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実現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 Internet Key Exchange（IKE; インターネット キー エクスチェンジ）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併用できますが、最初の実装には IPSec プロトコルが使用されます。IKE は、IPSec ピア認証を提供し、IPSec Security Association（SA; セキュリティ アソシエーション）をネゴシエートし、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。

この章の内容は、次のとおりです。

IPSec の概要

（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。

インターネットなどの保護されていないネットワーク上で重要な情報を伝達する場合は、IPSec によってセキュリティを確保します。IPSec はネットワーク レイヤで機能し、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。

- データ機密保護：IPSec 送信側で、ネットワーク上で送信するパケットを事前に暗号化できます。
- データ整合性：IPSec 受信側で、IPSec 送信側から送信されたパケットを認証し、送信中にデータが改ざんされていないかを確認できます。
- データ発信元認証：IPSec 受信側で、送信された IPSec パケットの発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 を使用すると、データの参照、改ざん、またはスプーフィングの危険を伴わずに、パブリック ネットワーク上でデータを送信できます。これにより、イントラネット、エクストラネット、リモート ユーザ アクセスを含む、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）などのアプリケーションの使用が可能になります。

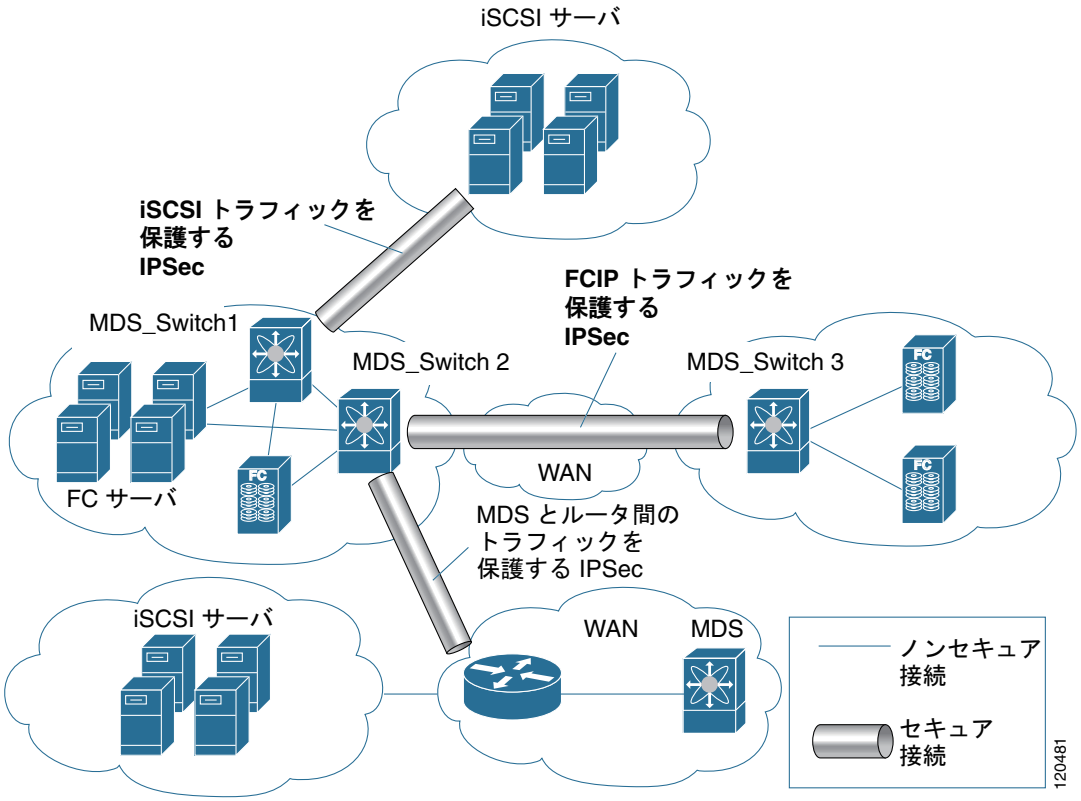
Cisco NX-OS ソフトウェアに実装された IPSec は、Encapsulating Security Payload（ESP）プロトコルをサポートしています。このプロトコルはデータをカプセル化して保護し、データ プライバシー サービス、オプションのデータ認証、およびオプションのリプレイ防止サービスを提供します。

（注） ESP プロトコルは、既存の Transmission Control Protocol（TCP; 伝送制御プロトコル）/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ユニット（Maximum Transmission Unit; 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 を使用する際、IPS モジュール（14+2 LC または 18+4 LC のいずれか）上の各ギガビット イーサネット インターフェイスをそれぞれ独自の IP サブネットに設定する必要があります。同じ IP サブネット内の IP アドレスまたはネットワークマスクが設定されたギガビット イーサネット インターフェイスが複数存在する場合、IKE パケットを適切なピアに送信できず、IPSec トンネルが起動しません。

図 7-1 に、いくつかの 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 でリプレイ防止サービスを提供できます。
- 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を実現します。

（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」（P.7-13）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」（P.7-13）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 Fabric Manager 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

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

- Cisco 18/4 ポート Multi-Service Module（MSM-18/4）モジュールおよび MDS 9222i Module-1 モジュール
- Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタの 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。
  - Authentication Header（AH; 認証ヘッダー）
  - 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

- セキュリティ アソシエーション 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復号化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 Database（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。
  - Security Parameter Index（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）：Message Digest 5（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ポート 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、トランスポート 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クス、宛先アドレス/マスクまたはプレフィクス長、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; 完全転送秘密）：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、前のキーおよび以降のキーに影響はありません。これは、以降のキーの取得元が前のキーではないからです。
- 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が判別されます。
  - 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; 高度暗号化規格）：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。
- Data Encryption Standard（DES; データ暗号化規格）：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 Initialization Vector（IV; 初期ベクトル）が必要です。IV は IPSec パケット内で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、配布が制限されています。米国以外の地域でイメージをインストールする場合には、輸出許可が必要です。米国政府の規制によって、発注が拒否されたり、遅れたりすることがあります。詳細については、製品を購入された代理店に問い合わせるか、export@cisco.com に電子メールで問い合わせてください。

- Message Digest 5（MD5）：HMAC バリアントを使用するハッシュ アルゴリズム。HMAC は認証データに使用されるキー付きのハッシュ バリアントです。
- Secure Hash Algorithm（SHA-1）：HMAC バリア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; メッセージ認証コード）。

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。
- 高度暗号化規格（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。
- データ暗号化規格（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、暗号化を開始する初期ベクトル（IV）が必要です。IV は IPSec パケット内で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、配布が制限されています。米国以外の地域でイメージをインストールする場合には、輸出許可が必要です。米国政府の規制によって、発注が拒否されたり、遅れたりすることがあります。詳細については、製品を購入された代理店に問い合わせるか、export@cisco.com に電子メールで問い合わせてください。

- Message Digest 5（MD5）：HMAC バリアントを使用するハッシュ アルゴリズム。HMAC は認証データに使用されるキー付きのハッシュ バリアントです。
- Secure Hash Algorithm（SHA-1）：HMAC バリアント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

ここでは、Certificate Authority（CA; 認証局）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。

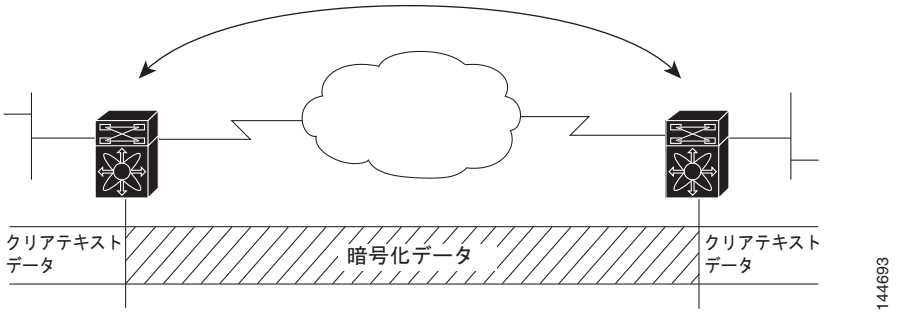
CA およびデジタル証明書を使用しない IPSec の実装

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（Rivest, Shamir, Adelman [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。

図 7-2 では、各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 IP 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。

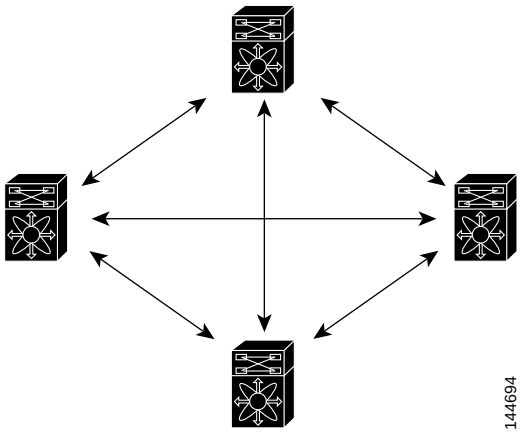
図 7-2　CA およびデジタル証明書を使用しない 2 台の IPSec スイッチ



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

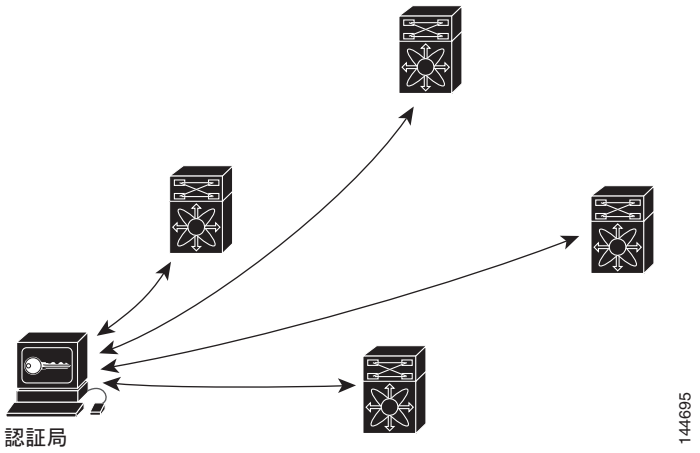


CA およびデジタル証明書を使用した IPSec の実装

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ダイナミックに認証できます。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、デバイスをダイナミック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、Certificate Revocation List（CRL; 証明書失効リスト）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には、スイッチの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）（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限り、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。

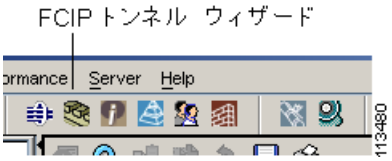
FCIP ウィザードを使用した IPSec の設定

Fabric Manager では、FCIP ウィザードを使用する 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。

Fabric Manager の FCIP ウィザードを使用して 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 7-5　　FCIP ウィザード



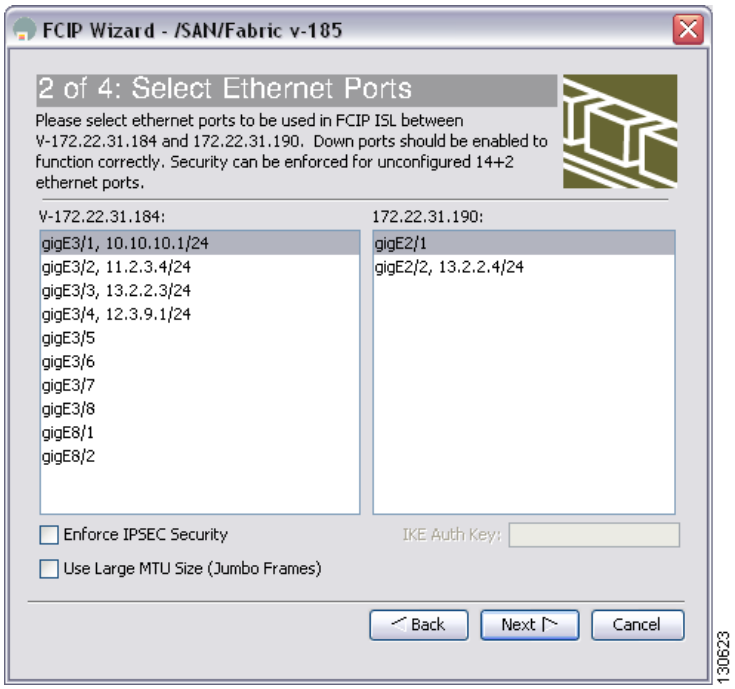
ステップ 2　FCIP リンクのエンドポイントとして動作するスイッチを選択し、[Next] ボタンをクリックします。

（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て、IKE Auth Key を設定します（図 7-6 を参照）。

図 7-6　FCIP リンク上での IPSec のイネーブル化



ステップ 5　[Next] ボタンをクリックします。[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] ボタンをクリックします。

ステップ 10　[Port VSAN] を [nontrunk/auto] に設定し、トランク トンネルに許可される Virtual Storage Area Network（VSAN; 仮想ストレージ エリア ネットワーク）のリストを設定します。この FCIP リンクに [Trunk Mode] を選択します。『*Cisco Fabric Manager IP Services Configuration Guide*』を参照してください。

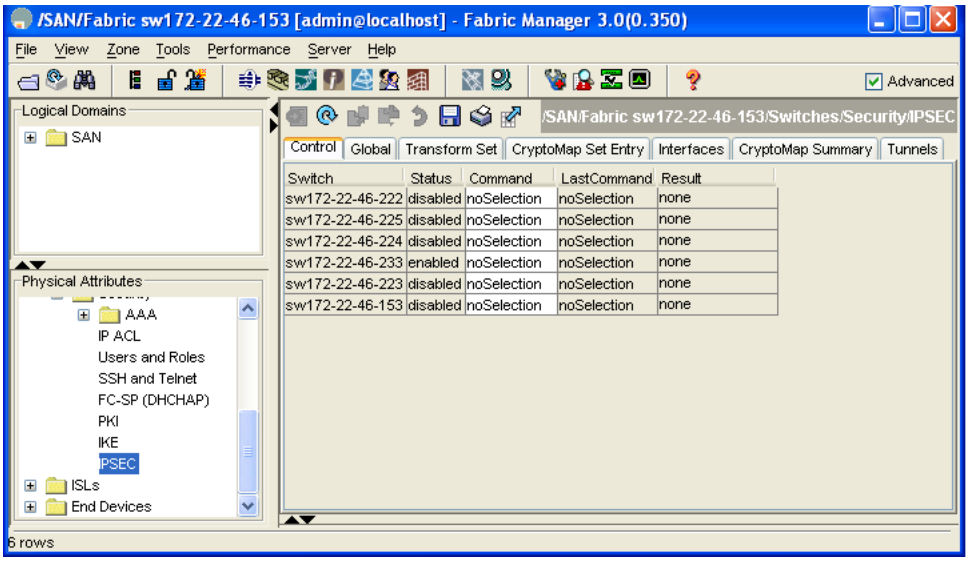
ステップ 11　FCIP リンクを作成するには、[Finish] ボタンをクリックします。FCIP リンクを作成しないで FCIP ウィザードを終了するには、[Cancel] ボタンをクリックします。

Fabric Manager を使用して、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。

[Information] ペインに IPSec の設定が表示されます（図 7-7 を参照）。

図 7-7　IPSec の設定

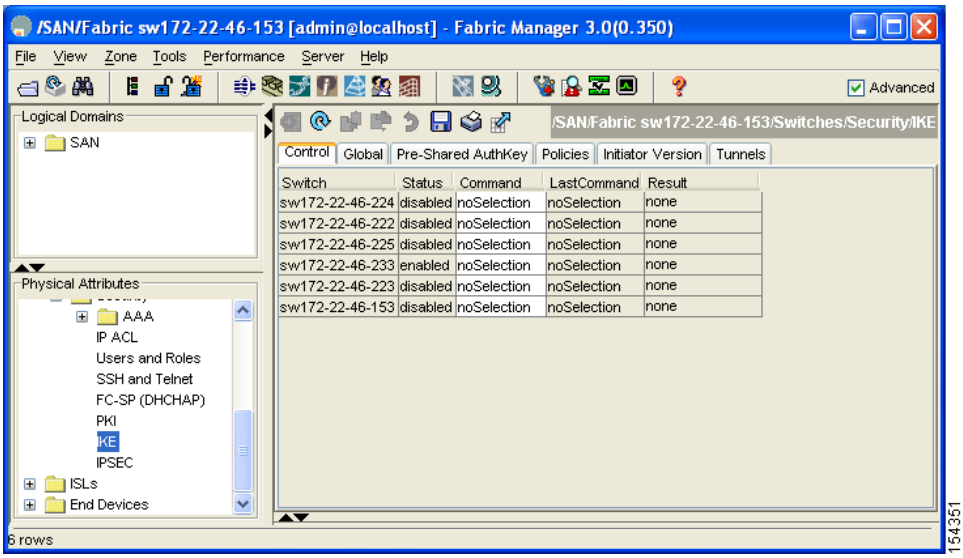


ステップ 2　[Control] タブがデフォルトです。[Status] カラムで、IPSec を適用するスイッチがイネーブルに設定されているかどうかを確認します。

ステップ 3　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IKE] を選択します。

[Information] ペインに IKE の設定が表示されます（図 7-8 を参照）。

図 7-8　IKE の設定



ステップ 4　[Control] タブがデフォルトです。[Status] カラムで、IKE を変更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、FCIP ウィザードを使用しない場合、IPSec および IKE を手動で設定する手順について説明します。「FCIP ウィザードを使用した IPSec の設定」（P.7-10）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。

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 Access Control List（ACL; 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

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 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 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 ポリシーは、IKE ネゴシエーション実行中に使用されるセキュリティ 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 バリアント）	**sha**	**sha**
	MD5（HMAC バリアント）	**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するピアからリモート ピアに対してすべてのポリシーが送信されると、リモート ピアが一致するポリシーを検索します。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。リモート ピアは、一致しているポリシーが見つかるまで、プライオリティの順に（最優先が最初）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ると、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。

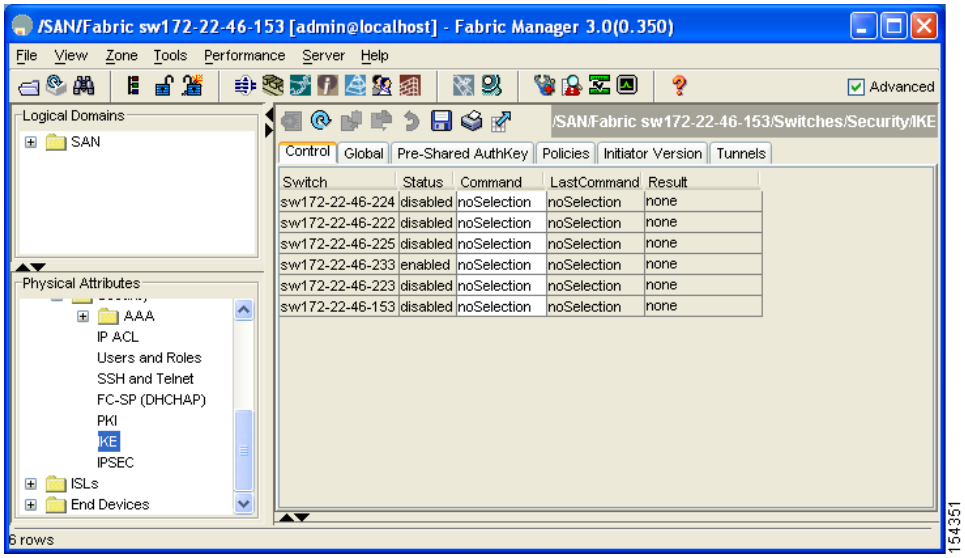
IKE ポリシーの設定

Fabric Manager を使用して IKE ポリシー ネゴシエーション パラメータを設定する手順は、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。

[Information] ペインに IKE の設定が表示されます（図 7-9 を参照）。

図 7-9　IKE の設定



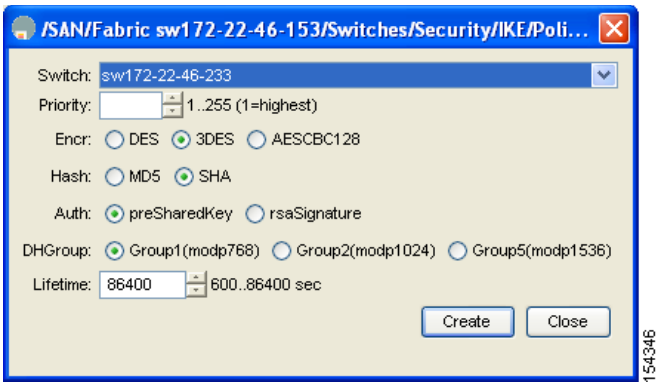
ステップ 2　[Policies] タブをクリックします。

[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] アイコンをクリックして、IKE ポリシーを作成します。

[Create Policy] 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　IKE の作成



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] ボタンをクリックします。変更内容を保存しないで終了するには、[Close] ボタンをクリックします。

（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。

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.7-15）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　通常の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。

ここで説明する内容は、次のとおりです。

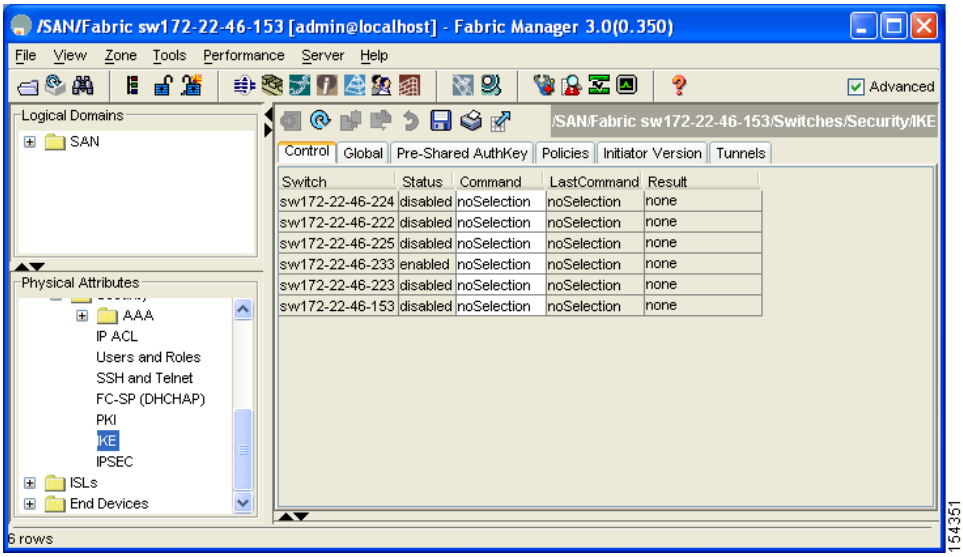
ピアのキープアライブ タイムの設定

Fabric Manager を使用して、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。

[Information] ペインに IKE の設定が表示されます（図 7-11 を参照）。

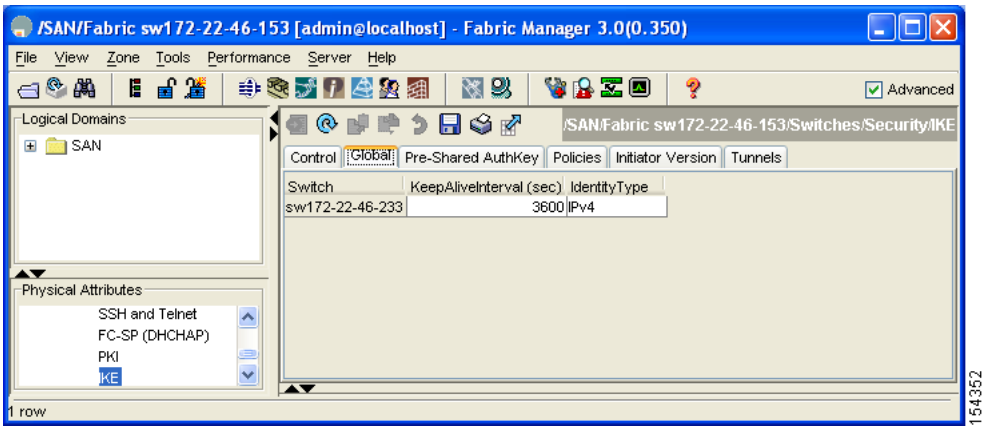
図 7-11　IKE の設定



ステップ 2　[Global] タブを選択します。

[Information] ペインに特定の IKE プロトコルのグローバル統計情報が表示されます（図 7-12 を参照）。

図 7-12　[IKE Global] タブの情報



ステップ 3　[KeepAliveInterval (sec)] に値（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 Domain of Interpretation（DOI; 解釈領域）に使用するものです。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

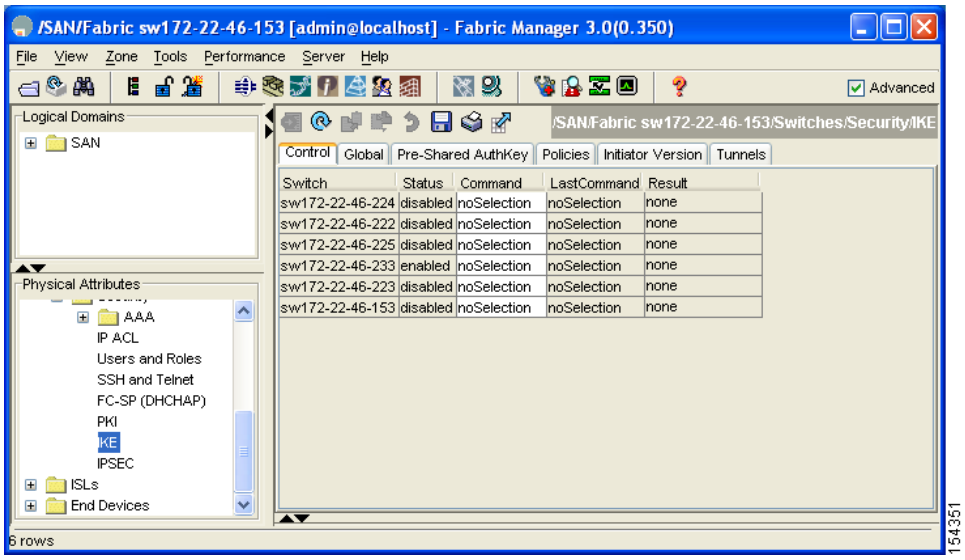
発信側バージョンの設定

Fabric Manager を使用して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。

[Information] ペインに IKE の設定が表示されます（図 7-13 を参照）。

図 7-13　IKE の設定



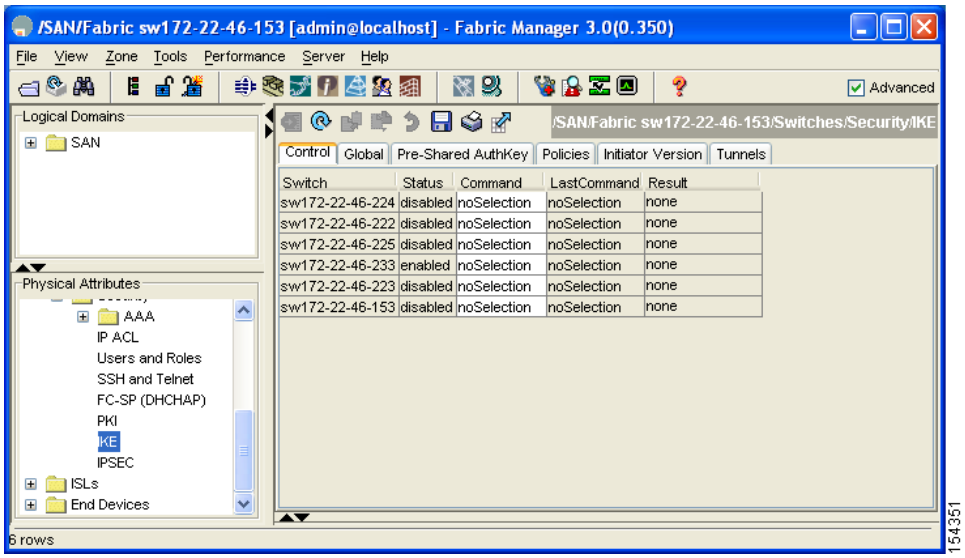
ステップ 2　[Initiator Version] タブを選択します。

[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] アイコンをクリックして、発信側バージョンを作成します。

[Create Initiator Version] ダイアログボックスが表示されます（図 7-14 を参照）。

図 7-14　[Create Initiator Version] ダイアログボックス



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] ボタンをクリックします。変更内容を保存しないで終了するには、[Close] ボタンをクリックします。

IKE トンネルまたはドメインのクリア

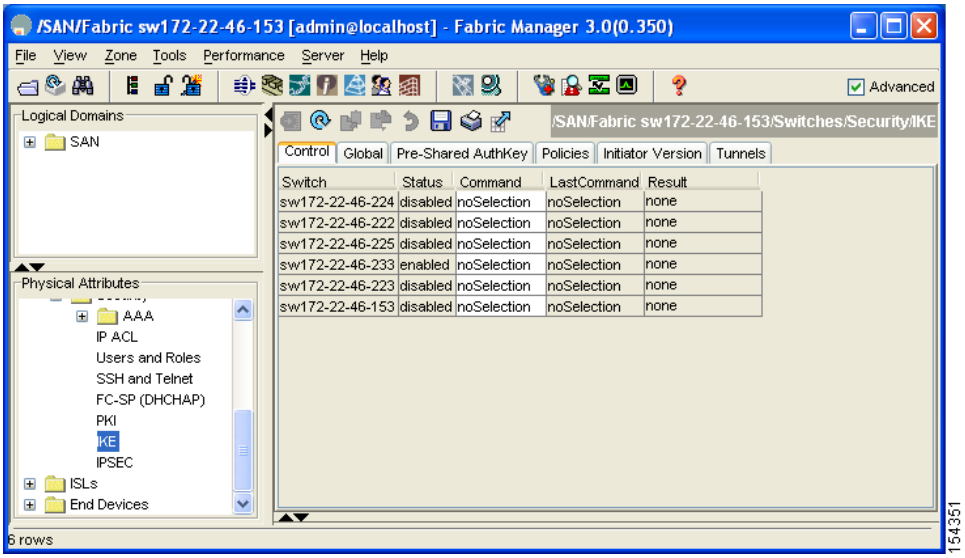
IKE 設定に IKE トンネル ID を指定していない場合、既存のすべての IKE ドメイン接続をクリアできます。

Fabric Manager を使用して、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。

[Information] ペインに IKE の設定が表示されます（図 7-15 を参照）。

図 7-15　IKE の設定



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] ボタンを選択して、トンネルをクリアします。

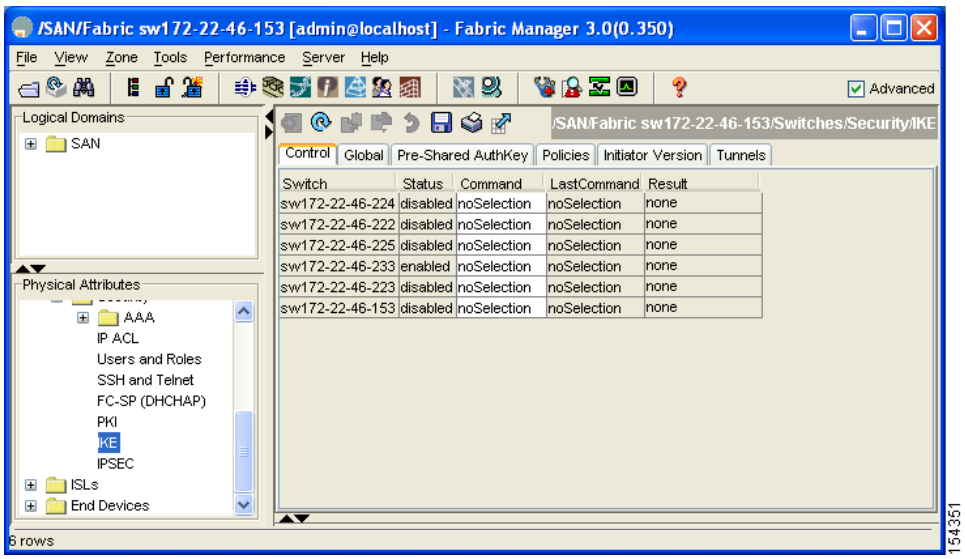
SA のリフレッシュ

Fabric Manager を使用して、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。

IKE の設定が表示されます（図 7-16 を参照）。

図 7-16　IKE の設定



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 IPv4-ACL

IP ACL（IPv4-ACL）は、すべての Cisco MDS 9000 ファミリ 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 のアクセス制御リストの設定」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したりできます。

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

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 によって保護するアウトバウンド トラフィックを選択する（permit = 保護を適用）。
- 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。
- インバウンド トラフィックを処理して、IPSec で保護されていたはずのトラフィックをフィルタリングして除外し、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。

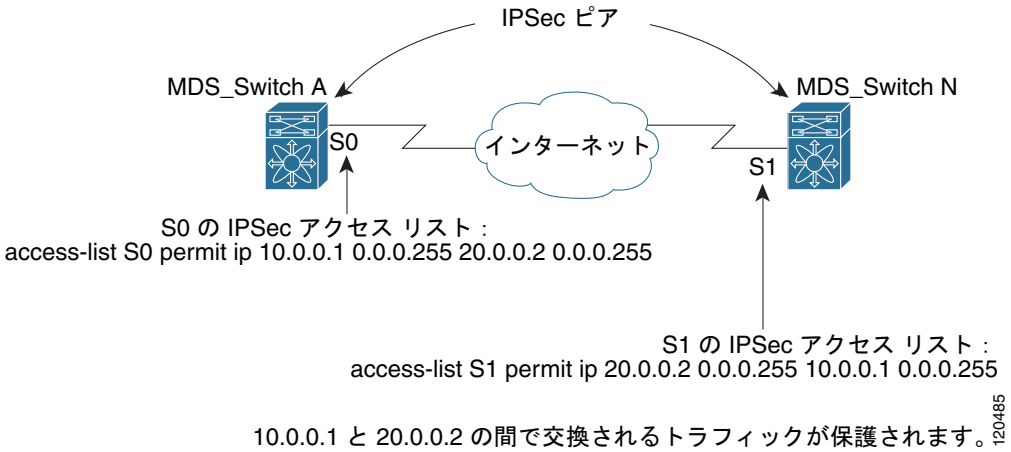
- IPSec 機能が考慮するのは、送信元/宛先 IPv4 アドレスとサブネット マスク、プロトコル、および 1 つのポート番号だけです。IPSec では、IPv6 はサポートされません。

  （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。
- 図 7-17 では、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 7-17　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。
- 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、Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）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。

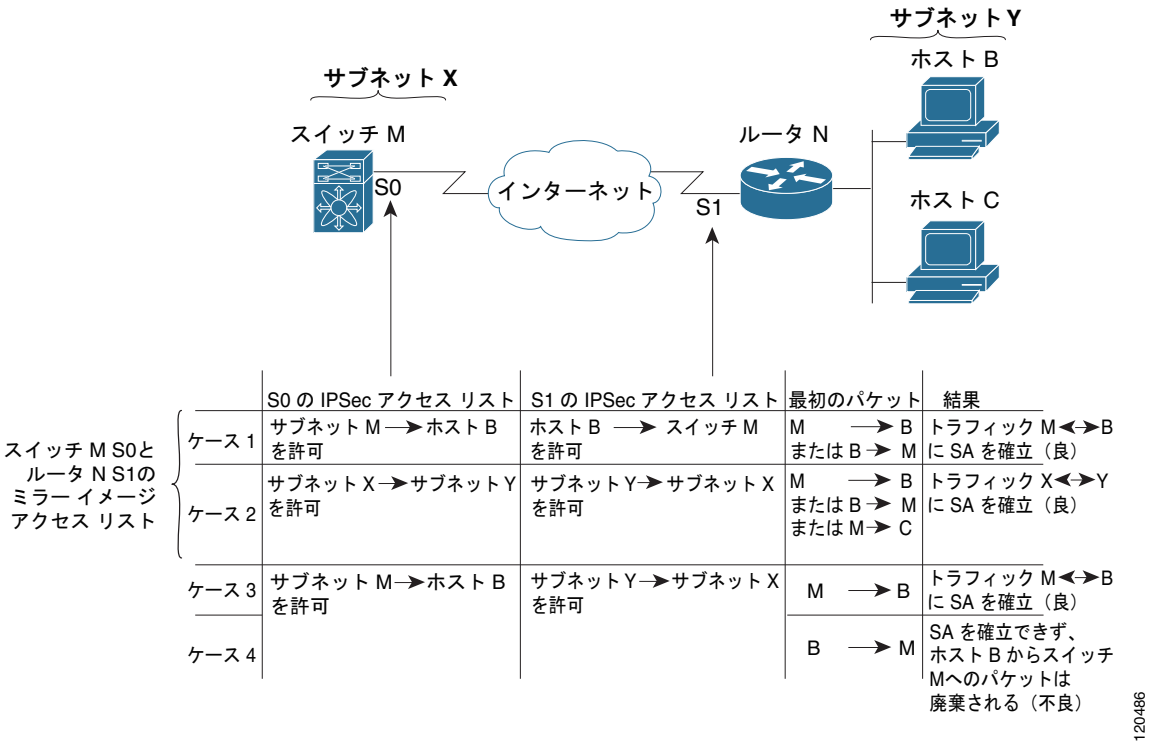
ミラー イメージ クリプト IPv4-ACL

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 7-18 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 7-18　ミラー イメージ設定の IPSec 処理



		S0 の IPSec アクセス リスト	S1 の IPSec アクセス リスト	最初のパケット	結果
スイッチ M S0とルータ N S1のミラー イメージ アクセス リスト	ケース 1	サブネット M → ホスト B を許可	ホスト B → スイッチ M を許可	M → B または B → M	トラフィック M ↔ B に SA を確立（良）
	ケース 2	サブネット X → サブネット Y を許可	サブネット Y → サブネット X を許可	M → B または B → M または M → C	トラフィック X ↔ Y に SA を確立（良）
	ケース 3	サブネット M → ホスト B を許可	サブネット Y → サブネット X を許可	M → B	トラフィック M ↔ B に SA を確立（良）
	ケース 4			B → M	SA を確立できず、ホスト B からスイッチ M へのパケットは廃棄される（不良）

図 7-18 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 7-18 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、Network Time Protocol（NTP; ネットワーク タイム プロトコル）、エコー、エコー応答用のパケットなど、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。

保護するパケットは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、保護対象外とする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

クリプト IPv4-ACL の作成については、第 5 章「IPv4 および IPv6 のアクセス制御リストの設定」を参照してください。

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、セキュリティ プロトコルおよびアルゴリズムの特定の組み合わせを表します。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、クリプト マップ エントリに 1 つまたは複数のトランスフォーム セットを指定できます。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 セキュリティ アソシエーションの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一のトランスフォーム 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 セキュリティ アソシエーションの一部として、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 セットの定義を変更すると、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内容が適用されます。変更内容は既存のセキュリティ アソシエーションには適用されませんが、新規のセキュリティ アソシエーション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には、セキュリティ アソシエーション データベースのすべてまたは一部をクリアします。

（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 バリアント）	**esp-sha1-hmac**
	MD5（HMAC バリアント）	**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

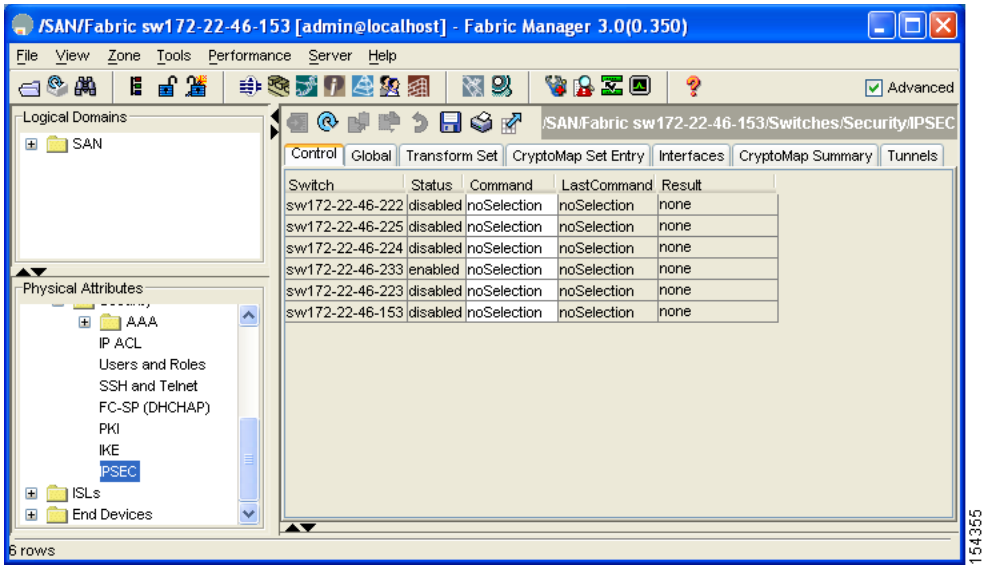
トランスフォーム セットの設定

Fabric Manager を使用してトランスフォーム 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。

IPSec の設定が表示されます（図 7-19 を参照）。

図 7-19　IPSec の設定

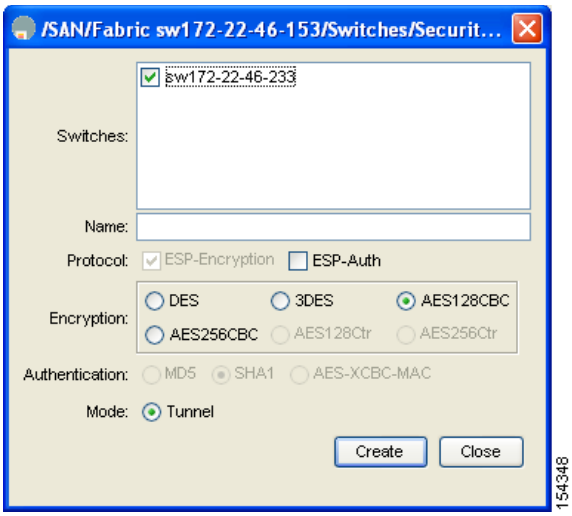


ステップ 2　[Information] ペインで [Transform Set] タブをクリックします。

ステップ 3　[Create Row] アイコンをクリックします。

[Create IPSEC] ダイアログボックスが表示されます（図 7-20 を参照）。

図 7-20　IPSec の作成



ステップ 4　[Create Transform Set] 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] ボタン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] ボタンをクリックします。

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 マップ名を持つ（ただし、マップ シーケンス番号が異なる）クリプト マップ エントリは、クリプト マップ セットとして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 エントリが互換性を持つためには、次の最低基準を満たしている必要があります。

- 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 マップが設定されたインターフェイス上で、トラフィックは、最初にプライオリティが高いマップ 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。

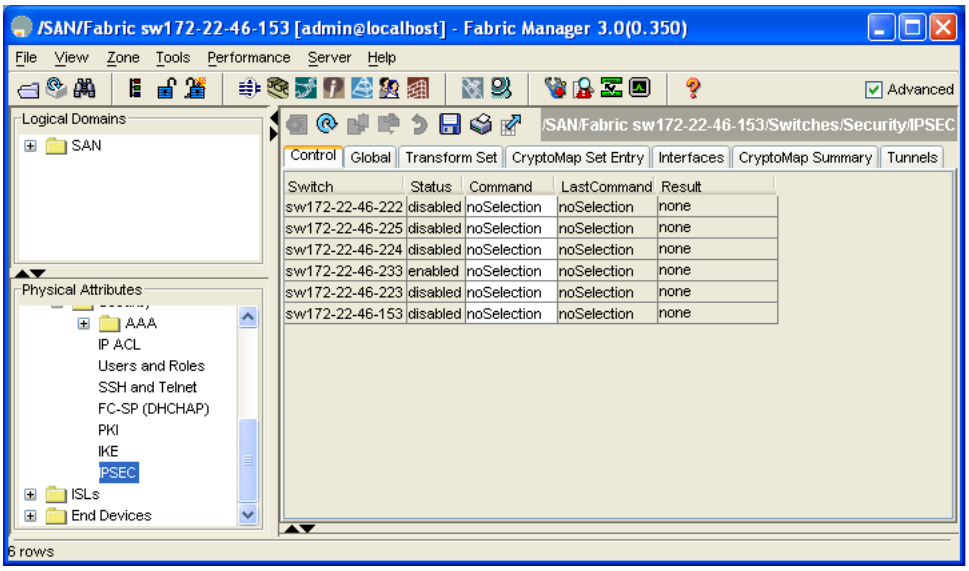
- ポリシーが適用される順序は、各クリプト マップのシーケンス番号によって決まります。シーケンス番号が小さいほど、プライオリティは高くなります。
- 各クリプト マップ エントリに使用できる IPv4-ACL は 1 つだけです（IPv4-ACL 自体には複数の permit エントリまたは deny エントリを設定できます）。
- トンネル エンドポイントが宛先アドレスと同じである場合は、auto-peer オプションを使用して、ピアをダイナミックに設定できます。
- IPSec を Microsoft iSCSI 発信側と効率的に相互運用するには、IPv4-ACL に TCP プロトコルとローカル 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

Fabric Manager を使用して必須のクリプト 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。[Information] ペインに IPSec の設定が表示されます（図 7-21 を参照）。

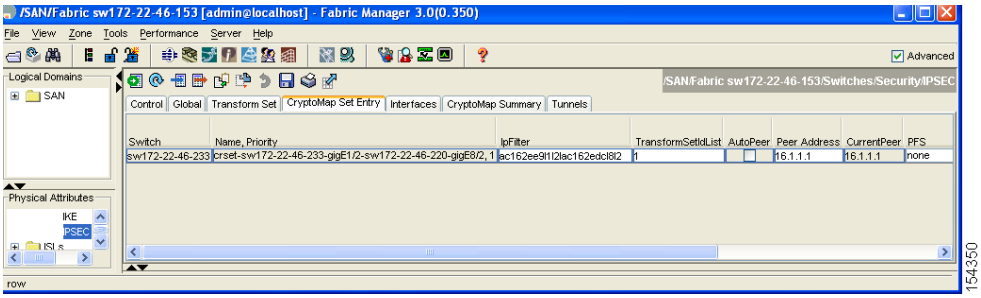
図 7-21　IPSec の設定



ステップ 2　[CryptoMap Set Entry] タブを選択します。

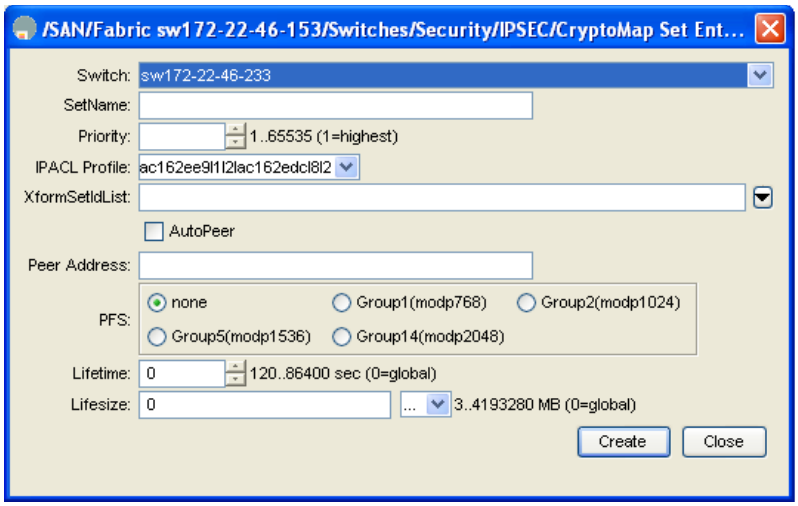
設定されている既存のクリプト マップが表示されます（図 7-22 を参照）。

図 7-22　既存のクリプト マップ



ステップ 3　（任意）[Create Row] アイコンをクリックして、クリプト マップ エントリを作成します。[Create Crypto Map] ダイアログボックスが表示されます（図 7-23 を参照）。

図 7-23　[Create Crypto Map] ダイアログボックス



ステップ 4　設定または変更したい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オンにするか、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.7-33）を参照してください。

ステップ 7　適切な [PFS] を選択します。「完全転送秘密の概要」（P.7-35）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.7-31）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は、[Create] ボタンをクリックします。既存のクリプト マップを変更する場合は、[Apply Changes] アイコンをクリックします。

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。

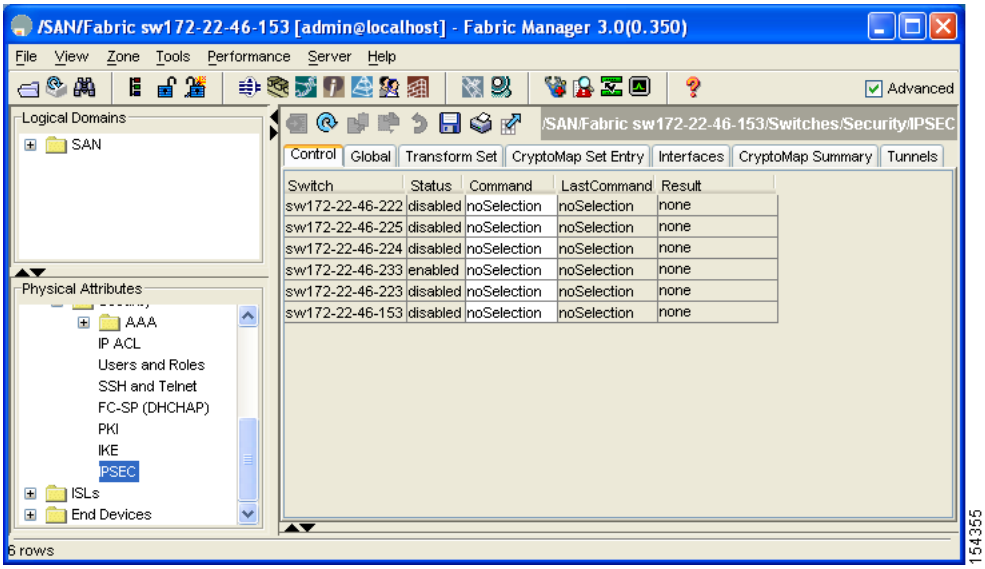
グローバル ライフタイム値の詳細については、「グローバル ライフタイム値」（P.7-38）を参照してください。

SA ライフタイムの設定

Fabric Manager を使用して、指定したクリプト マップの SA ライフタイムを設定する手順は、次のとおりです。

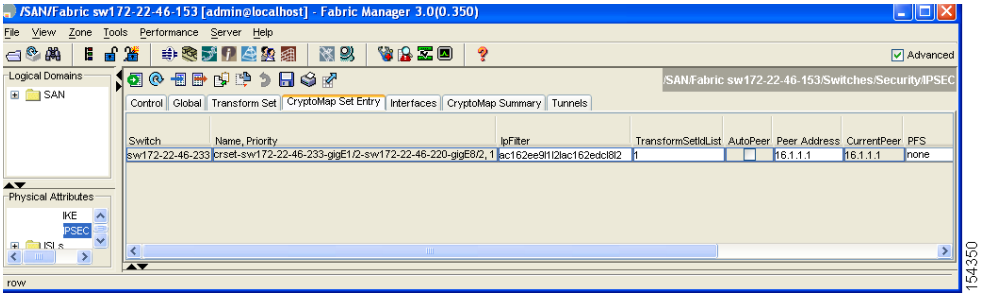
ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IPSEC] を選択します。[Information] ペインに IPSec の設定が表示されます（図 7-24 を参照）。

図 7-24　IPSec の設定



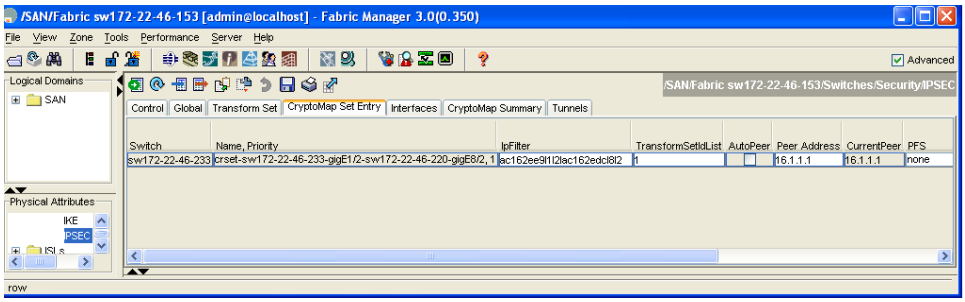
ステップ 2　[CryptoMap Set Entry] タブを選択します。設定されている既存のクリプト マップが表示されます（図 7-25 を参照）。

図 7-25　既存のクリプト マップ：左端カラム



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。別のカラムが表示されます（図 7-26 を参照）。

図 7-26　既存のクリプト マップ：右端カラム



ステップ 4　[Life Time(sec)] カラムをダブルクリックし、値を変更します。

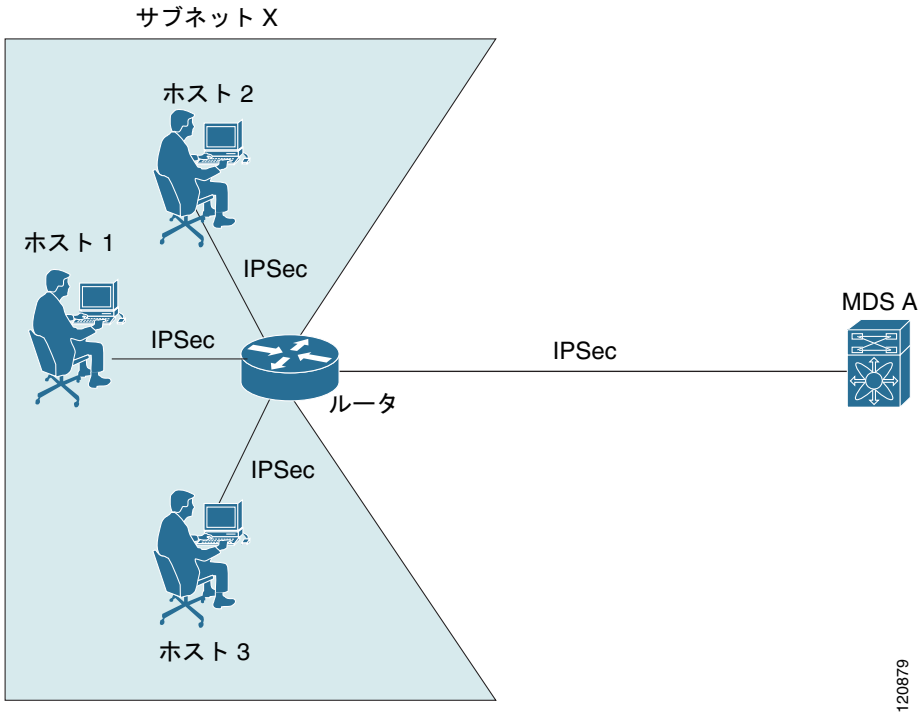
ステップ 5　[Apply Changes] アイコンをクリックして変更内容を保存します。

[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 [**AutoPeer**] 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 7-27 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 7-27　auto-peer オプションを使用した iSCSI のエンドツーエンド IPSec

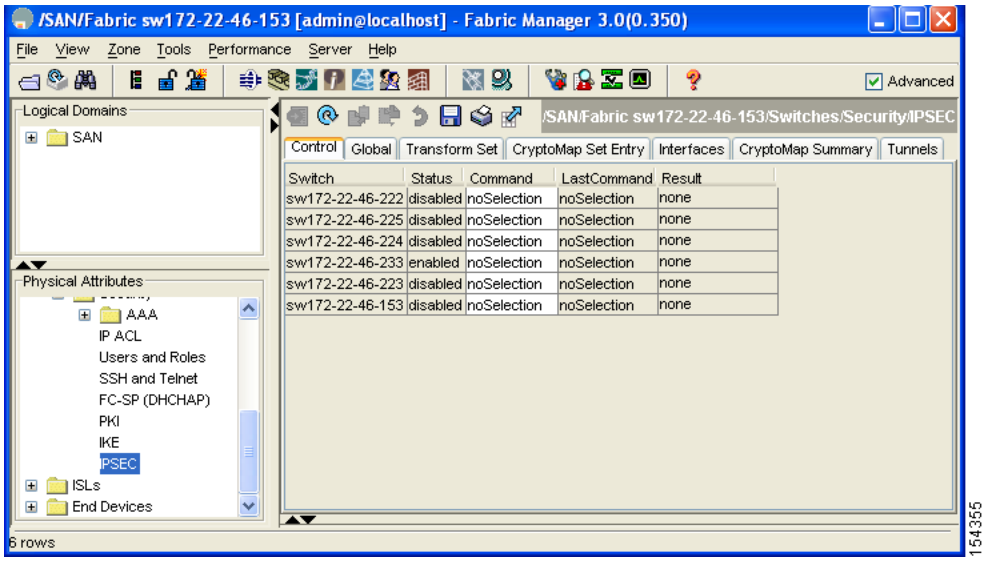


[AutoPeer] オプションの設定

Fabric Manager を使用して [AutoPeer] オプションを設定する手順は、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。[Information] ペインに IPSec の設定が表示されます（図 7-28 を参照）。

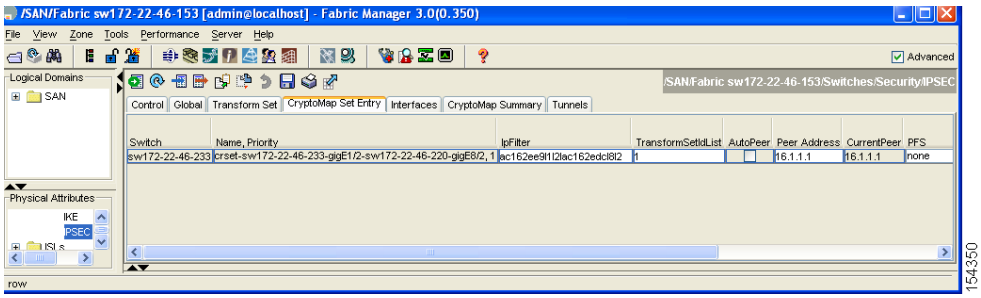
図 7-28　IPSec の設定



ステップ 2　[CryptoMap Set Entry] タブをクリックします。

設定されている既存のクリプト マップが表示されます（図 7-29 を参照）。

図 7-29　既存のクリプト マップ



ステップ 3　選択したクリプト マップ セット エントリの [AutoPeer] オプションを選択または選択解除します。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

完全転送秘密の概要

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 Perfect Forward Secrecy（PFS; 完全転送秘密）値を設定できます。

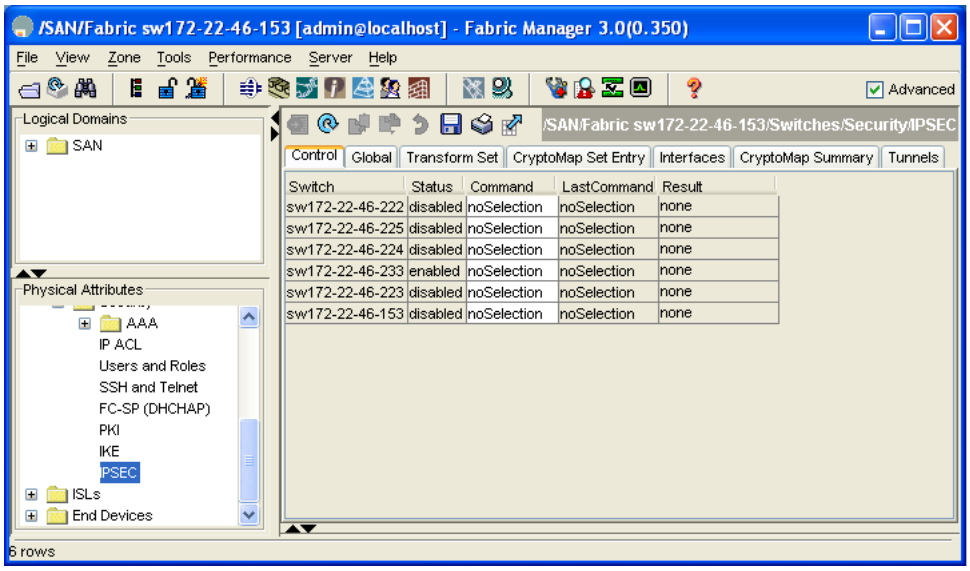
PFS 機能は、デフォルトではディセーブルです。PFS グループを設定する場合は、DH グループ 1、2、5、または 14 のうちの 1 つを設定できます。DH グループを指定しない場合、グループ 1 がデフォルトで使用されます。

完全転送秘密の設定

Fabric Manager を使用して 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。[Information] ペインに IPSec の設定が表示されます（図 7-30 を参照）。

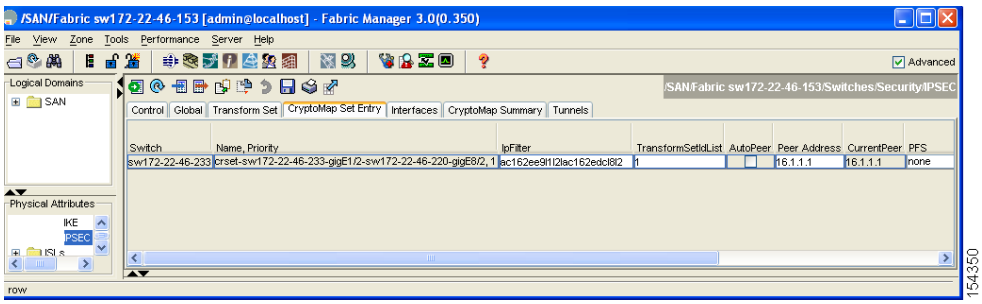
図 7-30　IPSec の設定



ステップ 2　[CryptoMap Set Entry] タブをクリックします。

設定されている既存のクリプト マップが表示されます（図 7-31 を参照）。

図 7-31　既存のクリプト マップ



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] アイコンをクリックして変更内容を保存します。

クリプト マップ セットの適用の概要

IPSec トラフィックが通過するインターフェイスごとに、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 セットを適用することはできません。

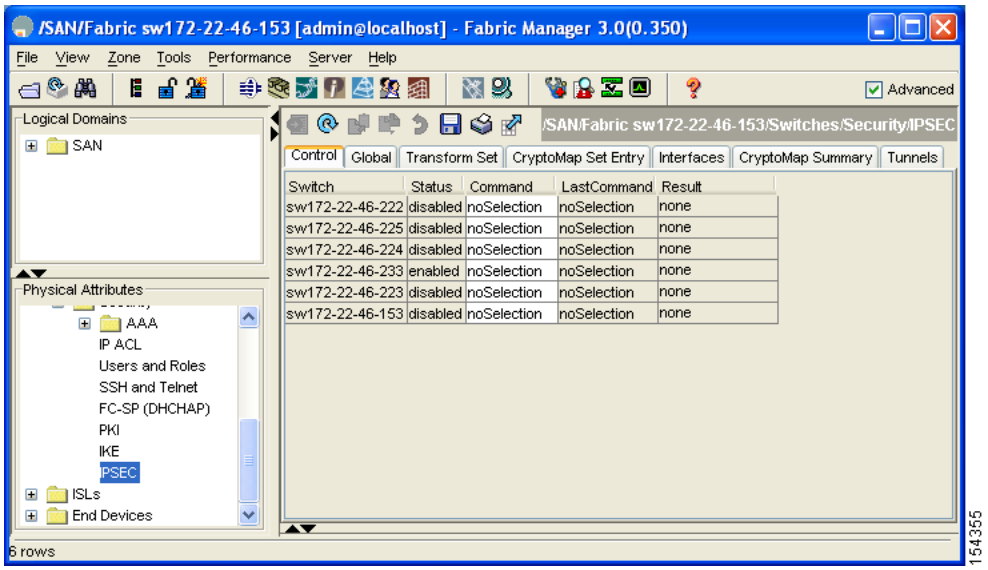
クリプト マップ セットの適用

Fabric Manager を使用してクリプト 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。

[Information] ペインに IPSec の設定が表示されます（図 7-32 を参照）。

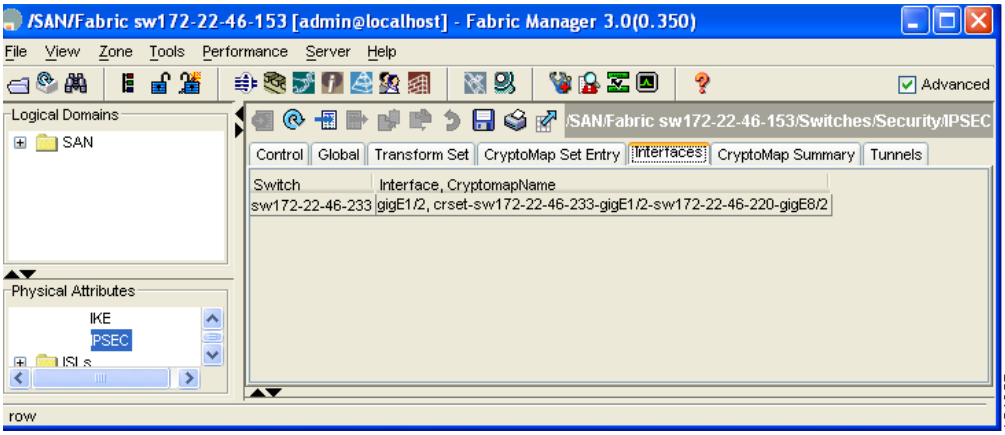
図 7-32　IPSec の設定



ステップ 2　[Interfaces] タブをクリックします。

クリプト マップ設定に既存のインターフェイスが表示されます（図 7-33 を参照）。

図 7-33　クリプト マップ インターフェイス



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] ボタンをクリックします。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] ボタンをクリックします。

IPSec のメンテナンス

設定の変更は、後続のセキュリティ アソシエーション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セキュリティ アソシエーションが再確立されるように、既存のセキュリティ アソシエーション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、セキュリティ アソシエーション データベースのうち、設定変更が影響する部分だけをクリアしてください（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セキュリティ アソシエーションだけをクリアします）。セキュリティ アソシエーション データベース全体をクリアするのは、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クリアします。

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。

Fabric Manager を使用してグローバル SA ライフタイムを設定する手順は、次のとおりです。

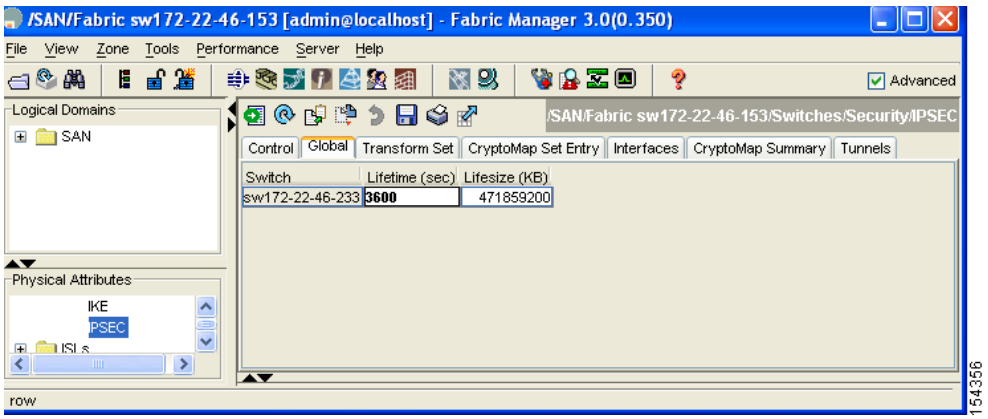
ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IPSEC] を選択します。

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、値を変更します（図 7-34 を参照）。

図 7-34　IPSec 設定の [Global] タブ



ステップ 5　[Apply Changes] アイコンをクリックして変更内容を保存します。

デフォルト設定値

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）