



IKE

IKE は ISAKMP と呼ばれ、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 ネットワークのセキュリティ アプライアンスを設定するには、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。

IKE Parameters

このパネルでは、VPN 接続を使用する場合のシステム全体の値を設定できます。次の項では、各オプションについて説明します。

インターフェイスでの IKE のイネーブル化

VPN 接続を使用する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。

IPSec over NAT-T のイネーブル化

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、デフォルトでディセーブルになっています。

- セキュリティ アプライアンスは、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は、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。

セキュリティ アプライアンスによる 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。

- セキュリティ アプライアンスでポート 4500 を開きます。
- このパネルで、IPSec over NAT-T をグローバルにイネーブルにします。

- **Configuration > VPN > IPsec > Pre-Fragmentation** パネルで、フラグメンテーションポリシーパラメータの 2 番目と 3 番目のオプションを選択します。これらのオプションにより、トラフィックは、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。

IPSec over TCP のイネーブル化

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、デフォルトでディセーブルになっています。



(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、セキュリティアプライアンス機能の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。

- セキュリティアプライアンスは、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。

セキュリティアプライアンス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セキュリティアプライアンス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。

セキュリティアプライアンスだけでなく、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、セキュリティアプライアンス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。

識別方式の決定

IKE ネゴシエーションでは、ピアが相互に相手を識別する必要があります。この識別方式は、次のオプションから選択できます。

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の検索に使用する文字列を使用します。
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。 <ul style="list-style-type: none"> • 事前共有キーの IP アドレス • 証明書認証の cert DN

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。Aggressive モードのほうが高速ですが、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、デフォルトでディセーブルになっています。

接続解除の前にピアに警告する

セキュリティ アプライアンス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。

セキュリティ アプライアンスは、(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 Cisco 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、その理由をデコードしてイベント ログまたはポップアップ パネルに表示します。この機能は、デフォルトでディセーブルになっています。

このパネルでは、セキュリティ アプライアンス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 デバイス
- 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

リポート前のアクティブセッションの終了を待機

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、セキュリティ アプライアンスがリポ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、デフォルトでディセーブルになっています。

フィールド

- **Enable IKE** : 設定されたすべてのインターフェイスの IKE ステータスを表示します。
 - **Interface** : 設定されたすべてのセキュリティ アプライアンスのインターフェイス名を表示します。
 - **IKE Enabled** : 設定されたインターフェイスごとに IKE がイネーブルになっているかどうかを示します。
 - **Enable/Disables** : 強調表示されたインターフェイスの IKE をイネーブルまたはディセーブルにします。
- **NAT Transparency** : IPSec over NAT-T および IPSec over TCP をイネーブルまたはディセーブルにできます。
 - **Enable IPSec over NAT-T** : IPSec over NAT-T をイネーブルにする場合に選択します。
 - **NAT Keepalive** : セキュリティ アプライアンスが NAT-T セッションを終了させるまでに許容する、トラフィックなしの経過時間を秒数で入力します。デフォルトは、20 秒です。範囲は、10 ~ 3600 秒 (1 時間) です。
 - **Enable IPSec over TCP** : IPSec over TCP をイネーブルにする場合に選択します。

- **Enter up to 10 comma-separated TCP port values** : IPSec over TCP をイネーブルにするポートを最大で 10 ポートまで入力します。ポート間はカンマで区切ります。スペースは不要です。デフォルトポートは、10,000、範囲は 1 ~ 65,635 です。
- **Identity to Be Sent to Peer** : IPSec のピアがお互いを識別する方法を設定できます。
 - **Identity** : IPSec のピアがお互いを識別する方法を、次の中から 1 つ選択します。

Address	ホストの IP アドレスを使用します。
Hostname	ホストの完全修飾ドメイン名を使用します。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の検索に使用する文字列を使用します。
Automatic	接続タイプ (事前共有キーの IP アドレスまたは証明書認証の cert DN) によって IKE ネゴシエーションを判断します。

- **Key Id String** : ピアが事前共有キーの検索に使用する英数文字列を入力します。
- **Disable inbound aggressive mode connections** : Aggressive モードの接続をディセーブルにする場合に選択します。
- **Alert peers before disconnecting** : セッションを接続解除する前に、セキュリティアプライアンスから限定された LAN-to-LAN ピアとリモートアクセスクライアントに通知する場合に選択します。
- **Wait for all active sessions to voluntarily terminate before rebooting** : セキュリティアプライアンスにより、すべてのアクティブなセッションが終了するまで、予定されたリブートを延期させる場合に選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

IKE Policies

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 は、データを保護するトンネルを作成します。

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。
- 暗号鍵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、セキュリティ アプライアンスは暗号鍵とハッシュ キーを導出します。
- セキュリティ アプライアンスが暗号鍵を置き換える前に、この暗号鍵を使用する最長時間の制限。

IKE ポリシーを何も設定しない場合、セキュリティ アプライアンスはデフォルトのポリシーを使用します。デフォルト ポリシーは常に最下位のプライオリティに設定され、パラメータごとのデフォルト値が含まれています。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

- **Policies** : 設定された IKE ポリシーごとのパラメータの設定値を表示します。
 - **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** : IKE ポリシーを追加、編集、または削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Add/Edit IKE 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 ～ 65,543 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	デフォルトは SHA-1 です。MD5 は、SHA-1 よりもダイジェストが小さく、わずかに速いとされています。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 バリエーションがこの攻撃を防ぎます。
md5	MD5	

Authentication : 各 IPSec ピアの ID を確立するためにセキュリティ アプライアンス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応じて柔軟に拡張できるわけではありませんが、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	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	Group 1 (768 ビット)	これはデフォルトです。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	Group 2 (1024 ビット)	
5	Group 5 (1536 ビット)	
7	Group 7 (楕円曲線フィールドのサイズが 163 ビット)	Group 7 は Movian VPN クライアント用ですが、Group 7 (ECC) をサポートするいずれのピアでも使用できます。

Lifetime (secs): Unlimited を選択するか、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、セキュリティ アプライアンスは以後の 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。暗号強度は、2~3 分ごとに行われる非常に高速なキーの再生成機能を使用しなくても、セキュリティを確保するのに十分強力です。シスコでは、デフォルトを使用することをお勧めします。

Time Measure: 時間基準を選択します。セキュリティ アプライアンスでは、次の値を使用できます。

120 ~ 86,400 秒

2 ~ 1,440 分

1 ~ 24 時間

1 日

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Assignment Policy

インターネットワーク接続は、IP アドレスによって実現します。IP アドレスは、送信者と受信者の両方に接続用の番号が割り当てられている必要があるという点で、電話番号に似ています。ただし実際の VPN では、2 つのアドレスセットを使用します。最初のセットは、パブリック ネットワークのクライアントとサーバを接続し、その接続が確立されると、2 番目のセットが VPN トンネル経由でクライアントとサーバを接続します。

セキュリティ アプライアンスのアドレス管理では、この IP アドレスの 2 番目のセットを扱います。これらのプライベート IP アドレスは、クライアントをトンネル経由でプライベート ネットワーク上のリソースに接続し、プライベート ネットワークに直接接続されているかのようなクライアント機能を提供します。また、ここでは、クライアントに割り当てられたプライベート IP アドレスのみを扱います。プライベート ネットワーク上のその他のリソースに割り当てられた IP アドレスは、セキュリティ アプライアンスの管理ではなく、ネットワーク管理業務の一部に位置づけられます。

したがって、ここで IP アドレスに言及する場合は、クライアントをトンネルのエンドポイントとして機能させる、プライベート ネットワークのアドレッシング方式で取得される IP アドレスを意味します。

Assignment Policy パネルでは、IP アドレスをリモートアクセス クライアントに割り当てる方法を選択できます。

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。AAA サーバの設定は、**Configuration > AAA Setup** パネルで行います。
- **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 > DHCP Server** パネルで DHCP サーバを設定します。

- **Use internal address pools** : セキュリティ アプライアンスにより、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** パネルで 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 プールに戻されたばかりの IP アドレスの再使用を遅延させます。遅延時間を長くすることによって、IP アドレスがアドレス プールに戻されてからすぐに再割り当てすると発生する可能性がある、ファイアウォールでの問題を防止します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

アドレス プール

IP Pool ボックスには、設定された各アドレス プールが、名前ごとに、それぞれの IP アドレス範囲 (たとえば、10.10.147.100 ~ 10.10.147.177) とともに表示されます。プールが存在しない場合、ボックスは空です。セキュリティ アプライアンスは、リストに表示される順番でこれらのプールを使用します。最初のプールのすべてのアドレスが割り当てられると、次のプールのアドレスが使用され、以下同様に処理されます。

ローカルでないサブネットのアドレスを割り当てる場合は、そのようなネットワーク用のルートの追加が容易になるように、サブネットの境界を担当するプールを追加することを推奨します。

フィールド

- **Pool Name** : 設定された各アドレス プールの名前を表示します。
- **Starting Address** : 設定されたそれぞれのプールで使用可能な最初の IP アドレスを示します。
- **Ending Address** : 設定されたそれぞれのプールで使用可能な最後の IP アドレスを示します。
- **Subnet Mask** : 設定されたそれぞれのプールにあるアドレスのサブネット マスクを示します。
- **Add** : 新しいアドレス プールを追加します。
- **Edit/Delete** : すでに設定されているアドレス プールを編集または削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Add/Edit IP Pool

これらのパネルにより、次の操作を実行できます。

- セキュリティ アプライアンスがクライアントにアドレスを割り当てるときに使用する、IP アドレスの新しいプールを追加します。
- 事前に設定した IP アドレス プールを変更します。

プール範囲内の IP アドレスを他のネットワーク リソースに割り当てることはできません。

フィールド

- **Name** : アドレス プールに英数字の名前を割り当てます。最大で 64 文字です。
- **Starting IP Address** : このプールで使用可能な最初の IP アドレスを入力します。たとえば 10.10.147.100 のように、ドット付き 10 進数表記を使用します。
- **Ending IP Address** : このプールで使用可能な最後の IP アドレスを入力します。たとえば 10.10.147.100 のように、ドット付き 10 進数表記を使用します。
- **Subnet Mask** : IP アドレス プールのサブネット マスクを選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

IPSec

最もセキュアなプロトコルであるとされている IPSec は、VPN トンネルの最も完全なアーキテクチャを提供します。IPSec は、LAN-to-LAN 接続と、クライアントと LAN 間の接続の両方で使用できます。

IPSec 用語での「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。2つのピアは、IPSec によるトンネルの確立時に、認証、暗号化、カプセル化、およびキー管理の方法を決め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2つのフェーズがあり、最初のフェーズでトンネルを確立 (IKE SA) し、2番目のフェーズでトンネル内のトラフィックを制御 (IPSec SA) します。

IPSec LAN-to-LAN 接続では、セキュリティアプライアンスは発信側または応答側として機能します。IPSec でのクライアントと LAN の間の接続では、セキュリティアプライアンス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、SA の提案を受け入れるか、拒否するか、または対案を提示します。すべての動作は、設定された SA パラメータに従って行われます。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。

VPN クライアントは、IPSec プロトコルに準拠し、特にセキュリティアプライアンスと連携して動作するように設計されています。一方、セキュリティアプライアンスは、さまざまなプロトコル準拠クライアントとの IPSec 接続を確立できます。同様にセキュリティアプライアンスは、セキュアゲートウェイと呼ばれることの多い他のプロトコル準拠 VPN デバイスとの間で LAN-to-LAN 接続を確立できます。

セキュリティアプライアンスは、次の IPSec アトリビュートをサポートします。

- 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、5、および 7
- 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)

Crypto Maps

このペインには、IPSec ルールを含め、現在設定されている暗号マップが表示されます。このペインで、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します。

フィールド



(注)

暗黙のルールを編集、削除、またはコピーすることはできません。セキュリティ アプライアンスは、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、その提案を無効にすることができます。

- **Add** : Add IPSec Rule ダイアログが開きます。このダイアログでは、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するか、または選択できます。
- **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、**inside:any** のように、**any** という語を含むインターフェイス名がアドレス カラムのリストに表示されている場合があります。**any** は、内部インターフェイスのすべてのホストにルールが適用され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、**outside:any** のように、**any** という語を含むインターフェイス名がアドレス カラムのリストに表示されている場合があります。**any** は、インターフェイス外部のすべてのホストにルールが適用され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、セキュリティ アプライアンス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、セキュリティ アプライアンスはこのアドレス 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 ピアを特定します。
- **PFS** : ルールの Perfect Forward Secrecy (PFS; 完全転送秘密) の設定値を表示します。
- **NAT-T Enabled** : ポリシーで NAT トラバース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 Reverse Route Injection (RRI; 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 ポリシーの場合にのみ有効) このポリシーの接続タイプとして、bidirectional、originate-only、または answer-only を指定します。
- **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のみ適用されます。
- **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** : (オプション) 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、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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Create 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 パネルでは、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。
- **Transform Set to Be Added** : ポリシーのトランスフォーム セットを選択し、**Add** をクリックして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 ボックス内でのトランスフォーム セットの順番を入れ替えます。暗号マップ エントリまたはダイナミック暗号マップ エントリには、最大で 11 のトランスフォーム セットを追加できます。
- **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 ポリシーの場合にのみ有効) **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。
 - **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、それぞれの新しい鍵が前のどの鍵とも関係がないという暗号化の概念です。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、セキュリティ アプライアンスがセッション 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。選択肢は次のとおりです。
 - **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 7 (ECC)** = PFS を使用し、Diffie-Hellman Group 7 (ECC) を使用して IPSec セッション キーを生成します。このときの楕円曲線フィールドサイズは 163 ビットです。このオプションは処理が最も速く、要求されるオーバーヘッドも最小です。Movian VPN クライアントで使用する目的で開発されていますが、Group 7 (ECC) をサポートするいずれのピアでも使用できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Create IPsec Rule/Tunnel Policy (Crypto Map) - Advanced タブ

フィールド

- **Security Association Lifetime** パラメータ：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。
- **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。
- **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。
 - **CA 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と、Enable entire chain transmission チェックボックスがオンになります。
 - **Enable entire chain transmission**：トラスト ポイント チェーン全体で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)、Group 7 (ECC) の中から選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Create IPsec Rule/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 or 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 ... をクリックしてサービスの参照ウィンドウを開き、サービスのリストから選択できます。
- **Description : Traffic Selection** 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、または ... をクリックしてサービスの参照ウィンドウを開き、サービスのリストから選択できます。
 - **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 ルールは許可されません。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 パネルを表示します。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 (unlabeled)**: Service ボックスで指定したサービスの照合で使用するブーリアン条件 (equal、not equal、greater than、less than、または range) を一覧表示します。
- **Service (unlabeled)**: 照合対象のサービス (https、kerberos 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。
- ...: サービスのリストを表示します。このリストから、Service ボックスに表示するサービスを選択できます。
- **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 (unlabeled)**: 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。... ボタンをクリックして、使用可能なタイプのリストを表示します。
- **オプション**
 - **Time Range** : 既存の時間範囲の名前を指定するか、または新しい範囲を作成します。
 - ...:Add Time Range ペインを表示します。このペインでは、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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルールテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Pre-Fragmentation

このパネルでは、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、最大伝送ユニット (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、セキュリティ アプライアンス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することができます。たとえば、クライアントがセキュリティ アプライアンスの背後の 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セキュリティ アプライアンスの MTU サイズを超過するパケットを伝送します。選択したオプションにより、セキュリティ アプライアンス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、セキュリティ アプライアンスのパブリック 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。

セキュリティ アプライアンスは、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、セキュリティ アプライアンスは、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、セキュリティ アプライアンスは、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、セキュリティ アプライアンスは 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。ここで例では、セキュリティ アプライアンスが 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** : すべての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** : 設定されたそれぞれの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** : インターフェイスごとの DF Bit Policy 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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Edit IPsec Pre-Fragmentation Policy

このパネルでは、親パネル (**Configuration > VPN > IPSec > Pre-Fragmentation**) で選択したインターフェイスの既存の IPsec の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** : 選択したインターフェイスを特定します。ダイアログボックスを使用してこのパラメータを変更することはできません。
- **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。セキュリティ アプライアンスは、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、セキュリティ アプライアンスは 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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

IPSec Transform Sets

このパネルでは、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

- **Transform Sets** : 設定されたトランスフォーム 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となります。
 - **ESP Encryption** : トランスフォーム セットの Encapsulating Security Protocol (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を開きます。このダイアログボックスでは、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を開きます。このダイアログボックスでは、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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Add/Edit Transform Set

このパネルでは、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となります。
 - **ESP Encryption** : トランスフォーム セットの Encapsulating Security Protocol (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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Load Balancing



(注)

VPN ロードバランシングを使用するには、Plus ライセンスが有効な ASA Model 5510、または ASA Model 5520 以降を使用する必要があります。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化する前に、この暗号ライセンスの存在をチェックします。アクティブな 3DES または AES ライセンスを検出できなかった場合、セキュリティ アプライアンスは、ロードバランシングのイネーブル化を回避し、さらにライセンスがこの使用を許可していない限り、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回避します。

このウィンドウでは、セキュリティ アプライアンスで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。

- ロードバランシング クラスタの設定。共通仮想クラスタ IP アドレス、UDP ポート（必要に応じて）、およびクラスタ用 IPSec 共有秘密情報を確立します。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。
- 参加デバイスの設定。デバイス上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します。これらの値は、デバイスごとに異なります。

リモートクライアント コンフィギュレーションで、複数のセキュリティ アプライアンス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は、セッションのトラフィックを最も負荷の小さいデバイスに転送して、すべてのデバイス間に負荷を分散します。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。



(注)

ロードバランシングは、Cisco VPN Client（リリース 3.0 以降）、Cisco VPN 3002 Hardware Client（リリース 3.5 以降）、または Easy VPN Client として動作している ASA 5505 で開始されたリモートセッションでのみ有効です。LAN 間接続を含む他のすべてのクライアントは、ロードバランシングがイネーブルなセキュリティ アプライアンスに接続することはできませんが、ロードバランシングに参加することはできません。

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-to-LAN ネットワークを論理的に仮想クラスタとしてグループ化します。

仮想クラスタ内のすべてのデバイスはセッション ロードを伝送します。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、着信コールをセカンダリ 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監視し、それぞれの作業負荷を追跡し、それに応じてセッション負荷を分散します。仮想クラスタ マスターの役割は、1 台の物理デバイスに固定されているのではなく、デバイス間で入れ替わることができます。たとえば、現在の仮想クラスタ マスターが故障すると、クラスタ内のセカンダリ デバイスの 1 つがその役割を引き継ぎ、即座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からは、単一の仮想クラスタ IP アドレスとして認識されます。この IP アドレスは、特定の物理デバイスに固定されているわけではありません。これは、現在の仮想クラスタ マスターに属しているため、仮想です。VPN クライアントが接続を確立しようとするとき、この仮想クラスタ IP アドレスにまず接続します。すると仮想クラスタ マスターは、クラスタ内の最も負荷の小さい利用可能なホストのパブリック IP アドレスをそのクライアントに

送り返します。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）。このように、仮想クラスター マスターは、トラフィックを均一かつ効率的にリソース間に割り当てます。



(注)

Cisco VPN Client、Cisco VPN 3002 Hardware Client、または Easy VPN Client として動作している ASA 5505 以外のすべてのクライアントは、通常どおりセキュリティ アプライアンスに直接接続し、仮想クラスター IP アドレスを使用しません。

クラスター内のマシンに障害が発生すると、終了したセッションはただちに仮想クラスター IP アドレスに再接続できます。仮想クラスター マスターは、次にこのような接続をクラスター内の他のアクティブ デバイスに割り当てます。仮想クラスター マスター自体に障害が発生した場合、クラスター内のセカンダリ デバイスがただちに新しい仮想セッション マスターの役割を自動的に引き継ぎます。クラスター内の複数のデバイスが故障した場合でも、クラスター内のいずれか 1 つのデバイスが稼働し、利用可能である限り、ユーザは引き続きそのクラスターに接続できます。

前提条件

ロードバランシングは、デフォルトで無効です。ロードバランシングは明示的に有効にする必要があります。

まず、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とともに、仮想クラスター IP アドレスの参照先の仮想クラスター IP のインターフェイスをあらかじめ設定する必要があります。

クラスターに参加するすべてのデバイスは、IP アドレス、暗号化設定、暗号鍵、およびポートについて、クラスター固有の値を共有する必要があります。クラスター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 インスタンスは、同じ IP ネットワークに属している必要があります。

フィールド

- **VPN Load Balancing** : 仮想クラスター デバイスのパラメータを設定します。
 - **Participate in Load Balancing Cluster** : このデバイスがロードバランシング クラスターの参加デバイスであることを指定します。
 - **VPN Cluster Configuration** : デバイスのパラメータを設定します。パラメータは、仮想クラスター全体で同じにする必要があります。すべてのクラスターに同一のクラスター設定を行う必要があります。
 - **Cluster IP Address** : 仮想クラスター全体を表す単一の IP アドレスを指定します。仮想クラスター内のすべてのセキュリティ アプライアンス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ーの 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がこのポートを使用している場合は、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。
 - **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。このチェックボックスをオンにする場合、共有秘密情報を指定し、確認する必要があります。仮想クラスター内のセキュリティ アプライアンスは、IPSec を使用して LAN 間トンネル経由で通信を行います。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。



(注) 暗号化を使用する場合は、ロードバランシングの内部インターフェイスをあらかじめ設定しておく必要があります。ロードバランシング内部インターフェイスでそのインターフェイスがイネーブルになっていない場合、クラスタ暗号化を設定しようと試みるとエラーメッセージが表示されます。

クラスタの暗号化を設定したときに、ロードバランシングの内部インターフェイスが有効でも、仮想クラスタのデバイスの参加を設定する前に無効にすると、**Participate in Load Balancing Cluster** チェックボックスを選択した時点でエラーメッセージが表示され、クラスタの暗号化を有効にできません。

- **IPSec Shared Secret** : IPSec 暗号化をイネーブルにしてある場合、IPSec ピア間に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** : 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。
- **VPN Server Configuration** : この特定のデバイスのパラメータを設定します。
 - **Interfaces** : 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、およびそれぞれの関連パラメータを設定します。
 - **Public** : 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** : 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。範囲は 1 ~ 10 です。優先順位は、このデバイスが起動時または他のマスターの故障時に仮想クラスタ マスターになる可能性を示します。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、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。

- **NAT Assigned IP Address** : このデバイスの IP アドレスが NAT によって変換される 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ない場合は、0.0.0.0 と入力します。
- **Send FQDN to client** : 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 マスターにより完全修飾ドメイン名が送信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。

IP アドレスではなく FQDN を使用してクライアントレス SSL VPN ロードバランシングをイネーブルにするには、次の設定手順を実行する必要があります。

ステップ 1 Send FQDN to client... 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** 使用するセキュリティ アプライアンス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。各セキュリティ アプライアンス 外部 IP アドレスに、検索で使用する DNS エントリを関連付けます。これらの DNS エントリは、逆ルックアップに対してもイネーブルになっている必要があります。
- 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セキュリティ アプライアンスでの DNS 検索をイネーブルにします。
- ステップ 4** セキュリティ アプライアンスで 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 IP アドレスを入力します。たとえば、192.168.1.1 (DNS サーバの IP アドレス) と入力できます。
- ステップ 5** OK および Apply をクリックします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

グローバル NAC パラメータの設定

セキュリティ アプライアンスは、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。これは、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。セキュリティ アプライアンスでネットワーク 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 ウィンドウでは、すべての NAC 通信に適用されるアトリビュートを設定できます。ウィンドウの一番上に表示される次のグローバル アトリビュートは、セキュリティ アプライアンスとリモート 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。1024 ~ 65535 の範囲で値を入力します。デフォルト設定は 21862 です。
- **Retry if no response** : セキュリティ アプライアンスが EAP over UDP メッセージを再送信する回数。このアトリビュートにより、**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。1 ~ 3 の範囲で値を入力します。デフォルト設定は 3 です。
- **Rechallenge Interval** : セキュリティ アプライアンスは、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、セキュリティ アプライアンス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** : セキュリティ アプライアンスは、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。「Retry if no response」設定の値と等しい EAPoUDP メッセージを送信した後に応答を受信しない場合、セキュリティ アプライアンスは、セッションを保持状態にします。セキュリティ アプライアンスは、ACS サーバから Access Reject メッセージを受信した後も、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、セキュリティ アプライアンスはリモート 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 ウィンドウの 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。セキュリティ アプライアンスは、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。このアトリビュートをブランクのままにすると、セキュリティ アプライアンス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ト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。**Trend** サーバなどの監査サーバは、ホストの IP アドレスを使用してチャレンジを直接ホストに送信し、そのヘルスを評価します。たとえば、ホストにチャレンジを送信して、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になっているかどうかを判断します。監査サーバは、リモート ホストとの相互通信を完了すると、トークンをポストチャ検証サーバに渡し、リモート ホストのヘルスを示します。
- **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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

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、セキュリティ アプライアンス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、または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 アトリビュートへの値の割り当て方法を説明します。

- [NAC について](#)
- [使用、要件、および制限](#)
- [フィールド](#)
- [次のステップ](#)

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。これらのチェック機能を *ポスチャ検証* と呼びます。ポスチャ検証を設定することにより、イントラネットの脆弱なホストへのアクセスを許可する前に、AnyConnect またはクライアントレス SSL VPN セッションが行われるホストのアンチウイルス ファイル、パーソナル ファイアウォール ルール、または侵入防御ソフトウェアが、確実に最新の状態になるようにします。ポスチャ検証には、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パッチによって更新されているかどうかの検査も組み込むことができます。NAC は、ユーザ認証およびトンネルの設定の後にのみ実行されます。NAC は、ホーム PC など、自動ネットワーク ポリシー適用に従わないホストからエンタープライズ ネットワークを保護する場合に特に有効です。

エンドポイントとセキュリティ アプライアンスの間にトンネルを確立すると、ポスチャ検証が実行されます。

クライアントがポスチャ検証要求に回答しない場合にはクライアントの IP アドレスをオプションの監査サーバに渡すように、セキュリティ アプライアンスを設定できます。Trend サーバなどの監査サーバは、ホストの IP アドレスを使用してチャレンジを直接ホストに送信し、そのヘルスを評価します。たとえば、ホストにチャレンジを送信して、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になっているかどうかを判断します。監査サーバは、リモート ホストとの相互通信を完了すると、トークンをポスチャ検証サーバに渡し、リモート ホストのヘルスを示します。

ポスチャ検証が正常に実行されるか、またはリモート ホストが正常に動作していることを示すトークンを受け取ると、ポスチャ検証サーバは、アプリケーションのセキュリティ アプライアンスに対するネットワーク アクセス ポリシーをトンネルのトラフィックに送信します。

セキュリティ アプライアンスが関係する NAC フレームワーク コンフィギュレーションでは、クライアントで実行されている Cisco Trust Agent のみがポスチャ エージェントの役割を担うことができ、また Cisco Access Control Server (ACS) のみがポスチャ検証サーバの役割を担うことができます。ACS は、ダイナミック ACL を使用してクライアントごとのアクセス ポリシーを判断します。

ACS は、ポスチャ検証サーバとしての機能を果たすほか、RADIUS サーバとしてトンネルを確立するために必要なログイン証明書を認証できます。



(注) セキュリティ アプライアンスで設定されている NAC フレームワーク ポリシーのみが、監査サーバの使用に対応しています。

ACS は、ポストチャ検証サーバとして動作するときに、アクセス コントロール リストを使用します。ポストチャ検証が正常に行われ、ACS がセキュリティ アプライアンス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 を指定する場合、セキュリティ アプライアンスは、リモート ホストからのすべての HTTP および HTTPS 要求をそのリダイレクト URL にリダイレクトします。ポストチャ検証サーバがアクセス ポリシーをセキュリティ アプライアンスにアップロードすると、関連付けられたすべてのトラフィックは、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 (またはその逆順) の両方を通過しなければならなくなります。

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 ホストとセキュリティ アプライアンスの間にトンネルが確立されるとポストチャ検証が実行されます。ただし NAC フレームワーク ポリシーでは、ポストチャ検証から除外されるオペレーティング システムが識別され、そのようなトラフィックをフィルタリングするオプションの ACL が指定されます。

使用、要件、および制限

NAC をサポートするように設定されている場合、セキュリティ アプライアンスは Cisco Secure Access Control Server のクライアントとして機能します。この場合は、最低でも 1 台の Access Control Server をネットワークに設置して NAC 認証サービスを提供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 フレームワーク コンフィギュレーションでは、シングルモードのみがサポートされます。

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 アトリビュートの隣にポリシー名が表示されます。アトリビュートまたは目的を、設定する他のアトリビュート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** : セキュリティ アプライアンスは、ポスト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。このタイマーの有効期限が過ぎると、ホスト ポスチャの変化を問い合わせるクエリー (ステータス クエリー) が発行されます。秒単位で、30 ~ 1800 の数値を入力します。デフォルト設定は 300 です。
- **Revalidation Period** : セキュリティ アプライアンスは、ポストチャ検証が成功するたびに、このタイマーを開始します。このタイマーの期限が切れると、次の無条件のポストチャ確認を開始します。セキュリティ アプライアンスは、再検証の間、ポストチャ検証を維持します。ポストチャ確認または再確認中に Access Control Server が使用できなくなると、デフォルト グループ ポリシーが有効になります。ポストチャを確認する間隔を秒数で入力します。範囲は 300 ~ 86400 です。デフォルト設定は 36000 です。

- **Default ACL** : (オプション) ポスチャ検証が失敗した場合、セキュリティ アプライアンスは、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、セキュリティ アプライアンスはデフォルト 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 アトリビュートの横のリストに 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。このアトリビュートの横にあるドロップダウン リストには、セキュリティ アプライアンスに設定され、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 つ以上のアトリビュートが表示されます。少なくとも、エントリごとにオペレーティング システムと Enabled 設定 (Yes または No) が表示されます。オプションのフィルタによって、リモート コンピュータの追加のアトリビュートと一致する 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。セキュリティ アプライアンスは、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。

次のステップ

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。グループ ポリシーに割り当てるには、**Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > General > More Options** を選択し、NAC Policy アトリビュート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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Add/Edit Posture Validation Exception

Add/Edit Posture Validation Exception ダイアログ ウィンドウでは、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アトリビュート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 **None** です。
- **Enable** : **Enabled** をオンにした場合にだけ、セキュリティ アプライアンスは、このウィンドウに表示されるアトリビュート設定がリモート 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、アトリビュート設定が無視されます。デフォルト設定はオフです。
- **Filter** : **Filter** (オプション) は、コンピュータのオペレーティング システムが **Operating System** アトリビュート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** アトリビュートの横のリストに **ACL** が表示されます。このボタンを使用して、**Filter** アトリビュートの横のリストに入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—