IKE、ロード バランシング、および NAC の構成

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 ネットワークの 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ます。また、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。

ロード バランシングは、VPN クラスタ内の 2 台以上の ASA 間で、VPN トラフィックを分散します。

ネットワーク アクセス コントロール（NAC）は、ネットワークへの本番アクセスの条件としてエンドポイントの準拠性チェックと脆弱性チェックを実行することにより、ワーム、ウイルス、および不正アプリケーションによる侵入および感染からエンタープライズのネットワークを保護します。これらのチェックは、*ポスチャ検証* と呼ばれます。

この章では、IKE、ロード バランシング、および NAC の構成方法について説明します。内容は次のとおりです。

インターフェイスでの IKE のイネーブル化

IKE を使用するには、使用する予定のインターフェイスごとに、IKE をイネーブルにする必要があります。

VPN 接続の場合

ステップ 1 ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] の順に進みます。

ステップ 2　[Access Interfaces] セクションで、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。

サイト間 VPN の場合

ステップ 1　ASDM で、[Configuration] > [Site-to-Site VPN] > [Connection Profiles] の順に進みます。

ステップ 2　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 パラメータの設定

IKE パラメータ

ASDM で、[Configuration] > [Site-to-Site VPN] > [Advanced] > [IKE Parameters] の順に進みます。

NAT 透過性

IPSec over NAT-T のイネーブル化

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] ペインのフラグメンテーション ポリシー 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 機能に対応す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。
- 1 度に 1 つのトンネルをサポートする VPN 3002 ハードウェア クライアントは、標準の IPsec、IPsec over TCP、NAT-Traversal、または IPsec over UDP を使用して接続できます。
- 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 とその接続先の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 がイネーブルのインターフェイスから ASA を管理することができなくなります。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。

ピアに送信された 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

インバウンド Aggressive モード接続のディセーブル化

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。

接続解除の前にピアに警告する

ASA のシャットダウンまたはリブート、セッション アイドル タイムアウト、最大接続時間の超過、または管理者による停止などのいくつかの理由で、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することがあります。

ASA は、（LAN-to-LAN コンフィギュレーションの場合）限定されたピアである VPN クライアントと VPN 3002 ハードウェア クライアントに、セッションが接続解除される直前に通知し、その理由を伝えることができます。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、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することができます。

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）。
- 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっている VPN 3002 ハードウェア クライアント。
- 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっている VPN 3000 シリーズ コンセントレータ

リブートの前にアクティブ セッション自発的に終了するのを待機

すべてのアクティブ セッションが自発的に終了した場合に限り、ASA が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。

IKEv1 のネゴシエーションで許可される SA の数

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 仕様の設定

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]：選択すると、SA 初期パケットへの応答として、ASA からクッキー チャレンジがピア デバイスに送信されるようになります。
  - [% threshold before incoming SAs are cookie challenged]：ASA に対して許可される SA の総数のうち、ネゴシエーション中であるものの割合（%）。この数に達すると、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。デフォルト値は 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。

IKE v2 固有の設定による 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はありません。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、攻撃者が攻撃を開始すると、ピア デバイスから SA 初期パケットが送信され、ASA からその応答が送信されますが、ピア デバイスからのそれ以降の応答が停止されます。ピア デバイスがこれを継続的に行うと、許可されている数の SA 要求が使い果たされてしまい、最終的に ASA が応答を停止してしまうことがあります。

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、それ以降到着した SA 初期パケットに対してクッキー チャレンジを行います。10,000 個の IKEv2 SA が許可される Cisco ASA 5580 では、5000 個の SA がオープンになると、それ以降の着信 SA に対してクッキー チャレンジが行われます。

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。

IKE ポリシーの作成

IKE の概要

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。

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。このアルゴリズムを使用して、ASA は暗号キーとハッシュ キーを導出します。
- ASA が暗号キーを置き換える前に、この暗号キーを使用する最長時間の制限。

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 ポリシーが何も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 ポリシーは常にプライオリティが最も低く設定され、各パラメータはデフォルト値に設定されます。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。

IKE ポリシーの設定

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec > IKE Policies]

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

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。
- [Add]/[Edit]/[Delete]：IKEv1 ポリシーを追加、編集、または削除するときにクリックします。
- [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。
- [Add]/[Edit]/[Delete]：IKEv2 ポリシーを追加、編集、または削除するときにクリックします。

IKEv1 ポリシーの追加

[Configuration] > [VPN] > [IKE] > [Policies] > [Add/Edit IKEv1 Policy]

フィールド

[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て拡張が困難ですが、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。
crack	モバイル IPSec がイネーブルになっているクライアントの IKE Challenge/Response for Authenticated Cryptographic Keys プロトコル。証明書以外の認証技術を使用します。

[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）	デフォルトの Group 2（1024 ビット Diffie-Hellman）は、Group 1 または 5 と比較して、CPU の実行時間は短いですが、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）	

[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

[Configuration] > [VPN] > [IKE] > [Policies] > [Add/Edit IKEv2 Policy]

フィールド

[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 md5	SHA 1 MD5	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。
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。
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 md5	SHA-1 MD5	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。
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

ポリシーの割り当て

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy]

[Assignment Policy] は、IP アドレスがリモート アクセス クライアントに割り当てられる方法を設定します。

フィールド

- [Use authentication server]：認証サーバから取得した IP アドレスをユーザ単位で割り当てる場合に選択します。IP アドレスが設定された認証サーバ（外部または内部）を使用している場合は、この方式を使用することを推奨します。許可サーバは、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups] ペインで設定されます。
- [Use DHCP]：DHCP サーバから IP アドレスを取得する場合に選択します。DHCP を使用する場合は、[Configuration] > [Remote Access VPN] > [DHCP Server] ペインでサーバを設定します。
- [Use internal address pools]：ASA により、内部で設定されたプールから IP アドレスを割り当てる場合に選択します。内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。この方法を使用する場合は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] ペインで IP アドレス プールを設定します。
  - [Allow the reuse of an IP address __ minutes after it is released]：IP アドレスがアドレス プールに戻された後に、IP アドレスを再利用するまでの時間を指定します。遅延時間を設けることにより、IP アドレスがすぐに再割り当てされることによって発生する問題がファイアウォールで生じないようにできます。デフォルトでは、これはチェックされません。つまり、ASA は遅延時間を課しません。遅延を追加する場合は、チェックボックスをオンにし、IP アドレスを再割り当てするまでの時間を 1 ～ 480 の範囲で指定します。

IPsec の設定

ASA では、IPsec は LAN-to-LAN VPN 接続に使用され、client-to-LAN VPN 接続にも IPsec を使用できます。IPSec 用語で「ピア」とは、リモート アクセス クライアントまたは別のセキュアなゲートウェイを意味します。

（注） ASA は、シスコのピア（IPv4 または IPv6））や、関連するすべての標準に準拠したサードパーティのピアとの LAN-to-LAN IPsec 接続をサポートしています。

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します。IPsec client-to-LAN 接続では、ASA は応答側としてだけ機能します。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
- Diffie-Hellman Group 1、2、および 5
- 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）

クリプト マップの追加

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [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。

フィールド

（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。

- [Add]：[Create IPSec Rule] が開きます。このダイアログボックスでは、ルールの基本、詳細、およびトラフィックの選択パラメータを設定できます。
- [Edit]：既存のルールを編集します。
- [Delete]：テーブルで選択したルールを削除します。
- [Cut]：テーブルで選択したルールを切り取り、コピーできるようにクリップボードに保持します。
- [Copy]：テーブルで選択したルールをコピーします。
- [Find]：検索する既存ルールのパラメータを指定するための [Find] ツールバーをイネーブルにします。

  - [Filter] : [is] または [contains] を選択し、フィルタ パラメータを入力することによって、Interface、Source、Destination Service、または Rule Query を基準にして検索結果をフィルタリングします。[...] 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。

- [Diagram] : 選択した IPSec ルールを示す図を表示します。
- [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、単語 any が付いたインターフェイス名が含まれることがあります（inside: any など）。any とは、内部インターフェイスにある任意のホストが、ルールによって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] オプション ボタンを参照）では、アドレス カラムに、単語 any が付いたインターフェイス名が含まれることがあります（outside: any など）。any とは、外部インターフェイスにある任意のホストが、ルールによって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。内部ホストが外部ホストへの接続を作成すると、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 マッピングを維持します。このアドレス マッピング構造は xlate と呼ばれ、一定の時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] : ポリシーで逆ルート注入がイネーブルになっているかどうかを示します。
- [Connection Type] :（スタティック トンネル ポリシーでだけ適用）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」という説明が加えられます。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、またはカラムをダブルクリックします。

- [Enable Anti-replay window size]：アンチ リプレイ 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。トラフィック シェーピングを使用する、階層型 QoS におけるプライオリティ キューイングに伴う副次的な影響としては、（「[Rule Actions] > [QoS] タブ」を参照）パケットの順番が変わる点が挙げられます。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。

IPSec ルール / トンネル ポリシー（クリプト マップ）の作成：[Basic] タブ

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Crypto Maps] : [Edit IPsec Rule] : [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 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。

フィールド

- [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 トンネルの場合にだけ該当）このポリシーの接続タイプを、bidirectional、originate-only、または answer-only から選択します。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。
- [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] : 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。

IPSec ルール / トンネル ポリシー（クリプト マップ）の作成：[Advanced] タブ

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Crypto Maps] : [Edit IPsec Rule] : [Advanced] タブ

フィールド

- [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。逆ルート注入（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。
- [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。

IPsec ルールの作成：[Traffic Selection] タブ

[Configuration] > [VPN] > [IPsec] > [IPSec Rules] > [Add/Edit Rule] > [Tunnel Policy (Crypto Map)]：[Traffic Selection] タブ

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。

フィールド

- [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。[...] をクリックして、次のフィールドを含む [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 ボタンを選択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 ボタンを選択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]：このルールを 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]：このルールを 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] ペインが表示され、ここで 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 のポート 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、kerberos、その他）を指定します。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。

- オプション
  - [Time Range]：既存の時間範囲の名前を指定するか、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。

Pre-Fragmentation

[Configuration] > [VPN] > [IPsec] > [Pre-Fragmentation]

このペインでは、任意のインターフェイスの IPSec の Pre-Fragmentation ポリシーと Do-Not-Fragment（DF）ビット ポリシーを設定します。

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 とクライアントの間のルータまたは 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場合に対処できます。たとえば、クライアントが ASA の背後の FTP サーバに対して FTP get コマンドを実行するとします。FTP サーバから送信されるパケットは、カプセル化されたときにパブリック インターフェイス上の ASA の MTU サイズを超過します。選択したオプションにより、ASA でのこれらのパケットの処理方法が決まります。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。カプセル化した後、ASA は、パブリック インターフェイスから送信する前に MTU の設定値を超えるパケットをフラグメント化します。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、ASA は、MTU の設定値を超えるトンネリングされたパケットをカプセル化する前に、フラグメント化します。これらのパケットで 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 が MTU を無効にし、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*インターフェイスであっても、[MTU] または [Pre-Fragmentation] オプションを変更すると、*すべての*既存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。

フィールド

- [Pre-Fragmentation]：設定済みインターフェイスごとに、現在の事前フラグメンテーションの設定を示します。
  - [Interface]：設定済みインターフェイスの名前を示します。
  - [Pre-Fragmentation Enabled]：インターフェイスごとに、事前フラグメンテーションがイネーブルになっているかどうかを示します。
  - [DF Bit Policy]：各インターフェイスの DF ビット ポリシーを示します。
- [Edit]：[Edit IPsec Pre-Fragmentation Policy] ダイアログボックスを表示します。

Edit IPSec Pre-Fragmentation Policy

[Configuration] > [VPN] > [IPsec] > [Pre-Fragmentation] > [Edit IPSec Pre-Fragmentation Policy]

このペインでは、親ペイン（[Configuration] > [VPN] > [IPSec] > [Pre-Fragmentation]）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 ポリシーを変更します。

フィールド

- [Interface]：選択されたインターフェイスの名前を識別します。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。これらのパケットで 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]）を選択します。

IPSec トランスフォーム セット

[Configuration] > [VPN] > [IPsec] > [Transform Sets]

このペインでは、トランスフォーム セットを表示、追加、または編集します。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。

フィールド

- [IKEv1 IPsec Proposals (Transform Sets)]：設定済みのトランスフォーム セットを示します。
  - [Name]：トランスフォーム セットの名前を示します。
  - [Mode]：トランスフォーム セットのモード（Tunnel）を示します。このパラメータにより、ESP 暗号化と認証を適用する場合のモードを指定します。言い換えると、ESP が適用されている元の IP パケットの部分を指定します。Tunnel 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隠されることになります。
  - [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。
  - [ESP Authentication]：トランスフォーム セットの ESP 認証アルゴリズムを示します。
- [Add]：[Add Transform Set] ダイアログボックスが開き、ここで新しいトランスフォーム セットを追加できます。
- [Edit]：[Edit Transform Set] ダイアログボックスが開き、ここで既存のトランスフォーム セットを変更できます。
- [Delete]：選択したトランスフォーム セットを削除します。確認されず、やり直しもできません。
- [IKEv2 IPsec Proposals]：設定済みのトランスフォーム セットを示します。
  - [Name]：**IKEv2 IPsec プロポーザル**の名前を示します。
  - [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。
- [Add]：[Add IPsec Proposal] ダイアログボックスが開き、ここで新しいプロポーザルを追加できます。
- [Edit]：[Edit IPsec Proposal] ダイアログボックスが開き、ここで既存のプロポーザルを変更できます。
- [Delete]：選択されているプロポーザルを削除します。確認されず、やり直しもできません。

Add/Edit IPsec Proposal（トランスフォーム セット）

（[Configuration] > [VPN] > [IPsec] > [Transform Sets] > [Add/Edit IPsec_Proposal_(Transform Set)]）

このペインでは、IPsec IKEv1 トランスフォーム セットを追加または変更します。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。

フィールド

- [Set Name]：このトランスフォーム セットの名前を指定します。
- [Properties]：このトランスフォーム セットのプロパティを設定します。これらのプロパティは、[Transform Sets] テーブルに表示されます。
  - [Mode]：トランスフォーム セットのモード（Tunnel）を示します。このフィールドは、ESP 暗号化と認証を適用する場合のモードを示します。言い換えると、ESP を適用している元の IP パケットの部分を指定します。Tunnel 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隠されることになります。
  - [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を選択します。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。
  - [ESP Authentication]：トランスフォーム セットの ESP 認証アルゴリズムを選択します。

（注） IPSec ESP（Encapsulating Security Payload）プロトコルでは、暗号化と認証の両方の機能が提供されます。パケット認証により、データが、データに記述されている送信元から送信されたことを保証します。これは、「データ整合性」とも呼ばれます。

Add/Edit IPsec Proposal

[Configuration] > [VPN] > [IPsec] > [Transform Sets] > [Add/Edit IPsec_Proposal]

このペインでは、IPsec IKEv2 プロポーザルを追加または変更します。プロポーザルは、データ フローで実行される操作の集合であり、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 つのプロポーザルで、ESP プロトコルと 3DES 暗号化、および HMAC-MD5 認証アルゴリズム（ESP-3DES-MD5）が指定されます。

フィールド

- [Name]：このプロポーザルの名前を指定します。
- [Encryption]：このプロポーザルのカプセル化セキュリティ プロトコル（ESP）を指定します。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]：このプロポーザルの ESP 認証アルゴリズムを選択します。ハッシュ アルゴリズムとは、ESP プロトコルのデータ整合性を保証するためのものです。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。

（注）　IPSec ESP（Encapsulating Security Payload）プロトコルでは、暗号化と認証の両方の機能が提供されます。パケット認証により、データが、データに記述されている送信元から送信されたことを保証します。これは、「データ整合性」とも呼ばれます。

ロード バランシングの設定

リモートクライアント コンフィギュレーションで、複数の ASA を同じネットワークに接続してリモート セッションを処理している場合、これらのデバイスでセッション負荷を分担するように設定できます。この機能は、*ロード バランシング*と呼ばれます。ロード バランシングでは、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。これによって、システム リソースを効率的に利用でき、パフォーマンスと可用性が向上します。

次の各項で、ロード バランシングについて説明します。

- 仮想クラスタの作成
- 地理的ロード バランシング
- ロード バランシングとフェールオーバーの比較
- ロード バランシングのライセンス要件
- ロード バランシングの前提条件
- 適格なクライアント
- High Availability and Scalability Wizard を使用した VPN クラスタ ロード バランシングの設定
- ロード バランシングの設定（ウィザードを使用しない場合）

仮想クラスタの作成

ロード バランシングを実装するには、同じプライベート LAN 間ネットワーク上の複数のデバイスを、論理的に*仮想クラスタ*としてグループ化します。

セッションの負荷は、仮想クラスタ内のすべてのデバイスに分散されます。仮想クラスタ内の 1 つのデバイスである*仮想クラスタ マスター*は、着信接続要求を*バックアップ デバイス*と呼ばれる他のデバイスに転送します。仮想クラスタ マスターは、クラスタ内のすべてのデバイスをモニタし、各デバイスの負荷を追跡して、その負荷に基づいてセッションの負荷を分散します。仮想クラスタ マスターの役割は、1 つの物理デバイスに結び付けられるものではなく、デバイス間でシフトできます。たとえば、現在の仮想クラスタ マスターで障害が発生すると、クラスタ内のバックアップ デバイスの 1 つがその役割を引き継いで、すぐに新しい仮想クラスタ マスターになります。

仮想クラスタは、外部のクライアントには 1 つの*仮想クラスタ IP アドレス*として表示されます。この IP アドレスは、特定の物理デバイスに結び付けられていません。現在の仮想クラスタ マスターに属しているため、仮想のアドレスです。接続の確立を試みている VPN クライアントは、最初にこの仮想クラスタ IP アドレスに接続します。仮想クラスタ マスターは、クラスタ内で使用できるホストのうち、最も負荷の低いホストのパブリック IP アドレスをクライアントに返します。2 回目のトランザクションで、クライアントは直接そのホストに接続します（この動作はユーザには透過的です）。仮想クラスタ マスターは、このようにしてリソース全体に均等かつ効率的にトラフィックを転送します。

クラスタ内のマシンで障害が発生すると、終了されたセッションはただちに仮想クラスタ IP アドレスに再接続できます。次に、仮想クラスタ マスターは、クラスタ内の別のアクティブ デバイスにこれらの接続を転送します。仮想クラスタ マスター自体に障害が発生した場合、クラスタ内のバックアップ デバイスが、ただちに新しい仮想セッション マスターを自動的に引き継ぎます。クラスタ内の複数のデバイスで障害が発生しても、クラスタ内のデバイスが 1 つ稼働していて使用可能である限り、ユーザはクラスタに引き続き接続できます。

ロードバランシング クラスタは、同じリリースまたは混在リリースの ASA で構成できます。ただし、次の制約があります。

- 同じリリースの ASA の両方で構成されるロードバランシング クラスタは、IPsec、AnyConnect、およびクライアントレス SSL VPN クライアントとクライアントレス セッションの組み合わせに対してロード バランシングを実行できます。
- 混在リリースの ASA または同じリリースの ASA で構成されるロードバランシング クラスタは、IPsec セッションのみをサポートできます。ただし、このようなコンフィギュレーションでは、ASA は、それぞれの IPsec のキャパシティに完全に到達しない可能性があります。「ロード バランシングとフェールオーバーの比較」（P.24）は、この状況を示しています。

Release 7.1(1) 以降、IPsec セッションと SSL VPN セッションは、クラスタ内の各デバイスが伝送する負荷を決定するときに均等にカウントまたは重み付けします。これは、ASA Release 7.0(x) ソフトウェアと VPN 3000 コンセントレータ用のロードバランシングの計算からの逸脱を意味しています。つまり、これらのプラットフォームでは、いずれも一部のハードウェア プラットフォームにおいて、IPsec セッションの負荷とは異なる SSL VPN セッションの負荷を計算する重み付けアルゴリズムを使用しています。

クラスタの仮想マスターは、クラスタのメンバにセッション要求を割り当てます。ASA は、すべてのセッション、SSL VPN または IPsec を同等と見なし、それらを同等に割り当てます。許可する IPsec セッションと SSL VPN セッションの数は、コンフィギュレーションおよびライセンスで許可されている最大数まで設定できます。

ロードバランシング クラスタで最大 10 のノードはテスト済みです。これよりクラスタが多くても機能しますが、そのようなトポロジは正式にはサポートされていません。

地理的ロード バランシング

ロード バランシング環境において DNS 解決が一定の間隔で変化する場合は、存続可能時間（TTL）の値をどのように設定するかを慎重に検討する必要があります。DNS ロード バランス設定が AnyConnect との組み合わせで適切に機能するには、マッピングを処理する ASA の名前が、その ASA が選択された時点からトンネルが完全に確立されるまでの間、同じである必要があります。所定の時間が経過してもクレデンシャルが入力されない場合は、ルックアップが再び開始して別の IP アドレスが解決済みアドレスとなることがあります。DNS のマッピング先が別の ASA に変更された後でクレデンシャルが入力された場合は、VPN トンネルの確立に失敗します。

VPN の地理的ロード バランシングでは、Cisco Global Site Selector（GSS）が使用されることがあります。GSS では DNS がロード バランシングに使用され、DNS 解決の存続可能時間（TTL）のデフォルト値は 20 秒となっています。GSS での TTL の値を大きくすると、接続失敗の確率を大幅に引き下げることができます。値を大きくすると、ユーザがクレデンシャルを入力してトンネルを確立するときの認証フェーズに十分な時間を取ることができます。

クレデンシャル入力のための時間を増やすには、「起動時接続」をディセーブルにすることも検討してください。

ロード バランシングとフェールオーバーの比較

ロード バランシングとフェールオーバーはどちらもハイ アベイラビリティ機能ですが、これらは機能も要件も異なります。場合によっては、ロード バランシングとフェールオーバーの両方を使用できます。次の項では、これらの機能の違いについて説明します。

*ロード バランシング*とは、リモートアクセス VPN トラフィックを、仮想クラスタ内のデバイス間で均等に分配するメカニズムのことです。この機能は、スループットまたはその他の要因を考慮しない単純なトラフィックの分散に基づいています。ロードバランシング クラスタは 2 つ以上のデバイスで構成され、そのうちの 1 つが仮想マスターとなり、それ以外はバックアップとなります。これらのデバイスは、完全に同じタイプである必要はなく、同じソフトウェア バージョンやコンフィギュレーションを使用する必要もありません。仮想クラスタ内のすべてのアクティブなデバイスがセッションの負荷を伝送します。ロードバランシングにより、トラフィックはクラスタ内の最も負荷の少ないデバイスに転送され、負荷はすべてのデバイス間に分散されます。これにより、システム リソースが効率的に使用され、パフォーマンスが向上し、ハイ アベイラビリティが実現されます。

フェールオーバー コンフィギュレーションでは、2 台の同一の ASA を、専用のフェールオーバー リンクと、ステートフル フェールオーバー リンク（任意）で接続します。アクティブ インターフェイスおよび装置のヘルスがモニタされて、所定のフェールオーバー条件に一致しているかどうかが判断されます。これらの条件に一致した場合は、フェールオーバーが行われます。フェールオーバーは、VPN とファイアウォールの両方のコンフィギュレーションをサポートします。

ASA は、アクティブ/アクティブ フェールオーバーとアクティブ/スタンバイ フェールオーバーの 2 つのフェールオーバーをサポートします。VPN 接続は、アクティブ/スタンバイの単一ルーテッド モードでのみ実行されます。Active/Active フェールーバーにはマルチコンテキスト モードが必要であるため、VPN 接続をサポートしません。

アクティブ/アクティブ フェールオーバーでは、両方の装置がネットワーク トラフィックを渡すことができます。これは、同じ結果になる可能性がありますが、真のロード バランシングではありません。フェールオーバーが行われると、残りのアクティブ装置が、設定されたパラメータに基づいて結合されたトラフィックの通過を引き継ぎます。したがって、アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにする必要があります。

アクティブ/スタンバイ フェールオーバーでは、1 つの装置だけがトラフィックを通過させることができ、もう 1 つの装置はスタンバイ状態で待機して、トラフィックを通過させません。アクティブ/スタンバイ フェールオーバーでは、2 番目の ASA を使用して、障害の発生した装置の機能を引き継ぎます。アクティブ装置が故障すると、スタンバイ状態に変わり、そしてスタンバイ装置がアクティブ状態に変わります。アクティブになる装置が、障害の発生した装置の IP アドレス（または、トランスペアレント ファイアウォールの場合は管理 IP アドレス）および MAC アドレスを引き継いで、トラフィックの転送を開始します。現在スタンバイになっている装置が、アクティブ装置のスタンバイの IP アドレスを引き継ぎます。アクティブ装置で障害が発生すると、スタンバイ装置は、クライアント VPN トンネルを中断することなく引き継ぎます。

ロード バランシングのライセンス要件

VPN ロード バランシングを使用するには、Plus ライセンスを備えた ASA モデル 5510、または ASA モデル 5520 以降が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロード バランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

適格なクライアント

ロード バランシングは、次のクライアントで開始されるリモート セッションでのみ有効です。

- Cisco AnyConnect Secure Mobility Client（Release 3.0 以降）
- Cisco ASA 5505 セキュリティ アプライアンス（Easy VPN クライアントとして動作する場合）
- IKE リダイレクトをサポートする IOS EZVPN クライアント デバイス（IOS 831/871）
- クライアントレス SSL VPN（クライアントではない）

ロード バランシングは、IPsec クライアント セッションと SSL VPN クライアントおよびクライアントレス セッションで機能します。LAN-to-LAN を含む他のすべての VPN 接続タイプ（L2TP、PPTP、L2TP/IPsec）は、ロード バランシングがイネーブルになっている ASA に接続できますが、これらの接続タイプはロード バランシングには参加できません。

ロード バランシングの前提条件

- ロード バランシングを設定する前に、まず ASA でパブリック インターフェイスとプライベート インターフェイスを設定する必要があります。これを行うには、[Configuration] > [Device Setup] > [Interfaces] を選択します。詳細については、一般的な操作のコンフィギュレーション ガイドの Chapter 8, “Starting Interface Configuration (ASA 5510 and Higher)” または Chapter 9, “Starting Interface Configuration (ASA 5505)” を参照してください。
- 仮想クラスタ IP アドレスが参照するインターフェイスを事前に設定する必要があります。
- クラスタに参加するすべてのデバイスは、同じクラスタ固有の値（IP アドレス、暗号化設定、暗号キー、およびポート）を共有する必要があります。クラスタ内のロードバランシング デバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

証明書の確認

AnyConnect でロード バランシングの証明書確認を実行し、IP アドレスによって接続がリダイレクトされている場合、クライアントにより、この IP アドレスを通してその名前チェックがすべて実行されます。リダイレクト IP アドレスが証明書の一般名、つまり subject alt name に一覧表示されていることを確認する必要があります。IP アドレスがこれらのフィールドに存在しない場合、証明書は非信頼と見なされます。

RFC 2818 で定義されたガイドラインに従って、**subject alt name** が証明書に組み込まれている場合、名前チェックにのみ **subject alt name** を使用し、一般名は無視します。証明書を提示しているサーバの IP アドレスが証明書の **subject alt name** で定義されていることを確認します。

スタンドアロン ASA の場合、IP アドレスはその ASA の IP です。クラスタリング環境では、証明書の設定により異なります。クラスタで使用されている証明書が 1 つの場合、それがクラスタの IP になり、証明書には Subject Alternative Name 拡張子があり、それぞれ ASA の IP と FQDN を持っています。クラスタで使用されている証明書が複数の場合、それが再度 ASA の IP アドレスになるはずです。

High Availability and Scalability Wizard を使用した VPN クラスタ ロード バランシングの設定

リモートクライアント コンフィギュレーションで、複数の ASA を同じネットワークに接続してリモート セッションを処理している場合、これらのデバイスでセッション負荷を分担するように設定できます。この機能はロード バランシングと呼ばれ、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。ロード バランシングにより、システム リソースが効率的に使用され、パフォーマンスとシステム アベイラビリティが向上します。

[VPN Cluster Load Balancing Configuration] 画面を使用して、デバイスがロード バランシング クラスタに参加するのに必要なパラメータを設定します。

ロード バランシングをイネーブルにするには、次の手順を実行します。

- 共通仮想クラスタ IP アドレス、UDP ポート（必要に応じて）、およびクラスタの IPsec 共有秘密情報を確立することによりロードバランシング クラスタを設定する。これらの値は、クラスタ内の各デバイスで同一です。
- デバイスでロード バランシングをイネーブルにし、デバイス固有のプロパティを定義することにより、参加デバイスを設定する。これらの値はデバイスによって異なります。

前提条件

暗号化を使用する場合は、インターフェイス内にロード バランシングを設定する必要があります。そのインターフェイスがロード バランシング内部インターフェイスでイネーブルになっていない場合、クラスタの暗号化を設定しようとするとエラー メッセージが表示されます。

手順の詳細

ロード バランシングを実装するには、次の手順を実行して、同じプライベート LAN-to-LAN ネットワーク上の 2 つ以上のデバイスを、論理的に仮想クラスタとしてグループ化します。

ステップ 1　[Wizards] > [High Availability and Scalability] を選択します。

ステップ 2　[Configuration Type] 画面で、[Configure VPN Cluster Load Balancing] をクリックしてから、[Next] をクリックします。

ステップ 3　仮想クラスタ全体を表す 1 つの IP アドレスを選択します。仮想クラスタ内のすべての ASA が共有するパブリック サブネットのアドレス範囲内で、IP アドレスを指定します。

ステップ 4　このデバイスが参加する仮想クラスタの UDP ポートを指定します。デフォルト値は 9023 です。別のアプリケーションでこのポートが使用されている場合は、ロード バランシングに使用する UDP の宛先ポート番号を入力します。

ステップ 5　IPsec 暗号化をイネーブルにして、デバイス間で通信されるすべてのロードバランシング情報が暗号化されるようにするには、[Enable IPsec Encryption] チェックボックスをオンにします。共有秘密を指定し、確認する必要があります。仮想クラスタ内の ASA は、IPsec を使用する LAN-to-LAN トンネルを介して通信します。IPsec 暗号化をディセーブルにするには、[Enable IPsec Encryption] チェックボックスをオフにします。

ステップ 6　IPsec 暗号化をイネーブルにするときに、IPsec ピア間の共有秘密を指定します。入力した値は、連続するアスタリスク文字として表示されます。

ステップ 7　クラスタ内のこのデバイスに割り当てるプライオリティを指定します。指定できる範囲は 1 ～ 10 です。プライオリティは、起動時または既存のマスターで障害が発生したときに、このデバイスが仮想クラスタ マスターになる可能性を表します。プライオリティを高く設定すると（たとえば 10）、このデバイスが仮想クラスタ マスターになる可能性が高くなります。

（注）　仮想クラスタ内のデバイスを異なるタイミングで起動した場合、最初に起動したデバイスが、仮想クラスタ マスターの役割を果たすと想定されます。どの仮想クラスタにもマスターが必要であるため、起動したときに仮想クラスタ内の各デバイスはチェックを行い、クラスタに仮想マスターがあることを確認します。仮想マスターがない場合、そのデバイスがマスターの役割を果たします。後で起動し、クラスタに追加されたデバイスは、セカンダリ デバイスになります。仮想クラスタ内のすべてのデバイスが同時に起動されたときは、最高の優先順位が設定されたデバイスが仮想クラスタ マスターになります。仮想クラスタ内の複数のデバイスが同時に起動され、いずれも最高の優先順位が設定されている場合、最も低い IP アドレスを持つデバイスが仮想クラスタ マスターになります。

ステップ 8　このデバイスのパブリック インターフェイスの名前または IP アドレスを指定します。

ステップ 9　このデバイスのプライベート インターフェイスの名前または IP アドレスを指定します。

ステップ 10　VPN クライアント接続をクラスタ デバイスにリダイレクトするとき、外部 IP アドレスの代わりにクラスタ デバイスのホスト名とドメイン名を使用して、VPN クラスタ マスターによって完全修飾ドメイン名が送信されるようにするには、[Send FQDN to client instead of an IP address when redirecting] チェックボックスをオンにします。

ステップ 11　[Next] をクリックします。[Summary] 画面でコンフィギュレーションを確認します。

ステップ 12　[Finish] をクリックします。

VPN クラスタ ロード バランシングの設定が ASA に送信されます。

ロード バランシングの設定（ウィザードを使用しない場合）

[Load Balancing] ペイン（[Configuration] > [Remote Access VPN] > [Load Balancing]）では、ASA のロード バランシングをイネーブルにすることができます。ロード バランシングをイネーブルにするには、次の手順を実行します。

- 共通仮想クラスタ IP アドレス、UDP ポート（必要に応じて）、およびクラスタの IPsec 共有秘密情報を確立することによりロードバランシング クラスタを設定する。これらの値は、クラスタ内のすべてのデバイスで同一です。
- デバイスでロード バランシングをイネーブルにし、デバイス固有のプロパティを定義することにより、参加デバイスを設定する。これらの値はデバイスによって異なります。

前提条件

- IPv6 アドレスを使用したクライアントが ASA の公開されている IPv4 アドレスに正常に接続するには、IPv6 から IPv4 へネットワーク アドレス変換が可能なデバイスがネットワークに存在する必要があります。
- 暗号化を使用する場合は、インターフェイス内にロード バランシングを設定する必要があります。そのインターフェイスがロード バランシング内部インターフェイスでイネーブルになっていない場合、クラスタの暗号化を設定しようとするとエラー メッセージが表示されます。

ステップ 1　[Configuration] > [Remote Access VPN] > [Load Balancing] の順に選択します。

ステップ 2　[Participate in Load Balancing] をオンにして、この ASA がロードバランシング クラスタに参加していることを指定します。

ロード バランシングに参加するすべての ASA に対してこの方法でロード バランシングをイネーブルにする必要があります。

ステップ 3　[VPN Cluster Configuration] エリアで、次のフィールドを設定します。これらの値は、仮想クラスタ全体で同じである必要があります。すべてのクラスタに同一のクラスタ設定を行う必要があります。

- [Cluster IPv4 Address] : IPv4 仮想クラスタ全体を表す単一の IPv4 アドレスを指定します。仮想クラスタ内のすべての ASA が共有するパブリック サブネットのアドレス範囲内で、IP アドレスを選択します。
  - [UDP Port] : このデバイスが参加する仮想クラスタの UDP ポートを指定します。デフォルト値は 9023 です。別のアプリケーションでこのポートが使用されている場合は、ロードバランシングに使用する UDP の宛先ポート番号を入力します。
- [Cluster IPv6 Address] : IPv6 仮想クラスタ全体を表す単一の IPv6 アドレスを指定します。仮想クラスタ内のすべての ASA が共有するパブリック サブネットのアドレス範囲内で、IP アドレスを選択します。IPv6 アドレスを使用したクライアントは、ASA クラスタの公開されている IPv6 アドレス経由または GSS サーバ経由で AnyConnect 接続を行うことができます。同様に、IPv6 アドレスを使用したクライアントは、ASA クラスタの公開されている IPv4 アドレス経由または GSS サーバ経由で AnyConnect VPN 接続を行うことができます。どちらのタイプの接続も ASA クラスタ内でロード バランシングできます。

（注） 少なくとも 1 台の DNS サーバに DNS サーバ グループが設定されており、ASA インターフェイスの 1 つで DNS ルックアップがイネーブルにされている場合、[Cluster IPv4 Address] および [Cluster IPv6 Address] フィールドでは、仮想クラスタの完全修飾ドメイン名も指定できます。

- [Enable IPSec Encryption] : IPSec 暗号化をイネーブルまたはディセーブルにします。このボックスをオンにして、共有秘密情報を指定して確認します。仮想クラスタ内の ASA は、IPsec を使用する LAN-to-LAN トンネルを介して通信します。デバイス間で通信されるすべてのロードバランシング情報が暗号化されるようにするには、このチェックボックスをオンにします。
- [IPSec Shared Secret] : IPSec 暗号化がイネーブルになっているときに、IPSec ピア間の共有秘密情報を指定します。ボックスに入力する値は、連続するアスタリスク文字として表示されます。
- [Verify Secret] : 共有秘密情報を再入力します。[IPSec Shared Secret] ボックスに入力された共有秘密情報の値を確認します。

ステップ 4　特定の ASA の [VPN Server Configuration] エリアのフィールドを設定します。

- [Public Interface] : このデバイスのパブリック インターフェイスの名前または IP アドレスを指定します。
- [Private Interface] : このデバイスのプライベート インターフェイスの名前または IP アドレスを指定します。
- [Priority] : クラスタ内でこのデバイスに割り当てるプライオリティを指定します。指定できる範囲は 1 ～ 10 です。プライオリティは、起動時または既存のマスターで障害が発生したときに、このデバイスが仮想クラスタ マスターになる可能性を表します。優先順位を高く設定すれば（10 など）、このデバイスが仮想クラスタ マスターになる可能性が高くなります。

（注）　仮想クラスタ内のデバイスを異なるタイミングで起動した場合、最初に起動したデバイスが、仮想クラスタ マスターの役割を果たすと想定されます。仮想クラスタにはマスターが必要であるため、起動したときに仮想クラスタ内の各デバイスはチェックを行い、クラスタに仮想マスターがあることを確認します。仮想マスターがない場合、そのデバイスがマスターの役割を果たします。後で起動し、クラスタに追加されたデバイスは、バックアップ デバイスになります。仮想クラスタ内のすべてのデバイスが同時に起動されたときは、最高の優先順位が設定されたデバイスが仮想クラスタ マスターになります。仮想クラスタ内の複数のデバイスが同時に起動され、いずれも最高の優先順位が設定されている場合、最も低い IP アドレスを持つデバイスが仮想クラスタ マスターになります。

- [NAT Assigned IPv4 Address] : このデバイスの IP アドレスを NAT によって変換した結果の IP アドレスを指定します。NAT を使用しない場合（またはデバイスが NAT を使用するファイアウォールの背後にはない場合）は、このフィールドを空白のままにしてください。
- [NAT Assigned IPv6 Address] : このデバイスの IP アドレスを NAT によって変換した結果の IP アドレスを指定します。NAT を使用しない場合（またはデバイスが NAT を使用するファイアウォールの背後にはない場合）は、このフィールドを空白のままにしてください。
- [Send FQDN to client] : このチェックボックスをオンにすると、VPN クラスタ マスターが VPN クライアント接続をクラスタ デバイスにリダイレクトするときに、外部 IP アドレスの代わりにクラスタ デバイスのホスト名とドメイン名を使用して完全修飾ドメイン名が送信されるようになります。

  デフォルトで、ASA はロードバランシング リダイレクションの IP アドレスだけをクライアントに送信します。DNS 名に基づく証明書が使用されている場合、その証明書はバックアップ デバイスにリダイレクトされたときに無効になります。

  VPN クラスタ マスターとして、ASA は、VPN クライアント接続を別のクラスタ デバイスにリダイレクトする場合に、DNS 逆ルックアップを使用して、そのクラスタ デバイス（クラスタ内の別の ASA）の外部 IP アドレスではなく完全修飾ドメイン名（FQDN）を送信できます。

  クラスタ内のロードバランシング デバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

  （注）　IPv6 を使用し、FQDNS をクライアントに送信するときに、これらの名前は DNS を通じて ASA で解決できる必要があります。

FQDN を使用したクライアントレス SSL VPN ロード バランシングのイネーブル化

ステップ 1　[Send FQDN to client instead of an IP address when redirecting] チェックボックスをオンにして、ロード バランシングでの FQDN の使用をイネーブルにします。

ステップ 2　使用する ASA の外部インターフェイスのエントリがまだ存在しない場合は、各インターフェイスのエントリを DNS サーバに追加します。ASA の各外部 IP アドレスには、ルックアップ用に関連付けられている DNS エントリが含まれている必要があります。これらの DNS エントリに対しては、逆ルックアップもイネーブルにする必要があります。

ステップ 3　[Configuration] > [Device Management] > [DNS] > [DNS Client] ダイアログボックスで、DNS サーバへのルートを持つインターフェイスの ASA での DNS ルックアップをイネーブルにします。

ステップ 4　ASA で DNS サーバの IP アドレスを定義します。これには、このダイアログボックスの [Add] をクリックします。[Add DNS Server Group] ダイアログボックスが開きます。追加する DNS サーバの IPv4 または IPv6 アドレスを入力します。たとえば、192.168.1.1 または 2001:DB8:2000::1 です。

ステップ 5　[OK] および [Apply] をクリックします。

グローバル NAC パラメータの設定

ASA は、Extensible Authentication Protocol（EAP）over UDP（EAPoUDP）のメッセージを使用して、リモート ホストのポスチャを確認します。ポスチャ検証は、リモート ホストにネットワーク アクセス ポリシーを割り当てる前に、そのホストがセキュリティの必要条件を満たしているかどうかを調べることです。ASA でネットワーク アドミッション コントロールを設定する前に、NAC 用に Access Control Server を設定しておく必要があります。

フィールド

[NAC] ペインでは、すべての NAC 通信に適用される属性を設定できます。ペインの一番上に表示される次のグローバル属性は、ASA とリモート ホストの間の EAPoUDP メッセージングに適用されます。

- [Port]：ホストの Cisco Trust Agent（CTA）との EAP over UDP 通信で使用するポート番号。この番号は、CTA で設定されているポート番号と一致する必要があります。値は 1024 ～ 65535 の範囲で入力します。デフォルト設定は 21862 です。
- [Retry if no response]：ASA が EAP over UDP メッセージを再送信する回数。この属性により、Rechallenge Interval の期限切れに対して送信されるメッセージの連続再試行回数を制限します。この設定は秒単位です。値は 1 ～ 3 の範囲で入力します。デフォルト設定は 3 です。
- [Rechallenge Interval]：ASA は、EAPoUDP メッセージをホストに送信するときにこのタイマーを開始します。ホストからの応答があるとタイマーがクリアされます。応答を受信する前にタイマーが期限切れになると、ASA はメッセージを再送信します。この設定は秒単位です。1 ～ 60 の範囲で値を入力します。デフォルト設定は 3 です。
- [Wait before new PV Session]：ASA は、リモート ホストの NAC セッションを保持状態にしたときにこのタイマーを開始します。セッションが保持状態になるのは、送信された EAPoUDP メッセージの数が [Retry if no response] 設定の値に達しても応答を受信できない場合です。ASA は、ACS サーバから「Access Reject」メッセージを受信した後にも、このタイマーを開始します。タイマーが期限切れになると、ASA はリモート ホストとの新しい EAP over UDP アソシエーションの開始を試みます。この設定は秒単位です。60 ～ 86400 の範囲で値を入力します。デフォルト設定は 180 です。

[NAC] ペインの [Clientless Authentication] 領域では、EAPoUDP 要求に応答しないホストの設定値を設定できます。CTA が実行されていないホストは、これらの要求に応答しません。

- [Enable clientless authentication]：クライアントレス認証をイネーブルにします。ASA は、ユーザ認証要求の形式で、設定されているクライアントレス ユーザ名とパスワードを Access Control Server に送信します。次に、ACS はクライアントレス ホストのアクセス ポリシーを要求します。この属性をブランクのままにすると、ASA はクライアントレス ホストのデフォルト ACL を適用します。
- [Clientless Username]：ACS のクライアントレス ホストに設定するユーザ名。デフォルト設定は clientless です。1 ～ 64 文字の ASCII 文字を入力します。先頭および末尾のスペース、ポンド記号（#）、疑問符（?）、一重または二重引用符（' と "）、アスタリスク（*）、山カッコ（< と >）は除外します。

- [Password] : ACS のクライアントレス ホストに設定するパスワード。デフォルト設定は clientless です。4 ～ 32 文字の ASCII 文字を入力します。
- [Confirm Password] : 確認のために再入力する、ACS のクライアントレス ホストに設定するパスワード。
- [Enable Audit] : クライアントがポスチャ検証要求に応答しない場合に、クライアントの IP アドレスをオプションの監査サーバに渡します。監査サーバ（Trend サーバなど）では、ホスト IP アドレスを使用して、ホストに対して直接チャレンジを行い、ホストのヘルスを評価します。たとえば、ホストに対してチャレンジを行い、そのウイルス チェック ソフトウェアがアクティブで最新の状態かどうかを判断します。監査サーバは、リモート ホストとの対話を完了すると、リモート ホストのヘルスを示すトークンをポスチャ検証サーバに渡します。
- [None] : クライアントレス認証と監査サービスをディセーブルにします。

ネットワーク アドミッション コントロールのポリシーの設定

[NAC Policies] テーブルには、ASA で設定されているネットワーク アドミッション コントロール（NAC）のポリシーが表示されます。

NAC ポリシーを追加、変更、または削除するには、次のいずれかの操作を実行します。

- NAC ポリシーを追加するには、[Add] を選択します。[Add NAC Framework Policy] ダイアログボックスが開きます。
- NAC ポリシーを変更するには、そのポリシーをダブルクリックするか、ポリシーを選択して [Edit] をクリックします。[Edit NAC Framework Policy] ダイアログボックスが開きます。
- NAC ポリシーを削除するには、ポリシーを選択して [Delete] をクリックします。

次の各項では、NAC、NAC の要件、およびポリシー属性への値の割り当て方法を説明します。

- NAC について
- 使用方法、要件、および制限
- フィールド
- 次の作業

NAC について

NAC では、ネットワークへのアクセスの条件としてエンドポイントの準拠性チェックと脆弱性チェックを実行することにより、ワーム、ウイルス、および不正アプリケーションによる侵入および感染からエンタープライズのネットワークを保護します。これらのチェックは、*ポスチャ検証* と呼ばれます。イントラネット上の脆弱なホストにアクセスする前に、ポスチャ検証を設定して、AnyConnect またはクライアントレス SSL VPN セッションを使用するホスト上のアンチウイルス ファイル、パーソナル ファイアウォール ルール、または侵入保護ソフトウェアが最新の状態であることを確認できます。ポスチャ検証の一部として、リモート ホストで実行されているアプリケーションが最新のパッチで更新されているか検証することもできます。NAC は、ユーザ認証およびトンネルの設定の完了後に行われます。自動ネットワーク ポリシー実施が適用されないホスト（ホーム PC など）からエンタープライズ ネットワークを保護する場合は、NAC が特に有用です。

エンドポイントと ASA 間でトンネルを確立すると、ポスチャ検証がトリガーされます。

クライアントがポスチャ検証の要求に応答しない場合は、ASA を設定して、そのクライアントの IP アドレスをオプションの監査サーバに渡すことができます。監査サーバ（Trend サーバなど）では、ホスト IP アドレスを使用して、ホストに対して直接チャレンジを行い、ホストのヘルスを評価します。た

とえば、ホストに対してチャレンジを行い、そのウイルス チェック ソフトウェアがアクティブで最新の状態かどうかを判断します。監査サーバは、リモート ホストとの対話を完了すると、リモート ホストのヘルスを示すトークンをポスチャ検証サーバに渡します。

ポスチャ検証が成功する、またはリモート ホストが正常であることを示すトークンを受信すると、ポスチャ検証サーバは、トンネル上のトラフィックに対するアプリケーション用のネットワーク アクセス ポリシーを ASA に送信します。

ASA を含む *NAC Framework* のコンフィギュレーションには、クライアントで実行されている Cisco Trust Agent だけがポスチャ エージェントの役割を果たすことができ、Cisco Access Control Server（ACS）だけがポスチャ検証サーバの役割を果たすことができます。ACS はダイナミック ACL を使用して、各クライアントのアクセス ポリシーを決定します。

RADIUS サーバである ACS は、ポスチャ検証サーバとしての役割を果たすことに加え、トンネルの確立に必要なログイン クレデンシャルを認証できます。

（注） ASA に設定されている NAC Framework ポリシーだけが、監査サーバの使用をサポートしています。

ACS はそのポスチャ検証サーバとしての役割において、アクセス コントロール リストを使用します。ポスチャ検証が成功し、ACS によって、ASA に送信するアクセス ポリシーの一部としてリダイレクト URL が指定されると、ASA は、リモート ホストからのすべての HTTP 要求と HTTPS 要求をリダイレクト URL にリダイレクトします。ポスチャ検証サーバによってアクセス ポリシーが ASA にアップロードされると、関連するすべてのトラフィックはその宛先に到達するためにセキュリティ アプライアンスと ACS（またはその逆も同じ）の両方を通過する必要があります。

NAC フレームワーク ポリシーがグループ ポリシーに割り当てられている場合は、リモート ホストと ASA の間にトンネルが確立されるとポスチャ検証が実行されます。ただし、NAC Framework ポリシーでは、ポスチャ検証を免除されているオペレーティング システムを特定し、そのようなトラフィックをフィルタリングするためにオプションの ACL を指定できます。

使用方法、要件、および制限

NAC をサポートするように設定すると、ASA は、Cisco Secure Access Control Server のクライアントとして機能します。そのため、NAC 認証サービスを提供するために、ネットワーク上に少なくとも 1 台の Access Control Server をインストールする必要があります。

ネットワークで 1 台以上の Access Control Server を設定した後は、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add or Edit External] メニュー オプションを使用して Access Control Server グループを登録する必要があります。その後、NAC ポリシーを追加します。

ASA による NAC フレームワークのサポートは、リモート アクセス IPSec セッションとクライアントレス SSL VPN セッションに限られています。NAC Framework コンフィギュレーションは、シングル モードだけをサポートしています。

ASA における NAC では、レイヤ 3（非 VPN）および IPv6 トラフィックはサポートされていません。

フィールド

- [Policy Name]：新しい NAC ポリシーの名前を最大 64 文字で入力します。

  NAC ポリシーのコンフィギュレーションに続いて、Network (Client) Access グループ ポリシーの NAC Policy 属性の隣にポリシー名が表示されます。属性または目的を、設定する他の属性または目的と区別できるように名前を割り当てます。

- [Status Query Period]：ASA は、ポスチャ検証とステータス クエリーの応答が成功するたびに、このタイマーを開始します。このタイマーが切れると、ホスト ポスチャの変化を調べるクエリー（*ステータス クエリー*と呼ばれる）がトリガーされます。30 ～ 1800 の範囲で秒数を入力します。デフォルトの設定は 300 秒です。
- [Revalidation Period]：ASA は、ポスチャ検証が成功するたびに、このタイマーを開始します。このタイマーが期限切れになると、次の無条件のポスチャ検証がトリガーされます。ASA では、再検証中はポスチャ検証が維持されます。ポスチャ検証または再検証中にアクセス コントロール サーバが使用できない場合、デフォルトのグループ ポリシーが有効になります。ポスチャを検証する間隔を秒数で入力します。指定できる範囲は 300 ～ 86400 です。デフォルトの設定は 36000 秒です。
- [Default ACL]：（任意）ポスチャ検証が失敗した場合、ASA は、選択された ACL に関連付けられているセキュリティ ポリシーを適用します。[None] を選択するか、リストの拡張 ACL を選択します。デフォルト設定は [None] です。設定が [None] のときにポスチャ検証に失敗した場合、ASA はデフォルト グループ ポリシーを適用します。

  [Manage] ボタンを使用して、ドロップダウン リストを読み込み、リストに ACL の設定を表示します。
- [Manage]：[ACL Manager] ダイアログボックスを開きます。クリックして、標準 ACL および各 ACL の ACE を表示、イネーブル化、ディセーブル化、削除します。[Default ACL] 属性の横のリストに [ACL] が表示されます。
- [Authentication Server Group]：ポスチャ検証用に使用する認証サーバ グループを指定します。この属性の横にあるドロップダウン リストには、ASA に設定され、リモート アクセス トンネルで利用できる RADIUS タイプのすべてのサーバ グループ名が表示されます。NAC をサポートするように設定された、少なくとも 1 台のサーバで構成される ACS グループを選択します。
- [Posture Validation Exception List]：ポスチャ検証からリモート コンピュータを除外する 1 つ以上の属性が表示されます。各エントリには、少なくともオペレーティング システムと、[Yes] または [No] いずれかの [Enabled] 設定が含まれています。オプションのフィルタが、リモート コンピュータの追加属性を一致させる ACL を識別します。ポスチャ検証からリモート コンピュータを除外するには、オペレーティング システムで構成されたエントリとフィルタの両方に一致する必要があります。ASA は、[Enabled] 設定が [No] に設定されているエントリを無視します。
- [Add]：エントリを [Posture Validation Exception] リストに追加します。
- [Edit]：[Posture Validation Exception] リストのエントリを修正します。
- [Delete]：エントリを [Posture Validation Exception] リストから削除します。

次の作業

NAC ポリシーのコンフィギュレーションに続いて、そのポリシーをアクティブにするためにグループ ポリシーに割り当てる必要があります。このようにするには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [General] > [More Options] を選択し、[NAC Policy] 属性の横にあるドロップダウン リストから NAC ポリシー名を選択します。

Add/Edit Posture Validation Exception

[Add/Edit Posture Validation Exception] ダイアログ ペインでは、オペレーティング システム、およびフィルタに一致するオプションの属性に基づいてリモート コンピュータをポスチャ検証から除外できます。

- [Operating System]：リモート コンピュータのオペレーティング システムを選択します。コンピュータでこのオペレーティング システムが実行されている場合は、ポスチャ検証から除外されます。デフォルト設定は空白です。

- [Enable] : [Enabled] をオンにした場合にだけ、ASA は、このペインに表示される属性設定がリモート コンピュータに存在するかどうかをチェックします。オフにした場合は、属性設定が無視されます。デフォルト設定では、無効になっています。
- [Filter]（任意）: コンピュータのオペレーティング システムが Operating System 属性の値に一致する場合に、トラフィックに ACL を適用してフィルタリングします。
- [Manage] : [ACL Manager] ダイアログボックスを開きます。クリックして、標準 ACL および各 ACL の ACE を表示、イネーブル化、ディセーブル化、削除します。[Default ACL] 属性の横のリストに [ACL] が表示されます。このボタンを使用して、[Filter] 属性の横のリストに入力します。