IKE

- IKE の設定 （1 ページ）
- IPsec の設定 （14 ページ）

IKE の設定

IKE は ISAKMP とも呼ばれ、2 台のホストで IPsec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーション プロトコルです。バーチャル プライベート ネットワーク用に ASA を設定するには、システム全体に適用するグローバル IKE パラメータを設定し、さらに、VPN 接続を確立するためにピアがネゴシエートする IKE ポリシーも作成します。

手順

ステップ 1 IKE の有効化 （1 ページ）を使用して無効にすることができます。

ステップ 2 サイト間 VPN の IKE パラメータ （2 ページ） を設定します。

ステップ 3 IKE ポリシー （9 ページ） を設定します。

IKE の有効化

手順

ステップ 1 VPN 接続に対して IKE を有効にする方法

a) ASDM で、[設定（Configuration）]>[リモートアクセスVPN（Remote Access VPN）]>[ネットワーク（クライアント）アクセス（Network (Client) Access）]>[Secure ClientAnyConnect 接続プロファイル（AnyConnect Connection Profiles）] を選択します。

b) [Access Interfaces] 領域で、IKE を使用するインターフェイスに対して、[IPsec (IKEv2) Access] の下にある [Allow Access] をオンにします。

ステップ 2 サイト間 VPN に対して IKE を有効にする方法

a) ASDM で、[Configuration] > [Site-to-Site VPN] > [Connection Profiles] を選択します。

b) IKEv1 および IKEv2 を使用するインターフェイスを選択します。

サイト間 VPN の IKE パラメータ

ASDM で、[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE Parameters] を選択します。

NAT の透過性

- [Enable IPsec over NAT-T]

  IPsec over NAT-T により IPSec ピアは、リモート アクセスと LAN-to-LAN の両方の接続を NAT デバイスを介して確立できます。NAT-T は UDP データグラムの IPsec トラフィックをカプセル化し、ポート 4500 を使用して、NAT デバイスにポート情報を提供します。NAT-T はすべての NAT デバイスを自動検出し、必要な場合だけ IPsec トラフィックをカプセル化します。この機能は、デフォルトでイネーブルにされています。

  - ASA は、データ交換を行うクライアントに応じて、標準の IPSec、IPSec over TCP、NAT-T、および IPSec over UDP を同時にサポートできます。
  - NAT-T と IPsec over UDP の両方がイネーブルになっている場合、NAT-T が優先されます。
  - イネーブルになっている場合、IPsec over TCP は他のすべての接続方式よりも優先されます。

  ASA による NAT-T の実装では、次の場合において、単一の NAT/PAT デバイスの背後にある IPSec ピアをサポートします。

  - LAN-to-LAN 接続。
  - LAN-to-LAN 接続または複数のリモート アクセス クライアントのいずれか。ただし、両方を混在させることはできません。

  NAT-T を使用するには、次の手順を実行する必要があります。

  - ポート 4500 を開くために使用するインターフェイスの ACL を作成します（[Configuration] > [Firewall] > [Access Rules]）。
  - このペインで、IPSec over NAT-T をイネーブルにします。
  - [Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Prefragmentation Policies] ペインの [Fragmentation Policy] パラメータで、[Enable IPsec Pre-fragmentation] で使用するインターフェイスを編集します。これが設定されている場合、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが移動できます。これによって、IP フラグメンテーションをサポートする NAT デバイスの動作が妨げられることはありません。

- Enable IPsec over TCP

  IPSec over TCP を使用すると、標準 ESP や標準 IKE が機能できない環境、または既存のファイアウォール ルールを変更した場合に限って機能できる環境で、VPN クライアントが動作可能になります。IPSec over TCP は TCP パケット内で IKE プロトコルと IPSec プロトコルをカプセル化し、NAT と PAT の両方のデバイスおよびファイアウォールによりセキュアなトンネリングを実現します。この機能はデフォルトで無効に設定されています。

（注） この機能は、プロキシベースのファイアウォールでは動作しません。

  IPsec over TCP は、リモート アクセス クライアントで動作します。また、すべての物理インターフェイスと VLAN インターフェイスでも動作します。これは、ASA 機能に対応しているクライアントに限られます。LAN-to-LAN 接続では機能しません。

  - ASA は、データ交換を行うクライアントに応じて、標準の IPSec、IPSec over TCP、NAT-Traversal、および IPSec over UDP を同時にサポートできます。
  - イネーブルになっている場合、IPsec over TCP は他のすべての接続方式よりも優先されます。

  ASA とその接続先クライアントの両方で IPsec over TCP をイネーブルにします。

  最大 10 個のポートを指定して、それらのポートに対して IPsec over TCP をイネーブルにできます。ポート 80（HTTP）やポート 443（HTTPS）などのウェルノウン ポートを入力すると、そのポートに関連付けられているプロトコルが機能しなくなることを示す警告がシステムに表示されます。その結果、ブラウザを使用して IKE 対応インターフェイスから ASA を管理できなくなります。この問題を解決するには、HTTP/HTTPS 管理を別のポートに再設定します。

  ASA だけでなく、クライアントでも TCP ポートを設定する必要があります。クライアントの設定には、ASA 用に設定したポートを少なくとも 1 つ含める必要があります。

ピアに送信される ID

IKE ネゴシエーションでピアが相互に相手を識別する [Identity] を選択します。

Address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
Hostname	ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
Key ID	リモート ピアが事前共有キーを検索するために使用する [Key Id String] を指定します。

Automatic	接続タイプによって IKE ネゴシエーションを決定します。 • 事前共有キーの IP アドレス • 証明書認証の cert DN。

セッション制御

- [Disable Inbound Aggressive Mode Connections]

  フェーズ 1 の IKE ネゴシエーションでは、Main モードと Aggressive モードのいずれかを使用できます。どちらのモードも同じサービスを提供しますが、Aggressive モードの場合にピア間で必要とされる交換処理は、3 つではなく 2 つだけです。Agressive モードの方が高速ですが、通信パーティの ID は保護されません。そのため、情報を暗号化するセキュアな SA を確立する前に、ピア間で ID 情報を交換する必要があります。この機能はデフォルトで無効に設定されています。

- [Alert Peers Before Disconnecting]

  - ASA のシャットダウンやリブート、セッション アイドル タイムアウト、最大接続時間の超過、管理者による停止など、いくつかの理由でクライアント セッションまたは LAN-to-LAN セッションがドロップされることがあります。
  - ASA は、切断される直前のセッションについて（LAN 間設定内の）限定されたピアに通知し、それらに理由を伝達します。アラートを受信したピアまたはクライアントは、その理由を復号化してイベント ログまたはポップアップ ペインに表示します。この機能はデフォルトで無効に設定されています。
  - このペインでは、ASA がそれらのアラートを送信して接続解除の理由を伝えることができるように、通知機能をイネーブルにできます。

  限定されたクライアントとピアには次のものが含まれます。

  - アラートがイネーブルになっているセキュリティ アプライアンス
  - バージョン 4.0 以降のソフトウェアを実行している VPN クライアント（設定は不要）

- [Wait for All Active Sessions to Voluntarily Terminate Before Rebooting]

  すべてのアクティブ セッションが自動的に終了した場合に限り ASA をリブートするように、スケジュールを設定できます。この機能はデフォルトで無効に設定されています。

- [Number of SAs Allowed in Negotiation for IKEv1]

  一時点でのネゴシエーション中 SA の総数を制限します。

IKE v2 特有の設定

追加のセッション制御は、オープン SA の数を制限する IKE v2 で使用できます。デフォルトでは、ASA はオープン SA の数を制限しません。

- [Cookie Challenge]：SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信できるようにします。
  - [% threshold before incoming SAs are cookie challenged]：ASA に対して許容される合計 SA のうち、ネゴシエーション中の SA の割合。この数値に達すると、以降の SA ネゴシエーションに対してクッキー チャレンジが行われます。範囲は 0 ～ 100% です。デフォルトは 50% です。
- [Number of Allowed SAs in Negotiation]：一時点でのネゴシエーション中 SA の総数を制限します。クッキー チャレンジと併用する場合は、有効なクロス チェックが行われるように、クッキー チャレンジのしきい値をこの制限よりも低くしてください。
- [Maximum Number of SAs Allowed]：ASA 上で許可される IKEv2 接続の数を制限します。デフォルトでは、ライセンスで指定されている最大接続数が上限です。
- [Notify Invalid Selector]：SA で受信された着信パケットがその SA のトラフィック セレクタと一致しない場合に、管理者はピアへの IKE 通知の送信を有効または無効にできます。この通知の送信はデフォルトでは、無効になっています。

IKE v2 特有の設定による DoS 攻撃の防止

着信セキュリティ アソシエーション（SA）識別のチャレンジを行うクッキー チャレンジを設定するか、オープンな SA の数を制限することにより、IPsec IKEv2 接続に対するサービス拒否（DoS）攻撃を防止できます。デフォルトでは、ASA はオープンな SA の数を制限せず、SA のクッキー チャレンジを行うこともありません。許可される SA の数を制限することもできます。これによって、それ以降は接続のネゴシエーションが行われなくなるため、クッキーチャレンジ機能では阻止できず現在の接続を保護できない可能性がある、メモリや CPU への攻撃を防止できます。

DoS 攻撃では、攻撃者は、ピア デバイスが SA 初期パケットを送信し、ASA がその応答を送信すると攻撃を開始しますが、ピア デバイスはこれ以上応答しません。ピア デバイスがこれを継続的に行うと、応答を停止するまで ASA で許可されるすべての SA 要求を使用できます。

クッキー チャレンジのしきい値（%）をイネーブルにすると、オープン SA ネゴシエーションの数が制限されます。たとえば、デフォルト設定の 50 % では、許可される SA の 50 % がネゴシエーション中（オープン）のときに、ASA は、到着した追加の SA 初期パケットのクッキー チャレンジを行います。

[**Number of SAs Allowed in Negotiation**] または [Maximum Number of SAs Allowed] とともに使用する場合は、有効なクロス チェックが行われるように、クッキー チャレンジのしきい値をこれらの設定よりも低くしてください。

[Configuration] > [Site-to-Site VPN] > [Advanced] > [System Options] を選択して、IPsec レベルのすべての SA の寿命を制限することもできます。

IKEv2 複数ピアクリプトマップについて

9.14(1) リリース以降、ASA IKEv2 は複数ピアクリプトマップをサポートするようになりました。トンネル内のピアがダウンすると、IKEv2 はリスト内の次のピアで SA の確立を試みます。最大 10 個のピアアドレスを持つクリプトマップを設定できます。IKEv2 でのこの複数ピアのサポートは、特に、複数ピアクリプトマップを使用して IKEv1 から移行する場合に役立ちます。

IKEv2 は双方向のクリプトマップのみをサポートします。したがって、複数ピアは双方向のクリプトマップにも設定され、トンネルを開始するピアからの要求を受け入れるために同じものが使用されます。

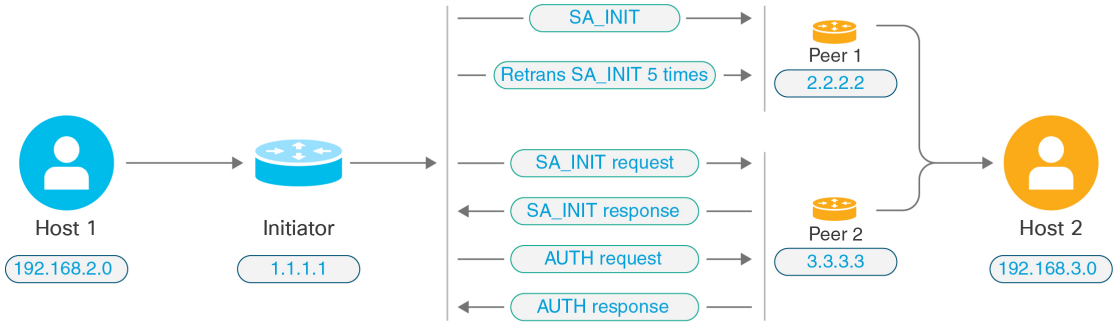
IKEv2 イニシエータの動作

IKEv2 はピア（Peer1 など）とのセッションを開始します。5 回の SA_INIT 再送信で Peer1 に到達できなかった場合、最終の再送信が実行されます。このアクティビティには約 2 分かかります。

Peer1 に障害が発生すると、SA_INIT メッセージが Peer2 に送信されます。Peer2 にも到達できない場合は、2 分後に Peer3 とのセッション確立が開始されます。

クリプトマップのピアリストにあるすべてのピアを使用すると、IKEv2 は、いずれかのピアと SA が確立されるまで、Peer1 からセッションを再度開始します。次の図に、この動作を示します。

図 *1:* イニシエータのプロセスフロー



（注） IKE SA を開始するには、継続的なトラフィックが必要です。そのため、試行が失敗するたびに次のピアに移動し、最終的に、到達可能なピアが SA を確立します。トラフィックが中断された場合は、次のピアで IKE SA を開始するために手動トリガーが必要になります。

IKEv2 レスポンダの動作

IKE SA のレスポンダデバイスがクリプトマップ内の複数のピアを使用して設定されている場合、IKE SA が試行されるたびに、イニシエータ IKE SA のアドレスが、クリプトマップ内の現在アクティブなピアのアドレスで検証されます。

たとえば、クリプトマップ内の現在アクティブなピア（レスポンダとして使用）が最初のピアである場合、IKE SA は Peer1 の IP アドレスから開始されます。同様に、クリプトマップ内の現在アクティブなピア（レスポンダとして使用）が 2 番目のピアである場合、IKE SA は Peer2 の IP アドレスから開始されます。

（注） ピアトラバーサルは、IKEv2 マルチピアトポロジのレスポンダ側ではサポートされません。

クリプトマップ変更時のピアインデックスのリセット

クリプトマップを変更すると、ピアインデックスがゼロにリセットされ、リスト内の最初のピアからトンネルが開始されます。次の表に、特定の状況での複数ピアインデックスの移行を示します。

表 *1 : SA* 前の複数ピアインデックスの移行

SA 前の状況	ピアインデックスの移動 ○/x/リセット
到達不能なピア	対応
フェーズ 1 プロポーザルの不一致	対応
フェーズ 2 プロポーザルの不一致	対応
DPD ACK 未受信	対応
AUTH フェーズ中のトラフィックセレクタの不一致	対応
Authentication failure（認証失敗）	対応
ピアに到達不能なためキー再生成に失敗	リセット

表 *2 : SA* 後の複数ピアインデックスの移行

SA 後の状況	ピアインデックスの移動 ○/x/リセット
プロポーザルの不一致によるキー再生成の失敗	リセット

SA 後の状況	ピアインデックスの移動 ○/x/リセット
キー再生成中のトラフィックセレクタの不一致	リセット
クリプトマップの変更	リセット
HA スイッチオーバー	x
clear crypto ikev2 sa	リセット
clear ipsec sa	リセット
IKEv2 SA タイムアウト	リセット

IKEv2 複数ピアの注意事項

IKEv1 および IKEv2 プロトコル

クリプトマップが両方のIKEバージョンおよび複数ピアで設定されている場合、次のピアに移動する前に、両方のバージョンの各ピアで SA の試行が行われます。

たとえば、2 つのピア P1 と P2 でクリプトマップが設定されている場合、IKEv2 の P1、IKEv1 の P1、IKEv2 の P2 のようにトンネルが開始されます。

高可用性

複数のピアを持つクリプトマップは、HA内のレスポンダデバイスへのトンネルを開始します。最初のデバイスに到達できない場合、次のレスポンダデバイスに移動します。

イニシエータデバイスは、レスポンダデバイスへのトンネルを開始します。アクティブデバイスがダウンすると、スタンバイデバイスは、アクティブデバイスのPeer2のIPアドレスに移動するクリプトマップに関係なく、Peer1 の IP アドレスからトンネルを確立しようとします。

集中クラスタ

複数のピアを持つクリプトマップは、集中クラスタの展開内にあるレスポンダデバイスへのトンネルを開始できます。最初のデバイスに到達できない場合、次のレスポンダデバイスへの移動を試みます。

イニシエータデバイスは、レスポンダデバイスへのトンネルを開始します。Peer1 に到達できない場合、クラスタ内のすべてのノードは次の Peer2 に移動します。

分散クラスタ

IKEv2複数ピアクリプトマップが設定されている場合、分散クラスタリングはサポートされません。

マルチコンテキストモード

マルチコンテキストモードでは、複数ピアの動作は各コンテキストに固有となります。

デバッグ コマンド

トンネルの確立に失敗した場合は、これらのコマンドを有効にして、問題をさらに分析します。

- **debug crypto ikev2 platform 255**
- **debug crypto ikev2 protocol 255**
- **debug crypto ike-common 255**

IKEv2 複数ピアに固有のデバッグログの例を次に示します。このログには、ピアの遷移が表示されます。

```
Sep 13 10:08:58 [IKE COMMON DEBUG]Failed to initiate ikev2 SA with peer 192.168.2.2,
initiate to next peer 192.168.2.3 configured in the multiple peer list of the crypto
map.
```

IKE ポリシー

[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE Policies]

このペインは、IKEv1 ポリシーと IKEv2 ポリシーを追加、編集、または削除するために使用します。

IKE ネゴシエーションの条件を設定するには、次に示す項目を含む IKE ポリシーを 1 つ以上作成します。

- 一意のプライオリティ（1 ～ 65,543、1 が最高のプライオリティ）。
- ピアの ID を確認する認証方式。
- データを保護し、プライバシーを守る暗号化方式。
- HMAC 方式。送信者の身元を保証し、搬送中にメッセージが変更されていないことを保証します。
- 暗号キー判別アルゴリズムを強化する Diffie-Hellman グループ。ASA はこのアルゴリズムを使用して、暗号キーとハッシュ キーを導出します。
- 暗号キーを置き換える前に、ASA がその暗号キーを使用する時間の上限。

各 IKE ネゴシエーションは、フェーズ 1 とフェーズ 2 と呼ばれる 2 つの部分に分かれます。フェーズ 1 は、以後の IKE ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 では、データを保護するトンネルが作成されます。

IKEv1 の場合は、各パラメータに対して 1 つの設定だけをイネーブルにできます。IKEv2 の場合は、1 つのプロポーザルで複数の設定（[Encryption]、[D-H Group]、[Integrity Hash]、および [PRF Hash]）を指定できます。

IKEポリシーが設定されていない場合、ASAはデフォルトのポリシーを使用します。デフォルトポリシーには各パラメータのデフォルト値が含まれており、ポリシーのプライオリティは常に最下位に設定されます。特定のパラメータの値を指定しない場合、デフォルト値が適用されます。

IKEネゴシエーションが開始されると、ネゴシエーションを開始するピアがそのポリシーすべてをリモート ピアに送信します。リモート ピアは、一致するポリシーがないかどうか、所有するポリシーをプライオリティ順に検索します。

暗号化、ハッシュ、認証、およびDiffie-Hellmanの値が同じで、SAライフタイムが送信されたポリシーのライフタイム以下の場合には、IKEポリシー間に一致が存在します。ライフタイムが等しくない場合は、（リモート ピア ポリシーからの）短い方のライフタイムが適用されます。一致するポリシーがない場合、IKE はネゴシエーションを拒否し、IKE SA は確立されません。

フィールド

- [IKEv1 Policies]：設定済み IKE ポリシーそれぞれのパラメータ設定を表示します。
  - [Priority #]：ポリシーのプライオリティを示します。
  - [Encryption]：暗号化方式を示します。
  - [Hash]：ハッシュ アルゴリズムを示します。
  - [D-H Group]：Diffie-Hellman グループを示します。
  - [Authentication]：認証方式を示します。
  - [Lifetime（secs）]：SA ライフタイムを秒数で示します。
- [IKEv2 Policies]：設定済み IKEv2 ポリシーそれぞれのパラメータ設定を表示します。
  - [Priority #]：ポリシーのプライオリティを示します。
  - [Encryption]：暗号化方式を示します。
  - [Integrity Hash]：ハッシュ アルゴリズムを示します。
  - [PRF Hash]：疑似乱数関数（PRF）ハッシュ アルゴリズムを示します。
  - [D-H Group]：Diffie-Hellman グループを示します。
  - [Lifetime（secs）]：SA ライフタイムを秒数で示します。

IKEv1 ポリシーの追加または編集

[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE Policies] > [Add/Edit IKE Policy]

[Priority #]：IKE ポリシーのプライオリティを設定する数字を入力します。範囲は 1 ～ 65535 で、1 が最高のプライオリティです。

[Encryption]：暗号化方式を選択します。これは、2 つの IPSec ピア間で伝送されるデータを保護する対称暗号化アルゴリズムです。次の中から選択できます。

des	56 ビット DES-CBC。安全性は低いですが、他の選択肢より高速です。デフォルト。
3des	168 ビット Triple DES。
aes	128 ビット AES。
aes-192	192 ビット AES。
aes-256	256 ビット AES。

[Hash]：データの整合性を保証するハッシュアルゴリズムを選択します。パケットが、そのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。

sha	SHA-1	デフォルト値はSHA-1です。MD5のダイジェストの方が小さく、SHA-1よりもやや速いと見なされています。しかし、MD5に対する攻撃が成功（これは非常に困難）しても、IKEが使用するHMACバリアントがこの攻撃を防ぎます。
md5	MD5	

[Authentication]：各 IPSec ピアの ID を確立するために ASA が使用する認証方式を選択します。事前共有キーは拡大するネットワークに対応した拡張が困難ですが、小規模ネットワークではセットアップが容易です。次の選択肢があります。

pre-share	事前共有キー。
rsa-sig	RSA シグニチャ アルゴリズムによって生成されたキー付きのデジタル証明書。

[D-H Group]：Diffie-Hellman グループ ID を選択します。この ID は、2 つの IPSec ピアが、相互に共有秘密情報を転送するのではなく、共有秘密情報を取り出すために使用します。

1	グループ 1（768 ビット）	「デフォルト」のグループ 2（1024 ビット Diffie-Hellman）は、グループ 1 または 5 と比較して、CPU の実行時間は短いものの、安全性は低くなります。
2	グループ 2（1024 ビット）	
5	グループ 5（1536 ビット）	
14	グループ 14（2048 ビット）	デフォルトの Diffie-Hellman グループはグループ 14（2048 ビット Diffie-Hellman）です。

[Lifetime (secs)]：[Unlimited] をオンにするか、SA ライフタイムを整数で入力します。デフォルトは 86,400 秒、つまり 24 時間です。ライフタイムを長くするほど、ASA は以後の IPSec セ

キュリティアソシエーションをより緩やかにセットアップします。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルトをそのまま使用することを推奨します。

[Time Measure]：時間基準を選択します。ASA では次の値を使用できます。

120 ～ 86,400 秒
2 ～ 1,440 分
1 ～ 24 時間
1 日

IKEv2 ポリシーの追加または編集

[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE Policies] > [Add/Edit IKEv2 Policy]

[Priority #]：IKEv2 ポリシーのプライオリティを設定する数字を入力します。範囲は 1 ～ 65535 で、1 が最高のプライオリティです。

[Encryption]：暗号化方式を選択します。これは、2 つの IPSec ピア間で伝送されるデータを保護する対称暗号化アルゴリズムです。次の中から選択できます。

des	56 ビット DES-CBC 暗号化を ESP に対して指定します。
3des	（デフォルト）トリプル DES 暗号化アルゴリズムを ESP に対して指定します。
aes	AES と 128 ビット キー暗号化を ESP に対して指定します。
aes-192	AES と 192 ビット キー暗号化を ESP に対して指定します。
aes-256	AES と 256 ビット キー暗号化を ESP に対して指定します。
aes-gcm	AES-GCM/GMAC 128 ビットのサポートを対称暗号化と整合性に対して指定します。
aes-gcm-192	AES-GCM/GMAC 192 ビットのサポートを対称暗号化と整合性に対して指定します。
aes-gcm-256	AES-GCM/GMAC 256 ビットのサポートを対称暗号化と整合性に対して指定します。
NULL	暗号化が行われないことを示します。

[D-H Group]：Diffie-Hellman グループ ID を選択します。この ID は、2 つの IPSec ピアが、相互に共有秘密情報を転送するのではなく、共有秘密情報を取り出すために使用します。

1	グループ 1（768 ビット）	これがデフォルトです。Group 2（1024 ビット Diffie-Hellman）では、実行に必要な CPU 時間が少なくなりますが、Group 2 または 5 より安全性が劣ります。
2	グループ 2（1024 ビット）	
5	グループ 5（1536 ビット）	
14	グループ 14	
19	グループ 19	
20	グループ 20	
21	グループ 21	
24	グループ 24	

[Integrity Hash]：ESP プロトコルのデータ整合性を保証するためのハッシュ アルゴリズムを選択します。パケットが、そのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。

sha	SHA 1	デフォルトは SHA 1 です。MD5 の方がダイジェストが小さく、SHA 1 よりもやや速いと見なされています。しかし、MD5 に対する攻撃が成功（これは非常に困難）しても、IKE が使用する HMAC バリアントがこの攻撃を防ぎます。
md5	MD5	
sha256	SHA 2、256 ビットのダイジェスト	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha384	**SHA 2, 384-bit digest**	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha512	**SHA 2, 512-bit digest**	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
null		AES-GCM または AES-GMAC が暗号化アルゴリズムとして設定されていることを示します。AES-GCM が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。

[Pseudo-Random Function (PRF)]：SA で使用されるすべての暗号化アルゴリズムのためのキー関連情報の組み立てに使用される PRF を指定します。

sha	SHA-1	デフォルト値はSHA-1です。MD5のダイジェストの方が小さく、SHA-1よりもやや速いと見なされています。しかし、MD5に対する攻撃が成功（これは非常に困難）しても、IKEが使用するHMACバリアントがこの攻撃を防ぎます。
md5	MD5	
sha256	SHA 2、256 ビットのダイジェスト	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha384	SHA 2、384 ビットのダイジェスト	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha512	SHA 2、512 ビットのダイジェスト	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。

[Lifetime (secs)]：[Unlimited] をオンにするか、SA ライフタイムを整数で入力します。デフォルトは 86,400 秒、つまり 24 時間です。ライフタイムを長くするほど、ASA は以後の IPsec セキュリティ アソシエーションをより迅速にセットアップします。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルトをそのまま使用することを推奨します。

ASA では次の値を使用できます。

120 ～ 86,400 秒
2 ～ 1,440 分
1 ～ 24 時間
1 日

IPsec の設定

ASA では、LAN-to-LAN VPN 接続に IPsec が使用され、client-to-LAN VPN 接続に IPsec を使用することも選択できます。IPsec の用語では、「ピア」は、リモート アクセス クライアントまたは別のセキュア ゲートウェイを指します。ASA は、シスコ ピア（IPv4 または IPv6）と、関連するすべての標準に準拠したサードパーティ ピアとの LAN-to-LAN IPsec 接続をサポートします。

トンネルを確立する間に、2 つのピアは、認証、暗号化、カプセル化、キー管理を制御するセキュリティ アソシエーションをネゴシエートします。これらのネゴシエーションには、トンネルの確立（IKE SA）と、トンネル内のトラフィックの制御（IPsec SA）という 2 つのフェーズが含まれます。

LAN-to-LAN VPN は、地理的に異なる場所にあるネットワークを接続します。IPsec LAN-to-LAN 接続では、ASA は発信側または応答側として機能することができます。IPsec client-to-LAN 接続では、ASA は応答側としてのみ機能します。発信側は SA を提案し、応答側は、設定された

SA パラメータに従って、SA の提示を受け入れるか、拒否するか、または対案を提示します。接続を確立するには、両方のエンティティで SA が一致する必要があります。

ASA は、次の IPSec 属性をサポートしています。

- 認証でデジタル証明書を使用するときに、フェーズ 1 ISAKMP セキュリティ アソシエーションをネゴシエートする場合の Main モード
- 認証で事前共有キーを使用するときに、フェーズ 1 ISAKMP セキュリティ アソシエーション（SA）をネゴシエートする場合の Aggressive モード
- 認証アルゴリズム：
  - ESP-MD5-HMAC-128
  - ESP-SHA1-HMAC-160
- 認証モード：
  - 事前共有キー
  - X.509 デジタル証明書
- 暗号化アルゴリズム：
  - AES-128、-192、および -256
  - 3DES-168
  - DES-56
  - ESP-NULL
- 拡張認証（XAuth）
- モード コンフィギュレーション（別名 ISAKMP コンフィギュレーション方式）
- トンネル カプセル化モード
- LZS を使用した IP 圧縮（IPCOMP）

手順

ステップ 1 暗号マップ （16 ページ） を設定します。
ステップ 2 IPsec 事前フラグメンテーション ポリシー （25 ページ） を設定します。
ステップ 3 IPsec Proposals (Transform Sets) （28 ページ） を設定します。

暗号マップ

[Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps]

このペインには、IPSec ルールに定義されている、現在設定されているクリプト マップが表示されます。ここでは、IPSec ルールを追加、編集、削除、切り取り、および貼り付けしたり、上下に移動させたりできます。

（注） 暗黙のルールは、編集、削除、またはコピーできません。ASA は、ダイナミック トンネル ポリシーが設定されている場合、リモート クライアントからトラフィックの選択提案を暗黙的に受け入れます。特定のトラフィックを選択することによって、その提案を無効化できます。

[Interface]、[Source]、[Destination]、[Destination Service]、または [Rule Query] を選択、[is] または [contains] を選択、あるいはフィルタ パラメータを入力することによって、ルールを**検索**（ルールの表示をフィルタ処理）することもできます。[...] をクリックして、選択可能なすべての既存エントリが示された参照ダイアログボックスを開きます。**ダイアグラム**は、ルールを図で表示するために使用します。

IPsec ルールでは以下を指定します。

- [Type: Priority]：ルールのタイプ（Static または Dynamic）とそのプライオリティを表示します。
- Traffic Selection
  - [#]：ルール番号を示します。
  - [Source]：トラフィックを [Remote Side Host/Network] カラムのリストにある IP アドレス宛てに送信するときに、このルールに従う IP アドレスを示します。詳細モード（[Show Detail] ボタンを参照）では、アドレス カラムに、「any」という語が含まれるインターフェイス名が表示される場合があります（例：「inside:any」）。any は、内部インターフェイスのすべてのホストがルールの影響を受けることを意味します。
  - [Destination]：トラフィックが [Security Appliance Side Host/Network] カラムのリストにある IP アドレスから送信されるときに、このルールに従う IP アドレスを一覧表示します。詳細モード（[Show Detail] ボタンを参照）では、アドレス カラムに、「any」という語が含まれるインターフェイス名が表示される場合があります（例：「outside:any」）。any は、外部インターフェイスのすべてのホストがルールの影響を受けることを意味します。さらに詳細モードでは、アドレス カラムに角カッコで囲まれた IP アドレスが含まれることもあります（[209.165.201.1-209.165.201.30] など）。これらのアドレスは、変換済みアドレスです。内部ホストによって外部ホストへの接続が作成されると、ASA は内部ホストのアドレスをプールのアドレスにマッピングします。ホストがアウトバウンド接続を作成した後、ASA はこのアドレス マッピングを保持します。このアドレス マッピング構造は xlate と呼ばれ、一定期間メモリに保持されます。
  - [Service]：ルールによって指定されるサービスとプロトコルを指定します（TCP、UDP、ICMP、または IP）。

- [Action]：IPSec ルールのタイプ（保護する、または保護しない）を指定します。

- [Transform Set]：ルールのトランスフォーム セットを表示します。
- [Peer]：IPsec ピアを識別します。
- [PFS]：ルールの完全転送秘密設定値を表示します。
- [NAT-T Enabled]：ポリシーで NAT Traversal が有効になっているかどうかを示します。
- [Reverse Route Enabled]：ポリシーでリバース ルート インジェクション（RRI）がイネーブルになっているかどうかを示します。RRI は設定で行われ、静的とみなされます。設定が変更または削除されるまでそのままになります。ASA は、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用してそれらのルートをプライベート ネットワークまたはボーダー ルータに通知します。
  - [Dynamic]：ダイナミックに指定されている場合、RRI は IPsec セキュリティ アソシエーション（SA）の確立成功時に作成され、IPsec SA が削除されると削除されます。

（注） ダイナミック RRI は IKEv2 ベースのスタティック暗号マップだけに適用されます。

- [Connection Type]：（スタティック トンネル ポリシーでのみ有効）。このポリシーの接続タイプを bidirectional、originate-only、または answer-only として識別します。
- [SA Lifetime]：ルールの SA ライフタイムを表示します。
- [CA Certificate]：ポリシーの CA 証明書を表示します。これは、スタティック接続にだけ適用されます。
- [IKE Negotiation Mode]：IKE ネゴシエーションで、Main モードまたは Aggressive モードを使用するかどうかを表示します。
- [Description]：（任意）このルールの簡単な説明を指定します。既存ルールの場合は、ルールの追加時に入力した説明になります。暗黙のルールには、「Implicit rule」という記述が含まれています。暗黙のルール以外のルールの説明を編集するには、このカラムを右クリックして [Edit Description] を選択するか、このカラムをダブルクリックします。
- [Enable Anti-replay window size]：リプレイ攻撃防止ウィンドウのサイズを、64 ～ 1028 の範囲の 64 の倍数で設定します。階層型 QoS ポリシーでのトラフィック シェーピングによるプライオリティ キューイング（「[Rule Actions] > [QoS] タブ」を参照）の副次的影響は、パケットの順番が変わることです。IPsec パケットでは、アンチ リプレイ ウィンドウ内にない不連続パケットにより、警告 syslog メッセージが生成されます。これらの警告は、プライオリティ キューイングの場合は誤報です。アンチ リプレイのパネル サイズを設定すると、誤報を回避することができます。
- [Enable IPsec Inner Routing Lookup]：デフォルトでは、IPSec トンネル経由で送信されるパケットに対してルックアップは実行されません。パケット単位の隣接関係ルックアップは

外部ESPパケットに対してのみ行われます。一部のネットワークトポロジでは、ルーティングの更新によって内部パケットのパスが変更されても、IPsecトンネルがまだアップ状態の場合、トンネルを介したパケットは正常にルーティングされず、宛先に到達できません。これを防止するには、IPSec内部パケットのパケットごとのルーティングルックアップをイネーブルにします。

[Create/Edit an IPsec Rule]：[Tunnel Policy (Crypto Map) - Basic] タブ

このペインでは、IPSecルールの新しいトンネルポリシーを定義します。ここで定義する値は、[OK] をクリックした後に [IPSec Rules] テーブルに表示されます。すべてのルールは、デフォルトで [IPSec Rules] テーブルに表示されるとすぐにイネーブルになります。

[Tunnel Policy] ペインでは、IPSec（フェーズ2）セキュリティアソシエーション（SA）のネゴシエートで使用するトンネルポリシーを定義できます。ASDMは、ユーザーのコンフィギュレーション編集結果を取り込みますが、[Apply] をクリックするまでは実行中のコンフィギュレーションに保存しません。

すべてのトンネルポリシーでは、トランスフォームセットを指定し、適用するセキュリティアプライアンスインターフェイスを特定する必要があります。トランスフォームセットでは、IPSecの暗号化処理と復号化処理を実行する暗号化アルゴリズムおよびハッシュアルゴリズムを特定します。すべてのIPSecピアが同じアルゴリズムをサポートするとは限らないため、多くのポリシーを指定して、それぞれに1つのプライオリティを割り当てるようにすることもできます。その後セキュリティアプライアンスは、リモートのIPSecピアとネゴシエートして、両方のピアがサポートするトランスフォームセットを一致させます。

トンネルポリシーは、スタティックまたはダイナミックにすることができます。スタティックトンネルポリシーでは、セキュリティアプライアンスでIPSec接続を許可する1つ以上のリモートIPSecピアまたはサブネットワークを特定します。スタティックポリシーを使用して、セキュリティアプライアンスで接続を開始するか、またはリモートホストから接続要求を受信するかどうかを指定できます。スタティックポリシーでは、許可されるホストまたはネットワークを識別するために必要な情報を入力する必要があります。

ダイナミックトンネルポリシーは、セキュリティアプライアンスとの接続を開始することを許可されるリモートホストについての情報を指定できないか、または指定しない場合に使用します。リモートVPN中央サイトデバイスとの関係で、セキュリティアプライアンスをVPNクライアントとしてしか使用しない場合は、ダイナミックトンネルポリシーを設定する必要はありません。ダイナミックトンネルポリシーが最も効果的なのは、リモートアクセスクライアントが、VPN中央サイトデバイスとして動作するセキュリティアプライアンスからユーザーネットワークへの接続を開始できるようにする場合です。ダイナミックトンネルポリシーは、リモートアクセスクライアントにダイナミックに割り当てられたIPアドレスがある場合、または多くのリモートアクセスクライアントに別々のポリシーを設定しないようにする場合に役立ちます。

[Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps] > [Create / Edit IPsec Rule] > [Tunnel Policy (Crypto Map) - Basic]

- [Interface]：このポリシーを適用するインターフェイス名を選択します。

- [Policy Type]：このトンネル ポリシーのタイプとして、[Static] または [Dynamic] を選択します。
- [Priority]：ポリシーのプライオリティを入力します。
- [IKE Proposals (Transform Sets)]：IKEv1 および IKEv2 の IPsec プロポーザルを指定します。
  - [IKEv1 IPsec Proposal]：ポリシーのプロポーザル（トランスフォーム セット）を選択して [Add] をクリックすると、アクティブなトランスフォーム セットのリストに移動します。[Move Up] または [Move Down] をクリックして、リスト ボックス内でのプロポーザルの順番を入れ替えます。クリプト マップ エントリまたはダイナミック クリプト マップ エントリには、最大で 11 のプロポーザルを追加できます。
  - [IKEv2 IPsec Proposal]：ポリシーのプロポーザル（トランスフォーム セット）を選択して [Add] をクリックすると、アクティブなトランスフォーム セットのリストに移動します。[Move Up] または [Move Down] をクリックして、リスト ボックス内でのプロポーザルの順番を入れ替えます。クリプト マップ エントリまたはダイナミック クリプト マップ エントリには、最大で 11 のプロポーザルを追加できます。
- [Peer Settings - Optional for Dynamic Crypto Map Entries]：ポリシーのピア設定値を設定します。
  - [Connection Type]：（スタティック トンネル ポリシーでのみ有効）。bidirectional、originate-only、または answer-only を選択して、このポリシーの接続タイプを指定します。LAN-to-LAN 接続の場合は、bidirectional または answer-only（originate-only ではない）を選択します。LAN-to-LAN 冗長接続の場合は、answer-only を選択します。originate only を選択した場合は、最大 10 個の冗長ピアを指定できます。単方向に対してだけ、originate only または answer only を指定できます。どちらもデフォルトでイネーブルになっていません。
  - [IP Address of Peer to Be Added]：追加する IPSec ピアの IP アドレスを入力します。9.14(1) 以降、ASA は IKEv2 で複数のピアをサポートしています。最大 10 ピアをクリプトマップに追加できます。
- [Enable Perfect Forwarding Secrecy]：ポリシーの PFS をイネーブルにする場合にオンにします。PFS は、新しいキーはすべて、あらゆる過去のキーと関係しないという暗号化コンセプトです。IPSec ネゴシエーションでのフェーズ 2 キーは、PFS を指定しない限りフェーズ 1 に基づいて生成されます。
- [Diffie-Hellman Group]：PFS をイネーブルにする場合は、ASA がセッション キーの生成に使用する Diffie-Hellman グループも選択する必要があります。次の選択肢があります。
  - [Group 1（768 ビット）]：PFS を使用し、Diffie-Hellman Group 1 を使用して IPSec セッション キーを生成します。このときの素数と generator 数は 768 ビットです。このオプションは高い安全性を示しますが、より多くの処理オーバーヘッドを必要とします。
  - [Group 2（1024 ビット）]：PFS を使用し、Diffie-Hellman Group 2 を使用して IPSec セッション キーを生成します。このときの素数と generator 数は 1024 ビットです。こ

のオプションは Group 1 より高い安全性を示しますが、より多くの処理オーバーヘッドを必要とします。

- [Group 5（1536 ビット）]：PFS を使用し、Diffie-Hellman Group 5 を使用して IPSec セッション キーを生成します。このときの素数と generator 数は 1536 ビットです。このオプションは Group 2 より高い安全性を示しますが、より多くの処理オーバーヘッドを必要とします。
- [Group 14 (2048-bits)]：完全転送秘密を使用し、IKEv2 に対して Diffie-Hellman グループ 14 を使用します。
- [Group 19]：完全転送秘密を使用し、IKEv2 に対する Diffie-Hellman グループ 19 を使用して、ECDH をサポートします。
- [Group 20]：完全転送秘密を使用し、IKEv2 に対して Diffie-Hellman グループ 20 を使用して、ECDH をサポートします。
- [Group 21]：完全転送秘密を使用し、IKEv2 に対して Diffie-Hellman グループ 21 を使用して、ECDH をサポートします。
- [Group 24]：完全転送秘密を使用し、IKEv2 に対して Diffie-Hellman グループ 24 を使用します。

[Create/Edit IPsec Rule]：[Tunnel Policy (Crypto Map) - Advanced] タブ

[Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps] > [Create / Edit IPsec Rule] > [Tunnel Policy (Crypto Map) - Advanced]

- [Enable NAT-T]：このポリシーの NAT Traversal（NAT-T）をイネーブルにします。
- [Enable Reverse Route Injection]：このポリシーの逆ルート注入をイネーブルにします。リバース ルート インジェクション（RRI）は、ダイナミック ルーティング プロトコルを使用する内部ルータのルーティング テーブルにデータを入力するために使用されます。ダイナミック ルーティング プロトコルの例としては、Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）（ASA を実行する場合）、ルーティング情報プロトコル（RIP）（リモート VPN クライアントや LAN-to-LAN セッションに使用）があります。RRI は設定で行われ、静的とみなされます。設定が変更または削除されるまでそのままになります。ASA は、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用してそれらのルートをプライベート ネットワークまたはボーダー ルータに通知します。送信元/宛先（0.0.0.0/0.0.0.0）を保護ネットワークとして指定する場合は、RRI をイネーブルにしないでください。デフォルトルートを使用するトラフィックに影響します。
  - [Dynamic]：ダイナミックに指定されている場合、RRI は IPsec セキュリティ アソシエーション（SA）の確立成功時に作成され、IPsec SA が削除されると削除されます。通常、RRI ルートは、ルートが存在せず、トラフィックを暗号化する必要がある場合に、トンネルを開始するために使用されます。ダイナミック RRI がサポートされると、トンネルが確立されるまでルートが存在しません。したがって、ダイナミック RRI が設定された ASA は通常、レスポンダとしてのみ動作します。

（注） ダイナミック RRI は IKEv2 ベースのスタティック暗号マップだけに適用されます。

- [Security Association Lifetime Settings]：セキュリティ アソシエーション（SA）の期間を設定します。このパラメータにより、IPsec SA キーのライフタイムの測定単位を指定します。ライフタイムは、IPsec SA が期限切れになるまでの存続期間を示し、新しいキーと再ネゴシエートする必要があります。
  - [Time]：時（hh）、分（mm）、および秒（ss）単位で SA のライフタイムを指定します。
  - [Traffic Volume]：キロバイト単位のトラフィックで SA ライフタイムを定義します。IPsec SA が期限切れになるまでのペイロードデータのキロバイト数を入力します。最小値は 100 KB、デフォルト値は 10000 KB、最大値は 2147483647 KB です。
- [Static Type Only Settings]：スタティック トンネル ポリシーのパラメータを指定します。
  - [Device Certificate]：使用する証明書を選択します。デフォルトの [None]（事前共有キーを使用）以外の値を選択する場合。[None] 以外を選択すると、[Send CA certificate chain] チェックボックスがオンになります。
  - [Send CA certificate chain]：トラスト ポイント チェーン全体の伝送をイネーブルにします。
  - [IKE Negotiation Mode]：IKE ネゴシエーション モード（Main または Aggressive）を選択します。このパラメータにより、キー情報の交換と SA のセットアップを行う場合のモードを設定します。ネゴシエーションの発信側が使用するモードを設定し、応答側は自動ネゴシエーションします。Aggressive モードは高速で、使用するパケットと交換回数を少なくすることができますが、通信パーティの ID は保護されません。Main モードは低速で、パケットと交換回数が多くなりますが、通信パーティの ID を保護します。このモードはより安全性が高く、デフォルトで選択されています。[Aggressive] を選択すると、[Diffie-Hellman Group] リストがアクティブになります。
  - [Diffie-Hellman Group]：適用する Diffie-Hellman グループを選択します。Group 1（768 ビット）、Group 2（1024 ビット）Group 5（1536 ビット）の中から選択します。
- [ESP v3]：着信 ICMP エラー メッセージを、暗号化マップとダイナミック暗号化マップのどちらに対して検証するかを指定し、セキュリティ単位のアソシエーション ポリシーを設定するか、トラフィック フロー パケットをイネーブルにします。
  - [Validate incoming ICMP error messages]：IPsec トンネルを介して受信され、プライベート ネットワーク上の内部ホストが宛先のこれらの ICMP エラー メッセージを検証するかどうかを選択します。

- [Enable Do Not Fragment (DF) policy]：IP ヘッダーに Do-Not-Fragment（DF）ビットセットを持つ大きなパケットを IPSec サブシステムがどのように処理するかを定義します。次のいずれかを選択します。

  [Clear DF bit]：DF ビットを無視します。

  [Copy DF bit]：DF ビットを維持します。

  [Set DF bit]：DF ビットを設定して使用します。

- [Enable Traffic Flow Confidentiality (TFC) packets]：トンネルを通過するトラフィックプロファイルをマスクするダミーの TFC パケットをイネーブルにします。

（注） TFC をイネーブルにする前に、[Tunnel Policy (Crypto Map)] の [Basic] タブで IKE v2 IPsec プロポーザルが設定されていなければなりません。

  バースト、ペイロード サイズ、およびタイムアウト パラメータを使用して、指定した SA で不定期にランダムな長さのパケットを生成します。

[Create/Edit IPsec Rule]：[Traffic Selection] タブ

[Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps] > [Create / Edit IPsec Rule] > [Traffic Selection]

このペインでは、保護する（許可）トラフィックまたは保護しない（拒否）トラフィックを定義できます。

- [Action]：このルールで実行するアクションを指定します。選択肢は、[protect] と [do not protect] です。
- [Source]：送信元ホストまたはネットワークの IP アドレス、ネットワーク オブジェクト グループ、またはインターフェイス IP アドレスを指定します。ルールでは、送信元と宛先の両方で同じアドレスを使用できません。[...] をクリックして、次のフィールドを含む [Browse Source] ダイアログボックスを開きます。
  - [Add/Edit]：送信元アドレスまたはグループを追加するには、[IP Address] または [Network Object Group] を選択します。
  - [Delete]：エントリを削除します。
  - [Filter]：表示される結果をフィルタリングする IP アドレスを入力します。
  - [Name]：続くパラメータが、送信元ホストまたはネットワークの名前を指定することを示します。
  - [IP Address]：続くパラメータが、送信元ホストまたはネットワークのインターフェイス、IP アドレス、およびサブネット マスクを指定することを示します。

- [Netmask]：IPアドレスに適用する標準サブネットマスクを選択します。このパラメータは、[IP Address] オプション ボタンを選択するときに表示されます。
- [Description]：説明を入力します。
- [Selected Source]：選択したエントリを送信元として含めるには [Source] をクリックします。

- [Destination]：宛先ホストまたはネットワークの IP アドレス、ネットワーク オブジェクト グループ、またはインターフェイス IP アドレスを指定します。ルールでは、送信元と宛先の両方で同じアドレスを使用できません。ここを ... [...] をクリックして、次のフィールドを含む [宛先の参照（Browse Destination）] ダイアログを開きます。
  - [Add/Edit]：[IP Address] または [Network Object Group] を選択して、宛先アドレスまたはグループを追加します。
  - [Delete]：エントリを削除します。
  - [Filter]：表示される結果をフィルタリングする IP アドレスを入力します。
  - [Name]：続くパラメータが、宛先ホストまたはネットワークの名前を指定することを示します。
  - [IP Address]：続くパラメータが、宛先ホストまたはネットワークのインターフェイス、IP アドレス、およびサブネット マスクを指定することを示します。
  - [Netmask]：IPアドレスに適用する標準サブネットマスクを選択します。このパラメータは、[IP Address] オプション ボタンを選択するときに表示されます。
  - [Description]：説明を入力します。
  - [Selected Destination]：選択したエントリを宛先として含めるには [Destination] をクリックします。

- [Service]：サービスを入力するか、または [...] をクリックして [Browse Service] ダイアログ ボックスを開き、サービスのリストから選択できます。
- [Description]：[Traffic Selection] のエントリの説明を入力します。
- More Options
  - [Enable Rule]：このルールをイネーブルにします。
  - [Source Service]：サービスを入力するか、[...] をクリックしてサービス参照ダイアログボックスを開き、サービスのリストから選択します。
  - [Time Range]：このルールを適用する時間範囲を定義します。
  - [Group]：続くパラメータが、送信元ホストまたはネットワークのインターフェイスとグループ名を指定することを示します。
  - [Interface]：IP アドレスのインターフェイス名を選択します。このパラメータは、[IP Address] オプション ボタンを選択するときに表示されます。

- [IP address]：このポリシーが適用されるインターフェイスの IP アドレスを指定します。このパラメータは、[IP Address] オプション ボタンを選択するときに表示されます。
- [Destination]：送信元、宛先のホストまたはネットワークについて、IP アドレス、ネットワーク オブジェクト グループ、またはインターフェイス IP アドレスを指定します。ルールでは、送信元と宛先の両方で同じアドレスを使用できません。これらのフィールドのいずれかで [...] をクリックし、次のフィールドを含む [Browse] ダイアログボックスを開きます。
- [Name]：送信元または宛先のホストまたはネットワークとして使用するインターフェイス名を選択します。このパラメータは、[Name] オプション ボタンを選択するときに表示されます。これは、このオプションに関連付けられる唯一のパラメータです。
- [Interface]：IP アドレスのインターフェイス名を選択します。このパラメータは、[Group] オプション ボタンをクリックするときに表示されます。
- [Group]：送信元または宛先のホストまたはネットワークに指定されたインターフェイスに存在するグループの名前を選択します。リストにエントリが何もない場合は、既存グループの名前を入力できます。このパラメータは、[Group] オプション ボタンをクリックするときに表示されます。

- [Protocol and Service]：このルールに関連するプロトコル パラメータとサービス パラメータを指定します。

（注） 「Any - any」IPsec ルールは使用できません。このタイプのルールにより、デバイスおよびそのピアが複数の LAN-to-LAN トンネルをサポートできなくなります。

- [TCP]：このルールを TCP 接続に適用することを指定します。これを選択すると、[Source Port] グループ ボックスと [Destination Port] グループ ボックスも表示されます。
- [UDP]：ルールを UDP 接続に適用することを指定します。これを選択すると、[Source Port] グループ ボックスと [Destination Port] グループ ボックスも表示されます。
- [ICMP]：ルールを ICMP 接続に適用することを指定します。これを選択すると、[ICMP Type] グループ ボックスも表示されます。
- [IP]：このルールを IP 接続に適用することを指定します。これを選択すると、[IP Protocol] グループ ボックスも表示されます。
- [Manage Service Groups]：[Manage Service Groups] ペインを表示します。このパネルでは、TCP/UDP サービス/ポートのグループを追加、編集、または削除できます。
- [Source Port] および [Destination Port]：[Protocol and Service] グループ ボックスで選択したオプション ボタンに応じて、TCP または UDP ポート パラメータが表示されます。

- [Service]：個々のサービスのパラメータを指定しようとしていることを示します。フィルタの適用時に使用するサービス名とブーリアン演算子を指定します。
- [Boolean operator]（ラベルなし）：[Service] ボックスで指定したサービスを照合するときに使用するブーリアン条件（等号、不等号、大なり、小なり、または範囲）を一覧表示します。
- [Service]（ラベルなし）：照合対象のサービス（https、ldaps、その他）を特定します。range サービス演算子を指定すると、このパラメータは 2 つのボックスに変わります。ボックスに、範囲の開始値と終了値を入力します。
- [...]：サービスのリストが表示され、ここで選択したサービスが [Service] ボックスに表示されます。
- [Service Group]：送信元ポートのサービス グループの名前を指定しようとしていることを示します。
- [Service]（ラベルなし）：使用するサービス グループを選択します。
- [ICMP Type]：使用する ICMP タイプを指定します。デフォルトは any です。[...] ボタンをクリックすると、使用可能なタイプのリストが表示されます。

- Options
  - [Time Range]：既存の時間範囲の名前を指定するか、または新しい範囲を作成します。
  - [...]：[Add Time Range] ペインが表示され、ここで新しい時間範囲を定義できます。
  - [Please enter the description below (optional)]：ルールについて簡単な説明を入力するためのスペースです。

IPsec 事前フラグメンテーション ポリシー

[Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Prefragmentation Policies]

IPSec Pre-Fragmentation ポリシーでは、パブリック インターフェイスを介してトラフィックをトンネリングするときに、最大伝送単位（MTU）の設定を超えるパケットの処理方法を指定します。この機能により、ASA とクライアント間のルータまたは NAT デバイスが IP フラグメントを拒否またはドロップする状況に対処できます。たとえば、クライアントが ASA の背後の FTP サーバーに対して FTP get コマンドを実行するとします。FTP サーバーから送信されるパケットは、カプセル化された場合にパブリック インターフェイス上の ASA の MTU サイズを超過する可能性があります。ASA でのこれらのパケットの処理方法は、選択されたオプションに応じて決まります。事前フラグメンテーション ポリシーは、ASA のパブリック インターフェイスから送出されるすべてのトラフィックに適用されます。

ASA は、トンネリングされたすべてのパケットをカプセル化します。このカプセル化の後、ASA は MTU の設定値を超えるパケットをフラグメント化して、パブリック インターフェイスから送信します。これがデフォルトのポリシーです。このオプションは、フラグメント化されたパケットが、障害なしでトンネル通過を許可される状況で機能します。FTP の例では、大き

なパケットがカプセル化されてから、IP レイヤでフラグメント化されます。中間デバイスは、フラグメントをドロップするか、または異常なフラグメントだけをドロップします。ロードバランシング デバイスが、異常フラグメントを取り入れる可能性があります。

事前フラグメンテーションをイネーブルにすると、カプセル化の前に、MTU の設定値を超えるトンネリングされたパケットがフラグメント化されます。これらのパケットに DF ビットが設定されている場合、ASA は DF ビットをクリアし、パケットをフラグメント化してからカプセル化します。このアクションにより、パブリック インターフェイスを離れる 2 つの独立した非フラグメント化 IP パケットが作成され、ピア サイトで再構成される完全なパケットにフラグメントを変換することにより、これらのパケットがピア サイトに正常に伝送されます。ここでの例では、ASA は MTU を無効化し、DF ビットをクリアすることによってフラグメンテーションを許可します。

（注） いずれのインターフェイスにおいても、MTU または事前フラグメンテーションのオプションを変更すると、すべての既存の接続が切断されます。たとえば、パブリック インターフェイスで 100 件のアクティブなトンネルが終了し、そのときに外部インターフェイスで [MTU] または [Pre-Fragmentation] オプションを変更すると、パブリック インターフェイスのすべてのアクティブなトンネルがドロップされます。

このペインでは、親ペインで選択したインターフェイスの既存の IPSec 事前フラグメンテーション ポリシーと Do-Not-Fragment（DF）ビット ポリシーを表示または**編集**します。

フィールド

- [Interface]：選択されたインターフェイスを識別します。このダイアログボックスを使用しても、このパラメータは変更できません。
- [Enable IPsec pre-fragmentation]：IPSec の事前フラグメンテーションをイネーブルまたはディセーブルにします。ASA は、カプセル化する前に、MTU の設定を超えるトンネリングされたパケットをフラグメント化します。これらのパケットに DF ビットが設定されている場合、ASA は DF ビットをクリアし、パケットをフラグメント化してからカプセル化します。このアクションにより、パブリック インターフェイスを離れる 2 つの独立した非フラグメント化 IP パケットが作成され、ピア サイトで再構成される完全なパケットにフラグメントを変換することにより、これらのパケットがピア サイトに正常に伝送されます。
- [DF Bit Setting Policy]：Do-Not-Fragment ビット ポリシー：[Copy]、[Clear]、または [Set]

IKEv2 フラグメンテーション オプションの設定

ASA では、IKEv2 フラグメンテーションをイネーブルまたはディセーブルにすることができ、IKEv2 パケットのフラグメント化で使用する MTU（最大伝送ユニット）を指定できます。また、管理者は次の画面で、優先するフラグメンテーション方式を設定できます。

[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE parameters]

デフォルトでは、すべてのIKEv2フラグメンテーション方式がイネーブルになり、MTUは576（IPv4 の場合）または 1280（IPv6 の場合）、優先される方式は IETF 標準 RFC-7383 となります。

次の点を考慮して、MTU を指定してください。

- 使用する MTU 値には、IP（IPv4/IPv6）ヘッダー＋UDP ヘッダーのサイズを含める必要があります。
- 管理者によって指定されていない場合、デフォルトの MTU は 576（IPv4 の場合）または 1280（IPv6 の場合）となります。
- 指定すると、同じ MTU が IPv4 と IPv6 の両方で使用されます。
- 有効範囲は 68 ～ 1500 です。

（注） MTU の設定時に ESP オーバーヘッドを考慮する必要があります。暗号化中に MTU に追加される ESP オーバーヘッドにより、暗号化後にパケットサイズが増加します。「packet too big」エラーが表示された場合は、MTU サイズを確認し、より低い MTU を設定してください。

次のサポートされているフラグメンテーション方式のいずれかを、IKEv2 の優先フラグメンテーション方式 として設定できます。

- IETF RFC-7383 標準ベースの IKEv2 フラグメンテーション。
  - この方式は、両方のピアがネゴシエーション中にサポートとプリファレンスを指定する場合に使用されます。
  - この方式を使用すると、フラグメンテーションの後に暗号化が実行され、各IKEv2フラグメント メッセージが個別に保護されます。
- シスコ独自のフラグメンテーション。
  - この方式は、これが AnyConnect クライアント などのピアによって提供される唯一の方法である場合、または両方のピアがネゴシエーション中にサポートとプリファレンスを指定する場合に使用されます。
  - この方式を使用すると、暗号化の後にフラグメンテーションが実行されます。受信側のピアは、すべてのフラグメントを受信するまで、メッセージを復号することも認証することもできません。
  - この方式は、シスコ以外のピアとの相互運用性はありません。

始める前に

- パスMTUディスカバリはサポートされていません。MTUは、ネットワークのニーズに合わせて手動で設定する必要があります。

- この設定はグローバルであり、設定の適用後に確立される SA に影響を及ぼします。適用以前の SA は影響を受けません。フラグメンテーションがディセーブルになっている場合でも同様です。
- 最大 100 のフラグメントを受信できます。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Site-to-Site VPN]** > **[Advanced]** > **[IKE parameters]** に移動します。
ステップ 2 [Enable fragmentation] フィールドを選択または選択解除します。
ステップ 3 [Fragmentation MTU] でサイズを指定します。
ステップ 4 [Preferred fragmentation method] で優先する方式を指定します。

IPsec Proposals (Transform Sets)

[Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Proposals (Transform Sets)]

トランスフォームは、データ フローで実行される操作のセットで、データ認証、データ機密性、およびデータ圧縮を実現します。たとえば、1 つのトランスフォームは、3DES 暗号化と HMAC-MD5 認証アルゴリズム（ESP-3DES-MD5）による ESP プロトコルです。

このペインは、後述する IKEv1 および IKEv2 トランスフォーム セットを表示、**追加**、**編集**、または**削除**するために使用します。各テーブルには、設定済みのトランスフォームセットの名前と詳細が表示されます。

[IKEv1 IPsec Proposals （Transform Sets）]

- [Mode]：ESP 暗号化と認証を適用するモード。これにより、ESP が適用されるオリジナルの IP パケットの部分が決定されます。
  - [Tunnel mode]（デフォルト）：ESP 暗号化と認証が元の IP パケット全体（IP ヘッダーとデータ）に適用されるため、本来の送信元アドレスと宛先アドレスが非表示になります。元の IP データグラム全体が暗号化され、新しい IP パケットのペイロードになります。このモードでは、ルータなどのネットワーク デバイスが IPsec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。トンネル モードの大きな利点は、エンド システムを変更しなくても IPsec を利用できるということです。また、トラフィック分析から保護することもできます。トンネル モードを使用すると、攻撃者にはトンネルのエンドポイントしかわからず、トンネリングされたパケットの本来の送信元と宛先はわかりません（これらがトンネルのエンドポイントと同じ場合でも同様）。

- [Transport mode]：IP ペイロードだけが暗号化され、元の IP ヘッダーはそのままになります。このモードには、各パケットに数バイトしか追加されず、パブリック ネットワーク上のデバイスに、パケットの最終的な送信元と宛先を認識できるという利点があります。転送モードでは、中間ネットワークでの特別な処理（たとえばQoS）を、IPヘッダーの情報に基づいて実行できるようになります。ただし、レイヤ4ヘッダーが暗号化されるため、パケットの検査が制限されます。

- [ESP Encryption]：トランスフォーム セットのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズム。ESP では、データ プライバシー サービス、オプションのデータ認証、およびリプレイ攻撃防止サービスが提供されます。ESPは、保護されているデータをカプセル化します。

- [ESP Authentication]：トランスフォーム セットの ESP 認証アルゴリズム。

[IKEv2 IPsec Proposals]

- [Mode]：ESP暗号化と認証を適用するモード。これにより、ESPが適用されるオリジナルの IP パケットの部分が決定されます。

  - [Tunnel mode]（デフォルト）：カプセル化モードがトンネルモードになります。トンネル モードでは、ESP 暗号化と認証が元の IP パケット全体（IP ヘッダーとデータ）に適用されるため、本来の送信元アドレスと宛先アドレスが非表示になります。元の IP データグラム全体が暗号化され、新しい IP パケットのペイロードになります。

    このモードでは、ルータなどのネットワーク デバイスが IPsec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。

    トンネルモードの大きな利点は、エンドシステムを変更しなくてもIPsecを利用できるということです。また、トラフィック分析から保護することもできます。トンネルモードを使用すると、攻撃者にはトンネルのエンドポイントしかわからず、トンネリングされたパケットの本来の送信元と宛先はわかりません（これらがトンネルのエンドポイントと同じ場合でも同様）。

  - [Transport mode]：ピアがサポートしていない場合、カプセル化モードは、トンネルモードにフォールバックするオプション付きの転送モードになります。transport モードでは IP ペイロードだけが暗号化され、元の IP ヘッダーはそのまま使用されます。

    このモードには、各パケットに数バイトしか追加されず、パブリックネットワーク上のデバイスに、パケットの最終的な送信元と宛先を認識できるという利点があります。転送モードでは、中間ネットワークでの特別な処理（たとえばQoS）を、IPヘッダーの情報に基づいて実行できるようになります。ただし、レイヤ4ヘッダーが暗号化されるため、パケットの検査が制限されます。

  - [Transport Required]：カプセル化モードは転送モードにしかなりません。トンネルモードにフォールバックすることはできません。

（注） 転送モードは、リモート アクセス VPN には推奨されません。

カプセル化モードのネゴシエーションの例は次のとおりです。

- イニシエータが転送モードを提案し、レスポンダがトンネル モードで応答した場合、イニシエータはトンネル モードにフォールバックします。
- 発信側が tunnel モードを提示し、応答側が transport モードで応答した場合、応答側は tunnel モードにフォールバックします。
- 発信側が tunnel モードを提示し、応答側が transport-require モードの場合、応答側はプロポーザルを送信しません。
- 同様に、イニシエータが transport-require モードで、レスポンダがトンネル モードの場合は、レスポンダから NO PROPOSAL CHOSEN が送信されます。

- [Encryption]：IKEv2 IPsec プロポーザルのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズムを示します。ESP では、データ プライバシー サービス、オプションのデータ認証、およびリプレイ攻撃防止サービスが提供されます。ESP は、保護されているデータをカプセル化します。
- [Integrity Hash]：ESP プロトコルのデータ整合性を保証するためのハッシュ アルゴリズムを示します。パケットが想定した発信元から発信されたこと、また搬送中に変更されていることを保証します。パケットが想定した発信元から発信されたこと、また搬送中に変更されていることを保証します。AES-GCM/GMAC が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。