



CHAPTER 7

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。

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。

この章では、次の事項について説明します。

- 「IPSec ネットワーク セキュリティの概要」 (P.7-1)
- 「IPSec の前提条件」 (P.7-20)
- 「注意事項と制限」 (P.7-20)
- 「デフォルト設定」 (P.7-22)
- 「FCIP Wizard を使用した IPSec のイネーブル化」 (P.7-23)
- 「IPSec および IKE の手動設定」 (P.7-25)
- 「クリプトの設定」 (P.7-28)
- 「IPSec のフィールドの説明」 (P.7-31)

IPSec ネットワーク セキュリティの概要

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せん。
- 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。

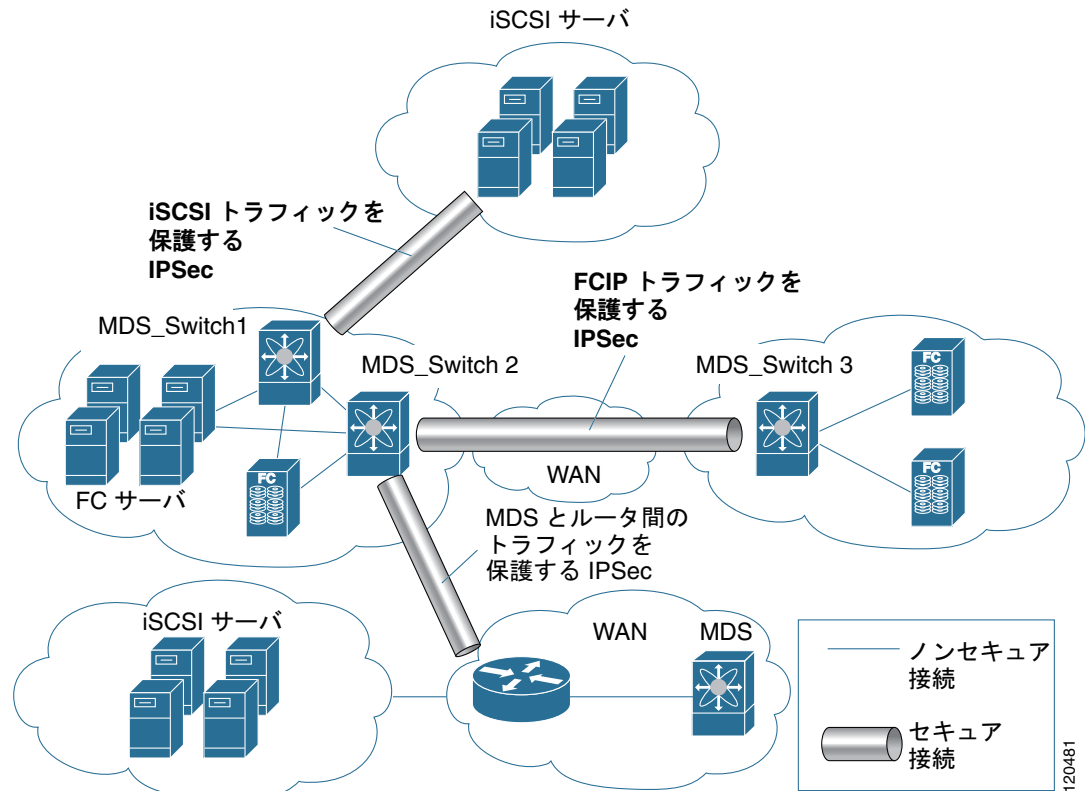


(注)

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



ここで説明する内容は、次のとおりです。

- 「IKE の概要」 (P.7-4)
- 「IPsec の互換性」 (P.7-4)
- 「IPsec および IKE に関する用語」 (P.7-5)
- 「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」 (P.7-6)
- 「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」 (P.7-6)
- 「IPsec デジタル証明書のサポートの概要」 (P.7-7)
- 「IKE 初期設定の概要」 (P.7-10)
- 「IKE ドメインの概要」 (P.7-10)
- 「IKE トンネルの概要」 (P.7-10)
- 「IKE ポリシー ネゴシエーションの概要」 (P.7-10)
- 「オプションの IKE パラメータの設定」 (P.7-12)

- 「クリプト IPv4-ACL の概要」 (P.7-12)
- 「IPsec のトランスフォーム セットの概要」 (P.7-15)
- 「クリプト マップ エントリの概要」 (P.7-16)
- 「SA ライフタイム ネゴシエーションの概要」 (P.7-17)
- 「AutoPeer オプションの概要」 (P.7-18)
- 「PFS の概要」 (P.7-18)
- 「クリプト マップ セット インターフェイスの適用の概要」 (P.7-19)
- 「IPsec のメンテナンス」 (P.7-19)
- 「グローバル ライフタイム値」 (P.7-19)

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。

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 Release 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 Release 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

- セキュリティ アソシエーションのバンドル
- セキュリティ アソシエーションの手動設定
- クリプト マップにおけるホスト単位のセキュリティ アソシエーション 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せん。

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トリに関する、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 バリエント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 バリエントです。
- Secure Hash Algorithm (SHA-1)：HMAC バリエントを使用するハッシュ アルゴリズム。
- 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。DH は、セッション キーを確立するために IKE 内で使用されます。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) : HMAC バリエーションを使用するハッシュ アルゴリズム。
- 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の概要

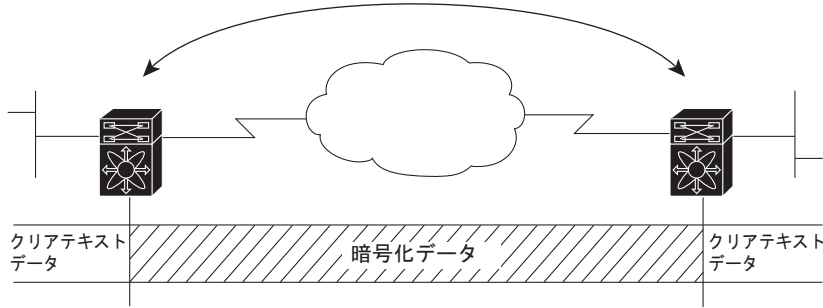
ここでは、認証局 (CA) およびデジタル証明書を使用した認証の利点について説明します。

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。

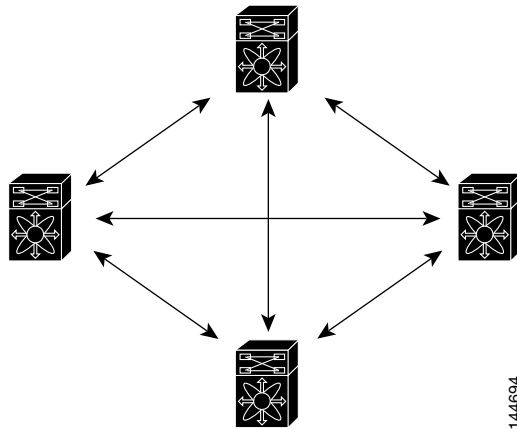
図 7-2 CA およびデジタル証明書を使用しない 2 台の IPsec スイッチ



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

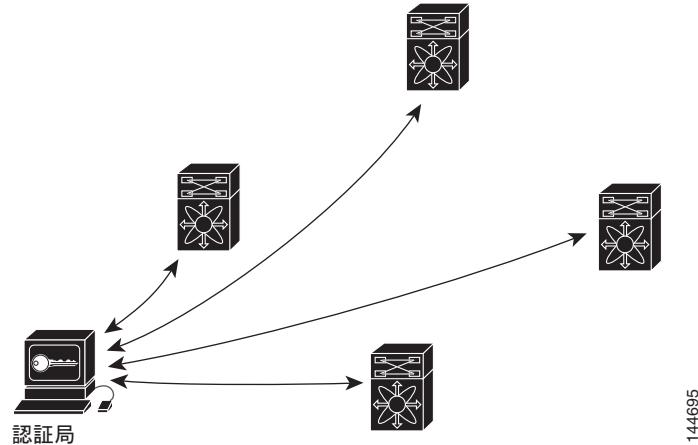


CA およびデジタル証明書を使用した IPsec の実装

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、両デバイスは相互に認証するために、証明書およびデジタル署名データを交換します。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 によるデバイスのダイナミックな認証



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。

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。DCNM-SAN 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 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。DCNM-SAN 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 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	sha
	MD5 (HMAC バリエーション)	md5	
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 または MD5、DH グループ 2	3DES、SHA-1
Cisco iSCSI 発信側 (Linux プラットフォームの Free Swan IPsec 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、リモートピアはプライオリティ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。

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」(P.7-26) 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

通常的环境ではスイッチが 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。

クリプト IPv4-ACL の概要

IP ACL (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。

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。

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 7-5 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 7-5 ミラー イメージ設定の IPsec 処理

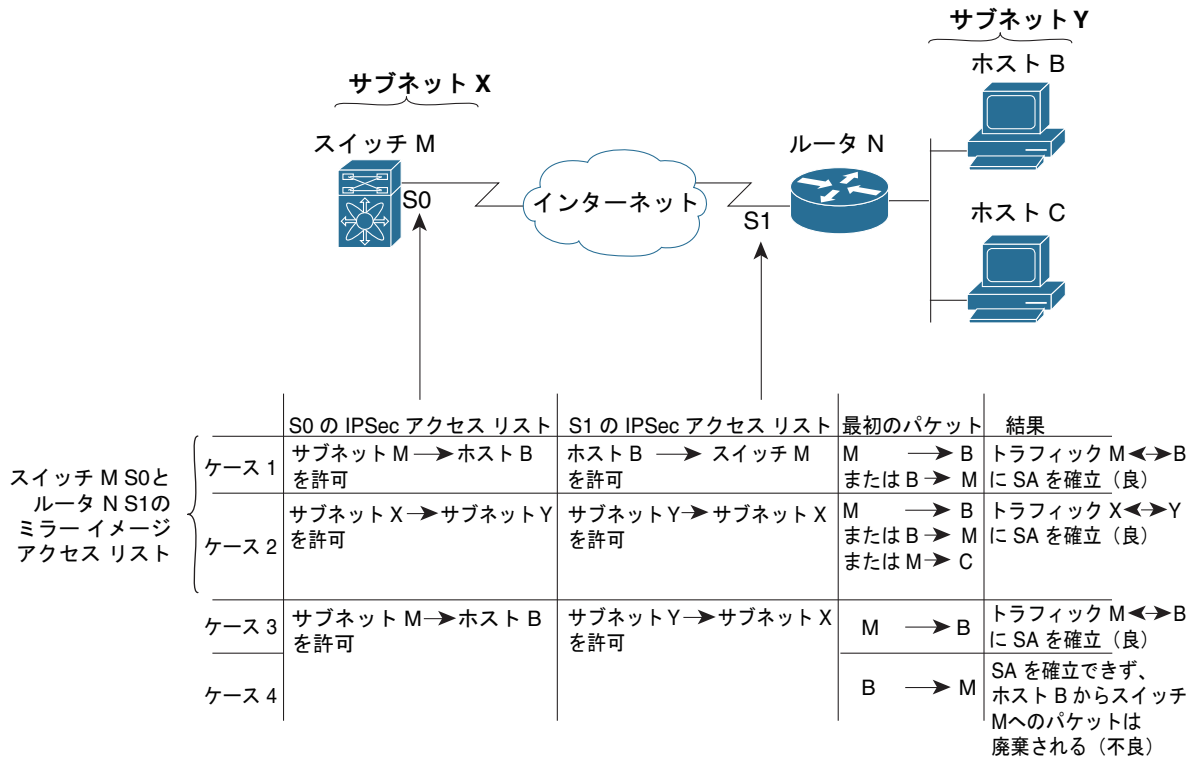


図 7-5 に示すように、2 つのピアのクリプト IPv4-ACL が相互のミラー イメージである場合、想定どおりに IPsec SA を確立できます。ただし、IPv4-ACL が相互のミラー イメージでない場合にも、IPsec SA を確立できることがあります。たとえば、図 7-5 のケース 3 および 4 のように、一方のピアの IPv4-ACL エントリが他方のピアの IPv4-ACL エントリのサブセットになっている場合です。IPsec SA の確立は、IPsec にとって非常に重要です。SA が存在しないと IPsec は機能せず、クリプト IPv4-ACL の条件と一致する packets 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 packets 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。

120486

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）。

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
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
	MD5 (HMAC バリエント)	esp-md5-hmac
	AES-XCBC-MAC	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 または MD5、 DH グループ 2	3DES、SHA-1
Cisco iSCSI 発信側 (Linux プラットフォームの Free Swan IPsec 実装)	3DES、MD5、DH グループ 1	3DES、MD5

クリプト 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 セットの作成が完了すると、次のように、IPsec SA のさまざまな部分を組み合わせたクリプト 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ず。

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場合には、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 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。

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。

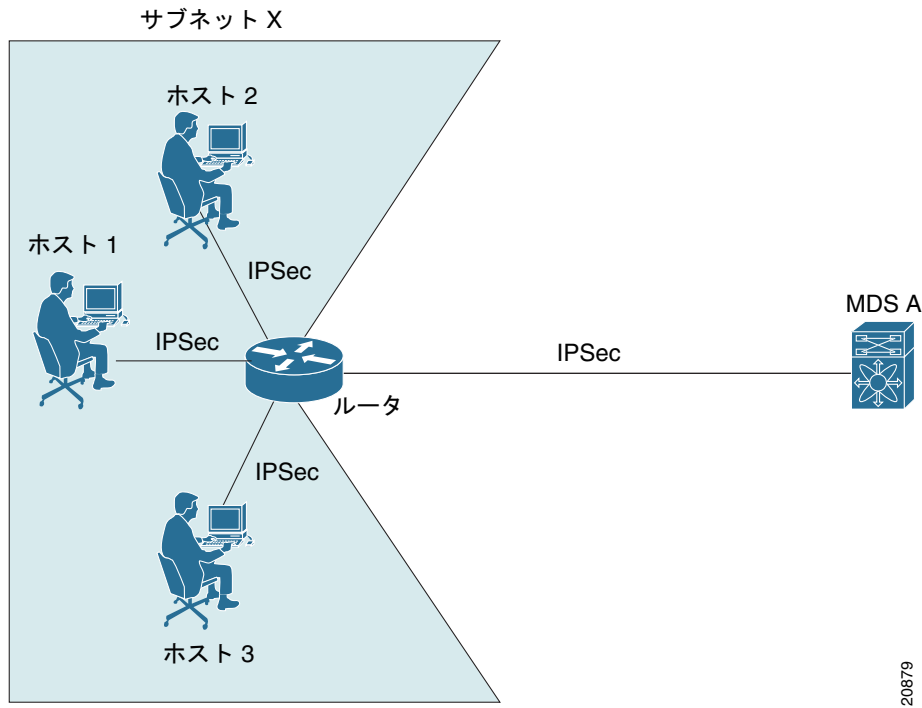
グローバル ライフタイム値の詳細については、「[グローバル ライフタイム値](#)」(P.7-19) を参照してください。

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 7-6 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。

図 7-6 auto-peer オプションを使用した iSCSI のエンドツーエンド IPsec



120879

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。

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。

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。

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。

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」(P.7-10) を参照してください。

注意事項と制限

ここでは、IPsec ネットワーク セキュリティに関する注意事項と制限事項について説明します。

- 「クリプト IPv4-ACL の注意事項」(P.7-20)
- 「クリプト マップ設定の注意事項」(P.7-22)

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트리ごとに、異なる IPv4-ACL を使用する必要があります。

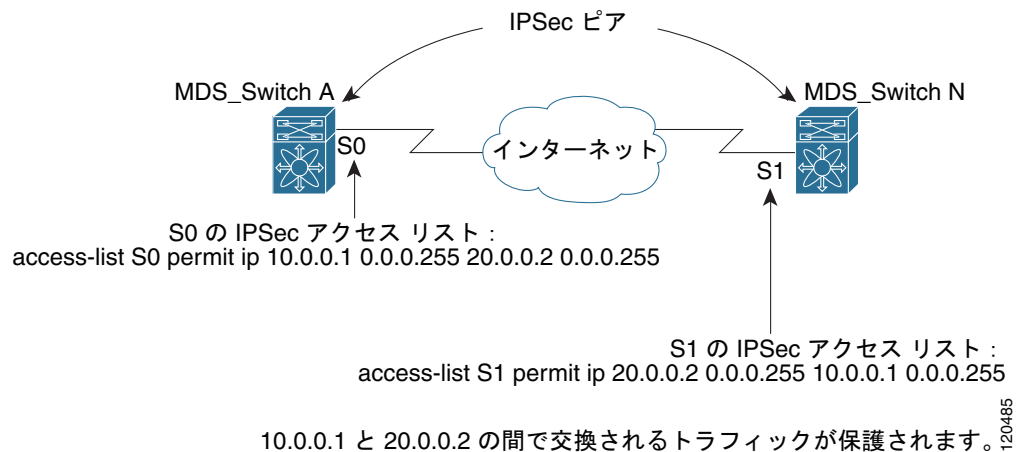
- インバウンドおよびアウトバウンドトラフィックは、同じアウトバウンド IPv4-ACL に対して評価されます。したがって、IPv4-ACL の条件は、スイッチからの発信トラフィックに対して順方向に、スイッチへの着信トラフィックに対して逆方向に適用されます。
- クリプト マップ エントリに割り当てられた各 IPv4-ACL フィルタは、1 つのセキュリティ ポリシー エントリと同等です。IPsec 機能は、各 MPS-14/2 モジュールおよび Cisco MDS 9216i スイッチに対して、最大 120 のセキュリティ ポリシー エントリをサポートします。
- スイッチ A の S0 イ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時に、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 7-7 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 7-7 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ないと見なされ、廃棄されます。
- 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。

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。

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	設定不可 (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)

FCIP Wizard を使用した IPsec のイネーブル化

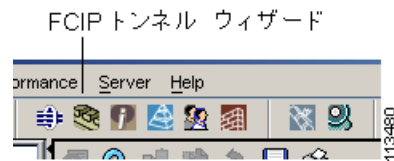
DCNM-SAN では、FCIP Wizard を使用する FCIP 設定の一環として IPsec および IKE をイネーブルにし、設定することによって、これらの機能を簡単に設定できます。

手順の詳細

FCIP Wizard を使用して IPsec をイネーブルにする手順は、次のとおりです。

- ステップ 1** ツールバーの [FCIP Wizard] アイコンをクリックします。

図 7-8 FCIP Wizard



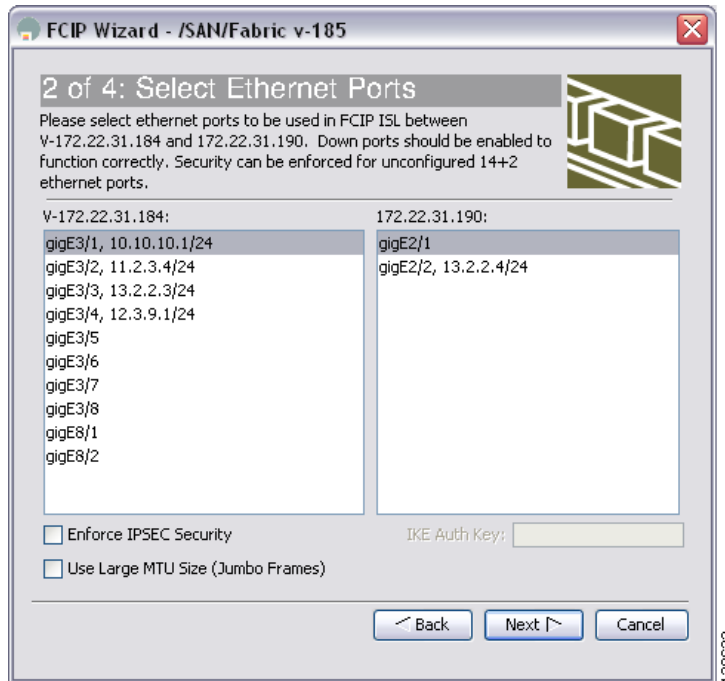
- ステップ 2** FCIP リンクのエンドポイントとして動作するスイッチを選択し、[Next] ボタンをクリックします。



(注) FCIP リンク上に IPsec を設定するには、これらのスイッチに MPS-14/2 モジュールが搭載されている必要があります。

- ステップ 3** FCIP リンクを形成する各 MPS-14/2 モジュール上のギガビットイーサネットポートを選択します。
- ステップ 4** [Enforce IPSEC Security] チェックボックスをオンにし、IKE Auth Key を設定します (図 7-9 を参照)。

図 7-9 FCIP リンク上での IPsec のイネーブル化



- ステップ 5** [Next] をクリックします。[Specify Tunnel Properties] ダイアログボックスに、TCP 接続特性が表示されます。
- ステップ 6** FCIP リンク上の TCP 接続の最小および最大帯域幅、および往復時間を設定します。[Measure] ボタンをクリックし、ギガビットイーサネットエンドポイント間の往復時間を測定します。
- ステップ 7** [Enable Write Acceleration] チェックボックスをオンにして、FCIP リンク上の FCIP 書き込みアクセラレーションをイネーブルにします。
- ステップ 8** [Enable Optimum Compression] チェックボックスをオンにして、FCIP リンク上の IP 圧縮をイネーブルにします。
- ステップ 9** FCIP トンネル パラメータを設定するには、[Next] をクリックします。
- ステップ 10** Port VSAN を nontrunk/auto に設定し、トランク トンネルの許可 VSAN リストを設定します。FCIP リンクの [Trunk Mode] を選択します。『*IP Services Configuration Guide, Cisco DCNM for SAN*』を参照してください。
- ステップ 11** FCIP リンクを作成するには、[Finish] をクリックします。FCIP リンクを作成しないで FCIP Wizard を終了するには、[Cancel] をクリックします。

手順の詳細

IPsec および IKE がイネーブルかどうかを確認する手順は、次のとおりです。

- ステップ 1** [Physical Attributes] ペインで、[Switches] > [Security] を展開し、[IPSEC] を選択します。
- ステップ 2** デフォルトは、[Control] タブです。[Status] カラムで、IPsec を適用するスイッチがイネーブルに設定されているかどうかを確認します。
- ステップ 3** [Physical Attributes] ペインで、[Switches] > [Security] を展開し、[IKE] を選択します。

- ステップ 4** デフォルトは、[Control] タブです。[Status] カラムで、IKE を適用するスイッチがイネーブルに設定されているかどうかを確認します。

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。

FCIP Wizard を使用していない場合は、「[FCIP Wizard を使用した IPsec のイネーブル化](#)」(P.7-23) を参照してください。

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。

前提条件

IKE 設定の完了後、IPsec を設定します。

手順の詳細

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。

ここで説明する内容は、次のとおりです。

- 「[IPsec の使用方法](#)」(P.7-25)
- 「[IKE ポリシーの設定](#)」(P.7-26)
- 「[ピアのキープアライブ タイムの設定](#)」(P.7-26)
- 「[発信側バージョンの設定](#)」(P.7-27)
- 「[IKE トンネルまたはドメインのクリア](#)」(P.7-27)
- 「[SA のリフレッシュ](#)」(P.7-27)

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」(P.7-25) 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、『*IP Services Configuration Guide, Cisco DCNM for SAN*』を参照してください)。

IKE ポリシーの設定

手順の詳細

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。

- ステップ 1** [Switches] > [Security] を展開し、[IKE] を選択します。
- ステップ 2** [Policies] タブをクリックします。
[Information] ペインに既存の IKE ポリシーが表示されます。
- ステップ 3** [Create Row] をクリックして、IKE ポリシーを作成します。
- ステップ 4** このスイッチの [Priority] を入力します。1 ~ 255 の値を入力できます。1 が最優先です。
- ステップ 5** 暗号化、ハッシュ、認証、および DH グループのフィールドで、適切な値を選択します。
- ステップ 6** ポリシーのライフタイムを入力します。600 ~ 86400 秒のライフタイムを入力できます。
- ステップ 7** このポリシーを作成するには、[Create] をクリックします。変更を保存しないで終了するには、[Close] をクリックします。

ピアのキープアライブ タイムの設定

手順の詳細

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。

- ステップ 1** [Switches] > [Security] を展開し、[IKE] を選択します。
- ステップ 2** [Global] タブをクリックします。
- ステップ 3** [KeepAliveInterval (sec)] の値 (秒数) を入力します。秒単位のキープアライブ インターバルは、管理対象デバイスの IKE エンティティがすべてのピアとともに、この概念的な行に対応するドメイン オブジェクト インタープリテーション (DOI) に使用するものです。
- ステップ 4** [Apply Changes] をクリックして変更を保存します。

発信側バージョンの設定

手順の詳細

発信側バージョンを設定する手順は、次のとおりです。

-
- ステップ 1 [Switches] > [Security] を展開し、[IKE] を選択します。
 - ステップ 2 [Initiator Version] タブをクリックします。
[Information] ペインにピアの既存の発信側バージョンが表示されます。
 - ステップ 3 [Create Row] をクリックして、発信側バージョンを作成します。
 - ステップ 4 IKE プロトコル発信側を設定するリモート ピアのスイッチを選択します。
 - ステップ 5 リモート ピアの IP アドレスを入力します。
IKEv1 は、リモート ピアに接続するときに使用される IKE プロトコル バージョンです。
 - ステップ 6 この発信側バージョンを作成するには、[Create] をクリックします。変更を保存しないで終了するには、[Close] をクリックします。
-

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。

手順の詳細

すべての IKE トンネルまたはドメインをクリアする手順は、次のとおりです。

-
- ステップ 1 [Physical Attributes] ペインで、[Switches] > [Security] を展開し、[IKE] を選択します。
 - ステップ 2 [Information] ペインで [Tunnels] タブをクリックします。
IKE トンネルが表示されます。
 - ステップ 3 [Action] カラムをクリックし、[Clear] を選択して、トンネルをクリアします。
-

SA のリフレッシュ

手順の詳細

IKEv2 設定の変更後に SA をリフレッシュする手順は、次のとおりです。

-
- ステップ 1 [Physical Attributes] ペインで、[Switches] > [Security] を展開し、[IKE] を選択します。
 - ステップ 2 [Information] ペインで、[Pre-Shared AuthKey] タブをクリックします。

ステップ 3 [Refresh Values] をクリックします。

クリプトの設定

ここでは、次の内容について説明します。

- 「トランスフォーム セットの設定」 (P.7-28)
- 「クリプト マップ エントリの作成」 (P.7-29)
- 「SA ライフタイムの設定」 (P.7-29)
- 「PFS の設定」 (P.7-30)
- 「クリプト マップ セットの適用」 (P.7-30)
- 「グローバル ライフタイム値の設定」 (P.7-30)

トランスフォーム セットの設定

手順の詳細

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。

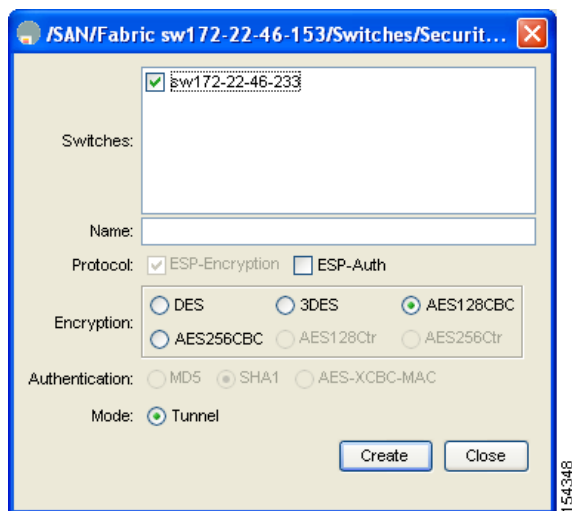
ステップ 1 [Physical Attributes] ペインで、[Switches] > [Security] を展開し、[IPSEC] を選択します。

ステップ 2 [Information] ペインで [Transform Set] タブをクリックします。

ステップ 3 [Create Row] をクリックします。

[Create IPSEC] ダイアログボックスが表示されます (図 7-10 を参照)。

図 7-10 IPsec の作成



ステップ 4 トランスフォーム セットの作成ダイアログボックスで、トランスフォーム セットを作成するスイッチを選択します。

- ステップ 5 トランスフォーム セットの名前とプロトコルを指定します。
- ステップ 6 暗号化および認証アルゴリズムを選択します。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。
- ステップ 7 [Create] をクリックしてトランスフォーム セットを作成するか、[Close] をクリックします。

クリプト マップ エントリの作成

手順の詳細

必須のクリプト マップ エントリを作成する手順は、次のとおりです。

- ステップ 1 [Physical Attributes] ペインで、[Switches] > [Security] を展開し、[IPSEC] を選択します。
- ステップ 2 [CryptoMap Set Entry] タブを選択します。
- ステップ 3 (任意) [Create Row] をクリックして、クリプト マップ エントリを作成します。
- ステップ 4 設定または変更するスイッチを選択します。クリプト マップを作成する場合には、クリプト マップの setName およびプライオリティを設定します。
- ステップ 5 ドロップダウン リストから、このクリプト マップの IPv4-ACL Profile および TransformSetIdList を選択します。
- ステップ 6 (任意) [AutoPeer] チェックボックスを選択します。または、クリプト マップを作成する場合は、ピアのアドレスを設定します。「AutoPeer オプションの概要」(P.7-18) を参照してください。
- ステップ 7 適切な PFS を選択します。「PFS の概要」(P.7-18) を参照してください。
- ステップ 8 Lifetime および LifeSize を設定します。「SA ライフタイム ネゴシエーションの概要」(P.7-17) を参照してください。
- ステップ 9 クリプト マップを作成する場合には、[Create] をクリックします。既存のクリプト マップを変更する場合には、[Apply Changes] をクリックします。

SA ライフタイムの設定

手順の詳細

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。

- ステップ 1 [Physical Attributes] ペインで、[Switches] > [Security] を展開し、[IPSEC] を選択します。
- ステップ 2 [CryptoMap Set Entry] タブを選択します。
- ステップ 3 スクロールして、ダイアログボックスの右半分を表示します。
- ステップ 4 [Life Time(sec)] カラムをダブルクリックして、値を変更します。
- ステップ 5 [Apply Changes] をクリックして変更を保存します。

PFS の設定

手順の詳細

PFS 値を設定する手順は、次のとおりです。

-
- ステップ 1 [Physical Attributes] ペインで、[Switches] > [Security] を展開し、[IPSEC] を選択します。
 - ステップ 2 [CryptoMap Set Entry] タブを選択します。
 - ステップ 3 [PFS] カラムのドロップダウンリストをクリックして、適切な値を選択します。
 - ステップ 4 [Apply Changes] をクリックして変更を保存します。
-

クリプト マップ セットの適用

手順の詳細

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。

-
- ステップ 1 [Physical Attributes] ペインで、[Switches] > [Security] を展開し、[IPSEC] を選択します。
 - ステップ 2 [Interfaces] タブをクリックします。
 - ステップ 3 設定するスイッチおよびインターフェイスを選択します。
 - ステップ 4 [CryptomapSetName] フィールドに、このインターフェイスに適用するクリプト マップの名前を入力します。
 - ステップ 5 選択したインターフェイスにクリプト マップを適用するには、[Create] をクリックします。クリプト マップを適用しないでダイアログボックスを閉じるには、[Close] をクリックします。
-

グローバル ライフタイム値の設定

手順の詳細

SA ライフタイムを設定する手順は、次のとおりです。

-
- ステップ 1 [Physical Attributes] ペインで、[Switches] > [Security] を選択し、[IPSEC] を選択します。
 - ステップ 2 [Information] ペイン内に IPsec 設定が表示されます。
 - ステップ 3 [Global] タブをクリックします。
 - ステップ 4 [Life Time(sec)] カラムをダブルクリックして、値を編集します。
 - ステップ 5 [Apply Changes] をクリックして変更を保存します。
-

IPsec のフィールドの説明

ここでは、IPsec のフィールドについて説明します。

IPsec

フィールド	説明
[Interface]、 [CryptomapName]	管理対象エンティティのインターフェイスへ、クリプト マップ セットのバインディングを設定します。

IKE グローバル

フィールド	説明
RemIdentity	管理対象デバイスの IKE エンティティがすべてのピアとともに、この概念的な行に対応する DOI に使用するキープアライブ インターバルを秒単位で表示します。
Key	管理対象デバイスの IKE エンティティがすべてのピアとともに、この概念的な行に対応する DOI に使用するキープアライブのタイプを表示します。

IKE 事前共有認証キー

フィールド	説明
KeepAliveInterval (sec)	この事前共有キーがローカル エンティティ上で設定されたピアのフェーズ 1 ID。
IdentityType	この概念的な行に対応するピアの認証に使用される事前共有認証キー。

IKE ポリシー

フィールド	説明
Priority	この ISAKMP ポリシー エントリのプライオリティ。小さい値を持つポリシーは、同じ DOI 内の高い値を持つポリシーよりも優先されます。
Encr	この ISAKMP ポリシー仕様によって指定された暗号化トランスフォーム。このポリシー項目を使用するインターネット キー交換 (IKE) トンネル設定は、指定された暗号化トランスフォームを使用して ISAKMP PDU を保護します。

IPsec のフィールドの説明

フィールド	説明
Hash	この ISAKMP ポリシー仕様によって指定されたハッシュ トランスフォーム。このポリシー項目を使用する IKE トンネル設定は、指定されたハッシュ トランスフォームを使用して ISAKMP PDU を保護します。
Auth	この ISAKMP ポリシー仕様によって指定されたピア認証方式。このポリシー エンティティを選択してピアとネゴシエートする場合、ローカル エンティティは、このオブジェクトによって指定された方法でピアを認証します。
DHGroup	メイン モードでの Diffie-Hellman 交換に使用される Oakley グループを指定します。このポリシー項目を選択してメイン モードを IKE ピアとネゴシエートする場合、ローカル エンティティは、このオブジェクトによって指定されたグループを選択して、ピアとの Diffie-Hellman 交換を実行します。
Lifetime (sec)	このポリシー仕様を使用して生成された IKE トンネルのライフタイムを秒単位で指定します。

IKE 発信側バージョン

フィールド	説明
Address	この概念的な行に対応するリモート ピアのアドレス。このオブジェクトは、 <code>cicIkeCfgInitiatorStatus</code> の対応する値がアクティブに等しい間は変更できません。
Version	<code>cicIkeCfgInitiatorPAddr</code> で指定されたリモート ピアに接続するとき使用される IKE プロトコルバージョン。このオブジェクトは、 <code>cicIkeCfgInitiatorStatus</code> の対応する値がアクティブに等しい間は変更できません。

IKE トンネル

フィールド	説明
LocalAddress	フェーズ 1 トンネルのローカル エンドポイントのアドレス。
RemoteAddress	フェーズ 1 トンネルのリモート エンドポイントのアドレス。
AuthMethod	この概念的な行に対応する制御トンネルのフェーズ 1 ネゴシエーションで使用される認証方式。
Action	このトンネルに適用するアクション。 <code>clear</code> の場合は、このトンネルがクリアされます。 <code>re-key</code> の場合は、このトンネルに対してキーの再生成が強制されます。このオブジェクトの読み取り後に、値 <code>none</code> が返されます。

IPSEC グローバル

フィールド	説明
Lifetime (sec)	グローバル ポリシーとして IPsec トンネルに割り当てられたデフォルト ライフタイム (秒単位) (特定のクリプト マップ定義で上書きされる可能性がある)。
Lifesize (KB)	グローバル ポリシーとして IPsec トンネルに割り当てられたデフォルト ライフ サイズ (KB) (ただし、特定のクリプト マップ定義で上書きされる場合を除く)。

IPSEC トランスフォーム セット

フィールド	説明
Id	トランスフォーム セットを一意に識別するトランスフォーム セットのシーケンス番号です。異なるトランスフォーム セットは、異なるシーケンス番号を持つ必要があります。
Protocol	このトランスフォーム セットのフェーズ 2 セキュリティ プロトコルのスイートを表します。
ESP Encryption	ESP 暗号化に使用されるトランスフォームを表します。
ESP Authentication	ESP プロトコルによる完全性チェックを実装するために使用されるトランスフォームを表します。
Mode	トランスフォーム セットのカプセル化モードを表します。

IPSEC クリプト マップ セット エントリ

フィールド	説明
IpFilter	このクリプト マップ エントリを使用して保護される IP プロトコル フィルタを指定します。長さ 0 のストリング値を持つ場合は、無効または適用不可です。
TransformSetIdList	この CipsStaticCryptomapEntry のメンバである cipsXformSetId のリスト。このオブジェクトの値は、0 個以上の 4 オクテット ストリングを連結したものです。各 4 オクテット ストリングは 1 つの 32 ビット cipsXformSetId 値を含みます (ネットワーク バイト オーダー)。長さ 0 のストリング値は、このリストにメンバが含まれないことを意味します。
AutoPeer	true の場合は、トンネルの作成中、宛先アドレスがピア アドレスであると見なされます。
Peer Address	このクリプト マップ エントリが現在接続されているピアの IP アドレス。
PFS	このポリシー項目に起因してインスタンス化されたトンネルで完全転送秘密 (PFS) を使用するかどうかを識別し、使用する場合は、Oakley のどのグループを使用するかを識別します。

フィールド	説明
LifeTime	この IPsec ポリシー エントリを使用して作成された IPsec セキュリティ アソシエーション (SA) のライフタイムを指定します。
Lifesize Value	この IPsec ポリシー エントリを使用して作成された IPsec SA のライフサイズ (伝送される可能性がある最大トラフィック (バイト数)) を識別します。この IPsec ポリシー エントリを使用してセキュリティ アソシエーション (SA) が作成された場合は、このオブジェクトの値をライフサイズとして取得します。

IPSEC インターフェイス

フィールド	説明
CryptomapName	スタティック クリプト マップ テーブルのインデックス。この文字列の値は、クリプト マップ セットを定義したときに NMS によって割り当てられた名前の文字列です。
InterfaceList	クリプト マップに属するインターフェイス。

IPSEC トンネル

フィールド	説明
Local Address	IPsec フェーズ 2 トンネルのローカル エンドポイントの IP アドレス。
RemoteAddress	IPsec フェーズ 2 トンネルのリモート エンドポイントの IP アドレスのタイプ。
ESP Encryption	IPsec フェーズ 2 トンネルのアウトバウンド セキュリティ アソシエーションによって使用される暗号化アルゴリズム。
ESP Encryption KeySize	ceipSecTunOutSaEncryptAlgo により示されるアルゴリズムとともに使用されるネゴシエーション キーのキー サイズ (ビット単位)。DES および 3DES のキー サイズは、それぞれ 56 および 168 です。AES の場合は、ネゴシエートされたキー サイズを示します。
ESP Authentication	IPsec フェーズ 2 トンネルにおけるインバウンドのカプセル化セキュリティ ペイロード (ESP) プロトコルのセキュリティ アソシエーションによって使用される認証アルゴリズム。
LifeSize (KB)	IPsec フェーズ 2 トンネルのネゴシエートされたライフ サイズ (KB 単位)。
LifeTime (sec)	IPsec フェーズ 2 トンネルのネゴシエートされたライフタイム (秒単位)。トンネルを手動で設定した場合、この MIB 要素の値は 0 となっている必要があります。
Action	MIB テーブル行のステータス。