憶します。N は複合機能のウィンドウ サイズです。X-N よりもシーケンス番号が小さいパケットはすべてドロップされます。現在、N は 64 に設定されています。

（注）　IPSec アンチリプレイ ウィンドウ サイズ機能は、Cisco IOS Release 12.2(18)SXF6 および Cisco IOS Release 12.2(33)SRA 以降でのみサポートされます。

64 パケット ウィンドウ サイズでは不十分な場合があります。たとえば、Cisco Quality of Service（QoS; サービス品質）はプライオリティが高いパケットを優先しますが、これによって、プライオリティが低いパケットが、リプレイされたパケットでない場合も、ドロップされることがあります。IPSec アンチリプレイ ウィンドウ サイズ機能を使用すると、64 を超えるパケットのシーケンス番号情報を保持できるように、ウィンドウ サイズを拡張できます。

IPSec アンチリプレイ ウィンドウ サイズのグローバルな拡張

IPSec アンチリプレイ ウィンドウをグローバルに拡張して、作成されたすべての SA に影響するように設定するには（暗号マップ単位で上書きされたものを除いて）、グローバル コンフィギュレーション モードで次の手順を実行します。

コマンド	説明
`Router(config)# crypto ipsec security-association replay window size [size]`	IPSec アンチリプレイ ウィンドウを、指定された *size* にグローバルに拡張します。 • *size* — （任意）ウィンドウ サイズ。有効値は 64、128、256、512、または 1024 です。この値がデフォルト値になります。

暗号マップ レベルでの IPSec アンチリプレイ ウィンドウの拡張

暗号マップ単位で IPSec アンチリプレイ ウィンドウを拡張するには（指定された暗号マップまたはプロファイルを使用して作成された SA に影響するように設定するには）、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンド	説明
ステップ 1	`Router(config)# crypto map map-name seq-num ipsec-isakmp`	暗号マップ コンフィギュレーション モードを開始し、ダイナミックに作成される暗号マップ設定のテンプレートとなる暗号プロファイルを作成します。 • *map-name* — マップ セットの識別名 • *seq-num* — 暗号マップ エントリに割り当てられたシーケンス番号 • ***ipsec-isakmp*** — IKE を使用して IPSec SA を確立し、この暗号マップ エントリで指定されたトラフィックを保護することを表します。
ステップ 2	`Router(config-crypto-map)# crypto ipsec security-association replay window size [size]`	特定の暗号マップ、ダイナミック クリプト マップ、または暗号プロファイルで指定されたポリシーを使用して作成される SA を制御します。 • *size* — （任意）ウィンドウ サイズ。有効値は 64、128、256、512、または 1024 です。この値がデフォルト値になります。

暗号マップ レベルでの IPSec アンチリプレイ ウィンドウ サイズ コンフィギュレーションの確認

IPSec アンチリプレイ ウィンドウ サイズが特定の暗号マップでイネーブルになっているかどうかを確認するには、その特定マップに対して **show crypto map** コマンドを入力します。アンチリプレイ ウィンドウ サイズがイネーブルになっている場合、イネーブルになっていることおよび設定されているウィンドウ サイズがディスプレイに示されます。アンチリプレイ ウィンドウ サイズがディセーブルになっている場合、コマンドの結果でその旨が示されます。

IPSec アンチリプレイ ウィンドウ サイズ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/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_iarwe.html

IPSec アンチ リプレイ ウィンドウ サイズの設定例は、「IPSec アンチリプレイ ウィンドウ サイズの設定例」（p.26-26）を参照してください。

（注）　IPSec VPN SPA によって検出されるアンチ リプレイ エラーの原因には、リオーダー、再キューイング、またはネットワーク内のフラグメンテーションなどがあります。中間者攻撃に対する防御として、IPSec VPN SPA はこのようなパケットをドロップします。これは予期されている動作です。

IPSec アンチリプレイ チェックのディセーブル化

IPSec アンチリプレイ チェックをディセーブルにするには、次のようにグローバル コンフィギュレーション モードで **crypto ipsec security-association replay disable** コマンドを入力します。

コマンド	説明
`Router(config)# crypto ipsec security-association replay disable`	IPSec アンチリプレイ チェックをディセーブルにします。

IPSec 優先ピアの設定

IPSec 優先ピア機能を使用すると、暗号マップの複数のピアをフェールオーバー構成で試行する場合の環境を制御できます。デフォルト ピアが存在する場合は、次回に接続を開始すると、ピア リスト内の次のピアでなく、デフォルト ピアに接続されます。現在のピアとのすべての接続がタイムアウトした場合、次回に接続を開始すると、デフォルト ピアに接続されます。

（注）　IPSec 優先ピア機能は、Cisco IOS Release 12.2(33)SRA 以降でのみサポートされています。

この機能には、次の機能が含まれます。

- デフォルト ピアの設定

  接続がタイムアウトした場合、現在のピアとの接続は切断されます。**set peer** コマンドを使用すると、先頭のピアをデフォルト ピアとして設定できます。デフォルト ピアが存在する場合は、次回に接続を開始すると、ピア リスト内の次のピアでなく、デフォルト ピアに接続されます。デフォルト ピアが応答しない場合、ピア リスト内の次のピアが現在のピアになり、今後、暗号マップを使用して接続しようとすると、このピアとの接続が試行されます。

  この機能は、リモート ピアの障害が原因で物理リンクのトラフィックが停止した場合に、便利です。Dead Peer Detection（DPD）はリモート ピアが使用不能であるにもかかわらず、このピアが引き続き現在のピアになっていることを示します。

  デフォルト ピアが設定されていると、以前は使用不能だったにもかかわらず、サービス状態に戻っている優先ピアへのフェールオーバーが容易になります。ユーザはフェールオーバーが発生した場合に備えて、特定のピアを優先させることができます。これは、障害の本来の原因がリモート ピアの故障でなく、ネットワーク接続問題である場合に便利です。

  デフォルト ピアを設定するには、「デフォルト ピアの設定」（p.26-16）を参照してください。

- デフォルト ピアを設定する場合の IPSec アイドル タイマー

  Cisco IOS ソフトウェアが稼働するルータでピアの IPSec SA を作成する場合、SA を維持するためのリソースを割り当てる必要があります。SA には、メモリといくつかの管理タイマーが必要です。アイドル ピアがあると、リソースが浪費されます。アイドル ピアによるリソースの浪費が大きくなると、ルータは他のピア用に新しい SA を作成できなくなる可能性があります。

  IPSec SA アイドル タイマーは、アイドル ピアに対応付けられた SA を削除して、リソースのアベイラビリティを向上させます。IPSec SA アイドル タイマーにより、アイドル ピアによるリソース浪費は防止されるため、新しい SA を作成するためにリソースが必要な場合に、使用できるリソースが多くなります（IPSec SA アイドル タイマーが設定されていない場合は、IPSec SA のグローバル ライフタイムのみが適用されます。ピアの活動状況に関係なく、グローバル タイマーの期限が切れるまで、SA は維持されます）。

  IPSec SA アイドルタイマーとデフォルト ピアが両方とも設定されている場合に、現在のピアとの接続がすべてタイムアウトすると、次回に接続を開始したときに、**set peer** コマンドで設定したデフォルト ピアに接続されます。デフォルト ピアが設定されていない場合に、接続がタイムアウトすると、現在のピアはタイムアウト状態を継続します。

  この拡張機能を使用すると、以前は使用不能だったにもかかわらず、現在はサービス状態になっている優先ピアへのフェールオーバーが容易になります。

  IPSec アイドル タイマーの設定については、「デフォルト ピアを使用する場合の IPSec アイドル タイマーの設定」（p.26-17）を参照してください。

IPSec 優先ピアの設定時の注意事項および制約事項

IPSec 優先ピアを設定する場合は、次の注意事項および制約事項に従ってください。

- デフォルト ピアを設定する場合は、次の注意事項および制約事項に従ってください。
  - デフォルト ピア機能は DPD と併用する必要があります。この機能は、DPD が稼働するリモート サイトで、定期的モードで使用するのが最も効果的です。DPD はデバイスの障害をすばやく検出し、次回の接続試行でデフォルト ピアが試行されるように、ピア リストをリセットします。
  - 暗号マップでデフォルト ピアに指定できるのは、1 つのピアのみです。
  - デフォルト ピアはピア リストの先頭ピアに指定する必要があります。
- デフォルト ピアと IPSec アイドル タイマーを併用するように設定する場合は、次の注意事項および制約事項に従ってください。
  - IPSec アイドル タイマーとデフォルト ピアの併用機能は、この機能が設定された暗号マップでのみ機能します。この機能をすべての暗号マップにグローバルに設定することはできません。
  - グローバル アイドル タイマーがある場合、暗号マップのアイドル タイマー値とグローバル値は異なっている必要があります。そうでない場合、アイドル タイマーは暗号マップに追加されません。

デフォルト ピアの設定

デフォルト ピアを設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto map map-name seq-num [ipsec-isakmp] [dynamic dynamic-map-name] [discover] [profile profile-name]`	暗号マップ コンフィギュレーション モードを開始し、ダイナミックに作成される暗号マップ設定のテンプレートとなる暗号プロファイルを作成します。 • *map-name* — マップ セットの識別名 • *seq-num* — 暗号マップ エントリに割り当てられたシーケンス番号 • ***ipsec-isakmp*** —（任意）IKE を使用して IPSec SA を確立し、この暗号マップ エントリで指定されたトラフィックを保護することを表します。 • ***dynamic*** *dynamic-map-name* —（任意）ポリシー テンプレートとして使用するダイナミック クリプト マップ セットの名前を指定します。 • ***discover*** —（任意）ピア検出をイネーブルにします。デフォルトでは、ピア検出はディセーブルです。 • ***profile*** *profile-name* —（任意）作成中の暗号プロファイルの名前
ステップ 2	`Router(config-crypto-map)# set peer {host-name [dynamic] [default] | ip-address [default]}`	暗号マップ エントリで IPSec ピアを指定します。指定した最初のピアがデフォルト ピアとして定義されます。 • *host-name* — IPSec ピアをホスト名で指定します。これはドメイン名と連結されるピアのホスト名です（myhost.example.com など）。 • ***dynamic*** —（任意）ルータが IPSec トンネルを確立する前に、Domain Name Server（DNS）検索を使用して IPSec ピアのホスト名を解決します。 • ***default*** —（任意）複数の IPSec ピアが存在する場合、最初のピアがデフォルト ピアになるように指定します。 • *ip-address* — IPSec ピアを IP アドレスで指定します。
ステップ 3	`Router(config-crypto-map)# exit`	暗号マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

デフォルト ピアを使用する場合の IPSec アイドル タイマーの設定

IPSec アイドル タイマーとデフォルト ピアを併用するように設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto map map-name seq-num [ipsec-isakmp] [dynamic dynamic-map-name] [discover] [profile profile-name]`	暗号マップ コンフィギュレーション モードを開始し、ダイナミックに作成される暗号マップ設定のテンプレートとなる暗号プロファイルを作成します。 • *map-name* — マップ セットの識別名 • *seq-num* — 暗号マップ エントリに割り当てられたシーケンス番号 • ***ipsec-isakmp*** —（任意）IKE を使用して IPSec SA を確立し、この暗号マップ エントリで指定されたトラフィックを保護することを表します。 • ***dynamic*** *dynamic-map-name* —（任意）ポリシー テンプレートとして使用するダイナミック クリプト マップ セットの名前を指定します。 • ***discover*** —（任意）ピア検出をイネーブルにします。デフォルトでは、ピア検出はディセーブルです。 • ***profile*** *profile-name* —（任意）作成中の暗号プロファイルの名前
ステップ 2	`Router(config-crypto-map)# set security-association idle-time seconds [default]`	デフォルト ピアを使用するまでに、現在のピアがアイドルのまま存続できる最大期間を指定します。 • *seconds* — デフォルト ピアを使用するまでに、現在のピアがアイドルのまま存続できる秒数を指定します。有効値は、600 ～ 86400 です。 • ***default*** —（任意）次の接続がデフォルト ピアとの間で確立されるように指定します。
ステップ 3	`Router(config-crypto-map)# exit`	暗号マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

IPSec 優先ピア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/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_ipspp.html

IPSec 優先ピアの設定例は、「IPSec 優先ピアの設定例」（p.26-29）を参照してください。

IPSec SA アイドル タイマーの設定

Cisco IOS ソフトウェアが稼働するルータでピアの IPSec SA を作成する場合、SA を維持するためのリソースを割り当てる必要があります。SA には、メモリといくつかの管理タイマーが必要です。アイドル ピアがあると、リソースが浪費されます。アイドル ピアによるリソースの浪費が大きくなると、ルータは他のピア用に新しい SA を作成できなくなる可能性があります。IPSec SA アイドル タイマー機能を使用すると、SA のアクティビティを監視する設定可能なタイマーが提供され、アイドル ピアの SA を削除できるようになります。アイドル タイマーは、グローバルに設定することも、暗号マップ単位で設定することも、ISAKMP プロファイルを使用して設定することもできます。この機能の利点は次のとおりです。

- リソースのアベイラビリティの向上
- Cisco IOS IPSec 構成のスケーラビリティの向上

IPSec SA アイドル タイマー設定時の注意事項

暗号マップ単位でアイドル タイマーを設定する場合は、次の注意事項に従ってください。

- IPSec VPN SPA は、CLI（コマンドライン インターフェイス）で設定された間隔を、切り上げて最も近い 10 分単位にします。たとえば、アイドル タイムアウトを 12 分に設定すると、IPSec VPN SPA は 20 分をアイドル タイムアウト値として使用します。5 分に設定すると、IPSec VPN SPA は 10 分をアイドル タイムアウト値として使用します。

（注） 最小 IPSec SA アイドル タイムの推奨値は 600 秒です。*seconds* に 600 未満の値を入力すると、アイドル タイムは 600 秒に設定されます。

- IPSec VPN SPA によるアイドル タイムアウト検出方式の特徴として、アイドル タイムアウトが検出されるまでにインターバル（10 分単位）の 1 ～ 3 倍の時間がかかる場合があります。たとえば、アイドル タイムアウトを 12 分に設定した場合、アイドル タイムアウトは 20 ～ 60 分の時間内に発生する可能性があります。
- アイドル タイマーをグローバルに設定すると、すべての SA にアイドル タイマーの設定が適用されます。
- 暗号マップにアイドル タイマーを設定すると、その暗号マップの下にあるすべての SA にアイドル タイマーの設定が適用されます。

IPSec SA アイドル タイマーのグローバルな設定

IPSec SA アイドル タイマーをグローバルに設定するには、次のようにグローバル コンフィギュレーション モードで **crypto ipsec security-association idle-time** コマンドを入力します。

コマンド	説明
`Router(config)# crypto ipsec security-association idle-time` *seconds*	*seconds* — アイドル タイマーで非アクティブなピアが SA を保持できる時間（秒）を指定します。範囲は 600 ～ 86400 秒です。

IPSec SA アイドル タイマーの暗号マップ単位での設定

特定の暗号マップに IPSec SA アイドル タイマーを設定するには、暗号マップを設定するときに、**set security-association idle-time** コマンドを使用します。

	コマンド	説明
ステップ 1	`Router(config)# crypto map map-name seq-number ipsec-isakmp`	暗号マップ エントリを作成または修正し、暗号マップ コンフィギュレーション モードを開始します。 • *map-name* — 暗号マップ セットの識別名 • *seq-number* — 暗号マップ エントリに割り当てるシーケンス番号。値が小さいほどプライオリティが高くなります。 • ***ipsec-isakmp*** — IKE を使用して IPSec SA を確立することを表します。
ステップ 2	`Router(config-crypto-map)# set security-association idle-time seconds`	*seconds* — アイドル タイマーで非アクティブなピアが SA を保持できる時間（秒）を指定します。範囲は 600 ～ 86400 秒です。

IPSec SA アイドル タイマーの設定についての詳細は、次の Cisco IOS マニュアルを参照してください。

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftsaidle.html

IPSec SA アイドル タイマーの設定例は、「IPSec SA アイドル タイマーの設定例」（p.26-29）を参照してください。

Distinguished Name（DN; 識別名）ベースの暗号マップの設定

Distinguished Name（DN; 認定者名）ベースの暗号マップ機能により、特定の証明書（特に、特定 DN の証明書）を持つピアの選択された暗号化インターフェイスだけに、アクセスを制限するようにルータを設定できます。

従来、ルータが暗号化ピアから証明書または共有秘密を受け入れる場合、Cisco IOS では暗号化ピアの IP アドレスによって制限する以外、ピアが暗号化インターフェイスと通信するのを防ぐ方法がありませんでした。この機能により、ピアが自身の認証に使用した DN に基づいて、ピアが使用できる暗号マップを設定し、特定の DN を持つ暗号化ピアがアクセスできる暗号化インターフェイスを制御できます。DN によって認証されたピアのみ使用可能な DN ベースの暗号マップ、またはホスト名によって認証されたピアのみ使用可能な暗号マップを設定できます。

DN ベース暗号マップ設定時の注意事項および制約事項

DN ベース暗号マップを設定する場合は、次の注意事項および制約事項に従ってください。

- アクセスを制限する DN の数が多い場合、少数のアイデンティティ セクションを参照する多数の暗号マップを指定するよりも、多数のアイデンティティ セクションを参照する少数の暗号マップを指定することを推奨します。

DN によって認証されたピアのみ使用可能な DN ベース暗号マップ、またはホスト名によって認証されたピアのみ使用可能な暗号マップベース DN を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明

ステップ 1	`Router(config)# crypto isakmp policy` *priority*
	`...`
	`Router(config-isakmp)# exit`
		ISAKMP ポリシーを定義し、ISAKMP ポリシー コンフィギュレーション モードを開始します。
		• *priority* — IKE ポリシーを指定し、このポリシーにプライオリティを割り当てます。1 ～ 10,000 の整数を使用します。プライオリティは 1 が最高、10,000 が最低です。
		各ピアで ISAKMP ポリシーを作成します。
		ISAKMP ポリシーの設定についての詳細は、『*Cisco IOS Security Configuration Guide*』を参照してください。

ステップ 2	`Router(config)# crypto map` *map-name seq-number* ***ipsec-isakmp***	暗号マップ エントリを作成または修正し、暗号マップ コンフィギュレーション モードを開始します。 • *map-name* — 暗号マップ セットの識別名 • *seq-number* — 暗号マップ エントリに割り当てるシーケンス番号。値が小さいほどプライオリティが高くなります。 • ***ipsec-isakmp*** — IKE を使用して IPSec SA を確立することを表します。

	コマンド	説明
ステップ 3	Router(config-crypto-map)# **identity** *name* ... Router(config-crypto-map)# **exit**	暗号マップにアイデンティティを適用します。 • *name* — 既定の DN のリストに対応付けられた、ルータのアイデンティティ このコマンドを適用した場合、アイデンティティ名でリストされているコンフィギュレーションと一致するホストだけが、指定した暗号マップを使用できます。 （注） 暗号マップに **identity** コマンドが使用されていない場合、暗号化ピアの IP アドレス以外には、暗号接続の制限はありません。 コンフィギュレーションに対応するように、その他のポリシー値を指定します。 暗号マップの設定についての詳細は、『*Cisco IOS Security Configuration Guide*』を参照してください。
ステップ 4	Router(config)# **crypto identity** *name*	ルータの証明書に所定の DN リストを備えたルータ アイデンティティを設定し、暗号アイデンティティ コンフィギュレーション モードを開始します。 • *name* — ステップ 3 で指定した名前を入力します。
ステップ 5	Router(crypto-identity)# **dn** *name=**string*** [,*name=**string***]｜ ***fqdn*** *name*	ルータのアイデンティティを DN またはホスト名（FQDN）に対応付け、特定の証明書を使用してピアへのアクセスを制限します。 • *name=**string*** — ルータの証明書に DN を入力します。複数の DN を対応付けることもできます。 • ***fqdn*** *name* — ピアが自身の認証に使用したホスト名（FQDN）またはルータの証明書にある DN を入力します。 ピアのアイデンティティは、交換された証明書の中のアイデンティティと一致している必要があります。

DN ベースの暗号マップ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/en/US/docs/ios/12_2t/12_2t4/feature/guide/ftdnacl.html

DN ベース暗号マップの設定例は、「Distinguished Name（DN; 識別名）ベースの暗号マップの設定例」（p.26-30）を参照してください。

シーケンス番号付き ACL

ACL は、一連の Access Control Entry（ACE; アクセス コントロール エントリ）で構成されます。シーケンス番号付き ACL を使用すると、ACE の前にシーケンス番号を入力でき、そのシーケンス番号によって ACE が処理されます。さらに、削除する ACE の前にあるシーケンス番号を使用して、ACE を個別に削除することもできます。シーケンス番号はコンフィギュレーションには表示されませんが、**show access-list** コマンドを使用して表示できます。

（注）　ACE を削除または修正すると、ACL が SPA に再設定されます。その結果、既存のセッションが切断される場合があります。

ACL の拒否ポリシー拡張機能の設定

ACL に拒否アドレス範囲を指定することによって、「ジャンプ」動作が行われます。拒否アドレス範囲にヒットした場合、検索が暗号マップの次のシーケンスに対応付けられている ACL の先頭に「ジャンプ」し、検索が続行します。これらのアドレスに平文のトラフィックを渡すには、暗号マップ内のシーケンスごとに拒否アドレス範囲を挿入する必要があります。この作業を行うと、アドレスの許可リストごとに、ACL で指定されたすべての拒否アドレス範囲が継承されます。拒否アドレス範囲によって、ソフトウェアでは許可リストから拒否アドレス範囲が除外され、ハードウェアにプログラミングする必要のある複数の許可アドレス範囲を作成します。この動作により、繰り返されたアドレス範囲を 1 つの拒否アドレス範囲としてハードウェアにプログラミングすることが可能になるので、1 つの ACL に複数の許可アドレス範囲が作成されます。この問題を回避するには、**crypto ipsec ipv4 deny-policy** {**jump** | **clear** | **drop**} コマンド セットを次の要領で使用します。

- **jump** キーワードを指定すると、標準的な「ジャンプ」動作が実行されます。
- **clear** キーワードを使用すると、ハードウェアに拒否アドレス範囲をプログラミングできます。この拒否アドレスは暗号化および復号化の際に除外されます。VPN モードが暗号接続の場合、拒否アドレスにヒットすると、そこで検索が停止し、トラフィックは平文の（暗号化されない）状態で渡されます。VPN モードが VRF の場合、拒否アドレスと一致するトラフィックはドロップされます。
- **drop** キーワードを指定すると、拒否アドレスにヒットした場合にトラフィックがドロップされます。

clear および **drop** キーワードを使用すると、ハードウェアにアドレス範囲が繰り返しプログラミングされるのを防止でき、結果的に TCAM スペースを効率よく利用できます。

ACL の拒否ポリシー拡張機能設定時の注意事項および制約事項

拒否ポリシー拡張機能を設定する場合は、次の注意事項および制約事項に従ってください。

- **crypto ipsec ipv4 deny-policy** {**jump** | **clear** | **drop**} コマンドは、1 つの IPSec VPN SPA に適用されるグローバル コマンドです。指定するキーワード（**jump**、**clear**、または **drop**）は、IPSec VPN SPA の ACE ソフトウェアに渡されます。デフォルトの動作は **jump** です。
- **clear** キーワードを VRF モードで使用すると、拒否アドレスのトラフィックは平文の状態で渡されるのではなく、ドロップされます。VRF モードでは、トラフィックを平文の状態では渡しません。
- IPSec VPN SPA に暗号マップがすでに設定されている場合、キーワード（**jump**、**clear**、または **drop**）を適用すると、既存のすべての IPSec セッションが一時的に削除および再起動され、ネットワーク トラフィックに影響が出ます。
- ACL に指定できる拒否エントリの数は、指定されたキーワードによって異なります。
  - **jump** — 1 つの ACL で最大 8 つの拒否エントリをサポート

（注）　固定限度ではなく、ACL の 8 つの拒否ジャンプ エントリ限度を考慮してください。設定によっては、実際の限度は 8 よりも少ないことがあります。

- **clear** — 1 つの ACL で最大 1,000 の拒否エントリをサポート
- **drop** — 1 つの ACL で最大 1,000 の拒否エントリをサポート

拒否ポリシー拡張機能の設定例は、「ACL の拒否ポリシー拡張機能の設定例」（p.26-30）を参照してください。

設定例

ここでは、次の設定例を示します。

AES の設定例

次に、**show running-config** コマンドの出力例を示します。この例では、AES 256 ビット キーをイネーブルに設定しています。

```
Router# show running-config

Current configuration : 1665 bytes
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname "Router1"
ip subnet-zero
no ip domain lookup
ip audit notify log
ip audit po max-events 100
crypto isakmp policy 10
encryption aes 256
authentication pre-share
lifetime 180
crypto isakmp key cisco123 address 10.0.110.1
crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac
mode transport
crypto map aesmap 10 ipsec-isakmp
set peer 10.0.110.1
set transform-set aesset
...
```

RRI の設定例

次に、RRI の設定例を示します。

スタティック クリプト マップを使用した RRI の設定例

次に、スタティック クリプト マップを使用した RRI の設定例を示します。この例では、RRI によって作成されたルートにタグ番号が付加されています。ルーティング プロセスはこのタグ番号を使用し、ルート マップを介してタグ付きルートを再配信できます。

```
Router(config)# crypto map mymap 1 ipsec-isakmp
Router(config-crypto-map)# reverse-route tag 5
```

ダイナミック クリプト マップを使用した RRI の設定例

次に、ダイナミック クリプト マップを使用した RRI の設定例を示します。

```
Router(config)# crypto dynamic-map mymap 1
Router(config-crypto-map)# reverse-route remote peer 10.1.1.1
```

既存の ACL が存在する場合の RRI の設定例

次に、既存の ACL が存在する場合の RRI の設定例を示します。

```
Router(config)# crypto map mymap 1 ipsec-isakmp
Router(config-crypto-map)# set peer 172.17.11.1
Router(config-crypto-map)# reverse-route static
Router(config-crypto-map)# set transform-set esp-3des-sha
Router(config-crypto-map)# match address 101

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

2 つのルートがある場合の RRI の設定例

次に、2 つのルートを設定する例を示します。1 つはリモート エンドポイント用で、もう 1 つは暗号マップの適用先となるインターフェイスを介してリモート エンドポイントに至るルート再帰用です。

```
Router(config-crypto-map)# reverse-route remote-peer
```

ユーザ定義ホップを使用した RRI の設定例

次に、ユーザ定義ネクスト ホップを経由してリモート プロキシに至るルートを 1 つ作成する例を示します。このネクスト ホップは、デフォルト ルートに再帰する場合を除き、再帰ルート検索を必要としません。

```
Router(config-crypto-map)# reverse-route remote-peer 10.4.4.4
```

QoS の設定例

次に、QoS の設定例を示します。

```
!
hostname router-1
!
mls qos
!
vlan 2-3,502-503
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 lifetime 500
crypto isakmp key 1234567890 address 15.0.0.2
crypto isakmp key 1234567890 address 15.0.1.2
!
crypto ipsec transform-set proposal1 esp-3des
!
crypto map cmap_1 local-address Vlan2
crypto map cmap_1 10 ipsec-isakmp
 set peer 15.0.0.2
 set transform-set proposal1
 match address 101
!
crypto map cmap_2 local-address Vlan3
crypto map cmap_2 10 ipsec-isakmp
 set peer 15.0.1.2
 set transform-set proposal1
 match address 102
!
interface Tunnel1
 ip address 1.0.0.1 255.255.255.0
 tunnel source 15.0.0.1
 tunnel destination 15.0.0.2
!
interface Tunnel2
 ip address 1.0.1.1 255.255.255.0
 tunnel source 15.0.1.1
 tunnel destination 15.0.1.2
!
interface GigabitEthernet3/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502-504,1002-1005
 switchport mode trunk
 no ip address
 mls qos trust cos
!
interface GigabitEthernet3/3
 ip address 12.0.0.1 255.255.255.0
 ip policy route-map r1
 load-interval 30
 no keepalive
 mls qos trust ip-precedence
!
interface GigabitEthernet6/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
!!!
!!! The following wrr-queue and rcv-queue commands are inserted automatically.
!!! These commands are only meaningful for a physical Ethernet port.
!!!
```

```
 wrr-queue cos-map 2 1 4
 priority-queue cos-map 1 5 6 7
 rcv-queue cos-map 1 3 4
!!!
!!!
 mls qos trust cos
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet6/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502-504,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 wrr-queue cos-map 2 1 4
 priority-queue cos-map 1 5 6 7
 rcv-queue cos-map 1 3 4
 mls qos trust cos
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan2
 ip address 15.0.0.1 255.255.255.0
 no mop enabled
 crypto map cmap_1
 crypto engine subslot 6/0
!
interface Vlan3
 ip address 15.0.1.1 255.255.255.0
 no mop enabled
 crypto map cmap_2
 crypto engine subslot 6/0
!
interface Vlan502
 no ip address
 crypto connect vlan 2
!
interface Vlan503
 no ip address
 crypto connect vlan 3
!
ip classless
ip route 13.0.0.0 255.0.0.0 Tunnel1
ip route 22.0.0.0 255.0.0.0 12.0.0.2
ip route 23.0.0.0 255.0.0.0 Tunnel2
!
access-list 101 permit gre host 15.0.0.1 host 15.0.0.2
access-list 102 permit gre host 15.0.1.1 host 15.0.1.2
!
route-map r1 permit 10
 match ip address 102
 set ip precedence priority!
```

IPSec アンチリプレイ ウィンドウ サイズの設定例

次に、IPSec アンチリプレイ ウィンドウ サイズの設定例を示します。

- IPSec アンチリプレイ ウィンドウのグローバルな設定例（p.26-27）
- IPSec アンチリプレイ ウィンドウの暗号マップ単位の設定例（p.26-28）

IPSec アンチリプレイ ウィンドウのグローバルな設定例

次に、アンチリプレイ ウィンドウ サイズをグローバルに 1,024 に設定する例を示します。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Gateway1
!
boot-start-marker
boot-end-marker
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
ip audit po max-events 100
no ftp-server write-enable
!
crypto isakmp policy 10
authentication pre-share
crypto isakmp key cisco123
address 192.165.201.2
!
crypto ipsec security-association replay window-size 1024
!
crypto ipsec transform-set basic esp-des esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp
set peer 192.165.201.2
set transform-set basic
match address 101
!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
!
interface Serial1/0
ip address 192.165.200.2 255.255.255.252
serial restart-delay 0
crypto map mymap
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.165.200.1
no ip http server
no ip http secure-server
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!access-list 101 remark Crypto ACL
!
control-plane
!
line con 0
line aux 0
line vty 0 4
end
```

IPSec アンチリプレイ ウィンドウの暗号マップ単位の設定例

次に、172.150.150.2 との IPSec 接続に対してアンチリプレイ チェックをディセーブルにし、172.150.150.3 および 172.150.150.4 との IPSec 接続に対してイネーブル（デフォルト ウィンドウ サイズは 64）にする例を示します。

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPN.tErFZ1
enable password ww
!
ip subnet-zero
cns event-service server
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco170
address 172.150.150.2
crypto isakmp key cisco180
address 172.150.150.3
crypto isakmp key cisco190
address 172.150.150.4
crypto ipsec transform-set 170cisco esp-des esp-md5-hmac
crypto ipsec transform-set 180cisco esp-des esp-md5-hmac
crypto ipsec transform-set 190cisco esp-des esp-md5-hmac
crypto map ETH0 17 ipsec-isakmp
set peer 172.150.150.2
set security-association replay disable
set transform-set 170cisco
match address 170
crypto map ETH0 18 ipsec-isakmp
set peer 150.150.150.3
set transform-set 180cisco
match address 180
crypto map ETH0 19 ipsec-isakmp
set peer 150.150.150.4
set transform-set 190cisco
match address 190
!
interface Ethernet0
ip address 172.150.150.1 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map ETH0
!
interface Serial0
ip address 172.160.160.1 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
ip classless
ip route 172.170.170.0 255.255.255.0 172.150.150.2
ip route 172.180.180.0 255.255.255.0 172.150.150.3
ip route 172.190.190.0 255.255.255.0 172.150.150.4
no ip http server
!
access-list 170 permit ip 172.160.160.0 0.0.0.255 172.170.170.0 0.0.0.255
access-list 180 permit ip 172.160.160.0 0.0.0.255 172.180.180.0 0.0.0.255
access-list 190 permit ip 172.160.160.0 0.0.0.255 172.190.190.0 0.0.0.255
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
```

```
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
end
```

IPSec 優先ピアの設定例

次に、IPSec 優先ピアの設定例を示します。

- デフォルト ピアの設定（p.26-29）
- デフォルト ピアを使用する場合の IPSec アイドル タイマーの設定例（p.26-29）

デフォルト ピアの設定

次に、デフォルト ピアの設定例を示します。この例では、IP アドレス 1.1.1.1 にある最初のピアがデフォルト ピアです。

```
Router(config)# crypto map tohub 1 ipsec-isakmp
Router(config-crypto-map)# set peer 1.1.1.1 default
Router(config-crypto-map)# set peer 2.2.2.2
Router(config-crypto-map)# exit
```

デフォルト ピアを使用する場合の IPSec アイドル タイマーの設定例

次に、デフォルト ピアを使用する場合の IPSec アイドル タイマーの設定例を示します。次の例では、現在のピアが 600 秒間アイドルであった場合、次の接続試行ではデフォルト ピア 1.1.1.1（**set peer** コマンドで指定）が使用されます。

```
Router (config)# crypto map tohub 1 ipsec-isakmp
Router(config-crypto-map)# set peer 1.1.1.1 default
Router(config-crypto-map)# set peer 2.2.2.2
Router(config-crypto-map)# set security-association idle-time 600 default
Router(config-crypto-map)# exit
```

IPSec SA アイドル タイマーの設定例

ここでは、IPSec SA アイドル タイマーを設定する例を示します。

- IPSec SA アイドル タイマーのグローバルな設定例（p.26-29）
- IPSec SA アイドル タイマーの暗号マップ単位での設定例（p.26-30）

IPSec SA アイドル タイマーのグローバルな設定例

次に、非アクティブなピアについて 600 秒後に SA をドロップするように、グローバルに IPSec SA アイドル タイマーを設定する例を示します。

```
Router(config)# crypto ipsec security-association idle-time 600
```

IPSec SA アイドル タイマーの暗号マップ単位での設定例

次に、暗号マップ「test」について、非アクティブなピアの SA を 600 秒後にドロップするように IPSec SA アイドル タイマーを設定する例を示します。

```
Router(config) # crypto map test 1 ipsec-isakmp
Router(config-crypto-map)# set security-association idle-time 600
```

Distinguished Name（DN; 識別名）ベースの暗号マップの設定例

次に、DN およびホスト名によって認証された DN ベースの暗号マップの設定例を示します。例には、さまざまなコマンドについての注釈も含まれています。

```
! DN based crypto maps require you to configure an IKE policy at each peer.
crypto isakmp policy 15
encryption 3des
hash md5
authentication rsa-sig
group 2
lifetime 5000
crypto isakmp policy 20
authentication pre-share
lifetime 10000
crypto isakmp key 1234567890 address 171.69.224.33
!
!The following is an IPSec crypto map (part of IPSec configuration). It can be used
only
! by peers that have been authenticated by DN and if the certificate belongs to
BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
set peer 172.21.114.196
set transform-set my-transformset
match address 124
identity to-bigbiz
!
crypto identity to-bigbiz
dn ou=BigBiz
!
!
! This crypto map can be used only by peers that have been authenticated by hostname
!and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
set peer 172.21.115.119
set transform-set my-transformset
match address 125
identity to-little-com
!
crypto identity to-little-com
fqdn little.com
!
```

ACL の拒否ポリシー拡張機能の設定例

次に、crypto ipsec ipv4 deny-policy の **clear** オプションを使用した設定例を示します。この例では、拒否アドレスにヒットすると検索が停止し、トラフィックは平文の（暗号化されていない）状態で通過させることができます。

```
Router(config)# crypto ipsec ipv4 deny-policy clear
```