



IPSec ネットワーク セキュリティの設定

IP Security (IPSec) プロトコルは、加入ピア間にデータ機密保持、データの整合性、およびデータ認証を提供するオープン規格のフレームワークです。IPSec は、Internet Engineering Task Force (IETF) により開発されました。IPSec は、ホストペア間、セキュリティゲートウェイペア間、またはセキュリティゲートウェイとホスト間の 1 つまたは複数のデータフローの保護など、IP レイヤにセキュリティサービスを提供します。IPSec 実装全体は、RFC 2401 の最新バージョンに準じています。Cisco NX-OS の IPSec は、RFC 2402 ~ RFC 2410 を実装しています。

IPSec はインターネットキー交換 (IKE) プロトコルを使用して、プロトコルおよびアルゴリズムのネゴシエーションを処理し、IPSec で使用される暗号キーおよび認証キーを生成します。IKE は他のプロトコルとともに使用できますが、その初期実装時は IPSec プロトコルで使用します。IKE は、IPSec ピアを認証し、IPSec セキュリティアソシエーションをネゴシエーションし、IPSec キーを確立します。IKE は RFC 2408、2409、2410、2412 を使用し、さらに draft-ietf-ipsec-ikev2-16.txt ドラフトを実装しています。



(注)

IPSec という用語は、IPSec データサービスのプロトコル全体および IKE セキュリティプロトコルを示す場合や、データサービスだけを示す場合に使用されることがあります。

この章は、次の項で構成されています。

- [IPSec の概要 \(7-2 ページ\)](#)
- [IKE の概要 \(7-4 ページ\)](#)
- [IPSec の前提条件 \(7-4 ページ\)](#)
- [IPSec の使用方法 \(7-4 ページ\)](#)
- [IPSec デジタル証明書のサポート \(7-8 ページ\)](#)
- [IPsec および IKE の手動設定 \(7-11 ページ\)](#)
- [オプションの IKE パラメータの設定 \(7-15 ページ\)](#)
- [クリプト IPv4-ACL \(7-18 ページ\)](#)
- [IPsec のメンテナンス \(7-30 ページ\)](#)
- [グローバル ライフタイム値 \(7-30 ページ\)](#)
- [IKE 設定の表示 \(7-32 ページ\)](#)
- [IPsec 設定の表示 \(7-32 ページ\)](#)
- [FCIP の設定例 \(7-36 ページ\)](#)
- [iSCSI の設定例 \(7-41 ページ\)](#)
- [デフォルト設定 \(7-42 ページ\)](#)

IPsec の概要

IP Security (IPsec) プロトコルは、加入ピア間にデータ機密保持、データの整合性、およびデータ認証を提供するオープン規格のフレームワークです。IPsec は、Internet Engineering Task Force (IETF) により開発されました。IPsec は、ホストペア間、セキュリティゲートウェイペア間、またはセキュリティゲートウェイとホスト間の1つまたは複数のデータフローの保護など、IP レイヤにセキュリティサービスを提供します。IPsec 実装全体は、RFC 2401 の最新バージョンに準じています。Cisco NX-OS の IPsec は、RFC 2402 ~ RFC 2410 を実装しています。

IPsec はインターネット キー交換 (IKE) プロトコルを使用して、プロトコルおよびアルゴリズムのネゴシエーションを処理し、IPsec で使用される暗号キーおよび認証キーを生成します。IKE は他のプロトコルとともに使用できますが、その初期実装時は IPsec プロトコルで使用します。IKE は、IPsec ピアを認証し、IPsec セキュリティアソシエーションをネゴシエーションし、IPsec キーを確立します。IKE は RFC 2408、2409、2410、2412 を使用し、さらに draft-ietf-ipsec-ikev2-16.txt ドラフトを実装しています。

IPsec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。IPsec はネットワーク層で機能し、参加する IPsec デバイス (ピア) 間の IP パケットを保護し、認証します。



(注) HP c-Class BladeSystem 対応 Cisco Fabric Switch および IBM BladeCenter 対応 Cisco Fabric Switch は、IPsec をサポートしていません。

IPsec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。IPsec はネットワーク層で機能し、参加する IPsec デバイス (ピア) 間の IP パケットを保護し、認証します。

IPsec は、次のネットワークセキュリティサービスを提供します。一般に、関与する2つの IPsec デバイス間でどのサービスが使用されるかは、ローカルセキュリティポリシーによって決まります。

- データ機密性: ネットワークにパケットを伝送する前に IPsec 送信側がパケットを暗号化できます。
- データ整合性: IPsec 受信者は、IPsec 送信者から送信されたパケットを認証し、伝送中にデータが変更されていないかを確認できます。
- データ送信元認証: IPsec 受信者は、送信された IPsec パケットの送信元を認証できます。このサービスは、データ整合性サービスに依存します。
- リプレイ防止: IPsec 受信側でリプレイ パケットを検出し、拒否できます。



(注) データ認証は、通常、データ整合性およびデータ発信元認証を意味します。この章では、特に明記されていないかぎり、データ認証にはリプレイ防止サービスも含まれます。

IPsec を使用すれば、データを、観察、変更、またはスプーフィングされることを心配することなく、パブリック ネットワークを介して転送できます。これにより、インターネット、エクストラ ネット、およびリモート ユーザ アクセスを含む、バーチャルプライベート ネットワーク (VPN) などのアプリケーションが可能となります。

Cisco NX-OS ソフトウェアに実装された IPsec は、カプセル化セキュリティ ペイロード (ESP) プロトコルをサポートしています。このプロトコルはデータをカプセル化して保護し、データ プライバシー サービス、オプションのデータ認証、およびオプションのリプレイ防止サービスを提供します。



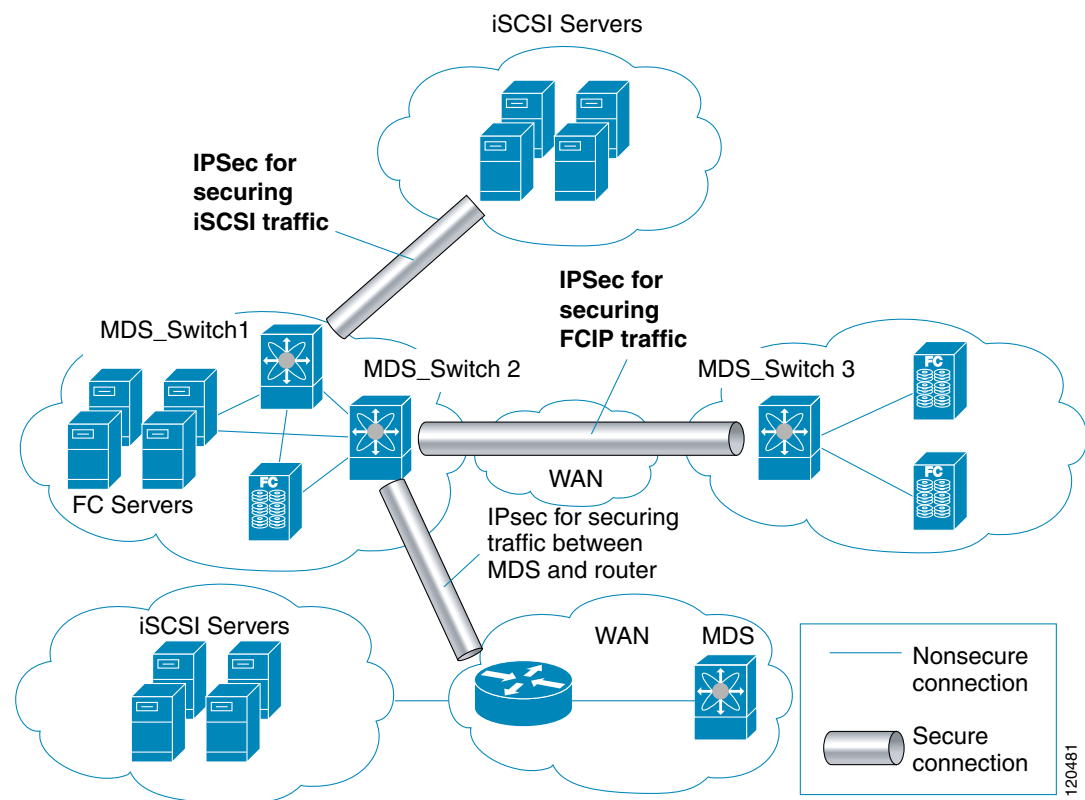
(注) カプセル化セキュリティ ペイロード (ESP) プロトコルは、既存の TCP/IP パケットに挿入されたヘッダーで、サイズは実際の暗号化およびネゴシエートされた認証アルゴリズムによって異なります。フラグメンテーションを防止するために、暗号化パケットは、インターフェイスの最大伝送単位 (MTU) と一致します。TCP のパス MTU の暗号化計算には、ESP ヘッダーの追加分、およびトンネルモードの外部 IP ヘッダーが考慮されます。MDS スイッチは、IPsec 暗号化によるパケット増加を 100 バイトまで許容します。



(注) IPsec および IKE を使用するとき、IPS モジュール (14+2 LC または 18+4 LC) 上の各ギガビットイーサネット インターフェイスは、独自の IP サブネット内で設定する必要があります。同じ IP サブネットの IP アドレスまたはネットワークマスクで複数のギガビットイーサネット インターフェイスが設定される場合、IKE パケットは正しいピアに送信されず、IPsec トンネルは起動しません。

図 7-1 に、各種 IPsec のシナリオを示します。

図 7-1 MPS-14/2 モジュールを使用する FCIP および iSCSI のシナリオ



IKE の概要

IKE は、IPsec セキュリティ アソシエーション (SA) を自動的にネゴシエートし、IPsec 機能を使用してすべてのスイッチのキーを生成します。IKE の具体的な利点は次のとおりです。

- IPsec SA をリフレッシュできます。
- IPsec でアンチ リプレイ サービスが使用可能です。
- 管理可能でスケーラブルな IPsec 設定をサポートします。
- ピアのダイナミック認証が可能です。



(注) HP c-Class BladeSystem 対応 Cisco Fabric Switch および IBM BladeSystem 対応 Cisco Fabric Switch は、IKE をサポートしていません。

IPsec の前提条件

IPsec 機能を使用するには、次の作業を実行する必要があります。

- ENTERPRISE_PKG ライセンスを取得します (『Cisco MDS 9000 Family NX-OS Licensing Guide』を参照)。
- IKE を設定します。「IKE 初期設定の概要」セクション (7-11 ページ) を参照してください。

IPsec の使用方法

IPsec 機能を使用する手順は、次のとおりです。

- ステップ 1 ENTERPRISE_PKG ライセンスを取得して、IPsec for Small Computer Systems Interface over IP (iSCSI) および IPsec for Fibre Channel over IP (FCIP) をイネーブルにします。詳細については、『Cisco MDS 9000 Family NX-OS Licensing Guide』を参照してください。
- ステップ 2 IKE を設定します。「IPsec および IKE の手動設定」セクション (7-11 ページ) を参照してください。



(注) IPsec 機能は、既存のパケットに新しいヘッダーを挿入します (詳細については、『Cisco MDS 9000 Family NX-OS IP Services Configuration Guide』を参照してください)。

ここでは、次の内容について説明します。

- IPsec の互換性 (7-5 ページ)
- IPsec および IKE に関する用語 (7-5 ページ)
- サポート対象の IPsec トランスフォームおよびアルゴリズム (7-7 ページ)
- サポート対象の IKE トランスフォームおよびアルゴリズム (7-7 ページ)

IPsec の互換性

IPsec 機能は、次の Cisco MDS 9000 ファミリー ハードウェアと互換性があります。

- Cisco 18/4 ポート マルチサービス モジュール (MSM-18/4) および MDS 9222i Module-1 モジュール。
- Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタに搭載された Cisco 14/2 ポート Multiprotocol Services (MPS-14/2) モジュール。
- 統合スーパーバイザ モジュールに 14/2 ポート マルチプロトコル機能を備えた Cisco MDS 9216i スイッチ。Cisco MDS 9216i スイッチの詳細については、『Cisco MDS 9200 Series Hardware Installation Guide』を参照してください。
- IPsec 機能は、管理インターフェイス上ではサポートされません。

IPsec 機能は、次のファブリック設定と互換性があります。

- Cisco MDS SAN-OS Release 2.0(1b) 以降または Cisco NX-OS 4.1(1) を実装している、2 台の接続された Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタ。
- Cisco MDS SAN-OS Release 2.0(1b) 以降または Cisco NX-OS 4.1(1) を実装し、任意の IPsec 互換デバイスに接続された Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタ。
- Cisco NX-OS 上に実装された IPsec 機能では、次の機能はサポートされません。
 - 認証ヘッダー (AH)
 - トランスポート モード
 - SA のバンドル
 - SA の手動設定
 - クリプト マップにおけるホスト単位の SA オプション
 - SA アイドル タイムアウト
 - ダイナミック クリプト マップ



(注) このマニュアルでは、クリプト マップという用語は、スタティック クリプト マップだけを意味します。

IPsec および IKE に関する用語

ここでは、この章で使用する用語について説明します。

- セキュリティ アソシエーション (SA) : IP パケットの暗号化および暗号解除に必要なエンタリに関する、2 つの参加ピア間の合意。ピア間に双方向通信を確立するには、ピアごとに各方向 (着信および発信) に対応する 2 つの SA が必要です。双方向の SA レコードのセットは、SA データベース (SAD) に保管されます。IPsec は IKE を使用して SA をネゴシエートし、起動します。各 SA レコードには、次の情報が含まれます。
 - セキュリティ パラメータ インデックス (SPI) : 宛先 IP アドレスおよびセキュリティ プロトコルと組み合わせて、特定の SA を一意に識別する番号。IKE を使用して SA を確立する場合、各 SA の SPI は疑似乱数によって生成された番号です。
 - ピア : IPsec に参加するスイッチなどのデバイス。IPsec をサポートする Cisco MDS スイッチまたはその他のシスコ製ルータなどがあります。

- トランスフォーム: データ認証およびデータ機密保持を提供するために実行される処理のリスト。Hash Message Authentication Code (HMAC)-MD5 認証アルゴリズムを使用する ESP プロトコルなどがあります。
- セッション キー: セキュリティ サービスを提供するためにトランスフォームによって使用されるキー。
- ライフタイム: SA を作成した時点から、ライフタイム カウンタ (秒およびバイト単位) がカウントされます。制限時間が経過すると、SA は動作不能になり、必要に応じて、自動的に再ネゴシエート (キーが再設定) されます。
- 動作モード: IPsec では通常、2 つの動作モード (トンネル モードおよびトランスペアレント モード) を使用できます。Cisco NX-OS に実装された IPsec は、トンネル モードだけをサポートします。IPsec トンネル モードは、ヘッダーを含めた IP パケットを暗号化して、認証します。ゲートウェイは、ホストおよびサブネットの代わりにトラフィックを暗号化します。
Cisco NX-OS に実装された IPsec では、トランスペアレント モードはサポートされません。



(注) トンネル モードという用語は、FCIP リンクで接続された 2 台のスイッチなど、2 つのピア間のセキュアな通信パスを示すためのトンネルとは異なります。

- リプレイ防止: 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。IPsec は、データ認証とシーケンス番号を組み合わせて使用することにより、このオプション サービスを提供します。
- データ認証: データ認証は整合性だけ、または整合性と認証の両方を意味することがあります (データ発信元認証はデータ整合性に依存します)。
 - データ整合性: データが変更されていないことを確認します。
 - データ発信元認証: 要求を受けた送信側からデータが実際に送信されたことを確認します。
- データ機密保護: 保護されたデータを傍受できないようにするセキュリティ サービス。
- データ フロー: 送信元アドレス/マスクまたはプレフィックス、宛先アドレス/マスクまたはプレフィックス長、IP ネクスト プロトコル フィールド、および送信元/宛先ポートの組み合わせで識別されるトラフィック グループ (プロトコルおよびポート フィールドにいずれかの値を設定できます)。これらの値の特定の組み合わせと一致するトラフィックは、1 つのデータ フローに論理的にグループ化されます。データ フローは、2 台のホスト間の単一の TCP 接続、あるいは 2 つのサブネット間のトラフィックを示します。IPsec 保護はデータ フローに適用されます。
- Perfect Forward Secrecy (PFS): 取得された共有シークレット値に対応する暗号特性。PFS を使用すると、1 つのキーが損なわれても、これ以降のキーは前のキーの取得元から取得されないため、前および以降のキーには影響しません。
- Security Policy Database (SPD): トラフィックに適用される順序付きポリシー リスト。ポリシーにより、パケットに IPsec 処理が必要かどうか、クリア テキストでの送信を許可するかどうか、または廃棄するかどうかを判別されます。
 - IPsec SPD は、クリプト マップのユーザ設定から取得されます。
 - IKE SPD はユーザが設定します。

サポート対象の IPsec トランスフォームおよびアルゴリズム

IPsec に実装されたコンポーネント テクノロジーには、次のトランスフォームが含まれます。

- **Advanced Encrypted Standard (AES)**: 暗号化アルゴリズム。AES は Cipher Block Chaining (CBC) またはカウンタ モードを使用して、128 ビットまたは 256 ビットを実装します。
- **データ暗号規格 (DES)**: パケットデータを暗号化するために使用され、必須の 56 ビット DES-CBC を実装します。CBC には、暗号化を開始するための初期ベクトル (IV) が必要です。IV は IPsec パケットに明示的に指定されます。
- **Triple DES (3DES)**: 信頼できないネットワーク上で重要な情報を送信できるようにする、168 ビット暗号キーを使用した強力な DES 形式です。



(注) 強力な暗号化を使用する Cisco NX-OS イメージは、米国政府の輸出規制の対象で、配信が制限されています。米国以外の国でインストールされるイメージには、輸出許可が必要です。米国政府の規制により、お客様の注文が拒否されたり、納入が遅れたりすることがあります。詳細については、営業担当者または販売業者、あるいは export@cisco.com までお問い合わせください。

- **Message Digest 5 (MD5)**: HMAC バリエーションを使用するハッシュ アルゴリズム。HMAC はデータの認証に使用されるキー付きハッシュ バリエーションです。
- **Secure Hash Algorithm (SHA-1, SHA-2)** はハッシュ メッセージ認証コード (HMAC) バリエーションを使用するハッシュ アルゴリズムです。Cisco MDS NX-OS リリース 7.3(0)D1(1) 以降の Cisco MDS 9250i マルチサービス ファブリック スイッチで、IPsec は SHA-2 をサポートします。
- **AES-XCBC-MAC**: AES アルゴリズムを使用する Message Authentication Code (MAC)。

サポート対象の IKE トランスフォームおよびアルゴリズム

IKE に実装されたコンポーネント テクノロジーには、次のトランスフォームが含まれます。

- **Diffie-Hellman (DH)**: 保護されていない通信チャネルを介して 2 つのパーティが共有シークレットを確立できるようにする、公開キー暗号化プロトコル。Diffie-Hellman は、IKE 内でセッション キーを確立するために使用されます。グループ 1 (768 ビット)、グループ 2 (1024 ビット)、およびグループ 5 (1536 ビット) がサポートされます。
- **Advanced Encrypted Standard (AES)**: 暗号化アルゴリズム。AES は、CBC を使用する 128 ビット、またはカウンタ モードを実装します。
- **データ暗号規格 (DES)**: パケットデータを暗号化するために使用され、必須の 56 ビット DES-CBC を実装します。CBC には、暗号化を開始するための初期ベクトル (IV) が必要です。IV は IPsec パケットに明示的に指定されます。
- **Triple DES (3DES)**: 信頼できないネットワーク上で重要な情報を送信できるようにする、168 ビット暗号キーを使用した強力な DES 形式です。



(注) 強力な暗号化を使用する Cisco NX-OS イメージは、米国政府の輸出規制の対象で、配信が制限されています。米国以外の国でインストールされるイメージには、輸出許可が必要です。米国政府の規制により、お客様の注文が拒否されたり、納入が遅れたりすることがあります。詳細については、営業担当者または販売業者、あるいは export@cisco.com までお問い合わせください。

- Message Digest 5 (MD5) : HMAC バリエーションを使用するハッシュ アルゴリズム。HMAC はデータの認証に使用されるキー付きハッシュ バリエーションです。
- Secure Hash Algorithm (SHA-1, SHA-2) はハッシュ メッセージ認証コード (HMAC) バリエーションを使用するハッシュ アルゴリズムです。IKEv2 は Cisco MDS NX-OS リリース 7.3(0)D1(1)以降、Cisco MDS 9250i マルチサービス ファブリック スイッチで SHA-2 をサポートします。



(注) IKEv1 は SHA-2 をサポートしません。

- スイッチの認証アルゴリズム: IP アドレスに基づく事前共有キーを使用します。

IPsec デジタル証明書のサポート

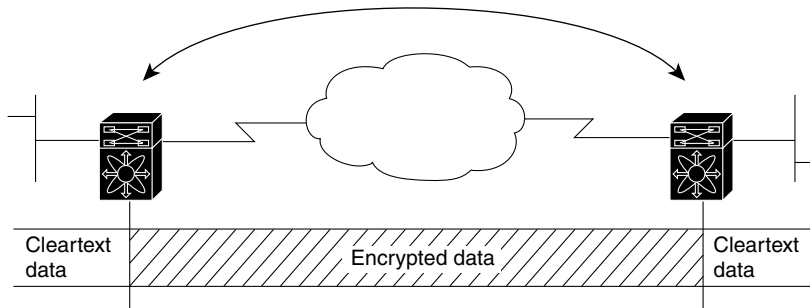
ここでは、認証局 (CA) およびデジタル証明書を使用した認証の利点について説明します。

CA およびデジタル証明書を使用しない IPsec の実装

CA およびデジタル証明書を使用しない場合、2 台の Cisco MDS スイッチ間で IPsec サービス (暗号化など) をイネーブルにするには、各スイッチに他方のスイッチのキー (RSA 公開キーまたは共有キーなど) が必要になります。IPsec サービスを使用するファブリック内の各スイッチに、RSA 公開キーまたは事前共有キーのどちらかを手動で指定する必要があります。また、ファブリックに新しいデバイスを追加する場合、安全な通信をサポートするには、ファブリック内の他方のスイッチを手動で設定する必要があります。各 (図 7-2 を参照) スイッチは他方のスイッチのキーを使用して、他方のスイッチのアイデンティティを認証します。この認証は、2 台のスイッチ間で IPsec トラフィックが交換される場合に、必ず実行されます。

複数の Cisco MDS スイッチをメッシュ トポロジで配置し、すべてのスイッチ間で IPsec トラフィックを交換させる場合には、最初に、すべてのスイッチ間に共有キーまたは RSA 公開キーを設定する必要があります。

図 7-2 CA およびデジタル証明書を使用しない 2 台の IPsec スイッチ

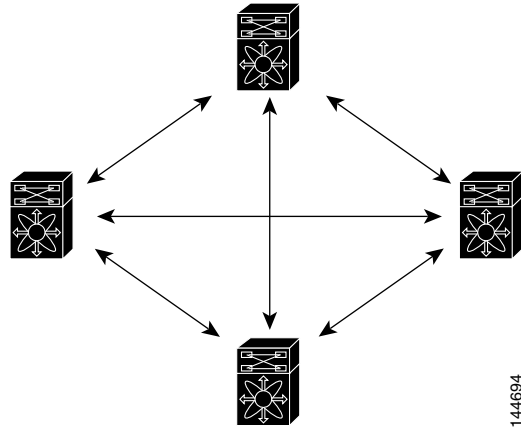


144693

IPsec ネットワークに新しいスイッチを追加するごとに、新しいスイッチと既存の各スイッチ間にキーを設定する必要があります (図 7-3 の場合、このネットワークに 1 台の暗号化スイッチを追加するには、新たに 4 つのスイッチ間キーの設定が必要になります)。

したがって、IPsec サービスを必要とするデバイスが増えるほど、キー管理は複雑になります。このアプローチでは、より大型で複雑な暗号化ネットワークには拡張できません。

図 7-3 CA およびデジタル証明書を使用しない 4 台の IPsec スイッチ

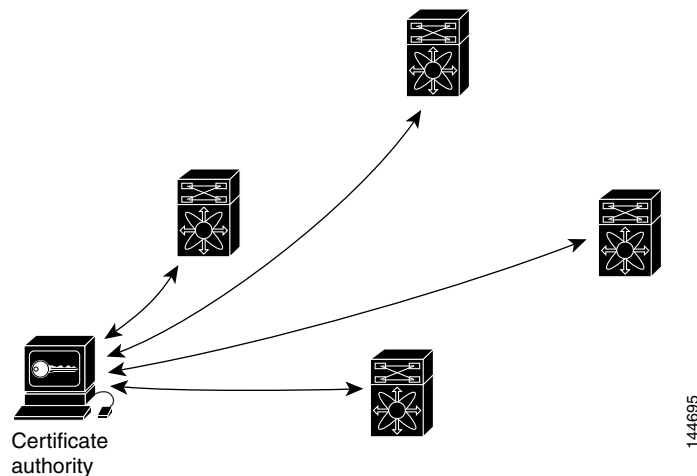


CA およびデジタル証明書を使用した IPsec の実装

CA およびデジタル証明書を使用する場合には、すべての暗号化スイッチ間にキーを設定する必要はありません。代わりに、加入させる各スイッチを CA に個別に登録し、各スイッチの証明書を要求します。この設定が完了していれば、各加入スイッチは、他のすべての加入スイッチを動的に認証できます。2 台のデバイスが通信する場合、証明書を交換し、データをデジタル署名して、お互いを認証します。ネットワークに新しいデバイスを追加する場合には、そのデバイスを CA に登録するだけでよく、他のデバイスの設定を変更する必要はありません。新しいデバイスが IPsec 接続を試みると、証明書が自動的に交換され、そのデバイスが認証されます。

図 7-4 に、デバイスを動的に認証するプロセスを示します。

図 7-4 CA によるデバイスの動的な認証



ネットワークに新しい IPsec スイッチを追加する場合、新しいスイッチが CA に証明書を要求するように設定するだけでよく、既存の他のすべての IPsec スイッチとの間に複数のキー設定を行う必要はありません。

IPsec デバイスによる CA 証明書の使用方法

2 台の IPsec スイッチが IPsec で保護されたトラフィックを交換するには、最初に相互に認証しあう必要があります。認証されていない場合、IPsec 保護が適用されません。この認証を行うには、IKE を使用します。

IKE では、2 つの方法を使用してスイッチを認証できます。CA を使用しない場合には事前共有キーを使用し、CA を使用する場合には RSA キー ペアを使用します。どちらの方法も、2 台のスイッチ間にキーが事前設定されている必要があります。

CA を使用しない場合、スイッチは RSA 暗号化事前共有キーを使用して、リモートスイッチに対して自身を認証します。

CA を使用する場合、スイッチはリモートスイッチに証明書を送信し、何らかの公開キー暗号法を実行することによって、リモートスイッチに対して自身を認証します。各スイッチは、CA により発行されて検証された、スイッチ固有の証明書を送信する必要があります。このプロセスが有効なのは、各スイッチの証明書にスイッチの公開キーがカプセル化され、各証明書が CA によって認証されることにより、すべての加入スイッチが CA を認証局として認識するからです。この機構は、RSA シグニチャを使用する IKE と呼ばれます。

スイッチは、証明書が期限切れになるまで、複数の IPsec ピアに対して、複数の IPsec セッション用に自身の証明書を継続的に送信できます。証明書が期限切れになった場合、スイッチ管理者は CA から新しい証明書を取得する必要があります。

また、CA は、IPsec に参加しなくなったデバイスの証明書を失効できます。失効された証明書は、他の IPsec デバイスから有効とは見なされません。失効された証明書は、証明書失効リスト (CRL) にリストされ、各ピアは相手側ピアの証明書を受け入れる前に、このリストを確認できます。

IKE の証明書サポートでは、次の考慮事項に留意してください。

- IKE 用の証明書をインストールする前に、スイッチの FQDN (ホスト名およびドメイン名) が設定されている必要があります。
- IKE が使用するのは、IKE 用または汎用として設定された証明書だけです。
- スイッチに設定された最初の IKE 用または汎用証明書が、IKE のデフォルトの証明書として使用されます。
- ピアが別の証明書を指定しないかぎり、すべての IKE ピアに対してデフォルトの証明書が使用されます。
- ピアが、そのピアが信頼する CA によって署名された証明書を要求した場合、IKE は、要求された証明書がスイッチに存在すれば、デフォルトの証明書でなくても、その証明書を使用します。
- デフォルトの証明書が削除された場合、次の IKE 用または汎用証明書が存在すれば、IKE はそれをデフォルトの証明書として使用します。
- IKE では、証明書チェーンはサポートされません。
- IKE は、CA チェーン全体ではなく、アイデンティティ証明書だけを送信します。ピア上で証明書が確認されるには、ピア上に同じ CA チェーンが存在する必要があります。

IPsec および IKE の手動設定

ここでは、IPsec および IKE を手動で設定する方法について説明します。

IPsec は、加入ピア間に安全なデータ フローを提供します。2 つのピア間では、異なる SA セットを使用する各トンネルで異なるデータ フローを保護することにより、複数の IPsec データ フローをサポートできます。

IKE 設定の完了後、IPsec を設定します。

各加入 IPsec ピアに IPsec を設定する手順は、次のとおりです。

-
- ステップ 1 トラフィック用の安全なトンネルを確立する必要があるピアを識別します。
 - ステップ 2 必要なプロトコルとアルゴリズムにより、トランスフォーム セットを設定します。
 - ステップ 3 クリプト マップを作成し、適切なアクセス コントロール リスト (IPv4-ACL)、トランスフォーム セット、ピア、およびライフタイム値を適用します。
 - ステップ 4 クリプト マップを、必要なインターフェイスに適用します。
-

ここでは、次の内容について説明します。

- [IKE 初期設定の概要 \(7-11 ページ\)](#)
- [IKE ドメインの概要 \(7-12 ページ\)](#)
- [IKE ドメインの設定 \(7-12 ページ\)](#)
- [IKE トンネルの概要 \(7-12 ページ\)](#)
- [IKE ポリシー ネゴシエーションの概要 \(7-12 ページ\)](#)
- [IKE ポリシーの設定 \(7-14 ページ\)](#)

IKE 初期設定の概要

IPsec 機能により必要なピアでデータ フローを確立するには、IKE 機能をイネーブルにして、設定しておく必要があります。Fabric Manager では、IKE の最初の設定時に、IKE が初期設定されます。

IPsec がイネーブルの場合には、IKE をディセーブルにできません。IKE 機能をディセーブルにすると、IKE 設定が実行コンフィギュレーションから消去されます。

IKE のイネーブル化

IKE をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# feature crypto ike	IKE 機能をイネーブルにします。
	switch(config)# no feature crypto ike	IKE 機能をディセーブル(デフォルト)にします。 (注) IKE 機能をディセーブルにする前に、IPsec をディセーブルにする必要があります。

IKE ドメインの概要

ローカル スイッチのスーパーバイザ モジュールにトラフィックを到達させるには、IPsec ドメインに IKE 設定を適用する必要があります。Fabric Manager では、IKE の設定時に IPsec ドメインが自動的に設定されます。

IKE ドメインの設定

ローカル スイッチのスーパーバイザ モジュールにトラフィックを到達させるには、IPsec ドメインに IKE 設定を適用する必要があります。

IPsec ドメインを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# crypto ike domain ipsec switch(config-ike-ipsec)#	IPsec ドメインに対する IKE の設定を許可します。

IKE トンネルの概要

IKE トンネルは、2つのエンドポイント間の安全な IKE セッションです。IKE は、IPsec SA ネゴシエーションで使用される IKE メッセージを保護するために、このトンネルを作成します。

Cisco NX-OS の実装では、2つのバージョンの IKE が使用されています。

- IKE バージョン 1 (IKEv1) は、RFC 2407、2408、2409、および 2412 を使用して実装されます。
- IKE バージョン 2 (IKEv2) は、より効率的な簡易バージョンで、IKEv1 とは相互運用できません。IKEv2 は、draft-ietf-ipsec-ikev2-16.txt ドラフトを使用して実装されます。

IKE ポリシー ネゴシエーションの概要

IKE ネゴシエーションを保護するには、各 IKE ネゴシエーションを共通(共有)IKE ポリシーで開始します。IKE ポリシーを使い、IKE ネゴシエーション中に使用するセキュリティ パラメータの組み合わせを定義します。デフォルトでは、IKE ポリシーは設定されません。各ピアに IKE ポリシーを作成する必要があります。このポリシーにより、以降の IKE ネゴシエーションを保護するために使用するセキュリティ パラメータを指定し、ピアの認証方法を指示します。最低 1 つのポリシーがリモートピアのポリシーと一致するように、各ピアに優先順位を付けた複数のポリシーを設定できます。

ポリシーは、暗号化アルゴリズム (DES、3DES、AES)、ハッシュ アルゴリズム (SHA、MD5)、および DH グループ (1、2、5) に基づいて設定できます。各ポリシーに、パラメータ値の異なる組み合わせを設定できます。設定したポリシーには、固有のプライオリティ番号を指定します。この番号の範囲は、1 (最上位のプライオリティ) ~ 255 (最下位のプライオリティ) です。スイッチに、複数のポリシーを設定できます。リモートピアに接続する必要がある場合、ローカルスイッチの少なくとも 1 つのポリシーが、リモートピアに設定されているパラメータ値と一致する必要があります。同じパラメータ設定のポリシーが複数ある場合には、最も小さい番号のポリシーが選択されます。

表 7-1 に、許可されるトランスフォームの組み合わせのリストを示します。

表 7-1 IKE トランスフォーム設定パラメータ

パラメータ	許容値	キーワード	デフォルト値
暗号化アルゴリズム	56 ビット DES-CBC	des	3des
	168 ビット DES	3des	
	128 ビット AES	aes	
ハッシュ アルゴリズム	SHA-1 (HMAC バリエーション)、SHA-2 (HMAC バリエーション) MD5 (HMAC バリエーション)	sha	sha
		sha256	
		sha512	
認証方式	事前共有キー	設定なし	事前共有キー
DH グループ識別名	768 ビット DH	1	1
	1024 ビット DH	2	
	1536 ビット DH	5	

次の表に、Microsoft Windows および Linux プラットフォームでサポートおよび検証されている、IPsec および IKE 暗号化認証アルゴリズムの設定を示します。

プラットフォーム	IKE	IPsec
Microsoft iSCSI 発信側 (Microsoft Windows 2000 プラットフォームの Microsoft IPsec 実装)	3DES、SHA-1、SHA-2、または MD5、DH グループ 2	3DES、SHA-1、SHA-2
Cisco iSCSI イニシエータ、Linux プラットフォームへの Free Swan IPsec の実装	3DES、MD5、DH グループ 1	3DES、MD5



(注)

ハッシュ アルゴリズムを設定すると、対応する HMAC バージョンが認証アルゴリズムとして使用されます。

IKE ネゴシエーションが開始されると、IKE は、両ピア上で同一の IKE ポリシーを検索します。ネゴシエーションを開始したピアがすべてのポリシーをリモートピアに送信し、リモートピアの方では一致するポリシーを探そうとします。リモートピアは、相手側ピアから受信したすべてのポリシーと自身の最優先ポリシーを比較することにより、一致しているポリシーを検索します。一致するポリシーが見つかるまで、リモートピアは優先順位が高い順に各ポリシーをチェックします。

2つのピアの暗号化、ハッシュアルゴリズム、認証アルゴリズム、および DH グループ値が同じであれば、一致していると判断されます。一致しているポリシーが見つかったら、IKE はセキュリティ ネゴシエーションを完了し、IPsec SA が作成されます。

一致しているポリシーが見つからない場合、IKE はネゴシエーションを拒否し、IPsec データフローは確立されません。

IKE ポリシーの設定

IKE ポリシー ネゴシエーション パラメータを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# crypto ike domain ipsec switch(config-ike-ipsec)#	IPsec ドメインをこのスイッチで設定できます。
ステップ 3	switch(config-ike-ipsec)# identity address	IKE プロトコルが IP アドレスを使用するようにアイデンティティ モードを設定します(デフォルト)。
	switch(config-ike-ipsec)# identity hostname	IKE プロトコルが完全修飾ドメイン名 (FQDN) を使用するようにアイデンティティ モードを設定します。 (注) FQDN は認証に RSA シグニチャを使用する必要があります。
ステップ 4	switch(config-ike-ipsec)# no identity	デフォルトのアイデンティティ モード (address) に戻ります。
	switch(config-ike-ipsec)# key switch1 address 10.10.1.1	ピアの IP アドレスに事前共有キーを関連付けます。
	switch(config-ike-ipsec)# no key switch1 address 10.10.1.1	事前共有キーとピアの IP アドレスの関連付けを削除します。
	switch(config-ike-ipsec)# key switch1 hostname switch1.cisco.com	ピアの FQDN と事前共有キーを関連付けます。 (注) FQDN を使用するには、ピアのスイッチ名とドメイン名を設定する必要があります。
ステップ 5	switch(config-ike-ipsec)# no key switch1 hostname switch1.cisco.com	事前共有キーとピアの IP アドレスの関連付けを削除します。
	switch(config-ike-ipsec)# policy 1 switch(config-ike-ipsec-policy)#	設定するポリシーを指定します。
ステップ 6	switch(config-ike-ipsec)# no policy 1	指定されたポリシーを削除します。
	switch(config-ike-ipsec-policy)# encryption des	暗号化ポリシーを設定します。
ステップ 7	switch(config-ike-ipsec-policy)# no encryption des	デフォルトは 3DES 暗号化です。
	switch(config-ike-ipsec-policy)# group 5	DH グループを設定します。
ステップ 8	switch(config-ike-ipsec-policy)# no group 5	デフォルトは DH グループ 1 です。
	switch(config-ike-ipsec-policy)# hash md5	ハッシュ アルゴリズムを設定します。
	switch(config-ike-ipsec-policy)# no hash md5	デフォルトは SHA です。

	コマンド	目的
ステップ 9	<code>switch(config-ike-ipsec-policy)# authentication pre-share</code>	認証方式を事前共有キーを使用するように設定します(デフォルト)。
	<code>switch(config-ike-ipsec-policy)# authentication rsa-sig</code>	認証方式を RSA シグニチャを使用するように設定します。 (注) 認証のために RSA シグニチャを使用するには、FQDN を使用してアイデンティティ認証モードを設定する必要があります(ステップ 3 を参照)。
	<code>switch(config-ike-ipsec-policy)# no authentication</code>	デフォルト値(pre-share)に戻します。



(注) IKE 証明書は FQDN タイプのサブジェクト名を使用するので、認証方式が `rsa-sig` の場合には、IKE 用のアイデンティティ ホスト名が設定されていることを確認してください。



(注) Cisco MDS NX-OS リリース 5.2(x) にダウングレードする前に、事前共有キーを解除します。ダウングレードを完了したら、`key key-name hostname host` または `key key-name address ip-address` コマンドを使用して、事前共有キーを再設定します。

オプションの IKE パラメータの設定

IKE 機能には、オプションで次のパラメータを設定できます。

- 各ポリシーのライフタイム アソシエーション: ライフタイムの範囲は 600 ~ 86,400 秒です。デフォルトは、86,400 秒(1 日)です。各ポリシーのライフタイム アソシエーションは、IKE ポリシーの設定時に設定します。「IKE ポリシーの設定」セクション(7-14 ページ)を参照してください。
- 各ピアのキープアライブ タイム(IKEv2 を使用する場合): キープアライブの範囲は 120 ~ 86,400 秒です。デフォルトは、3,600 秒(1 時間)です。
- 各ピアの発信側バージョン: IKEv1 または IKEv2(デフォルト)。発信側バージョンの選択は、リモート デバイスがネゴシエーションを開始する場合、相互運用性に影響しません。このオプションは、ピア デバイスが IKEv1 をサポートしていて、指定したデバイスを IKE の発信側として動作させる場合に設定します。FCIP トンネルの発信側バージョンを設定する場合には、次の事項に注意してください。
 - FCIP トンネルの両側のスイッチが MDS SAN-OS Release 3.0(1) 以降または Cisco NX-OS 4.1(1) を実行している場合、IKEv1 だけを使用するには、FCIP トンネルの両側に発信側バージョン IKEv1 を設定する必要があります。FCIP トンネルの一方の側が IKEv1 を使用し、他方の側が IKEv2 を使用している場合には、FCIP トンネルは IKEv2 を使用します。
 - FCIP トンネルの片側のスイッチが MDS SAN-OS Release 3.0(1) 以降または Cisco NX-OS 4.1(1b) を実行し、FCIP トンネルの他方の側のスイッチが MDS SAN-OS Release 2.x を実行している場合、どちらか(または両方)の側に IKEv1 を設定すると、FCIP トンネルは IKEv1 を使用します。



(注) 2.x MDS スイッチと 3.x MDS スイッチ間の IPsec 構築では、IKEv1 だけがサポートされます。



注意 通常環境ではスイッチが IKE 発信側として動作しない場合でも、発信側バージョンの設定が必要になることがあります。このオプションを常に使用することにより、障害時にトラフィックフローをより速く回復できます。



ヒント

キープアライブタイムが適用されるのは、IKEv2 ピアだけで、すべてのピアではありません。



(注)

ホストの IPsec 実装により IPsec キー再設定を開始する場合には、Cisco MDS スイッチの IPsec のライフタイム値を、必ず、ホストのライフタイム値よりも大きい値に設定してください。

この項では、次のトピックについて取り上げます。

- [ポリシーのライフタイムアソシエーションの設定\(7-16 ページ\)](#)
- [ピアのキープアライブタイムの設定\(7-17 ページ\)](#)
- [発信側バージョンの設定\(7-17 ページ\)](#)
- [IKE トンネルまたはドメインのクリア\(7-17 ページ\)](#)
- [SA のリフレッシュ\(7-18 ページ\)](#)

ポリシーのライフタイムアソシエーションの設定

各ポリシーのライフタイムアソシエーションを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config terminal switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# crypto ike domain ipsec switch(config-ike-ipsec)#	IPsec ドメインをこのスイッチで設定できます。
ステップ 3	switch(config-ike-ipsec)# policy 1 switch(config-ike-ipsec-policy)#	設定するポリシーを指定します。
ステップ 4	switch(config-ike-ipsec-policy) lifetime seconds 6000	6,000 秒のライフタイムを設定します。
	switch(config-ike-ipsec-policy) # no lifetime seconds 6000	設定したライフタイム値を削除し、デフォルトの 86,400 秒に設定します。

ピアのキープアライブ タイムの設定

各ピアのキープアライブ タイムを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# config terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# crypto ike domain ipsec switch(config-ike-ipsec)#	IPsec ドメインをこのスイッチで設定できます。
ステップ 3	switch(config-ike-ipsec)# keepalive 60000	すべてのピアのキープアライブタイムを 60,000 秒に設定します。
	switch(config-ike-ipsec)# no keepalive 60000	設定したキープアライブタイムを削除し、デフォルトの 3,600 秒に設定します。

発信側バージョンの設定

IPv4 を使用して発信側バージョンを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# crypto ike domain ipsec switch(config-ike-ipsec)#	IPsec ドメインをこのスイッチで設定できます。
ステップ 3	switch(config-ike-ipsec)# initiator version 1 address 10.10.10.1	デバイス 10.10.10.0 で IKE を開始するときに、IKEv1 を使用するようにスイッチを設定します (注) IKE は、IPv4 アドレスをサポートし、IPv6 アドレスはサポートしません。
	switch(config-ike-ipsec)# no initiator version 1 address 10.10.10.1	指定デバイスについてデフォルトの IKEv2 に設定します。
	switch(config-ike-ipsec)# no initiator version 1	すべてのデバイスについてデフォルトの IKEv2 に設定します。

IKE トンネルまたはドメインのクリア

IKE 設定に IKE トンネル ID を指定していない場合は、EXEC モードで **clear crypto ike domain ipsec sa** コマンドを発行することにより、既存のすべての IKE ドメイン接続をクリアできます。

```
switch# clear crypto ike domain ipsec sa
```



注意

IKEv2 トンネル内のすべての SA を削除すると、その IKE トンネルは自動的に削除されます。

IKE 設定に SA を指定している場合、EXEC モードで **clear crypto ike domain ipsec sa IKE_tunnel-ID** コマンドを発行して、指定した IKE トンネル ID 接続をクリアできます。

```
switch# clear crypto ike domain ipsec sa 51
```



注意

IKEv2 トンネルを削除すると、その IKE トンネルの下の関連付けられた IPsec トンネルが自動的に削除されます。

SA のリフレッシュ

IKEv2 設定変更が行われた後に SA をリフレッシュするには、**crypto ike domain ipsec rekey IPv4-ACL-index** コマンドを使用します。

クリプト IPv4-ACL

IP アクセス コントロール リスト (IPv4-ACL) は、すべての Cisco MDS 9000 ファミリー スイッチに基本的なネットワーク セキュリティを提供します。IPv4 IP-ACL は、設定された IP フィルタに基づいて IP 関連トラフィックを制限します。IPv4-ACL の作成および定義の詳細については、[第 5 章「IPv4 および IPv6 のアクセス コントロール リストの設定」](#)を参照してください。

クリプト マップのコンテキストでは、IPv4-ACL は標準の IPv4-ACL と異なります。標準の IPv4-ACL は、インターフェイス上で転送またはブロックするトラフィックを判別します。たとえば、IPv4-ACL を作成して、サブネット A とサブネット Y 間のすべての IP トラフィックを保護したり、ホスト A とホスト B 間の Telnet トラフィックを保護できます。

ここでは、次の内容について説明します。

- [クリプト IPv4-ACL の概要 \(7-18 ページ\)](#)
- [クリプト IPv4-ACL の作成 \(7-22 ページ\)](#)
- [IPsec のトランスフォーム セットの概要 \(7-23 ページ\)](#)
- [トランスフォーム セットの設定 \(7-24 ページ\)](#)
- [暗号マップ エントリの概要 \(7-24 ページ\)](#)
- [クリプト マップ エントリの作成 \(7-26 ページ\)](#)
- [SA ライフタイム ネゴシエーションの概要 \(7-27 ページ\)](#)
- [SA ライフタイムの設定 \(7-27 ページ\)](#)
- [AutoPeer オプションの概要 \(7-28 ページ\)](#)
- [AutoPeer オプションの設定 \(7-29 ページ\)](#)
- [PFS の概要 \(7-29 ページ\)](#)
- [PFS の設定 \(7-29 ページ\)](#)
- [クリプト マップ セット インターフェイスの適用の概要 \(7-29 ページ\)](#)
- [クリプト マップ セットの適用 \(7-30 ページ\)](#)

クリプト IPv4-ACL の概要

クリプト IPv4-ACL は、暗号による保護が必要な IP トラフィックと、必要ではないトラフィックとを定義するために使用します。

IPsec のクリプト マップ エントリに関連付けるクリプト IPv4-ACL には、4 つの主要な機能があります。

- IPsec で保護する発信トラフィックを選択する (permit に一致したものが保護の対象)。
- IPsec SA のネゴシエーションの開始時に、新しい SA で保護するデータフロー (1 つの permit エントリで指定) を示す。
- 着信トラフィックを処理して、IPsec で保護すべきであったトラフィックをフィルタリングして廃棄する。
- IPsec ピアからの IKE ネゴシエーションの処理時に、要求されたデータフローのために、IPsec SA の要求を受け入れるかどうかを判別する。



ヒント

一部のトラフィックに1つのタイプのIPsec保護(暗号化だけ、など)を適用し、他のトラフィックに異なるタイプのIPsec保護(認証と暗号化の両方など)を適用する場合には、2つのIPv4-ACLを作成してください。異なるIPsecポリシーを指定するには、異なるクリプトマップで両方のIPv4-ACLを使用します。



(注) IPsec は、IPv6-ACL をサポートしていません。

クリプト IPv4-ACL の注意事項

IPsec 機能に関する IPv4-ACL を設定する場合には、次の注意事項に従ってください。

- Cisco NX-OS ソフトウェアで使用できるのは、名前ベースの IPv4-ACL だけです。
- IPv4-ACL をクリプト マップに適用するときは、次のオプションを適用します。
 - 許可 (permit) : トラフィックに IPsec 機能を適用します。
 - 拒否 (deny) : クリア テキストを許可します (デフォルト)。



(注) IKE トラフィック (UDP ポート 500) は、必ずクリア テキストで送信されます。

- IPsec 機能が考慮するのは、送信元/宛先 IPv4 アドレスとサブネット マスク、プロトコル、および 1 つのポート番号だけです。IPsec では、IPv6 はサポートされません。

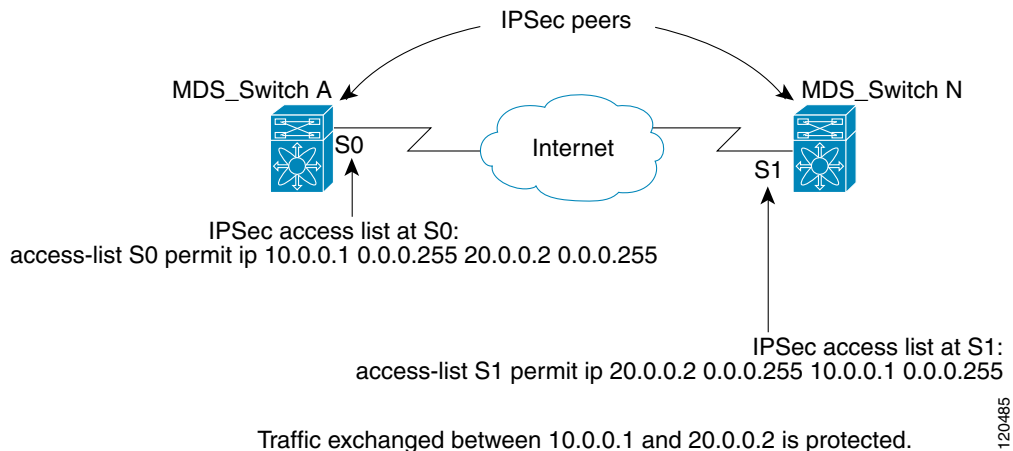


(注) IPsec 機能はポート番号範囲をサポートしていないので、指定されている場合には上位ポート番号フィールドは無視されます。

- permit オプションを指定すると、対応するクリプト マップ エントリで指定されたポリシーを使用して、指定条件に一致するすべての IP トラフィックが暗号によって保護されます。
- deny オプションを指定すると、トラフィックは暗号によって保護されません。最初の deny ステートメントにより、トラフィックはクリア テキストで送信されます。
- 定義するクリプト IPv4-ACL がインターフェイスに適用されるのは、対応するクリプト マップ エントリを定義して、インターフェイスにクリプト マップ セットを適用したあとです。
- 同じクリプト マップ セットの エントリごとに、異なる IPv4-ACL を使用する必要があります。
- インバウンドおよびアウトバウンド トラフィックは、同じアウトバウンド IPv4-ACL に対して評価されます。したがって、IPv4-ACL の条件は、スイッチからの発信トラフィックに対して順方向に、スイッチへの着信トラフィックに対して逆方向に適用されます。

- クリプト マップ エントリに割り当てられた各 IPv4-ACL フィルタは、1つのセキュリティ ポリシー エントリと同等です。IPsec 機能は、各 MPS-14/2 モジュールおよび Cisco MDS 9216i スイッチに対して、最大 120 のセキュリティ ポリシー エントリをサポートします。
- スイッチ A の S0 インターフェイスから発信されたデータがスイッチ インターフェイス S1 にルーティングされるときに、スイッチ インターフェイス S0 (IPv4 アドレス 10.0.0.1) とスイッチ インターフェイス S1 (IPv4 アドレス 20.0.0.2) 間のトラフィックに IPsec 保護 (図 7-5 を参照) が適用されます。10.0.0.1 から 20.0.0.2 へのトラフィックの場合、スイッチ A の IPv4-ACL エントリは次のように評価されます。
 - 送信元 = IPv4 アドレス 10.0.0.1
 - 宛先 = IPv4 アドレス 20.0.0.2
 20.0.0.2 から 10.0.0.1 へのトラフィックの場合、スイッチ A の IPv4-ACL エントリは次のように評価されます。
 - 送信元 = IPv4 アドレス 20.0.0.2
 - 宛先 = IPv4 アドレス 10.0.0.1

図 7-5 クリプト IPv4-ACL の IPsec 処理



- IPsec に使用する指定のクリプト IPv4-ACL に複数のステートメントを設定した場合には、一致した最初の permit ステートメントにより、IPsec SA の有効範囲が判別されます。その後、トラフィックがクリプト IPv4-ACL の別の permit ステートメントと一致した場合には、新しい、別の IPsec SA がネゴシエートされ、新たに一致した IPv4-ACL ステートメントと一致するトラフィックが保護されます。
- クリプト マップ エントリに IPsec がフラグ設定されている場合、クリプト IPv4-ACL 内の permit エントリと一致する保護されていないインバウンドトラフィックは、IPsec によって保護されていると見なされ、廃棄されます。
- すべての IP-ACL を表示するには、**show ip access-list** コマンドを使用できます。トラフィックをフィルタリングするために使用される IP-ACL は、暗号化にも使用されます。
- IPsec を Microsoft iSCSI 発信側と効率的に相互運用するには、IPv4-ACL に TCP プロトコルとローカル iSCSI TCP ポート番号 (デフォルトは 3260) を指定します。この設定により、ギガビットイーサネット インターフェイスのシャットダウン、VRRP スイッチオーバー、ポート障害などにより処理が中断されても、暗号化 iSCSI セッションを迅速に回復できます。

- IPv4-ACL エントリの次の例では、MDS スイッチの IPv4 アドレスが 10.10.10.50 で、暗号化 iSCSI セッションが実行中のリモート Microsoft ホストが 10.10.10.16 であることを示しています。

```
switch(config)# ip access-list aclmsiscsi2 permit tcp 10.10.10.50 0.0.0.0 range port
3260 3260 10.10.10.16 0.0.0.0
```

ミラーイメージクリプト IPv4-ACL

ローカル ピアで定義されたクリプト マップ エントリがある場合は、このエントリで指定されたすべてのクリプト IPv4-ACL に対して、リモート ピアでミラー イメージクリプト IPv4-ACL を定義します。この設定により、ローカルで適用された IPsec トラフィックをリモート ピアで正しく処理できるようになります。


ヒント

また、クリプト マップ エントリ自体が共通のトランスフォームをサポートし、ピアとして他のシステムを参照する必要があります。

図 7-6 に、ミラー イメージ IPv4-ACL を使用した場合と、使用しない場合のサンプル シナリオを示します。

図 7-6 ミラーイメージ設定の IPsec 処理

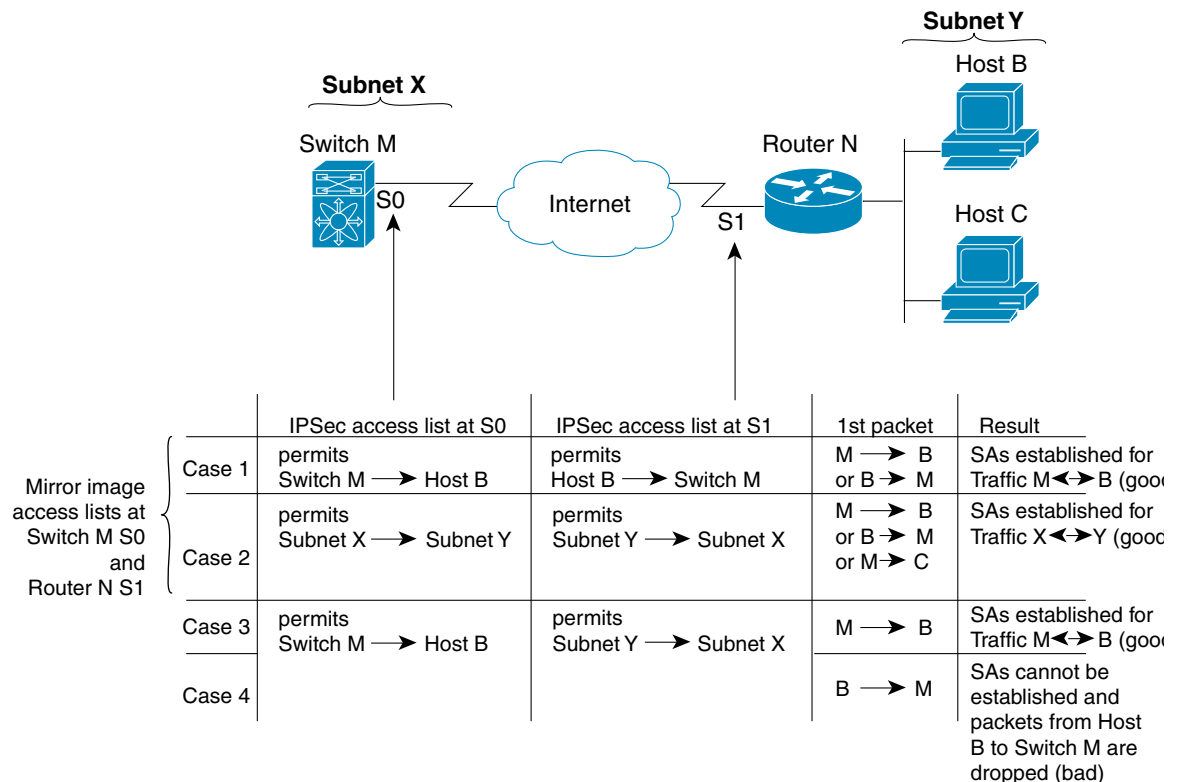


図 7-6 に示すように、2 つのピアのクリプト IPv4-ACL が相互のミラー イメージである場合、想定どおりに IPsec SA を確立できます。ただし、IPv4-ACL が相互のミラー イメージでない場合にも、IPsec SA を確立できることがあります。たとえば、図 7-6 のケース 3 および 4 のように、一方のピアの IPv4-ACL エントリが他方のピアの IPv4-ACL エントリのサブセットになっている場合です。IPsec SA の確立は、IPsec にとって非常に重要です。SA が存在しないと IPsec は機能せず、クリプト IPv4-ACL の条件と一致するパケットは、IPsec セキュリティで保護されて転送される代わりに、すべて廃棄されます。

ケース 4 では、SA を確立できません。開始元パケットが終了すると、クリプト IPv4-ACL に従って必ず SA が要求されるためです。ケース 4 では、ルータ N はサブネット X とサブネット Y 間のすべてのトラフィックを保護するように要求します。ただし、このトラフィックはスイッチ M のクリプト IPv4-ACL で許可される特定のフローのスーパーセットであるため、要求は許可されません。スイッチ M の要求はルータ N のクリプト IPv4-ACL で許可される特定のフローのサブセットであるため、ケース 3 は機能します。

ピア IPsec デバイスにクリプト IPv4-ACL をミラー イメージとして設定しないと、設定が複雑化するので、ミラー イメージクリプト IPv4-ACL を使用することを強く推奨します。

クリプト IPv4-ACL の any キーワード



ヒント

IPsec で使用するミラー イメージクリプト IPv4-ACL は、**any** オプションを使用しないで設定することを推奨します。

IPsec インターフェイスを経由してマルチキャスト トラフィックを転送すると、**permit** ステートメントの **any** キーワードは廃棄されます。これは、マルチキャスト トラフィックの転送が失敗する原因になります。

permit any ステートメントを使用すると、すべてのアウトバウンド トラフィックが保護され(保護されたすべてのトラフィックが、対応するクリプト マップ エントリで指定されたピアに送信され)、すべてのインバウンド トラフィックの保護が必要になります。ルーティング プロトコル、NTP、エコー、エコー応答用のパケットを含む、IPsec で保護されないすべてのインバウンド パケットは、自動的に廃棄されます。

保護するパケットを確実に定義する必要があります。**permit** ステートメント内で **any** オプションを使用する必要がある場合は、保護しないすべてのトラフィックを除外する一連の **deny** ステートメントを、**permit** ステートメントの前に付加する必要があります(付加しない場合、これらのトラフィックが **permit** ステートメントの対象になります)。

クリプト IPv4-ACL の作成

IPv4-ACL を作成するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ip access-list List1 permit ip 10.1.1.100 0.0.0.255 11.1.1.100 0.0.0.255	指定のネットワークから、または指定のネットワークへの、すべての IP トラフィックを許可します。



(注) **show ip access-list** コマンドでは暗号マップ エントリは表示されません。関連エントリを表示するには、**show crypto map** コマンドを使用します。

必要に応じて、**permit** および **deny** ステートメントを追加します(第5章「IPv4 および IPv6 のアクセス コントロール リストの設定」を参照)。各 **permit** および **deny** は、保護する必要がある IP パケットを指示するための条件を指定します。

IPsec のトランスフォーム セットの概要

トランスフォーム セットは、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IPsec SA のネゴシエーション中に、ピアは特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。

複数のトランスフォーム セットを指定し、これらのトランスフォーム セットの1つまたは複数を選択してクリプト マップ エントリに指定できます。クリプト マップ エントリで定義されたトランスフォーム セットは、このクリプト マップ エントリのアクセス リストで指定されたデータ フローを保護するために、IPsec SA ネゴシエーションで使用されます。

IKE との IPsec セキュリティ アソシエーションのネゴシエーション中に、ピアは両方のピア上で同じトランスフォーム セットを検索します。同一のトランスフォーム セットが検出された場合には、そのトランスフォーム セットが選択され、両方のピアの IPsec SA の一部として、保護するトラフィックに適用されます。



ヒント

トランスフォーム セット定義を変更した場合には、トランスフォーム セットを参照するクリプト マップ エントリだけに変更が適用されます。変更は既存の SA には適用されませんが、新規 SA を確立するために以降のネゴシエーションで使用されます。新規設定を即座に有効にする場合には、SA データベースのすべてまたは一部を消去します。



(注) IPsec をイネーブルにすると、Cisco NX-OS ソフトウェアにより、AES-128 暗号化および SHA-1 認証アルゴリズムを使用したデフォルトのトランスフォーム セット (`ipsec_default_transform_set`) が自動的に作成されます。

表 7-2 に、IPsec で使用できるトランスフォームの組み合わせを示します。

表 7-2 IPsec トランスフォーム設定パラメータ

パラメータ	許容値	キーワード
暗号化アルゴリズム	56 ビット DES-CBC	esp-des
	168 ビット DES	esp-3des
	128 ビット AES-CBC	esp-aes 128
	128 ビット AES-CTR ¹	esp-aes 128 ctr
	256 ビット AES-CBC	esp-aes 256
	256 ビット AES-CTR ¹	esp-aes 256 ctr

表 7-2 IPsec トランスフォーム設定パラメータ(続き)

パラメータ	許容値	キーワード
ハッシュ/認証アルゴリズム ¹ (任意)	SHA-1(HMAC バリエント)	esp-sha1-hmac
	SHA-2(HMAC バリエント)	esp-sha256-hmac
	MD5(HMAC バリエント)	esp-sha512-hmac
	AES-XCBC-MAC	esp-md5-hmac esp-aes-xcbc-mac

1. AES カウンタ(CTR)モードを設定する場合には、認証アルゴリズムも設定する必要があります。

次の表に、Microsoft Windows および Linux プラットフォームでサポートおよび検証されている、IPsec および IKE 暗号化認証アルゴリズムの設定を示します。

プラットフォーム	IKE	IPsec
Microsoft iSCSI 発信側 (Microsoft Windows 2000 プラットフォームの Microsoft IPsec 実装)	3DES、SHA-1、SHA-2、または MD5、DH グループ 2	3DES、SHA-1、SHA-2
Cisco iSCSI イニシエータ、Linux プラットフォームへの Free Swan IPsec の実装	3DES、MD5、DH グループ 1	3DES、MD5

トランスフォーム セットの設定

トランスフォーム セットを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	<code>switch# config terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# crypto transform-set domain ipsec test esp-3des esp-md5-hmac</code>	3DES 暗号化アルゴリズムと MD5 認証アルゴリズムを指定する、test というトランスフォーム セットを設定します。表 7-2 を参照して、トランスフォームの組み合わせが使用可能かどうかを確認してください。
	<code>switch(config)# no crypto transform-set domain ipsec test esp-3des esp-md5-hmac</code>	適用されたトランスフォーム セットを削除します。
	<code>switch(config)# crypto transform-set domain ipsec test esp-3des</code>	3DES 暗号化アルゴリズムを指定する、test というトランスフォーム セットを設定します。この例では、デフォルトの認証は実行されません。
	<code>switch(config)# no crypto transform-set domain ipsec test esp-3des</code>	適用されたトランスフォーム セットを削除します。

暗号マップ エントリの概要

クリプト IPv4-ACL とトランスフォーム セットの設定が完了すると、次のように、IPsec SA のさまざまな部分を組み合わせる暗号マップ エントリを作成できます。

- IPsec で保護するトラフィック(クリプト IPv4-ACL 単位)。クリプト マップ セットには、それぞれ異なる IPv4-ACL を使用する複数のエントリを設定できます。
- SA セットで保護するフローの詳細度。
- IPsec で保護されるトラフィックの宛先(リモート IPsec ピアの名前)。
- IPsec トラフィックが使用するローカル アドレス(インターフェイスに適用)。
- 現在のトラフィックに適用する IPsec セキュリティ(1 つまたは複数のトランスフォーム セットから選択)。
- IPsec SA を定義するその他のパラメータ。

同じクリプト マップ名(マップ シーケンス番号が異なる)を持つクリプト マップ エントリは、クリプト マップ セットにグループ化されます。

クリプト マップ セットをインターフェイスに適用すると、次のイベントが発生します。

- そのインターフェイス用の Security Policy Database (SPD) が作成されます。
- インターフェイスを経由するすべての IP トラフィックが、SPD に対して評価されます。

クリプト マップ エントリにより保護を必要とするアウトバウンド IP トラフィックが確認されると、クリプト マップ エントリ内のパラメータに従って、SA とリモート ピアのネゴシエーションが行われます。

SA のネゴシエーションでは、クリプト マップ エントリから取得したポリシーが使用されます。ローカル スイッチがネゴシエーションを開始した場合、ローカル スイッチはクリプト マップ エントリに指定されたポリシーを使用して、指定された IPsec ピアに送信するオファーを作成します。IPsec ピアがネゴシエーションを開始した場合、ローカル スイッチはクリプト マップ エントリのポリシーを調べて、ピアの要求(オファー)を受け入れるか、または拒否するかを判断します。

2 つの IPsec ピア間で IPsec を成立させるには、両方のピアのクリプト マップ エントリに互換性のあるコンフィギュレーション ステートメントが含まれている必要があります。

ピア間の SA の確立

2 つのピアが SA を確立する場合、各ピアのクリプト マップ エントリの 1 つまたは複数と、相手ピアのクリプト マップ エントリの 1 つに互換性がなければなりません。

2 つのクリプト マップ エントリで互換性が成立するには、少なくとも次の基準を満たす必要があります。

- クリプト マップ エントリに、互換性のあるクリプト IPv4-ACL (ミラー イメージ IPv4-ACL など)が含まれていること。応答側のピア エントリがローカルで暗号化されている場合、IPv4-ACL がこのピアのクリプト IPv4-ACL で許可されている必要があります。
- クリプト マップ エントリが互いに相手ピアを識別しているか、または自動ピアが設定されていること。
- 特定のインターフェイスに複数のクリプト マップ エントリを作成するときは、各マップ エントリの seq-num を使用して、マップ エントリにランクを設定します。seq-num の値が小さいほど、プライオリティは高くなります。クリプト マップ セットがあるインターフェイスでは、トラフィックは、最初にプライオリティの高いマップ エントリに対して評価されます。
- IKE ネゴシエーションを実行して SA を確立するには、クリプト マップ エントリに最低 1 つの共通トランスフォーム セットが含まれている必要があります。IPsec SA のネゴシエーション中に、両ピアは特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。

パケットが特定の IPv4-ACL 内の permit エントリと一致すると、対応するクリプト マップ エントリにタグが付けられ、接続が確立されます。

クリプトマップ設定の注意事項

クリプトマップ エントリを設定する場合には、次の注意事項に従ってください。

- ポリシーが適用される順序は、各クリプトマップのシーケンス番号によって決まります。シーケンス番号が小さいほど、プライオリティは高くなります。
- 各クリプトマップ エントリに使用できる IPv4-ACL は 1 つだけです (IPv4-ACL 自体には複数の permit エントリまたは deny エントリを設定できます)。
- トンネルエンドポイントが宛先アドレスと同じである場合は、auto-peer オプションを使用して、ピアをダイナミックに設定できます。
- IPsec を Microsoft iSCSI 発信側と効率的に相互運用するには、IPv4-ACL に TCP プロトコルとローカル iSCSI TCP ポート番号 (デフォルトは 3260) を指定します。この設定により、ギガビットイーサネットインターフェイスのシャットダウン、VRRP スイッチオーバー、ポート障害などにより処理が中断されても、暗号化 iSCSI セッションを迅速に回復できます。

クリプトマップエントリの作成



(注) 暗号マップ エントリで指定されたピアの IP アドレスがリモートの Cisco MDS スイッチの VRRP IP アドレスである場合、IP アドレスが **secondary** オプションを使用して作成されることを確認します (詳細については、『Cisco MDS 9000 Family NX-OS IP Services Configuration Guide』を参照してください)。

必須の暗号マップ エントリを作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# config terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# crypto map domain ipsec SampleMap 31 ips-hacl1(config-crypto-map-ip)#	シーケンス番号が 31 の SampleMap というエントリに対し、暗号マップ設定モードを開始します。
	switch(config)# no crypto map domain ipsec SampleMap 3	指定されたクリプトマップ エントリを削除します。
ステップ 3	switch(config-crypto-map-ip)# match address SampleAcl	このクリプトマップ エントリのコンテキストで、IPsec によって保護するトラフィックと保護しないトラフィックを決定する ACL を指定します。
	switch(config-crypto-map-ip)# no match address SampleAcl	一致したアドレスを削除します。
ステップ 4	switch(config-crypto-map-ip)# set peer 10.1.1.1	特定のピアの IPv4 アドレスを設定します。 (注) IKE は、IPv4 アドレスのみをサポートし、IPv6 アドレスはサポートしません。
ステップ 5	switch(config-crypto-map-ip)# no set peer 10.1.1.1	設定されたピアを削除します。

	コマンド	目的
ステップ 6	<code>switch(config-crypto-map-ip)# set transform-set SampleTransform1 SampleTransform2</code>	指定した暗号マップ エントリに対し許可するトランスフォーム セットを指定します。複数のトランスフォーム セットをプライオリティ順(最高のプライオリティのものが最初)に列挙します。
	<code>switch(config-(crypto-map-ip))# no set transform-set</code>	すべてのトランス フォーム セットのアソシエーションを削除します(トランスフォーム セットの名前の指定に関係なく)。

SA ライフタイム ネゴシエーションの概要

SA 固有のライフタイム値を設定することにより、グローバル ライフタイム値(サイズおよびタイム)を書き換えることができます。

SA ライフタイム ネゴシエーション値を指定する場合、指定したクリプト マップにライフタイム値を設定することもできます。この場合、設定されたライフタイム値によってグローバルな設定値が上書きされます。クリプト マップ固有のライフタイムを指定しない場合には、グローバル値(またはグローバルなデフォルト値)が使用されます。

グローバル ライフタイム値の詳細については、「[グローバル ライフタイム値](#)」セクション(7-30 ページ)を参照してください。

SA ライフタイムの設定

指定したクリプト マップ エントリの SA ライフタイムを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	<code>switch# config terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# crypto map domain ipsec SampleMap 31</code> <code>switch(config-crypto-map-ip)#</code>	シーケンス番号が 31 の SampleMap というエントリに対し、暗号マップ設定サブモードを開始します。
ステップ 3	<code>switch(config-crypto-map-ip)# set security-association lifetime seconds 8640</code>	暗号マップのエントリに対するグローバルなライフタイムとは異なる IPsec SA ライフタイムを使用して、この暗号マップのエントリに対する SA ライフタイムを指定します。
	<code>switch(config-crypto-map-ip)# no set security-association lifetime seconds 8640</code>	エントリ固有の設定を削除し、グローバル設定に戻します。
ステップ 4	<code>switch(config-crypto-map-ip)# set security-association lifetime gigabytes 4000</code>	指定したトラフィック量(GB 単位)が SA を使用して FCIP リンクを通過した後、この SA のトラフィック量ライフタイムがタイムアウトするように設定します。ライフタイムの範囲は 1 ~ 4095 GB です。

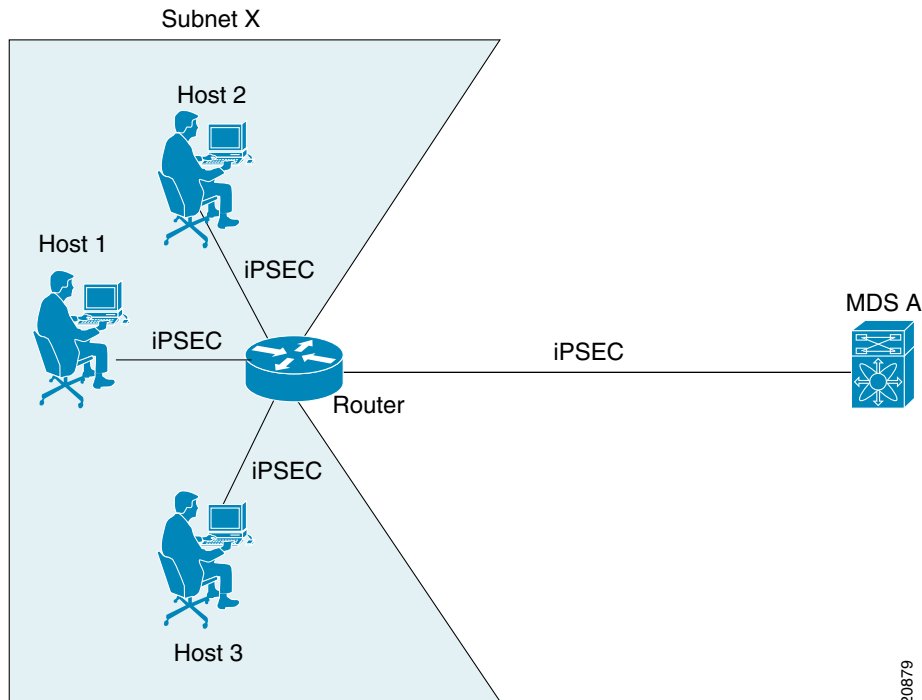
AutoPeer オプションの概要

クリプト マップ内でピア アドレスを **auto-peer** として設定した場合は、トラフィックの宛先エンドポイントが SA のピア アドレスとして使用されます。同じクリプト マップを使用して、クリプト マップの IPv4-ACL エントリで指定されたサブネット内の各エンドポイントに、固有の SA を設定できます。**auto-peer** を使用すると、トラフィック エンドポイントが IPsec に対応している場合に、設定が簡素化されます。**auto-peer** は、同じサブネット内の複数の iSCSI ホストで個別の設定が必要ない場合、特に役立ちます。

図 7-7 に、**auto-peer** オプションによって設定が簡素化される例を示します。**auto-peer** オプションを使用すると、サブネット X からの全ホストについて、1つのクリプト マップ エントリだけを使用してスイッチとの SA を確立できます。各ホストは独自の SA を確立しますが、クリプト マップ エントリは共有されます。**auto-peer** オプションを使用しない場合、各ホストに1つのクリプト マップ エントリが必要になります。

詳細については、「[iSCSI の設定例](#)」セクション(7-41 ページ)を参照してください。

図 7-7 **auto-peer** オプションを使用した iSCSI のエンドツーエンド IPsec



120879

AutoPeer オプションの設定

auto-peer オプションを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# crypto map domain ipsec SampleMap 31 ips-hacl(config-crypto-map-ip)#	シーケンス番号が 31 の SampleMap というエントリに対し、暗号マップ設定モードを開始します。
ステップ 3	switch(config-crypto-map-ip)# set peer auto-peer	ソフトウェアに (SA セットアップの間に)宛先ピアの IP アドレスを動的に選択するように指示します。
	switch(config-crypto-map-ip)# no set peer auto-peer	auto-peer 設定を削除します。

PFS の概要

SA ライフタイム ネゴシエーション値を指定する場合、オプションでクリプト マップの完全転送秘密 (PFS) 値を設定できます。

PFS 機能は、デフォルトではディセーブルです。PFS グループを設定する場合は、DH グループ 1、2、5、または 14 のうちの 1 つを設定できます。DH グループを指定しない場合、グループ 1 がデフォルトで使用されます。

PFS の設定

PFS 値を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# config terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# crypto map domain ipsec SampleMap 31 ips-hacl(config-crypto-map-ip)#	シーケンス番号が 31 の SampleMap というエントリに対し、暗号マップ設定モードを開始します。
ステップ 3	switch(config-crypto-map-ip)# set pfs group 2	IPsec がこの暗号マップ エントリの新しい SA を要求した場合、PFS を要求するように、または IPsec ピアから受信する要求に PFS が含まれることを要求するように指定します。
	switch(config-crypto-map-ip)# no set pfs	設定済みの DH グループを削除し、工場出荷時のデフォルトである PFS のディセーブル化に戻します。

クリプト マップ セット インターフェイスの適用の概要

IPsec トラフィック フローが通過する各インターフェイスにクリプト マップ セットを適用する必要があります。インターフェイスにクリプト マップ セットを適用すると、スイッチはそのインターフェイスのすべてのトラフィックを指定されたクリプト マップ セットに対して評価し、指定されたポリシーを接続中または SA ネゴシエーション中に使用して、トラフィックが暗号によって保護されるようにします。

1つのインターフェイスに適用できるクリプトマップセットは1つだけです。複数のインターフェイスに同じクリプトマップを適用できます。ただし、各インターフェイスに複数のクリプトマップセットを適用できません。

クリプトマップセットの適用

クリプトマップセットをインターフェイスに適用する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# config terminal switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# interface gigabitethernet 4/1 switch(config-if)#	IPsec 暗号マップが適用される、必要なギガビットイーサネットインターフェイス (および必要な場合はサブインターフェイス) を選択します。
ステップ 3	switch(config-if)# crypto map domain ipsec cm10	暗号マップセットを選択したインターフェイスに適用します。
ステップ 4	switch(config-if)# no crypto map domain ipsec	現在このインターフェイスに適用されている暗号マップを削除します。

IPsec のメンテナンス

設定の変更は、後続の SA のネゴシエーション時まで適用されません。新しい設定をすぐに適用するには、変更した設定を使用して SA が再確立されるように、既存の SA をクリアする必要があります。スイッチが IPsec トラフィックをアクティブに処理している場合には、SA データベースのうち、設定変更が影響する部分だけを消去してください (つまり、指定のクリプトマップセットによって確立された SA だけを消去します)。SA データベース全体を消去するのは、大規模な変更を行った場合、またはルータが他の IPsec トラフィックをほとんど処理していない場合だけにしてください。



ヒント

show crypto sa domain interface gigabitethernet slot/port コマンドの出力から SA インデックスを得ることができます。

SA データベースの一部を消去するには、次のコマンドを使用します。

```
switch# clear crypto sa domain ipsec interface gigabitethernet 2/1 inbound sa-index 1
```

グローバル ライフタイム値

クリプトマップ エントリにライフタイムが設定されていない場合、新しい IPsec SA のネゴシエーション時にグローバル ライフタイム値が使用されます。

タイムまたはトラフィック ボリュームの 2 つのライフタイムを設定できます。どちらか一方のライフタイムに到達すると、SA は期限切れになります。デフォルトのライフタイムは 3,600 秒 (1 時間) および 450 GB です。

グローバル ライフタイムを変更した場合、新しいライフタイム値は既存の SA には適用されず、以降に確立される SA のネゴシエーションに使用されます。新しいライフタイム値をすぐに使用する場合は、SA データベースのすべてまたは一部を消去します。

特定のクリプト マップ エントリにライフタイム値が設定されていない場合、スイッチは新規 SA を要求するときに、ピアへの要求内でグローバル ライフタイム値を指定します。この値は、新規 SA のライフタイム値として使用されます。ピアからのネゴシエーション要求を受信すると、スイッチは使用中の IKE バージョンによって決まる値を使用します。

- IKEv1 を使用して IPsec SA を設定する場合、SA ライフタイム値は、2つの候補のうち小さい方の値になります。トンネルの両端で、同じ値がプログラムされます。
- IKEv2 を使用して IPsec SA を設定する場合、各端の SA に独自のライフタイム値が設定されるので、両端の SA は個別に期限切れになります。

SA(および対応するキー)は、指定時間(秒単位)または指定トラフィック量(バイト単位)のどちらか一方が先に経過した時点で、期限切れになります。

既存の SA のライフタイムしきい値に到達する前に、新しい SA がネゴシエートされます。これは、既存の SA が期限切れになる前にネゴシエーションを完了するためです。

新しい SA は、次のいずれかのしきい値に先に到達した時点でネゴシエートされます。

- ライフタイムが期限切れになる 30 秒前
- ライフタイムの残りのバイト数が約 10% になったとき

ライフタイムが期限切れになった時点でトラフィックが送受信されていない場合、新しい SA はネゴシエートされません。新しい SA がネゴシエートされるのは、IPsec が別の保護対象パケットを確認した場合だけです。

グローバル SA ライフタイムを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	<code>switch# config terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# crypto global domain ipsec security-association lifetime seconds 86400</code>	指定した秒数が経過した後、IPsec SA のグローバル ライフタイムがタイムアウトするように設定します。グローバル ライフタイムの範囲は 120 ~ 86400 秒です。
	<code>switch(config)# no crypto global domain ipsec security-association lifetime seconds 86400</code>	出荷時デフォルトの 3,600 秒に戻します。
ステップ 3	<code>switch(config)# crypto global domain ipsec security-association lifetime gigabytes 4000</code>	指定したトラフィック量(GB 単位)が SA を使用して FCIP リンクを通過した後、IPsec SA のグローバルトラフィック量ライフタイムがタイムアウトするように設定します。グローバル ライフタイムの範囲は 1~4095 GB です。
	<code>switch(config)# crypto global domain ipsec security-association lifetime kilobytes 2560</code>	グローバルトラフィック量のライフタイムを設定します(KB 単位)。グローバル ライフタイムの範囲は 2560 ~ 2147483647 KB です。
	<code>switch(config)# crypto global domain ipsec security-association lifetime megabytes 5000</code>	グローバルトラフィック量のライフタイムを設定します(MB 単位)。グローバル ライフタイムの範囲は 3 ~ 4193280 MB です。
	<code>switch(config)# no crypto global domain ipsec security-association lifetime megabytes</code>	現在設定されている値に関係なく、工場出荷時のデフォルトの 450 GB に戻します。

IKE 設定の表示

show コマンドのセットを使用して、IKE 情報を確認できます。例 7-1 ~ 7-5 を参照してください。

例 7-1 各 IKE ポリシー用に設定されたパラメータの表示

```
switch# show crypto ike domain ipsec
keepalive 60000
```

例 7-2 イニシエータ設定の表示

```
switch# show crypto ike domain ipsec initiator
initiator version 1 address 1.1.1.1
initiator version 1 address 1.1.1.2
```

例 7-3 キーの設定の表示

```
switch# show crypto ike domain ipsec key
key abcdefgh address 1.1.1.1
key bcdefghi address 1.1.2.1
```

例 7-4 IKE 用の現在確立されたポリシーの表示

```
switch# show crypto ike domain ipsec policy 1
Priority 1, auth pre-shared, lifetime 6000 secs, encryption 3des, hash md5, DH group 5
Priority 3, auth pre-shared, lifetime 86300 secs, encryption aes, hash sha1, DH group 1
Priority 5, auth pre-shared-key, lifetime 86400 secs, encryption 3des, hash sha256, DH
group 1
```

例 7-5 IKE 用の現在確立された SA の表示

```
switch# show crypto ike domain ipsec sa
Tunn  Local Addr      Remote Addr      Encr  Hash  Auth Method  Lifetime
-----
1*    172.22.31.165[500] 172.22.31.166[500] 3des  sha1  preshared key  86400
2     172.22.91.174[500] 172.22.91.173[500] 3des  sha1  preshared key  86400
-----
NOTE: tunnel id ended with * indicates an IKEv1 tunnel
```

IPsec 設定の表示

show コマンドのセットを使用して、IPsec 情報を確認できます。例 7-6 ~ 7-19 を参照してください。

例 7-6 指定された ACL の情報の表示

```
switch# show ip access-list acl10
ip access-list acl10 permit ip 10.10.10.0 0.0.0.255 10.10.10.0 0.0.0.255 (0 matches)
```

例 7-6 では、表示出力一致に、この条件を満たすインターフェイス(暗号マップではない)だけが表示されます。

例 7-7 トランスフォーム セットの設定の表示

```
switch# show crypto transform-set domain ipsec
Transform set: 1/1 {esp-3des esp-sha256-hmac}
    will negotiate {tunnel}
Transform set: ipsec_default_transform_set {esp-aes 128 esp-sha1-hmac}
    will negotiate {tunnel}
```

例 7-8 設定されたすべての暗号マップの表示

```
switch# show crypto map domain ipsec
Crypto Map "cm10" 1 ipsec
  Peer = Auto Peer
  IP ACL = acl10
    permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
  Transform-sets: 3des-md5, des-md5,
  Security Association Lifetime: 4500 megabytes/3600 seconds
  PFS (Y/N): N
  Interface using crypto map set cm10:
    GigabitEthernet4/1
Crypto Map "cm100" 1 ipsec
  Peer = Auto Peer
  IP ACL = acl100
    permit ip 10.10.100.0 255.255.255.0 10.10.100.0 255.255.255.0
  Transform-sets: 3des-md5, des-md5,
  Security Association Lifetime: 4500 megabytes/3600 seconds
  PFS (Y/N): N
  Interface using crypto map set cm100:
    GigabitEthernet4/2
```

例 7-9 特定のインターフェイス用の暗号マップ情報の表示

```
switch# show crypto map domain ipsec interface gigabitethernet 4/1
Crypto Map "cm10" 1 ipsec
  Peer = Auto Peer
  IP ACL = acl10
    permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
  Transform-sets: 3des-md5, des-md5,
  Security Association Lifetime: 4500 megabytes/3600 seconds
  PFS (Y/N): N
  Interface using crypto map set cm10:
    GigabitEthernet4/1
```

例 7-10 指定した暗号マップ情報の表示

```
switch# show crypto map domain ipsec tag cm100
Crypto Map "cm100" 1 ipsec
  Peer = Auto Peer
  IP ACL = acl100
    permit ip 10.10.100.0 255.255.255.0 10.10.100.0 255.255.255.0
  Transform-sets: 3des-md5, des-md5,
  Security Association Lifetime: 4500 megabytes/3600 seconds
  PFS (Y/N): N
  Interface using crypto map set cm100:
    GigabitEthernet4/2
```

例 7-11 指定したインターフェイス用の SA アソシエーションの表示

```
switch# show crypto sad domain ipsec interface gigabitethernet 4/1
interface: GigabitEthernet4/1
  Crypto map tag: cm10, local addr.10.10.10.1
  protected network:
  local ident (addr/mask): (10.10.10.0/255.255.255.0)
  remote ident (addr/mask): (10.10.10.4/255.255.255.255)
  current_peer: 10.10.10.4
    local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.4
    mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
    current outbound spi: 0x30e000f (51249167), index: 0
    lifetimes in seconds:: 3600
    lifetimes in bytes:: 423624704
    current inbound spi: 0x30e0000 (51249152), index: 0
    lifetimes in seconds:: 3600
    lifetimes in bytes:: 423624704
```

例 7-12 すべての SA アソシエーションの表示

```
switch# show crypto sad domain ipsec
interface: GigabitEthernet4/1
  Crypto map tag: cm10, local addr.10.10.10.1
  protected network:
  local ident (addr/mask): (10.10.10.0/255.255.255.0)
  remote ident (addr/mask): (10.10.10.4/255.255.255.255)
  current_peer: 10.10.10.4
    local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.4
    mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
    current outbound spi: 0x30e000f (51249167), index: 0
    lifetimes in seconds:: 3600
    lifetimes in bytes:: 423624704
    current inbound spi: 0x30e0000 (51249152), index: 0
    lifetimes in seconds:: 3600
    lifetimes in bytes:: 423624704
```

例 7-13 ポリシー データベースに関する情報の表示

```
switch# show crypto spd domain ipsec
Policy Database for interface: GigabitEthernet4/1, direction: Both
# 0:      deny  udp any port eq 500 any
# 1:      deny  udp any any port eq 500
# 2:      permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
# 63:     deny  ip any any
Policy Database for interface: GigabitEthernet4/2, direction: Both
# 0:      deny  udp any port eq 500 any <-----UDP デフォルト エントリ
# 1:      deny  udp any any port eq 500 <-----UDP デフォルト エントリ
# 3:      permit ip 10.10.100.0 255.255.255.0 10.10.100.0 255.255.255.0
# 63:     deny  ip any any <-----クリア テキストのデフォルト
                                           エントリ
```

例 7-14 特定のインターフェイス用の SPD 情報の表示

```
switch# show crypto spd domain ipsec interface gigabitethernet 4/2
Policy Database for interface: GigabitEthernet3/1, direction: Both
# 0:      deny  udp any port eq 500 any
# 1:      deny  udp any any port eq 500
# 2:      permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
# 127:    deny  ip any any
```

例 7-15 特定のインターフェイスの詳細な iSCSI セッション情報の表示

```

switch# show iscsi session detail
Initiator iqn.1987-05.com.cisco:01.9f39f09c7468 (ips-host16.cisco.com)
  Initiator ip addr (s): 10.10.10.5
  Session #1 (index 24)
    Discovery session, ISID 00023d000001, Status active

  Session #2 (index 25)
    Target ibml
    VSAN 1, ISID 00023d000001, TSIH 0, Status active, no reservation
    Type Normal, ExpCmdSN 42, MaxCmdSN 57, Barrier 0
    MaxBurstSize 0, MaxConn 1, DataPDUInOrder Yes
    DataSeqInOrder Yes, InitialR2T Yes, ImmediateData No
    Registered LUN 0, Mapped LUN 0
    Stats:
      PDU: Command: 41, Response: 41
      Bytes: TX: 21388, RX: 0
    Number of connection: 1
    Connection #1
      iSCSI session is protected by IPsec <-----iSCSI セッション保護ステータス
      Local IP address: 10.10.10.4, Peer IP address: 10.10.10.5
      CID 0, State: Full-Feature
      StatSN 43, ExpStatSN 0
      MaxRecvDSLength 131072, our_MaxRecvDSLength 262144
      CSG 3, NSG 3, min_pdu_size 48 (w/ data 48)
      AuthMethod none, HeaderDigest None (len 0), DataDigest None (len 0)
      Version Min: 0, Max: 0
      FC target: Up, Reorder PDU: No, Marker send: No (int 0)
      Received MaxRecvDSLen key: Yes

```

例 7-16 特定のインターフェイス用の FCIP 情報の表示

```

switch# show interface fcip 1
fcip1 is trunking
  Hardware is GigabitEthernet
  Port WWN is 20:50:00:0d:ec:08:6c:c0
  Peer port WWN is 20:10:00:05:30:00:a7:9e
  Admin port mode is auto, trunk mode is on
  Port mode is TE
  Port vsan is 1
  Speed is 1 Gbps
  Trunk vsans (admin allowed and active) (1)
  Trunk vsans (up) (1)
  Trunk vsans (isolated) ()
  Trunk vsans (initializing) ()
  Using Profile id 1 (interface GigabitEthernet2/1)
  Peer Information
    Peer Internet address is 10.10.11.1 and port is 3225
  FCIP tunnel is protected by IPsec <----- FCIP トンネル保護のステータス
  Write acceleration mode is off
  Tape acceleration mode is off
  Tape Accelerator flow control buffer size is 256 KBytes
  IP Compression is disabled
  Special Frame is disabled
  Maximum number of TCP connections is 2
  Time Stamp is disabled
  QOS control code point is 0
  QOS data code point is 0
  B-port mode disabled
  TCP Connection Information
    2 Active TCP connections

```

```

Control connection: Local 10.10.11.2:3225, Remote 10.10.11.1:65520
Data connection: Local 10.10.11.2:3225, Remote 10.10.11.1:65522
2 Attempts for active connections, 0 close of connections
TCP Parameters
Path MTU 1400 bytes
Current retransmission timeout is 200 ms
Round trip time: Smoothed 2 ms, Variance: 1
Advertized window: Current: 124 KB, Maximum: 124 KB, Scale: 6
Peer receive window: Current: 123 KB, Maximum: 123 KB, Scale: 6
Congestion window: Current: 53 KB, Slow start threshold: 48 KB
Current Send Buffer Size: 124 KB, Requested Send Buffer Size: 0 KB
CWM Burst Size: 50 KB
5 minutes input rate 128138888 bits/sec, 16017361 bytes/sec, 7937 frames/sec
5 minutes output rate 179275536 bits/sec, 22409442 bytes/sec, 46481 frames/sec
10457037 frames input, 21095415496 bytes
  308 Class F frames input, 32920 bytes
  10456729 Class 2/3 frames input, 21095382576 bytes
  9907495 Reass frames
  0 Error frames timestamp error 0
63792101 frames output, 30250403864 bytes
  472 Class F frames output, 46816 bytes
  63791629 Class 2/3 frames output, 30250357048 bytes
  0 Error frames

```

例 7-17 スイッチのグローバル IPsec 統計情報の表示

```

switch# show crypto global domain ipsec
IPsec global statistics:
  Number of crypto map sets: 3
  IKE transaction stats: 0 num, 256 max
  Inbound SA stats: 0 num
  Outbound SA stats: 0 num

```

例 7-18 指定したインターフェースの IPsec 統計情報の表示

```

switch# show crypto global domain ipsec interface gigabitethernet 3/1
IPsec interface statistics:
  IKE transaction stats: 0 num
  Inbound SA stats: 0 num, 512 max
  Outbound SA stats: 0 num, 512 max

```

例 7-19 グローバル SA ライフタイム値の表示

```

switch# show crypto global domain ipsec security-association lifetime
Security Association Lifetime: 450 gigabytes/3600 seconds

```

FCIP の設定例

図 7-8 では 1 つの FCIP リンク (トンネル 2) の IPsec の実装に注目しています。トンネル 2 は MDS A と MDS C 間で暗号化データを伝送します。

図 7-8 FCIP のシナリオの IP セキュリティの使用

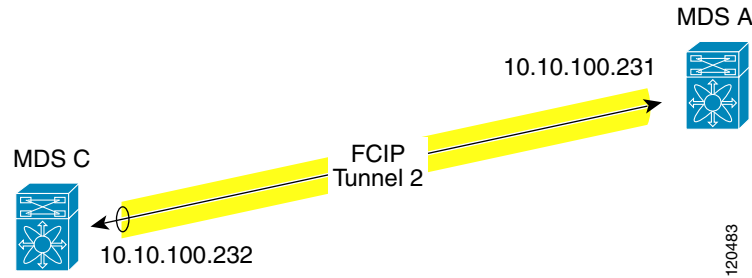


図 7-8 に示す FCIP シナリオで IPsec を設定するには、次の手順を実行します。

ステップ 1 スイッチ MDS A で IKE および IPsec をイネーブルにします。

```
sw10.1.1.100# conf t
sw10.1.1.100(config)# feature crypto ike
sw10.1.1.100(config)# feature crypto ipsec
```

ステップ 2 スイッチ MDS A に IKE を設定します。

```
sw10.1.1.100(config)# crypto ike domain ipsec
sw10.1.1.100(config-ike-ipsec)# key ctct address 10.10.100.232
sw10.1.1.100(config-ike-ipsec)# policy 1
sw10.1.1.100(config-ike-ipsec-policy)# encryption 3des
sw10.1.1.100(config-ike-ipsec-policy)# hash md5
sw10.1.1.100(config-ike-ipsec-policy)# end
sw10.1.1.100#
```

ステップ 3 スイッチ MDS A に ACL を設定します。

```
sw10.1.1.100# conf t
sw10.1.1.100(config)# ip access-list acl1 permit tcp 10.10.100.231 0.0.0.0 10.10.100.232 0.0.0.0
```

ステップ 4 スイッチ MDS A にトランスフォーム セットを設定します。

```
sw10.1.1.100(config)# crypto transform-set domain ipsec tfs-02 esp-aes 128 esp-sha1-hmac
```

ステップ 5 スイッチ MDS A に暗号マップを設定します。

```
sw10.1.1.100(config)# crypto map domain ipsec cmap-01 1
sw10.1.1.100(config-crypto-map-ip)# match address acl1
sw10.1.1.100(config-crypto-map-ip)# set peer 10.10.100.232
sw10.1.1.100(config-crypto-map-ip)# set transform-set tfs-02
sw10.1.1.100(config-crypto-map-ip)# set security-association lifetime seconds 3600
sw10.1.1.100(config-crypto-map-ip)# set security-association lifetime gigabytes 3000
sw10.1.1.100(config-crypto-map-ip)# set pfs group5
sw10.1.1.100(config-crypto-map-ip)# end
sw10.1.1.100#
```

ステップ 6 スイッチ MDS A の暗号マップ セットにインターフェイスをバインドします。

```
sw10.1.1.100# conf t
sw10.1.1.100(config)# int gigabitethernet 7/1
sw10.1.1.100(config-if)# ip addr 10.10.100.231 255.255.255.0
sw10.1.1.100(config-if)# crypto map domain ipsec cmap-01
sw10.1.1.100(config-if)# no shut
sw10.1.1.100(config-if)# exit
sw10.1.1.100(config)#
```

ステップ 7 スイッチ MDS A に FCIP を設定します。

```
sw10.1.1.100(config)# feature fcip
sw10.1.1.100(config)# fcip profile 2
sw10.1.1.100(config-profile)# ip address 10.10.100.231
sw10.1.1.100(config-profile)# int fcip 2
sw10.1.1.100(config-if)# peer-info ipaddr 10.10.100.232
sw10.1.1.100(config-if)# use-profile 2
sw10.1.1.100(config-if)# no shut
sw10.1.1.100(config-if)# end
sw10.1.1.100#
```

ステップ 8 スイッチ MDS A の設定を確認します。

```
sw10.1.1.100# show crypto global domain ipsec security-association lifetime
Security Association Lifetime: 4500 megabytes/3600 seconds

sw10.1.1.100# show crypto map domain ipsec
Crypto Map "cmap-01" 1 ipsec
  Peer = 10.10.100.232
  IP ACL = acl1
    permit ip 10.10.100.231 255.255.255.255 10.10.100.232 255.255.255.255
  Transform-sets: tfs-02,
  Security Association Lifetime: 3000 gigabytes/3600 seconds
  PFS (Y/N): Y
  PFS Group: group5
Interface using crypto map set cmap-01:
  GigabitEthernet7/1

sw10.1.1.100# show crypto transform-set domain ipsec
Transform set: tfs-02 {esp-aes 128 esp-sha1-hmac}
  will negotiate {tunnel}

sw10.1.1.100# show crypto spd domain ipsec
Policy Database for interface: GigabitEthernet7/1, direction: Both
# 0:      deny  udp any port eq 500 any
# 1:      deny  udp any any port eq 500
# 2:      permit ip 10.10.100.231 255.255.255.255 10.10.100.232 255.255.255.255
# 63:     deny  ip any any

sw10.1.1.100# show crypto ike domain ipsec
keepalive 3600

sw10.1.1.100# show crypto ike domain ipsec key
key ctct address 10.10.100.232

sw10.1.1.100# show crypto ike domain ipsec policy
Priority 1, auth pre-shared, lifetime 86300 secs, encryption 3des, hash md5, DH group 1
```

ステップ 9 スイッチ MDS C で IKE および IPsec をイネーブルにします。

```
sw11.1.1.100# conf t
sw11.1.1.100(config)# feature crypto ike
sw11.1.1.100(config)# feature crypto ipsec
```

ステップ 10 スイッチ MDS C に IKE を設定します。

```
sw11.1.1.100(config)# crypto ike domain ipsec
sw11.1.1.100(config-ike-ipsec)# key ctct address 10.10.100.231
sw11.1.1.100(config-ike-ipsec)# policy 1
sw11.1.1.100(config-ike-ipsec-policy)# encryption 3des
sw11.1.1.100(config-ike-ipsec-policy)# hash md5
sw11.1.1.100(config-ike-ipsec-policy)# exit
sw11.1.1.100(config-ike-ipsec)# end
sw11.1.1.100#
```

ステップ 11 スイッチ MDS C に ACL を設定します。

```
sw11.1.1.100# conf t
sw11.1.1.100(config)# ip access-list acl1 permit ip 10.10.100.232 0.0.0.0 10.10.100.231
0.0.0.0
```

ステップ 12 スイッチ MDS C にトランスフォーム セットを設定します。

```
sw11.1.1.100(config)# crypto transform-set domain ipsec tfs-02 esp-aes 128 esp-sha1-hmac
```

ステップ 13 スイッチ MDS C に暗号マップを設定します。

```
sw11.1.1.100(config)# crypto map domain ipsec cmap-01 1
sw11.1.1.100(config-crypto-map-ip)# match address acl1
sw11.1.1.100(config-crypto-map-ip)# set peer 10.10.100.231
sw11.1.1.100(config-crypto-map-ip)# set transform-set tfs-02
sw11.1.1.100(config-crypto-map-ip)# set security-association lifetime seconds 3600
sw11.1.1.100(config-crypto-map-ip)# set security-association lifetime gigabytes 3000
sw11.1.1.100(config-crypto-map-ip)# set pfs group5
sw11.1.1.100(config-crypto-map-ip)# exit
sw11.1.1.100(config)#
```

ステップ 14 スイッチ MDS C のクリプト マップ セットにインターフェイスをバインドします。

```
sw11.1.1.100(config)# int gigabitethernet 1/2
sw11.1.1.100(config-if)# ip addr 10.10.100.232 255.255.255.0
sw11.1.1.100(config-if)# crypto map domain ipsec cmap-01
sw11.1.1.100(config-if)# no shut
sw11.1.1.100(config-if)# exit
sw11.1.1.100(config)#
```

ステップ 15 スイッチ MDS C の FCIP を設定します。

```
sw11.1.1.100(config)# feature fcip
sw11.1.1.100(config)# fcip profile 2
sw11.1.1.100(config-profile)# ip address 10.10.100.232
sw11.1.1.100(config-profile)# int fcip 2
sw11.1.1.100(config-if)# peer-info ipaddr 10.10.100.231
sw11.1.1.100(config-if)# use-profile 2
sw11.1.1.100(config-if)# no shut
sw11.1.1.100(config-if)# exit
sw11.1.1.100(config)# exit
```

ステップ 16 スイッチ MDS C の設定を確認します。

```
sw11.1.1.100# show crypto global domain ipsec security-association lifetime
Security Association Lifetime: 4500 megabytes/3600 seconds

sw11.1.1.100# show crypto map domain ipsec
Crypto Map "cmap-01" 1 ipsec
  Peer = 10.10.100.231
  IP ACL = acl1
    permit ip 10.10.100.232 255.255.255.255 10.10.100.231 255.255.255.255
  Transform-sets: tfs-02,
  Security Association Lifetime: 3000 gigabytes/3600 seconds
  PFS (Y/N): Y
  PFS Group: group5
Interface using crypto map set cmap-01:
  GigabitEthernet1/2

sw11.1.1.100# show crypto spd domain ipsec
Policy Database for interface: GigabitEthernet1/2, direction: Both
# 0:      deny  udp any port eq 500 any
# 1:      deny  udp any any port eq 500
# 2:      permit ip 10.10.100.232 255.255.255.255 10.10.100.231 255.255.255.255
# 63:     deny  ip any any
```

```

sw11.1.1.100# show crypto sad domain ipsec
interface: GigabitEthernet1/2
  Crypto map tag: cmap-01, local addr.10.10.100.232
  protected network:
  local ident (addr/mask): (10.10.100.232/255.255.255.255)
  remote ident (addr/mask): (10.10.100.231/255.255.255.255)
  current_peer: 10.10.100.231
    local crypto endpt.: 10.10.100.232, remote crypto endpt.: 10.10.100.231
    mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
  current outbound spi: 0x38f96001 (955867137), index: 29
  lifetimes in seconds:: 3600
  lifetimes in bytes:: 3221225472000
  current inbound spi: 0x900b011 (151040017), index: 16
  lifetimes in seconds:: 3600
  lifetimes in bytes:: 3221225472000

sw11.1.1.100# show crypto transform-set domain ipsec
Transform set: tfs-02 {esp-aes 128 esp-sha1-hmac}
  will negotiate {tunnel}

sw11.1.1.100# show crypto ike domain ipsec
keepalive 3600

sw11.1.1.100# show crypto ike domain ipsec key

key ctct address 10.10.100.231

sw11.1.1.100# show crypto ike domain ipsec policy
Priority 1, auth pre-shared, lifetime 86300 secs, encryption 3des, hash md5, DH
group 1

sw11.1.1.100# show crypto ike domain ipsec sa
Tunn  Local Addr          Remote Addr          Encr  Hash  Auth Method  Lifetime
-----
1*    10.10.100.232[500]    10.10.100.231[500]  3des  md5   preshared key  86300
-----
NOTE: tunnel id ended with * indicates an IKEv1 tunnel

```

ステップ 17 スイッチ MDS A の設定を確認します。

```

sw10.1.1.100# show crypto sad domain ipsec
interface: GigabitEthernet7/1
  Crypto map tag: cmap-01, local addr.10.10.100.231
  protected network:
  local ident (addr/mask): (10.10.100.231/255.255.255.255)
  remote ident (addr/mask): (10.10.100.232/255.255.255.255)
  current_peer: 10.10.100.232
    local crypto endpt.: 10.10.100.231, remote crypto endpt.: 10.10.100.232
    mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
  current outbound spi: 0x900b01e (151040030), index: 10
  lifetimes in seconds:: 3600
  lifetimes in bytes:: 3221225472000
  current inbound spi: 0x38fe700e (956198926), index: 13
  lifetimes in seconds:: 3600
  lifetimes in bytes:: 3221225472000

sw10.1.1.100# show crypto ike domain ipsec sa
Tunn Local Addr          Remote Addr          Encr  Hash  Auth Method  Lifetime
-----
1 10.10.100.231[500]    10.10.100.232[500]  3des  md5   preshared key  86300

```

これで、スイッチ MDS A および MDS C の両方に IPsec を設定しました。

iSCSI の設定例

図 7-9 では、サブネット 12.12.1/24 のホストと MDS A の間の iSCSI セッションに注目しています。**auto-peer** オプションを使用して、サブネット 12.12.1.0/24 からのホストが、MDS スイッチのギガビットイーサネットポート 7/1 へ接続しようとしたときに、ホストと MDS の間に SA が作成されます。**auto-peer** を使用して、1 つの暗号マップだけが、同じサブネット内のすべてのホストの SA を作成するために必要です。**auto-peer** がないと、ホストごとに 1 つの暗号マップが必要です。

図 7-9 iSCSI のエンドツーエンド IPsec

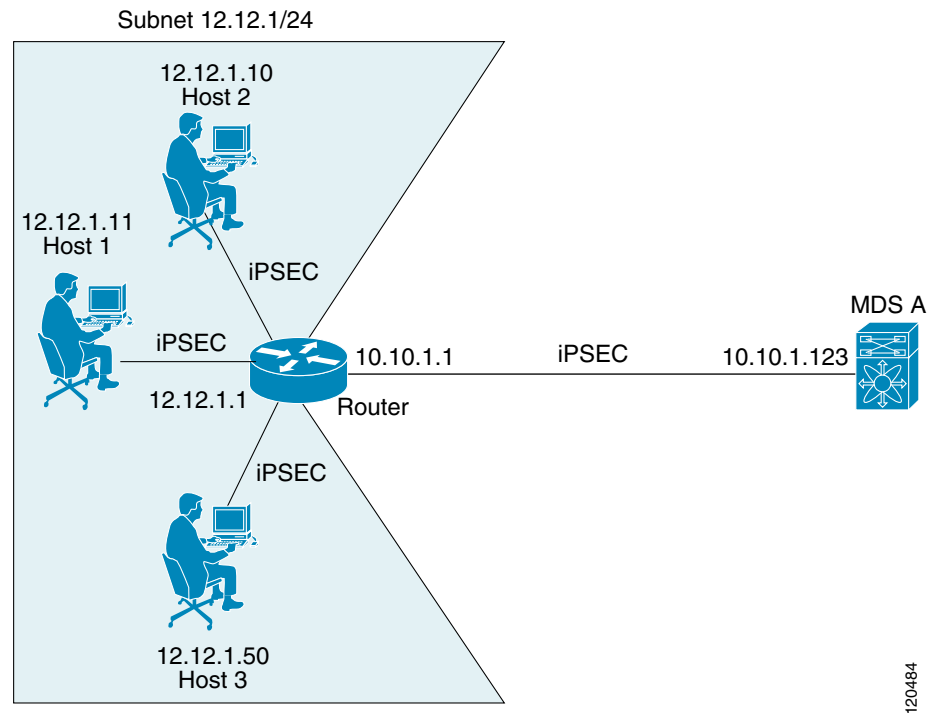


図 7-9 に示す iSCSI シナリオで IPsec を設定するには、次の手順を実行します。

ステップ 1 スイッチ MDS A に ACL を設定します。

```
sw10.1.1.100# conf t
sw10.1.1.100(config)# ip access-list acl1 permit tcp 10.10.1.0 0.0.0.255 range port 3260
3260 12.12.1.0 0.0.0.255
```

ステップ 2 スイッチ MDS A にトランスフォーム セットを設定します。

```
sw10.1.1.100(config)# crypto transform-set domain ipsec tfs-01 esp-3des esp-md5-hmac
```

ステップ 3 スイッチ MDS A に暗号マップを設定します。

```
sw10.1.1.100(config)# crypto map domain ipsec cmap-01 1
sw10.1.1.100(config-crypto-map-ip)# match address acl1
sw10.1.1.100(config-crypto-map-ip)# set peer auto-peer
sw10.1.1.100(config-crypto-map-ip)# set transform-set tfs-01
sw10.1.1.100(config-crypto-map-ip)# end
sw10.1.1.100#
```

ステップ 4 スイッチ MDS A の暗号マップ セットにインターフェイスをバインドします。

```
sw10.1.1.100# conf t
sw10.1.1.100(config)# int gigabitethernet 7/1
sw10.1.1.100(config-if)# ip address 10.10.1.123 255.255.255.0
sw10.1.1.100(config-if)# crypto map domain ipsec cmap-01
sw10.1.1.100(config-if)# no shut
sw10.1.1.100(config-if)# end
sw10.1.1.100#
```

Cisco MDS IPsec および iSCSI 機能を使用して、MDS A に IPsec を設定しました。

デフォルト設定

表 7-3 に、IKE パラメータのデフォルト設定を示します。

表 7-3 IKE パラメータのデフォルト値

パラメータ	デフォルト
IKE	ディセーブル
IKE バージョン	IKE version 2
IKE 暗号化アルゴリズム	3DES
IKE ハッシュ アルゴリズム	SHA
IKE 認証方式	事前共有キーを使用。
IKE DH グループ識別名	グループ 1
IKE ライフタイム アソシエーション	86,400 00 秒(24 時間)
各ピアの IKE キープアライブ タイム (v2)	3,600 秒(1 時間)

表 7-4 に、IPsec パラメータのデフォルト設定を示します。

表 7-4 IPsec パラメータのデフォルト値

パラメータ	デフォルト
IPsec	ディセーブル
トラフィックへの IPsec の適用	拒否(deny): クリア テキストを許可
IPsec PFS	ディセーブル
IPsec グローバル ライフタイム (トラフィック量)	450 GB
IPsec グローバル ライフタイム (タイム)	3,600 秒(1 時間)