ASDM ブック 3：Cisco Secure Firewall ASA シリーズ VPN ASDM 7.23 コンフィギュレーション ガイド

最終更新：2025 年 10 月 24 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

このマニュアルについて

ここでは、このガイドを使用する方法について説明します。

本書の目的

このマニュアルの目的は、を使用して Secure Firewall ASA上での VPN 設定を支援することです。Web ベースの GUI アプリケーションである Adaptive Security Device Manager（ASDM）。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

このマニュアルは、ASA シリーズに適用されます。このマニュアルを通じて、「ASA」という語は、特に指定がない限り、サポートされているモデル全般に該当します。

関連資料

詳細については、『*Navigating the Cisco ASA Series Documentation*』（http://www.cisco.com/go/asadocs）を参照してください。

表記法

このマニュアルでは、文字、表示、および警告に関する次の規則に準拠しています。

文字表記法

表記法	説明
boldface	コマンド、キーワード、ボタン ラベル、フィールド名、およびユーザー入力テキストは、**boldface**で示しています。メニューベース コマンドの場合は、メニュー項目を [ ] で囲み、コマンドのフル パスを示しています。
italic	ユーザーが値を指定する変数は、イタリック体で示しています。 イタリック体は、マニュアル タイトルと一般的な強調にも使用されています。
等幅	システムが表示するターミナル セッションおよび情報は、等幅文字で記載されます。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[ ]	角カッコの中の要素は、省略可能です。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
[ ]	システム プロンプトに対するデフォルトの応答も、角カッコで囲んで記載されます。
< >	パスワードなどの出力されない文字は、山カッコ（< >）で囲んで示しています。
!、#	コードの先頭に感嘆符（!）または番号記号（#）がある場合は、コメント行であることを示します。

読者への警告

このマニュアルでは、読者への警告に以下を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

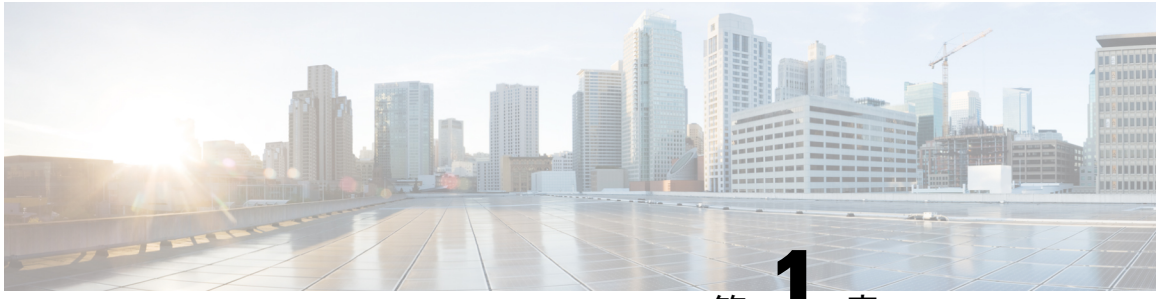
ワンポイント アドバイス	時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。
警告	「警告」の意味です。人身事故を予防するための注意事項が記述されています。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によって求めるビジネス成果を得るには、Cisco Services [英語] にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。



第 1 章

VPN ウィザード

VPN の概要

ASA は、ユーザーがプライベート接続と見なす TCP/IP ネットワーク（インターネットなど）全体でセキュアな接続を確立することにより、バーチャル プライベート ネットワークを構築します。これによって、single-user-to-LAN 接続と LAN-to-LAN 接続を確立できます。

セキュアな接続はトンネルと呼ばれ、ASA はトンネリング プロトコルを使用して、セキュリティパラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを介したパケットの送受信、パケットのカプセル化解除を行います。ASA は、双方向トンネルのエンドポイントとして機能します。たとえば、プレーン パケットを受信してカプセル化し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティアプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。

VPN ウィザードを使用すると、基本的な LAN-to-LAN とリモート アクセス VPN 接続を設定して、事前共有キーまたはデジタル証明書を認証用に割り当てることができます。ASDM を使用して拡張機能を編集および設定してください。

ここでは、次の 4 つの VPN ウィザードについて説明します。

- セキュアクライアント VPN ウィザード （5 ページ）

  Cisco Secure Client AnyConnect VPN モジュールは、ASA へのセキュアな SSL 接続または IPsec（IKEv2）接続を提供し、これにより、リモートユーザーによる企業リソースへのフル VPN トンネリングが可能になります。事前にクライアントがインストールされていない場合、リモート ユーザーは、クライアントレス VPN 接続を受け入れるように設定されたインターフェイスの IP アドレスをブラウザに入力します。ASA は、リモート コンピュー

タのオペレーティング システムに適合するクライアントをダウンロードします。ダウンロードが完了すると、クライアントが自動的にインストールされて設定され、セキュアな接続が確立されます。接続が終了すると、ASA の設定に応じて、クライアントはそのまま残るか、またはアンインストールされます。以前からインストールされているクライアントの場合は、ユーザーの認証時に、ASA によってクライアントのリビジョンが点検され、必要に応じてアップグレードされます。

セキュアクライアント VPN ウィザードは、ASA がマルチコンテキストモードのときにユーザーコンテキストのみで利用可能になります。必要なコンテキストのストレージとリソース クラスは、システム コンテキストから設定する必要があります。

Cisco セキュアクライアント パッケージとプロファイルファイルを使用するには、コンテキストごとのストレージが必要です。各コンテキストのライセンスの割り当てには、リソース クラスが必要です。使用するライセンスは、セキュアクライアント Premium です。

（注） このウィザードの残りの設定は、シングルコンテキストの場合と同じです。

- IPsec IKEv2 Remote Access Wizard （13 ページ）

IKEv2 によって、他のベンダーの VPN クライアントが ASA に接続できます。これにより、セキュリティが強化されるとともに、国や地方自治体が規定している IPsec リモートアクセス要件を満たすことができます。

IPSec IKEv2 リモート アクセス ウィザードは、ASA がマルチコンテキスト モードのときにユーザー コンテキストのみで利用可能になります。必要なコンテキストのリソース クラスは、ライセンス割り当て用のシステム コンテキストから設定する必要があります。使用するライセンスは、セキュアクライアント Premium です。

（注） このウィザードの残りの設定は、シングルコンテキストの場合と同じです。

- IPsec IKEv1 Remote Access Wizard （8 ページ）
- IPsec Site-to-Site VPN Wizard （3 ページ）

LAN-to-LAN 接続で IPv4 と IPv6 の両方のアドレッシングが使用されている場合、ASA で VPN トンネルがサポートされるのは、両方のピアが ASA であり、かつ両方の内部ネットワークのアドレッシング方式が一致している（両方とも IPv4 または IPv6）ときです。これは、両方のピアの内部ネットワークが IPv6 で外部ネットワークが IPv6 の場合にも当てはまります。

IPsec Site-to-Site VPN Wizard

2 台の ASA デバイス間のトンネルは「サイトツーサイト トンネル」と呼ばれ、双方向です。サイトツーサイト VPN トンネルでは、IPsec プロトコルを使用してデータが保護されます。

Peer Device Identification

- [Peer IP Address]：他のサイト（ピア デバイス）の IP アドレスを設定します。
- [VPN Access Interface]：サイトツーサイト トンネルに使用するインターフェイスを選択します。
- [Crypto Map Type]：このピアに使用されるマップのタイプ（スタティックまたはダイナミック）を指定します。

保護するトラフィック

このステップでは、ローカル ネットワークおよびリモート ネットワークを指定します。これらのネットワークでは、IPsec 暗号化を使用してトラフィックが保護されます。

- [Local Networks]：IPsec トンネルで使用されるホストを指定します。
- [Remote Networks]：IPsec トンネルで使用されるネットワークを指定します。

セキュリティ

このステップでは、ピアデバイスとの認証の方法を設定します。単純な設定を選択するか、事前共有キーを指定できます。またさらに詳細なオプションについては、以下に説明する [Customized Configuration] を選択できます。

- [IKE Version]：どちらのバージョンを使用するかに応じて、[IKEv1] または [IKEv2] チェックボックスをオンにします。
- IKE version 1 Authentication Methods
  - [Pre-shared Key]：事前共有キーを使用すると、リモート ピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPsec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

    IPsec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモート サイトの管理者と事前共有キーを交換してください。
  - [Device Certificate]：ローカル ASA とリモート IPsec ピア間の認証で証明書を使用する場合にクリックします。

    デジタル証明書による IPSec トンネルの確立に使用するセキュリティ キーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP

アドレスなどの、ユーザーまたはデバイスを識別する情報が記述されています。またデジタル証明書には、公開キーのコピーも含まれています。

2 つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。

- IKE version 2 Authentication Methods
  - [Local Pre-shared Key]：IPsec IKEv2 認証方式と暗号化アルゴリズムを指定します。
  - [Local Device Certificate]：VPN アクセスの認証を、セキュリティ アプライアンスを通して行います。
  - [リモート ピア事前共有キー（Remote Peer Pre-shared Key）]：ローカル ASA とリモート IPsec ピア間の認証用の事前共有キーを入力します。
  - [リモート ピア ポスト量子キー（Remote Peer Post Quantum Key）]：IKEv2 セッション用のポスト量子事前共有キー（PPK）を指定するには、このチェックボックスをオンにします。PPK は 256 ビット、64 文字の 16 進文字列で、量子コンピュータ攻撃からセッションを保護します。IKEv2セッションでは、事前共有キーベースの認証とともに PPK を使用できます。
    - [リモートピアポスト量子キーID（Remote Peer Post Quantum Key Identity）]：PPK の ID を指定します。
  - [Remote Peer Certificate Authentication]：このチェックボックスがオンのときは、ピア デバイスが証明書を使用してこのデバイスに対して自身の認証を行うことができます。
- [Encryption Algorithms]：このタブでは、データの保護に使用する暗号化アルゴリズムのタイプを選択します。
  - [IKE Policy]：IKEv1/IKEv2 認証方式を指定します。
  - [IPsec Proposal]：IPsec 暗号化アルゴリズムを指定します。
- Perfect Forward Secrecy
  - [Enable Perfect Forwarding Secrecy (PFS)]：フェーズ 2 IPsec キーの生成において、Perfect Forward Secrecy を使用するかどうか、および使用する番号のサイズを指定します。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は、PFS がイネーブルになるまで、フェーズ 2 キーはフェーズ 1 キーに基づいています。PFS では、キーの生成に Diffie-Hellman 方式が採用されています。

    PFS によって、秘密キーの 1 つが将来解読されても、一連の長期公開キーおよび秘密キーから派生したセッション キーは解読されなくなります。

    PFS は、接続の両側でイネーブルにする必要があります。

- [Diffie-Hellman Group]：Diffie-Hellman グループ ID を選択します。2 つの IPsec ピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。デフォルトのグループ 14（2048 ビット Diffie-Hellman）。

NAT Exempt

- [Exempt ASA side host/network from address translation]：ドロップダウン リストを使用して、アドレス変換から除外するホストまたはネットワークを選択します。

セキュアクライアント VPN ウィザード

このウィザードは、 Cisco Secure Clientの AnyConnect VPN モジュールからの VPN 接続を受け入れるように ASA を設定するときに使用します。このウィザードでは、フル ネットワーク アクセスができるように IPsec（IKEv2）プロトコルまたは SSL VPN プロトコルを設定します。VPN 接続が確立したときに、ASA によって自動的に Cisco Secure Client の AnyConnect VPN モジュールがエンドユーザーのデバイスにアップロードされます。

Connection Profile Identification

[Connection Profile Identification] では、リモート アクセス ユーザーに対する ASA を指定します。

- [Connection Profile Name]：リモート アクセス ユーザーが VPN 接続のためにアクセスする名前を指定します。
- [VPN Access Interface]：リモート アクセス ユーザーが VPN 接続のためにアクセスするインターフェイスを選択します。

VPN Protocols

この接続プロファイルに対して許可する VPN プロトコルを指定します。

セキュアクライアント のデフォルトは SSL です。接続プロファイルの VPN トンネル プロトコルとして IPsec をイネーブルにした場合は、IPsec をイネーブルにしたクライアント プロファイルを作成して展開することも必要になります（作成するには、ASDM のプロファイル エディタを使用します）。

WebLaunch の代わりに セキュアクライアント を事前展開する場合は、最初のクライアント接続に SSL を使用し、セッション中に ASA からクライアントプロファイルを受け取ります。以降の接続では、クライアントはそのプロファイルで指定されたプロトコル（SSL または IPsec）を使用します。IPsec が指定されたプロファイルをクライアントとともに事前展開した場合は、最初のクライアント接続で IPsec が使用されます。IPsec をイネーブルにした状態のクライアントプロファイルを事前展開する方法の詳細については、『*Secure Client Administrator Guide*』を参照してください。

- SSL

- IPsec (IKE v2)
- [Device Certificate]：リモート アクセス クライアントに対する ASA を指定します。セキュアクライアント の機能の中には、Always on や IPsec/IKEv2 のように、有効なデバイス証明書が ASA に存在することを要件とするものがあります。
- [Manage]：[Manage] を選択すると [Manage Identity Certificates] ウィンドウが開きます。
  - [Add]：ID 証明書とその詳細情報を追加するには、[Add] を選択します。
  - [Show Details]：特定の証明書を選択して [Show Details] をクリックすると、[Certificate Details] ウィンドウが開き、その証明書の発行対象者と発行者が表示されるほか、シリアル番号、使用方法、対応するトラストポイント、有効期間などが表示されます。
  - [Delete]：削除する証明書を強調表示して [Delete] をクリックします。
  - [Export]：証明書を強調表示して [Export] をクリックすると、その証明書をファイルにエクスポートできます。このときに、暗号化パスフレーズを付けるかどうかを指定できます。
  - [Enroll ASA SSL VPN with Entrust]：Entrust からの SSL Advantage デジタル証明書を使用すると、すぐに ASA SSL VPN アプライアンスの稼働を開始できます。

Client Images

ASA は、クライアントデバイスがエンタープライズ ネットワークにアクセスするときに、最新の セキュアクライアント パッケージをそのデバイスに自動的にアップロードすることができます。ブラウザのユーザーエージェントとイメージとの対応を、正規表現を使用して指定できます。また、接続の設定に要する時間を最小限にするために、最もよく使用されるオペレーティング システムをリストの先頭に移動できます。

認証方法

この画面では、認証情報を指定します。

- [AAA server group]：ASA がリモート AAA サーバー グループにアクセスしてユーザーを認証できるようにします。AAA サーバー グループを、事前設定されたグループのリストから選択するか、[New] をクリックして新しいグループを作成します。
- [Local User Database Details]：ASA に格納されているローカル データベースに新しいユーザーを追加します。
  - [Username]：ユーザーのユーザー名を作成します。
  - [Password]：ユーザーのパスワードを作成します。
  - [Confirm Password]：確認のために同じパスワードを再入力します。
  - [Add/Delete]：ローカル データベースにユーザーを追加またはデータベースから削除します。

Client Address Assignment

リモート セキュアクライアント ユーザのための IP アドレス範囲を指定します。

- [IPv4 Address Pools]：SSL VPN クライアントは、ASA に接続したときに新しい IP アドレスを受け取ります。クライアントレス接続では新しい IP アドレスは不要です。アドレスプールでは、リモート クライアントが受け取ることのできるアドレス範囲が定義されます。既存の IP アドレス プールを選択するか、[New] をクリックして新しいプールを作成します。

  [New] を選択した場合は、開始と終了の IP アドレスおよびサブネット マスクを指定する必要があります。

- [IPv6 Address Pool]：既存の IP アドレス プールを選択するか、[New] をクリックして新しいプールを作成します。

（注） IPv6アドレス プールは、IKEv2接続プロファイル用には作成できません。

Network Name Resolution Servers

リモートユーザーが内部ネットワークにアクセスするときにどのドメイン名を解決するかを指定します。

- [DNS Servers]：DNS サーバーの IP アドレスを入力します。
- [WINS Servers]：WINS サーバーの IP アドレスを入力します。
- [Domain Name]：デフォルトのドメイン名を入力します。

NAT Exempt

ASA 上でネットワーク変換がイネーブルに設定されている場合は、VPN トラフィックに対してこの変換を免除する必要があります。

セキュアクライアント の導入

次の2つの方法のいずれかを使用して、セキュアクライアントプログラムをクライアントデバイスにインストールできます。

- [Web起動（Web launch）]：セキュアクライアント パッケージは、Web ブラウザを使用して ASA にアクセスしたときに自動的にインストールされます。

（注） Web launch はマルチ コンテキスト モードではサポートされません。

- [事前展開（Pre-deployment）]：手動で セキュアクライアント パッケージをインストールします。

[Allow Web Launch] は、すべての接続に影響が及ぶグローバル設定です。このチェックボックスがオフ（許可しない）の場合は、セキュアクライアント SSL 接続とクライアントレス SSL 接続は機能しません。

事前展開の場合は、disk0:/test2_client_profile.xml プロファイル バンドルの中に .msi ファイルがあり、このクライアントプロファイルを ASA から セキュアクライアント パッケージに入れておく必要があります。これは、IPsec 接続を期待したとおりに確実に動作させるためです。

IPsec IKEv1 Remote Access Wizard

（注） Cisco VPN Client は耐用年数末期で、サポートが終了しています。Secure Clientにアップグレードする必要があります。

IKEv1 Remote Access Wizard を使用して、モバイル ユーザーなどの VPN クライアントに安全なリモート アクセスを設定し、リモート IPsec ピアに接続するインターフェイスを指定します。

- [VPN Tunnel Interface]：リモート アクセス クライアントで使用するインターフェイスを選択します。ASA に複数のインターフェイスがある場合は、このウィザードを実行する前に ASA でインターフェイスを設定します。
- [Enable inbound IPsec sessions to bypass interface access lists]：IPsec 認証済みの着信セッションを ASA によって常に許可するようにします（つまり、インターフェイスの access-list 文をチェックしないようにします）。着信セッションがバイパスするのは、インターフェイス ACL だけです。設定されたグループ ポリシー、ユーザー、およびダウンロードされた ACL は適用されます。

リモート アクセス クライアント

さまざまなタイプのリモート アクセス ユーザーが、この ASA への VPN トンネルを開くことができます。このトンネルの VPN クライアントのタイプを選択します。

- VPN Client Type
  - [Easy VPN Remote product]
  - [Microsoft Windows client using L2TP over IPsec]：PPP 認証プロトコルを指定します。選択肢は、PAP、CHAP、MS-CHAP-V1、MS-CHAP-V2、および EAP-PROXY です。

    [PAP]：認証中にクリアテキストのユーザー名とパスワードを渡すので、安全ではありません。

[CHAP]：サーバーのチャレンジに対する応答で、クライアントは暗号化されたチャレンジとパスワードおよびクリアテキストのユーザー名を返します。このプロトコルは、PAP より安全ですが、データは暗号化されません。

[MS-CHAP, Version 1]：CHAP と似ていますが、サーバーは、CHAP のようなクリアテキストのパスワードではなく、暗号化したパスワードだけを保存および比較するので安全です。

[MS-CHAP, Version 2]：MS-CHAP, Version 1 以上のセキュリティ強化機能が含まれています。

[EAP-Proxy]：EAP をイネーブルにします。これによって ASA は、PPP 認証プロセスを外部の RADIUS 認証サーバーに代行させることができます。

リモートクライアントでプロトコルが指定されていない場合は、指定しないでください。

- 指定するのは、クライアントからトンネル グループ名が username@tunnelgroup として送信される場合です。

VPN クライアント認証方式とトンネル グループ名

認証方式を設定し、接続ポリシー（トンネル グループ）を作成するには、[VPN Client Authentication Method and Name] ペインを使用します。

- [Authentication Method]：リモート サイト ピアは、事前共有キーか証明書のいずれかを使用して認証します。
  - [Pre-shared Key]：ローカル ASA とリモート IPsec ピア間の認証で事前共有キーを使用する場合にクリックします。

    事前共有キーを使用すると、リモート ピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPsec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

    IPsec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモートサイトの管理者と事前共有キーを交換してください。

  - [Pre-shared Key]：1～128 文字の英数字文字列を入力します。

  - [Certificate]：ローカル ASA とリモート IPsec ピア間の認証で証明書を使用する場合にクリックします。このセクションを完了するには、事前に CA に登録し、1 つ以上の証明書を ASA にダウンロードしておく必要があります。

    デジタル証明書による IPSec トンネルの確立に使用するセキュリティ キーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなどの、ユーザーまたはデバイスを識別する情報が記述されています。またデジタル証明書には、公開キーのコピーも含まれています。

デジタル証明書を使用するには、デジタル証明書を発行する認証局（CA）に各ピアを登録します。CA は、信頼できるベンダーまたは組織内で設置したプライベート CA の場合もあります。

2 つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。

[Certificate Signing Algorithm]：デジタル証明書署名アルゴリズムを表示します（RSA の場合は rsa-sig）。

- [Tunnel Group Name]：名前を入力して、この IPsec 接続のトンネル接続ポリシーを含むレコードを作成します。接続ポリシーでは、認証、許可、アカウンティング サーバー、デフォルト グループ ポリシー、および IKE 属性を指定できます。この VPN ウィザードで設定する接続ポリシーは、認証方式を指定し、ASA のデフォルトのグループ ポリシーを使用します。

クライアント認証

[Client Authentication] ペインでは、ASA がリモート ユーザーを認証するときに使用する方法を選択します。次のオプションのいずれかを選択します。

- [Authenticate using the local user database]：ASA の内部の認証方式を使用する場合にクリックします。この方式は、ユーザーの数が少なくて安定している環境で使用します。次のペインでは、ASA に個々のユーザーのアカウントを作成できます。
- [Authenticate using an AAA server group]：リモート ユーザー認証で外部サーバー グループを使用する場合にクリックします。
  - [AAA Server Group Name]：先に構成された AAA サーバー グループを選択します。
  - [New ...]：新しい AAA サーバー グループを設定する場合にクリックします。

User Accounts

[User Accounts] ペインでは、認証を目的として、ASA の内部ユーザー データベースに新しいユーザーを追加します。

Address Pool

[Address Pool] ペインでは、ASA がリモート VPN クライアントに割り当てるローカル IP アドレスのプールを設定します。

- [Tunnel Group Name]：このアドレス プールが適用される接続プロファイル（トンネル グループ）の名前が表示されます。この名前は、[VPN Client Name and Authentication Method] ペイン（ステップ 3）で設定したものです。
- [Pool Name]：アドレス プールの記述 ID を選択します。
- [New...]：新しいアドレス プールを設定します。

- [Range Start Address]：アドレス プールの開始 IP アドレスを入力します。
- [Range End Address]：アドレス プールの終了 IP アドレスを入力します。
- [Subnet Mask]：（任意）これらの IP アドレスのサブネット マスクを選択します。

Attributes Pushed to Client (任意)

[Attributes Pushed to Client (Optional)] ペインでは、DNS サーバーと WINS サーバーに関する情報およびデフォルト ドメイン名をリモート アクセス クライアントに渡すように、ASA を設定します。

- [Tunnel Group]：アドレス プールが適用される接続ポリシーの名前を表示します。この名前は、[VPN Client Name and Authentication Method] ペインで設定したものです。
- [Primary DNS Server]：プライマリ DNS サーバーの IP アドレスを入力します。
- [Secondary DNS Server]：セカンダリ DNS サーバーの IP アドレスを入力します。
- [Primary WINS Server]：プライマリ WINS サーバーの IP アドレスを入力します。
- [Secondary WINS Server]：セカンダリ WINS サーバーの IP アドレスを入力します。
- [Default Domain Name]：デフォルトのドメイン名を入力します。

IKE Policy

Internet Security Association and Key Management Protocol（ISAKMP）とも呼ばれる IKE は、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。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 Policy] ペインでは、フェーズ 1 IKE ネゴシエーションの条件を設定します。この条件には、データを保護し、プライバシーを守る暗号化方式、ピアの ID を確認する認証方式、および暗号キー判別アルゴリズムを強化する Diffie-Hellman グループが含まれます。ASA はこのアルゴリズムを使用して、暗号キーとハッシュ キーを導出します。

- [Encryption]：フェーズ 2 ネゴシエーションを保護するフェーズ 1 SA を確立するために ASA が使用する、対称暗号化アルゴリズムを選択します。ASA は、次の暗号化アルゴリズムをサポートしています。

アルゴリズム	説明
DES	データ暗号規格。56 ビット キーを使用します。
3DES	Triple DES。56 ビット キーを使用して暗号化を 3 回実行します。
AES-128	高度暗号化規格。128 ビット キーを使用します。
aes-192	192 ビット キーを使用する AES。

アルゴリズム	説明
AES-256	256 ビット キーを使用する AES。

デフォルトの 3DES は DES よりもセキュアですが、暗号化と復号化には、より多くの処理を必要とします。同様に、AES オプションによるセキュリティは強力ですが、必要な処理量も増大します。

- [Authentication]：認証やデータ整合性の確保のために使用するハッシュ アルゴリズムを選択します。デフォルトは SHA です。MD5 のダイジェストは小さく、SHA よりもわずかに速いとされています。MD5 は、（きわめて困難ですが）攻撃により破れることが実証されています。しかし、ASA で使用される Keyed-Hash Message Authentication Code（HMAC）バージョンはこの攻撃を防ぎます。
- [Diffie-Hellman Group]：Diffie-Hellman グループ ID を選択します。2 つの IPsec ピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。デフォルト DH グループ 14（2048 ビット）は、グループ 2 およびグループ 5 よりも安全性が高いと見なされます。

IPsec Settings（任意）

[IPsec Settings (Optional)] ペインでは、アドレス変換が不要なローカル ホスト/ネットワークを指定します。デフォルトでは、ASA は、ダイナミックまたはスタティックなネットワーク アドレス変換（NAT）を使用して、内部のホストおよびネットワークの実 IP アドレスを外部ホストから隠します。NAT は、信頼できない外部ホストによる攻撃の危険性を最小限に抑えますが、VPN によって認証および保護されているホストに対しては不適切な場合があります。

たとえば、ダイナミック NAT を使用する内部ホストは、プールから無作為に選択したアドレスと照合することにより、その IP アドレスを変換させます。外部ホストからは、変換されたアドレスだけが見えるようになります。本当の IP アドレスにデータを送信することによってこれらの内部ホストに到達しようとするリモート VPN クライアントは、NAT 免除ルールを設定しない限り、これらのホストには接続できません。

（注） すべてのホストとネットワークを NAT から免除する場合は、このペインでは何も設定しません。エントリが 1 つでも存在すると、他のすべてのホストとネットワークは NAT に従います。

- [Interface]：選択したホストまたはネットワークに接続するインターフェイスの名前を選択します。
- [Exempt Networks]：選択したインターフェイス ネットワークから免除するホストまたはネットワークの IP アドレスを選択します。
- [Enable split tunneling]：リモート アクセス クライアントからのパブリック インターネット宛のトラフィックを暗号化せずに送信する場合に選択します。スプリット トンネリングにより、保護されたネットワークのトラフィックが暗号化され、保護されていないネットワークのトラフィックは暗号化されません。スプリット トンネリングをイネーブルにする

と、ASA は、認証後に IP アドレスのリストをリモート VPN クライアントにプッシュします。リモート VPN クライアントは、ASA の背後にある IP アドレスへのトラフィックを暗号化します。他のすべてのトラフィックは暗号化されずに直接インターネットに送り出され、ASA は関与しません。

- [Enable Perfect Forwarding Secrecy (PFS)]：フェーズ 2 IPsec キーの生成において、Perfect Forward Secrecy を使用するかどうか、および使用する番号のサイズを指定します。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は、PFS がイネーブルになるまで、フェーズ 2 キーはフェーズ 1 キーに基づいています。PFS では、キーの生成に Diffie-Hellman 方式が採用されています。

  PFS によって、秘密キーの 1 つが将来解読されても、一連の長期公開キーおよび秘密キーから派生したセッション キーは解読されなくなります。

  PFS は、接続の両側でイネーブルにする必要があります。

  - [Diffie-Hellman Group]：Diffie-Hellman グループ ID を選択します。2 つの IPsec ピアは、相互に共有秘密情報を転送することなく共有秘密情報を導出するためにこの ID を使用します。デフォルト DH グループ 14（2048 ビット）は、グループ 2 およびグループ 5 よりも安全性が高いと見なされます。

Summary

設定に問題なければ、[Finish] をクリックします。ASDM によって LAN-to-LAN のコンフィギュレーションが保存されます。[Finish] をクリックした後は、この VPN ウィザードを使用してこのコンフィギュレーションを変更することはできません。ASDM を使用して拡張機能を編集および設定してください。

IPsec IKEv2 Remote Access Wizard

IKEv2 Remote Access Wizard を使用して、モバイル ユーザーなどの VPN クライアントに安全なリモート アクセスを設定し、リモート IPsec ピアに接続するインターフェイスを指定します。

Connection Profile Identification

[Connection Profile Name] に接続プロファイルの名前を入力し、[VPN Access Interface] で IPsec IKEv2 リモート アクセスに使用する VPN アクセス インターフェイスを選択します。

- [Connection Profile Name]：名前を入力して、この IPsec 接続のトンネル接続ポリシーを含むレコードを作成します。接続ポリシーでは、認証、許可、アカウンティング サーバー、デフォルト グループ ポリシー、および IKE 属性を指定できます。この VPN ウィザードで設定する接続ポリシーは、認証方式を指定し、ASA のデフォルトのグループ ポリシーを使用します。
- [VPN Access Interface]：リモート IPsec ピアとのセキュアなトンネルを確立するインターフェイスを選択します。ASA に複数のインターフェイスがある場合は、このウィザードを

実行する前に VPN コンフィギュレーションを計画し、セキュアな接続を確立する予定のリモート IPsec ピアごとに、使用するインターフェイスを特定しておく必要があります。

標準規格に基づく IPSec（IKEv2）認証ページ

[IKE Peer Authentication]：リモート サイト ピアは、事前共有キー、証明書、または EAP を使用したピア認証のいずれかを使用して認証します。

- [Pre-shared Key]：1～128 文字の英数字文字列を入力します。

  事前共有キーを使用すると、リモートピアの数が限定的でかつネットワークが安定している場合、通信をすばやく簡単にセットアップできます。それぞれの IPsec ピアは、セキュアな接続を確立する相手のピアごとにコンフィギュレーション情報を必要とするため、大規模なネットワークではスケーラビリティの問題が生じる場合があります。

  IPsec ピアの各ペアは、事前共有キーを交換してセキュアなトンネルを確立する必要があります。セキュアな方法を使用して、リモートサイトの管理者と事前共有キーを交換してください。

- [Enable Certificate Authentication]：オンにすると、認証に証明書を使用できます。
- [Enable peer authentication using EAP]：オンにすると、認証に EAP を使用できます。このチェックボックスをオンにした場合は、ローカル認証に証明書を使用する必要があります。
- [Send an EAP identity request to the client]：リモート アクセス VPN クライアントに EAP 認証要求を送信できます。
- [ポスト量子キー（Post Quantum Key）]：IKEv2 セッション用のポスト量子事前共有キー（PPK）を指定するには、このチェックボックスをオンにします。PPK は 256 ビット、64 文字の 16 進文字列で、量子コンピュータ攻撃からセッションを保護します。IKEv2 セッションでは、事前共有キーベースの認証とともに PPK を使用できます。
  - [ポスト量子キー識別子（Post Quantum Key Identity）]：PPK の ID を指定します。

Mobike RRC

- [Enable Return Routability Check for mobike]：Mobike が有効になっている IKE/IPSEC セキュリティ アソシエーションにおけるダイナミック IP アドレスの変更をチェックする Return Routability を有効にします。

[IKE Local Authentication]

- ローカル認証をイネーブルにして、事前共有キーまたは証明書のいずれかを選択します。
  - [Preshared Key]：1 ～ 128 文字の英数字文字列を入力します。
  - [Certificate]：ローカル ASA とリモート IPsec ピア間の認証で証明書を使用する場合にクリックします。このセクションを完了するには、事前に CA に登録し、1 つ以上の証明書を ASA にダウンロードしておく必要があります。

デジタル証明書による IPSec トンネルの確立に使用するセキュリティ キーを効率よく管理できます。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなどの、ユーザーまたはデバイスを識別する情報が記述されています。またデジタル証明書には、公開キーのコピーも含まれています。

デジタル証明書を使用するには、デジタル証明書を発行する認証局（CA）に各ピアを登録します。CA は、信頼できるベンダーまたは組織内で設置したプライベート CA の場合もあります。

2 つのピアが通信する場合は、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアをネットワークに追加する場合は、そのピアを CA に登録します。他のピアが追加の設定を行う必要はありません。

認証方法

IPsec IKEv2 リモート アクセスでは RADIUS 認証のみがサポートされています。

- [AAA Server Group]：先に構成された AAA サーバー グループを選択します。
- [New]：新しい AAA サーバー グループを設定する場合にクリックします。
- [AAA Server Group Details]：この領域を使用して、AAA サーバー グループを必要に応じて変更します。

Client Address Assignment

IPv4 および IPv6 のアドレス プールを作成するか、選択します。リモート アクセス クライアントには、IPv4 または IPv6 のプールのアドレスが割り当てられます。両方を設定した場合は、IPv4 アドレスが優先されます。詳細については、「ローカル *IP* アドレス プールの設定」を参照してください。

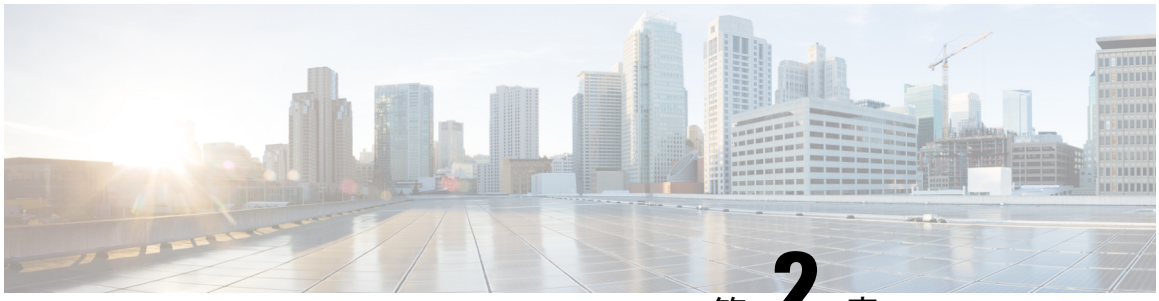
Network Name Resolution Servers

リモート ユーザーが内部ネットワークにアクセスするときにどのようにドメイン名を解決するかを指定します。

- [DNS Servers]：DNS サーバーの IP アドレスを入力します。
- [WINS Servers]：WINS サーバーの IP アドレスを入力します。
- [Default Domain Name]：デフォルトのドメイン名を入力します。

NAT Exempt

- [Exempt VPN traffic from Network Address Translation]：ASA で NAT がイネーブルになっている場合は、このチェックボックスをオンにする必要があります。



第 2 章

IKE

IKE の設定

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

手順

ステップ 1 IKE の有効化 （17 ページ）を使用して無効にすることができます。

ステップ 2 サイト間 VPN の IKE パラメータ （18 ページ） を設定します。

ステップ 3 IKE ポリシー （25 ページ） を設定します。

IKE の有効化

手順

ステップ 1 VPN 接続に対して IKE を有効にする方法

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

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

ステップ 2 サイト間 VPN に対して IKE を有効にする方法

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

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

サイト間 VPN の IKE パラメータ

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

NAT の透過性

- [Enable IPsec over NAT-T]

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

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

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

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

  NAT-T を使用するには、次の手順を実行する必要があります。

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

- Enable IPsec over TCP

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

（注） この機能は、プロキシベースのファイアウォールでは動作しません。

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

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

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

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

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

ピアに送信される ID

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

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

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

セッション制御

- [Disable Inbound Aggressive Mode Connections]

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

- [Alert Peers Before Disconnecting]

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

  限定されたクライアントとピアには次のものが含まれます。

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

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

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

- [Number of SAs Allowed in Negotiation for IKEv1]

  一時点でのネゴシエーション中 SA の総数を制限します。

IKE v2 特有の設定

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

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

IKE v2 特有の設定による DoS 攻撃の防止

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

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

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

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

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

IKEv2 複数ピアクリプトマップについて

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

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

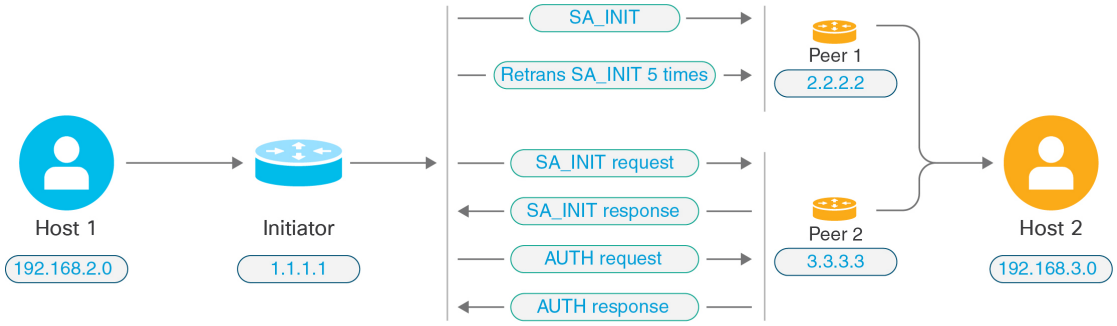
IKEv2 イニシエータの動作

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

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

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

図 *1:* イニシエータのプロセスフロー



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

IKEv2 レスポンダの動作

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

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

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

クリプトマップ変更時のピアインデックスのリセット

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

表 *1 : SA* 前の複数ピアインデックスの移行

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

表 *2 : SA* 後の複数ピアインデックスの移行

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

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

IKEv2 複数ピアの注意事項

IKEv1 および IKEv2 プロトコル

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

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

高可用性

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

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

集中クラスタ

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

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

分散クラスタ

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

マルチコンテキストモード

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

デバッグ コマンド

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

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

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

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

IKE ポリシー

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

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

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

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

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

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

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

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

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

フィールド

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

IKEv1 ポリシーの追加または編集

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IKEv2 ポリシーの追加または編集

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

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

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

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

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

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

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

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

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

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

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

ASA では次の値を使用できます。

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

IPsec の設定

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

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

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

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

ASA は、次の IPSec 属性をサポートしています。

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

手順

ステップ 1 暗号マップ （32 ページ） を設定します。
ステップ 2 IPsec 事前フラグメンテーション ポリシー （41 ページ） を設定します。
ステップ 3 IPsec Proposals (Transform Sets) （44 ページ） を設定します。

暗号マップ

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

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

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

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

IPsec ルールでは以下を指定します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  [Clear DF bit]：DF ビットを無視します。

  [Copy DF bit]：DF ビットを維持します。

  [Set DF bit]：DF ビットを設定して使用します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IPsec 事前フラグメンテーション ポリシー

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

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

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

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

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

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

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

フィールド

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

IKEv2 フラグメンテーション オプションの設定

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

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

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

次の点を考慮して、MTU を指定してください。

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

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

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

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

始める前に

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

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

手順

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

IPsec Proposals (Transform Sets)

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

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

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

[IKEv1 IPsec Proposals （Transform Sets）]

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

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

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

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

[IKEv2 IPsec Proposals]

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

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

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

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

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

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

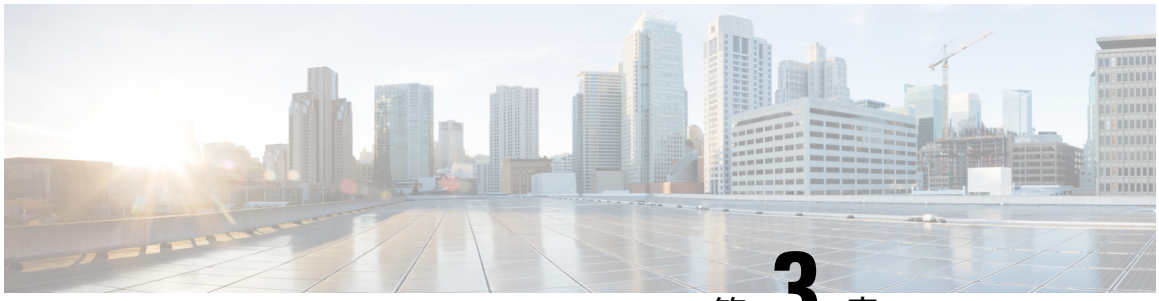
  - [Transport Required]：カプセル化モードは転送モードにしかなりません。トンネル モードにフォールバックすることはできません。

（注） 転送モードは、リモート アクセス VPN には推奨されません。

カプセル化モードのネゴシエーションの例は次のとおりです。

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

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



第 3 章

ハイアベイラビリティ オプション

ハイアベイラビリティ オプション

分散型 VPN クラスタリング、ロード バランシング、およびフェールオーバーは、それぞれ機能と要件が異なるハイアベイラビリティ機能です。状況によっては、複数の機能を導入環境で使用することがあります。以降では、これらの機能について説明します。分散型VPNとフェールオーバーの詳細については、『ASA General Operations ASDM Configuration Guide』の適切なリリースを参照してください。ロード バランシングの詳細は以下に記載されています。

Secure Firewall eXtensible オペレーティングシステム（FXOS）シャーシ上の VPN とクラスタリング

ASA FXOS クラスタは、S2S VPN に対する相互排他的な 2 つのモード（集中型または分散型）のいずれかをサポートしています。

- 集中型 VPN モード。デフォルト モードです。集中モードでは、VPN 接続はクラスタの制御ユニットとのみ確立されます。

  VPN機能を使用できるのは制御ユニットだけであり、クラスタの高可用性機能は活用されません。制御ユニットで障害が発生した場合は、すべての既存のVPN接続が失われ、VPN接続されたユーザーにとってはサービスの中断となります。新しい制御ユニットが選定されたときに、VPN 接続を再確立する必要があります。

  VPN トンネルをスパンドインターフェイスのアドレスに接続すると、接続が自動的に制御ユニットに転送されます。VPN 関連のキーと証明書は、すべてのユニットに複製されます。

- 分散型 VPN モード。このモードでは、S2S IPsec IKEv2 VPN 接続が ASA クラスタのメンバー全体に分散され、拡張性が提供されます。クラスタのメンバー全体に VPN 接続を分散することで、クラスタの容量とスループットの両方を最大限に活用できるため、集中型 VPN の機能を超えて大幅に VPN サポートを拡張できます。

（注） 集中型 VPN クラスタリング モードは、S2S IKEv1 と S2S IKEv2 をサポートしています。

分散型 VPN クラスタリング モードは、S2S IKEv2 のみをサポートしています。

分散型 VPN クラスタリング モードは、Firepower 9300 でのみサポートされています。

リモート アクセス VPN は、集中型または分散型の VPN クラスタリング モードではサポートされていません。

VPN ロード バランシング

VPN ロードバランシングは、VPN ロードバランシンググループ内のデバイス間でリモートアクセス VPN トラフィックを均一に分散するメカニズムです。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。VPN ロードバランシンググループは、2つ以上のデバイスで構成されます。1つのデバイスがディレクタとなり、その他のデバイスはメンバーデバイスとなります。グループのデバイスは、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構成を使用する必要もありません。

VPN ロードバランシンググループ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。VPN ロードバランシングにより、トラフィックはグループ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

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 が専用のフェールオーバー リンクで接続され、必要に応じて、ステートフル フェールオーバー リンク（任意）でも接続されます。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ーされて、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設定をサポートしています。

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。

VPN ロード バランシング

VPN ロードバランシングについて

リモートクライアント構成で、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、VPN ロードバランシンググループを作成して、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。VPN 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。これにより、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。

VPN ロードバランシンググループ内のすべてのデバイスがセッションの負荷を伝送します。グループ内の 1 つのデバイスであるディレクタは、着信接続要求をメンバーデバイスと呼ばれる他のデバイスに転送します。ディレクタは、グループ内のすべてのデバイスを監視し、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。ディレクタの役割は、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、現在のディレクタで障害が発生すると、グループ内のメンバーデバイスの 1 つがその役割を引き継いで、すぐに新しいディレクタになります。

VPN ロードバランシンググループは、外部のクライアントには 1 つの仮想 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。これは現在のディレクタに属しています。接続の確立を試みている VPN クライアントは、最初に仮想 IP アドレスに接続します。ディレクタは、グループ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 回めのトランザクション（ユーザーに対しては透過的）になると、クライアントはホストに直接接続します。VPN ロードバランシンググループのディレクタは、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。

グループ内の ASA 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 IP アドレスに再接続できます。次に、ディレクタは、グループ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。ディレクタで障害が発生した場合、グループ内のメンバーデバイスが、ただちに新しいディレクタを自動的に引き継ぎます。グループ内の複数のデバイスで障害が発生しても、グループ内のいずれかのデバイスが稼働していて使用可能である限り、ユーザーはグループに引き続き接続できます。

VPN ロード バランシング クラスタ デバイスごとに、パブリック/外部（lbpublic）およびプライベート/内部（lbprivate）インターフェイスを設定する必要があります。

- [パブリックインターフェイス（Public interface）]：クラスタ IP アドレスへの初期通信に使用されるデバイスの外部インターフェイス。このインターフェイスは、Hello ハンドシェイクに使用されます。
- [プライベートインターフェイス（Private interface）]：ロード バランシング クラスタ メンバー間のメッセージングに使用されるデバイスの内部インターフェイス。これらのメッセージには、ロードバランシングに関連するキープアライブ、トポロジメッセージ、およびアウトオブサービス メッセージが含まれます。

VPN ロードバランシングのアルゴリズム

VPN ロード バランシング グループ ディレクタは、IP アドレスの昇順でソートされたグループ メンバーのリストを保持します。各メンバーの負荷は、整数のパーセンテージ（アクティブなセッションの数）として計算されます。セキュアクライアント 非アクティブセッションは、VPN ロードバランシングで SSL VPN ロードに含められません。ディレクタは、IPsec トンネルと SSL VPN トンネルを負荷が最も低いデバイスに、その他のデバイスより負荷が 1% 高くなるまでリダイレクトします。すべてのメンバーがディレクタよりも 1% 高くなると、ディレクタはトラフィックを自身にリダイレクトします。

たとえば、1 つのディレクタと 2 つのメンバーがある場合、次のサイクルが当てはまります。

（注） すべてのノードは 0% から始まり、すべての割合は四捨五入されます。

1. ディレクタは、すべてのメンバーにディレクタよりも 1% 高い負荷がある場合、接続を使用します。
2. ディレクタが接続を使用しない場合、最も負荷率の低いメンバーがセッションを処理します。
3. すべてのメンバーに同じ割合の負荷がかかっている場合、セッション数が最も少ないメンバーがセッションを取得します。
4. すべてのメンバーに同じ割合の負荷と同じ数のセッションがある場合、IP アドレスが最も小さいメンバーがセッションを取得します。

VPN ロードバランシンググループ構成

VPN ロードバランシンググループは、同じリリースまたは混在リリースの ASA から構成できます。ただし、次の制約があります。

- 同じリリースの 2 台の ASA から構成される VPN ロードバランシンググループは、IPsec、セキュアクライアント、およびクライアントレス SSL VPN クライアントセッションの組み合わせに対して VPN ロードバランシングを実行できます。
- 混在リリースの ASA を含む VPN ロードバランシンググループは、IPsec セッション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達しない可能性があります。

グループのディレクタは、グループのメンバー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。

VPN ロードバランシンググループでは最大 10 のノードがテスト済みです。これより大きなグループも機能しますが、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。

VPN ロード バランシング ディレクタの選択

ディレクタの選択プロセス

仮想クラスタ内の各非マスターは、ローカル トポロジ データベースを維持します。このデータベースは、クラスタのトポロジが変更されるたびにマスターによって更新されます。各非マスターは、マスターから Hello 応答を受信できないか、最大再試行回数に達してもマスターからキープアライブ応答を受信できない場合に、マスター選択状態になります。

メンバーは、ディレクタ選択の際に次の機能を実行します。

- ローカル トポロジ データベースで検出された各ロードバランシングユニットの優先順位を比較します。
- 同じ優先順位のユニットが 2 つ検出された場合は、下位の IP アドレスが選択されます。
- そのメンバー自体が選択された場合、選択されたメンバーは仮想 IP アドレスを要求します。
- 他のいずれかのメンバーが選択された場合、最初のメンバーは選択されたマスターにHello要求を送信します。
- 2 つのメンバーユニットが仮想 IP アドレスを要求しようとすると、ARP サブシステムが IP アドレスの重複状態を検出し、上位の MAC アドレスを持つメンバーにディレクタロールを辞退するように求める通知を送信します。

Hello ハンドシェイク

各メンバーは、起動時に外部インターフェイスの仮想クラスタ IP アドレスに Hello 要求を送信します。Hello 要求を受信すると、マスターは固有の Hello 要求をメンバーに送信します。ディレクタ以外のメンバーは、ディレクタからの Hello 要求を受信すると、Hello 応答を返します。これで Hello ハンドシェイクは終了になります。

Hello ハンドシェイクが完了すると、暗号化が設定されている場合、内部インターフェイスで接続が開始されます。最大再試行回数に達してもメンバーが Hello 応答を受信できない場合、メンバーはマスター選択状態になります。

キープアライブ メッセージ

メンバーとディレクタの間でHelloハンドシェイクが完了すると、各メンバーユニットは、キープアライブ要求を負荷情報とともにマスターに定期的に送信します。ディレクタからの未処理のキープアライブ応答がない場合、通常の処理中にメンバーユニットによってキープアライブ

要求が1秒間隔で送信されます。これは、前の要求からのキープアライブ応答が受信されている限り、次のキープアライブ要求が 1 秒後に送信されることを意味します。メンバーが前のキープアライブ要求に対するディレクタからのキープアライブ応答を受信しなかった場合、1 秒後にキープアライブ要求は送信されません。代わりに、メンバーのキープアライブ タイムアウト ロジックが開始されます。

キープアライブタイムアウトは次のように機能します。

1. メンバーがディレクタからの未処理のキープアライブ応答を待っている場合、そのメンバーは通常の 1 秒間隔のキープアライブ要求を送信しません。
2. メンバーは 3 秒間待機し、4 秒後にキープアライブ要求を送信します。
3. メンバーは、ディレクタからのキープアライブ応答がない限り、上のステップ 2 を 5 回繰り返します。
4. その後、メンバーはディレクタの不在を宣言し、新しいディレクタ選択サイクルを開始します。

VPN ロードバランシングについてよく寄せられる質問（FAQ）

マルチ コンテキスト モード

Q. マルチコンテキストモードで VPN ロードバランシングはサポートされますか。

A. VPN ロードバランシングもステートフル フェールオーバーもマルチコンテキストモードではサポートされていません。

IP アドレス プールの枯渇

Q. ASA は、IP アドレス プールの枯渇をその VPN ロードバランシング方式の一部と見なしますか。

A. いいえ。リモート アクセス VPN セッションが、IP アドレス プールが枯渇したデバイスに転送された場合、セッションは確立されません。ロードバランシング アルゴリズムは、負

荷に基づき、各メンバーが提供する整数の割合（アクティブセッション数および最大セッション数）として計算されます。

固有の IP アドレス プール

Q. VPN ロードバランシングを導入するには、異なる ASA 上のセキュアクライアントまたは IPsec クライアントの IP アドレスプールを固有にする必要がありますか。

A. はい。IP アドレス プールはデバイスごとに固有にする必要があります。

同じデバイスでの VPN ロードバランシングとフェールオーバーの使用

Q. 単一のデバイスで、VPN 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か。

A. はい。この構成では、クライアントはグループの IP アドレスに接続し、グループ内で最も負荷の少ない ASA にリダイレクトされます。そのデバイスで障害が発生すると、スタンバイ装置がすぐに引き継ぎ、VPN トンネルにも影響を及ぼしません。

複数のインターフェイスでの VPN ロードバランシング

Q. 複数のインターフェイスで SSL VPN をイネーブルにする場合、両方のインターフェイスに VPN ロードバランシングを実装することはできますか。

A. パブリックインターフェイスとして VPN ロードバランシンググループに参加するインターフェイスは 1 つしか定義できません。これは、CPU 負荷のバランスをとることを目的としています。複数のインターフェイスは同じ CPU に集中するため、複数のインターフェイスで VPN ロードバランシングを使用してもパフォーマンスは向上しません。

VPN ロードバランシンググループの最大同時セッション数

Q. それぞれ 100 ユーザーの SSL VPN ライセンスを持つ 2 つの Firepower 1150 が展開されているとします。この場合、VPN ロードバランシンググループで許可されるユーザーの最大合計数は、200 同時セッションでしょうか。または 100 同時セッションだけでしょうか。さらに 100 ユーザー ライセンスを持つ 3 台目のデバイスを追加した場合、300 の同時セッションをサポートできますか。

A. VPN ロードバランシングを使用すると、すべてのデバイスがアクティブになるため、グループでサポートできる最大セッション数は、グループ内の各デバイスのセッション数の合計になります。この例の場合は、300 になります。

VPN ロードバランシングのライセンス

VPN ロード バランシングのライセンス要件は次のとおりです。

- アクティブな 3DES/AES ライセンス。

  ASA は、VPN ロード バランシングを有効にする前に、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 ライセンスを検出できない場

合、ASA は、VPN 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、VPN ロードバランシングシステムによる 3DES の内部構成も回避します。

- ファイアウォールでアクティブ化された、この機能の有効な Security Plus ライセンス。
- スマート アカウントにこれらの Security Plus ライセンスを十分に持っている必要があります。

VPN ロードバランシングの前提条件

VPN ロード バランシングに関するガイドラインと制限事項 （54 ページ）も参照してください。

- VPN ロードバランシングはデフォルトでは無効になっています。VPN ロードバランシングは明示的にイネーブルにする必要があります。
- 最初にパブリック（外部）およびプライベート（内部）インターフェイスを設定しておく必要があります。この項では、これ以降の参照に外部および内部の名前を使用します。

  これを行うには、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に移動します。
- 仮想 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。共通仮想 IP アドレス、UDP ポート（必要に応じて）、およびグループの IPsec 共有秘密を確立します。
- グループに参加するすべてのデバイスは、IP アドレス、暗号設定、暗号キー、およびポートというクラスタ固有の同一値を共有する必要があります。
- VPN ロードバランシンググループの暗号化を使用するには、まず、内部インターフェイスを指定して **crypto ikev1 enable** コマンドを実行することで、内部インターフェイスで IKEv1 をイネーブルにする必要があります。そうしない場合、VPN ロードバランシンググループ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。
- アクティブ/アクティブ ステートフル フェールオーバー、または VPN ロードバランシングを使用している場合、ローカル CA 機能はサポートされません。ローカル CA を別の CA の下位に置くことはできません。ローカル CA はルート CA にしかなれません。

VPN ロード バランシングに関するガイドラインと制限事項

適格なクライアント

VPN 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。

- Secure Client（リリース 3.0 以降）
- ASA 5505（Easy VPN クライアントとして動作している場合）

- Firepower 1010（Easy VPN クライアントとして動作している場合）
- 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）

クライアントの考慮事項

VPN 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 クライアントセッションで機能します。LAN-to-LAN を含めて、他のすべての VPN 接続タイプ（L2TP、PPTP、L2TP/IPsec）は、VPN 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、VPN ロードバランシングには参加できません。

複数の ASA ノードがロードバランシングのためにグループ化され、セキュアクライアント 接続にグループ URL の使用が必要な場合、個々の ASA ノードで以下を行う必要があります。

- 各リモートアクセス接続プロファイルに、各 VPN ロードバランシング仮想アドレス（IPv4 および IPv6）のグループ URL を設定します。
- このノードの VPN ロードバランシング パブリック アドレスに対してグループ URL を設定します。

ロードバランシンググループ

ASA は、VPN ロードバランシンググループごとに 10 台のデバイスをサポートします。

コンテキスト モード

マルチ コンテキスト モードでは、VPN ロード バランシングはサポートされません。

FIPS

クラスタ暗号化は FIPS ではサポートされていません。

証明書の確認

セキュアクライアント で VPN 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、クライアントによるすべての名前チェックは、この IP アドレスを通して実行されます。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ーの 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。VPN ロードバランシンググループ環境では、証明書の構成により異なります。グループが 1 つの証明書を使用している場合、証明書は、仮想 IP アドレスおよびグループ FQDN の SAN 拡張機能を保持するほか、各 ASA の IP および FQDN を備えたサブジェクト代替名の拡張機能を含む必要があります。グ

ループが複数の証明書を使用している場合、各 ASA の証明書は、仮想 IP の SAN 拡張機能、グループ FQDN、個々の ASA の IP アドレスおよび FQDN を保持する必要があります。

地理的 VPN ロードバランシング

VPN 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 ロードバランス構成が セキュアクライアント との組み合わせで適切に機能するには、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、ASA の名前からアドレスへのマッピングが同じまま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、ユーザー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。

IKE/IPSec セキュリティ アソシエーション

クラスタ暗号化セッションは、VPN ロードバランサトポロジのスタンバイに同期されません。

VPN 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 VPN 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。VPN 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の可用性が向上します。

VPN ロードバランシングを使用するには、グループ内の各デバイスで以下を実行します。

- 共通の VPN ロードバランシンググループ属性を設定することによって、VPN ロードバランシンググループを設定します。これには、仮想 IP アドレス、UDP ポート（必要に応じて）、およびグループの IPsec 共有秘密が含まれます。グループに参加するすべてのデバイスには、グループ内でのデバイスの優先順位を除き、同一のグループ構成を設定する必要があります。
- デバイスで VPN ロードバランシングを有効にし、パブリックアドレスとプライベートアドレスなどのデバイス固有のプロパティを定義することにより、参加するデバイスを設定します。これらの値はデバイスによって異なります。

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

手順

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 VPN ロードバランシンググループ全体を表す 1 つの IP アドレスを選択します。グループ内のすべての 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 VPN ロードバランシンググループの 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、VPN 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 VPN 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。

ステップ 6 **IPsec 共有秘密**を指定して確認します。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 グループ内でこのデバイスに割り当てる優先順位を指定します。値の範囲は 1 ～ 10 です。優先順位は、起動時または既存のディレクタで障害が発生したときに、このデバイスがグループディレクタになる可能性を表します。優先順位を高く設定すると（たとえば 10）、このデバイスがディレクタになる可能性が高くなります。

（注）
VPN ロードバランシンググループ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、ディレクタの役割を果たすと想定されます。グループ内の各デバイスは起動するとチェックを行い、グループにディレクタ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、グループに追加されたデバイスは、グループメンバーになります。グループ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ディレクタになります。グループ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ディレクタになります。

ステップ 8 [Public Interface of This Device] を選択します。

ステップ 9 [Private Interface of This Device] を選択します。

ステップ 10 VPN クライアント接続を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デバイスのホスト名とドメイン名を使用して、ディレクタ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 ロードバランシンググループの構成が ASA に送信されます。

次のタスク

複数の ASA ノードがロードバランシングのためにグループ化され、セキュアクライアント 接続にグループ URL の使用が必要な場合、個々の ASA ノードで以下を行う必要があります。

- 各リモートアクセス接続プロファイルに、各VPNロードバランシング仮想アドレス（IPv4 および IPv6）のグループ URL を設定します。
- このノードの VPN ロードバランシング パブリック アドレスに対してグループ URL を設定します。

グループ URL は、[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [セキュアクライアント接続プロファイル（Connection Profiles）] > [接続プロファイル名（connection profile name）] > [追加または編集（Add or Edit）] > [詳細設定（Advanced）] > [グループエイリアス/グループ URL（Group Alias / Group URL）] ペインで設定します。

VPN 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）

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Load Balancing]** を選択します。

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から、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示す単一の 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から、IP アドレスを選択します。IPv6 アドレスを使用しているクライアントは、ASA クラスタ

の公開されている IPv6 アドレス経由または GSS サーバー経由でセキュアクライアント接続を実行できます。同様に、IPv6 アドレスを使用しているクライアントは、ASA クラスタの公開されている IPv4 アドレス経由または GSS サーバー経由でセキュアクライアント VPN 接続を実行できます。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 サーバーに DNS サーバー 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 を使用して LAN-to-LAN トンネル経由で通信します。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。 値の範囲は 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 によって変換した後の 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 クライアント接続を別のクラスタ デバイス（クラスタ内の別の ASA）にリダイレクトするときに、この ASA は VPN クラスタ マスターとして、DNS 逆ルックアップを使用し、そのクラスタデバイスの（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。

次のタスク

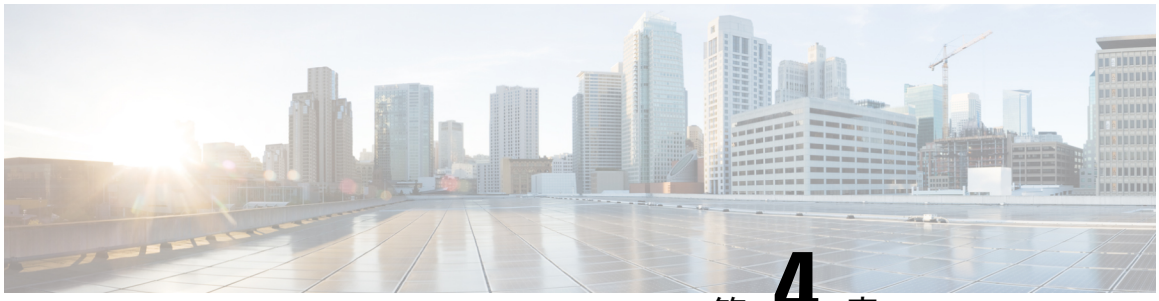
複数の ASA ノードがロードバランシングのためにクラスタ化され、セキュアクライアント 接続にグループ URL の使用が必要な場合、個々の ASA ノードで以下を行う必要があります。

- 各リモート アクセス接続プロファイルに、各ロード バランシング仮想クラスタ アドレス（IPv4 および IPv6）のグループ URL を設定します。
- このノードの VPN ロード バランシング パブリック アドレスに対してグループ URL を設定します。

グループ URL は、[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [セキュアクライアント接続プロファイル（Connection Profiles）] > [接続プロファイル名（connection profile name）] > [追加または編集（Add or Edit）] > [詳細設定（Advanced）] > [グループエイリアス/グループ URL（Group Alias / Group URL）] ペインで設定します。

VPN ロードバランシングの機能履歴

機能名	リリース	機能情報
SAML を使用した VPN ロードバランシング	9.17(1)	ASA は、SAML 認証を使用した VPN ロ グをサポートするようになりました。
VPN ロードバランシング	7.2(1)	この機能が導入されました。



第 4 章

一般的な VPN 設定

システム オプション

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPSec] > [System Options] ペイン（または [Configuration] > [Site-to-Site VPN] > [Advanced] > [System Options] を使用して到達）を使用すると、ASA 上の IPsec セッションと VPN セッションに固有の機能を設定できます。

- [Limit maximum number of active IPsec VPN sessions]：アクティブな IPsec VPN セッションの最大数の制限をイネーブルまたはディセーブルにします。範囲は、ハードウェア プラットフォームとソフトウェア ライセンスによって異なります。
  - [Maximum IPsec Sessions]：アクティブな IPsec VPN セッションの最大許可数を指定します。このフィールドは、上記のチェックボックスをオンにして、アクティブな IPsec VPN セッションの最大数を制限した場合にだけアクティブになります。
- [L2TP Tunnel Keep-alive Timeout]：キープアライブ メッセージの頻度を秒単位で指定します。範囲は 10 ～ 300 秒です。デフォルトは 60 秒です。これは、Network（Client）Access 専用の高度なシステム オプションです。
- VPN トンネルの確立時に、既存のフローを再分類します。
- [Preserve stateful VPN flows when the tunnel drops]：ネットワーク拡張モード（NEM）での IPsec トンネル フローの保持をイネーブルまたはディセーブルにします。永続的な IPsec トンネル フロー機能をイネーブルにすると、[Timeout] ダイアログボックスでトンネルが再作成される限り、セキュリティ アプライアンスがステート情報にアクセスできるため、データは正常にフローを続行します。このオプションは、デフォルトで無効です。

（注） トンネル TCP フローはドロップされないため、クリーンアップは TCP タイムアウトに依存します。ただし、特定のトンネル フローのタイムアウトがディセーブルになってる場合、手動または他の方法（ピアからの TCP RST など）によってクリアされるまで、そのフローはシステム内で保持されます。

- [IPsec Security Association Lifetime]：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。または [unlimited] をオンにします。最小値は 100 KB、デフォルト値は 10000 KB、最大値は 2147483647 KB です。

- [Enable PMTU (Path Maximum Transmission Unit) Aging]：管理者が PMTU のエージングをイネーブルにすることができます。
  - [Interval to Reset PMTU of an SA (Security Association)]：PMTU 値が元の値にリセットされる秒数を入力します。

- [Enable inbound IPSec sessions to bypass interface access-lists]。[Group policy and per-user authorization ACLs still apply to the traffic]：ASA は、VPN トラフィックが ASA インターフェイスで終了することをデフォルトで許可するので、IKE または ESP（またはその他のタイプの VPN パケット）をアクセス ルールで許可する必要はありません。このオプションをオンにしている場合は、復号化された VPN パケットのローカル IP アドレスに対するアクセス ルールは不要です。VPN トンネルは VPN セキュリティ メカニズムを使用して正常に終端されたので、この機能によって、構成が簡略化され、セキュリティ リスクを負うことなく、デバイスのパフォーマンスが最大化されます。（グループ ポリシーおよびユーザー単位の許可 ACL は、引き続きトラフィックに適用されます）。

  このオプションをオフにすることにより、アクセス ルールをローカル IP アドレスに適用することを強制的に適用できます。アクセス ルールはローカル IP アドレスに適用され、VPN パケットが復号化される前に使用されていた元のクライアント IP アドレスには適用されません。

- [Permit communication between VPN peers connected to the same interface]：この機能をイネーブルまたはディセーブルにします。

  同じインターフェイスを介して着信クライアント VPN トラフィックを暗号化せずに、または暗号化してリダイレクトすることもできます。同じインターフェイスを介して VPN トラフィックを暗号化せずに送信する場合は、そのインターフェイスに対する NAT をイネーブルにし、プライベート IP アドレスをパブリックにルーティング可能なアドレスに変換する必要があります（ただし、ローカル IP アドレス プールですでにパブリック IP アドレスを使用している場合は除きます）。

- [Compression Settings]：圧縮をイネーブルにする機能（WebVPN および SSL VPN クライアント）を指定します。圧縮はデフォルトでイネーブルになっています。

最大 VPN セッション数の設定

VPN セッションまたは セキュアクライアント VPN セッションで許可される最大数を指定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Advanced]** > **[Maximum VPN Sessions]** を選択します。

ステップ 2 [最大セキュアクライアントセッション数（Maximum Sessions）] フィールドにセッションの最大許容数を入力します。

有効値は、1 からのライセンスで許容されるセッションの最大数までです。

ステップ 3 [Maximum Other VPN Sessions] フィールドで、許可する最大の VPN セッション数を入力します。これには、Cisco VPN クライアント（IPsec IKEv1）と LAN-to-LAN VPN セッションが含まれます。

有効値は、1 からのライセンスで許容されるセッションの最大数までです。

ステップ 4 [適用（Apply）] をクリックします。

DTLS の設定

Datagram Transport Layer Security（DTLS）を使用すると、SSL VPN 接続を確立しているセキュアクライアント で、2 つのトンネル（SSL トンネルと DTLS トンネル）を同時に使用できます。DTLS を使用すると、SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

始める前に

このヘッドエンドで DTLS を設定し、使用する DTLS のバージョンを確認するには、SSL 設定（257 ページ）を参照してください。

DTLS を TLS 接続にフォール バックさせるには、デッドピア検知（DPD）をイネーブルにする必要があります。DPD をイネーブルにしない場合、DTLS 接続で問題が発生すると、TLS にフォール バックする代わりに接続は終了します。DPD の詳細については、内部グループポリシー、セキュアクライアント、デッドピア検出 （103 ページ）を参照してください。

手順

ステップ 1 セキュアクライアント VPN 接続に対して DTLS オプションを指定します。

a) [設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [Secure Client AnyConnect接続プロファイル（Secure Client Connection Profiles）]**[アクセスインターフェイス（Access Interfaces）]** セクションに移動します。

b) [インターフェイス（Interface）] テーブルの セキュアクライアント 接続に設定するインターフェイスの行で、インターフェイスでイネーブルにするプロトコルをオンにします。

- [SSL Access / Allow Access] をオンにするかイネーブルにした場合、[Enable DTLS] はデフォルトでオンまたはイネーブルになります。
- DTLS を無効にするには、[Enable DTLS] をオフにします。SSL VPN 接続は SSL VPN トンネルのみに接続します。

c) [Port Settings] を選択し、**SSL ポート**を設定します。

- [HTTPS Port]：HTTPS（ブラウザベース）SSL 接続用にイネーブルにするポート。範囲は 1 ～ 65535 です。デフォルトはポート 443 です。
- [DTLS Port]：DTLS 接続用にイネーブルにする UDP ポート。範囲は 1 ～ 65535 です。デフォルトはポート 443 です。

ステップ 2 特定のグループ ポリシーに対して DTLS オプションを指定します。

a) [設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループポリシー（Group Policies）] > [追加/編集（ Add/Edit）] > [詳細設定（Advanced）] > [セキュアクライアント] に移動します。

b) [Datagram Transport Layer Security (DTLS)] の [Inherit]（デフォルト）、[Enable]、または [Disable] を選択します。

c) [DTLS Compression] の [Inherit]（デフォルト）、[Enable]、または [Disable] を選択し、DTLS の圧縮を設定します。

DNS サーバー グループの設定

[Configuration] > [Remote Access VPN] > [DNS] ダイアログボックスでは、サーバー グループ名、サーバー、タイムアウトの秒数、許容リトライ回数、およびドメイン名を含む、設定済みの DNS サーバーがテーブルに表示されます。このダイアログボックスで、DNS サーバー グループを追加、編集、または削除できます。

- [Add or Edit]：[Add or Edit DNS Server Group] ダイアログボックスが開きます。別の場所にあるヘルプ
- [Delete]：選択した行をテーブルから削除します。確認されず、やり直しもできません。
- [DNS Server Group]：この接続の DNS サーバー グループとして使用するサーバーを選択します。デフォルトは DefaultDNS です。
- [Manage]：[Configure DNS Server Group] ダイアログボックスが開きます。

暗号化コアのプールの設定

対称型マルチプロセッシング（SMP）プラットフォームでの暗号化コアの割り当てを変更して、セキュアクライアントTLS/DTLSトラフィックのスループットを向上させることができます。この変更によって、SSL VPNデータパスが高速化され、セキュアクライアント、スマートトンネル、およびポート転送において、ユーザーが認識できるパフォーマンス向上が実現します。次の手順では、シングル コンテキスト モードまたはマルチ コンテキスト モードで暗号化コアのプールを設定します。

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Advanced]** > **[Crypto Engine]** を選択します。

ステップ 2 [Accelerator Bias] ドロップダウン リストから、暗号アクセラレータ プロセッサの割り当て方法を選択します。

（注）
このフィールドは、機能がデバイスで使用可能な場合にだけ表示されます。

- [balanced]：暗号化ハードウェア リソースを均等に分散します（Admin/SSL および IPsec コア）。
- [ipsec]：IPsec を優先するように暗号化ハードウェア リソースを割り当てます（SRTP 暗号化音声トラフィックを含む）。
- [ssl]：Admin/SSL を優先するように暗号化ハードウェア リソースを割り当てます。SSL ベースの セキュアクライアント リモートアクセス VPN セッションをサポートする場合は、このバイアスを使用します。

ステップ 3 [適用（Apply）] をクリックします。

SSL VPN 接続用のクライアント アドレス指定

このダイアログボックスを使用して、グローバル クライアント アドレスの割り当てポリシーを指定し、インターフェイスに固有のアドレス プールを設定します。このダイアログボックスを使用して、インターフェイスに固有のアドレス プールを追加、編集、または削除することもできます。ダイアログボックス下部のテーブルには、設定されているインターフェイス固有のアドレス プールの一覧が表示されます。

- [Global Client Address Assignment Policy]：すべての IPsec 接続と SSL VPN Client 接続（セキュアクライアント接続を含む）に影響するポリシーを設定します。ASA は、アドレスを見つけるまで、選択されたソースを順番に使用します。
  - [Use authentication server]：クライアント アドレスのソースとして、ASA が認証サーバーの使用を試みるように指定します。
  - [Use DHCP]：クライアント アドレスのソースとして、ASA が DHCP の使用を試みるように指定します。
  - [Use address pool]：クライアント アドレスのソースとして、ASA がアドレス プールの使用を試みるように指定します。
- [Interface-Specific IPv4 Address Pools]：設定されているインターフェイス固有のアドレス プールの一覧を表示します。

- [Interface-Specific IPv6 Address Pools]：設定されているインターフェイス固有のアドレス プールの一覧を表示します。
- [Add]：[Assign Address Pools to Interface] ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスおよび割り当てるアドレス プールを選択できます。
- [Edit]：インターフェイスとアドレス プールのフィールドに値が取り込まれた状態で、[Assign Address Pools to Interface] ダイアログボックスが開きます。
- [Delete]：選択したインターフェイスに固有のアドレス プールを削除します。確認されず、やり直しもできません。

Assign Address Pools to Interface

このダイアログボックスを使用して、インターフェイスを選択し、そのインターフェイスにアドレス プールを 1 つ以上割り当てます。

- [Interface]：アドレス プールの割り当て先インターフェイスを選択します。デフォルトは DMZ です。
- [Address Pools]：指定したインターフェイスに割り当てるアドレス プールを指定します。
- [Select]：[Select Address Pools] ダイアログボックスが開きます。このダイアログボックスでは、このインターフェイスに割り当てるアドレス プールを 1 つ以上選択できます。選択内容は、[Assign Address Pools to Interface] ダイアログボックスの [Address Pools] フィールドに表示されます。

Select Address Pools

[Select Address Pools] ダイアログボックスには、クライアント アドレスの割り当てで選択可能なプール名、開始アドレスと終了アドレス、およびアドレス プールのサブネットマスクが表示され、リストのエントリを追加、編集、削除できます。

- [Add]：[Add IP Pool] ダイアログボックスが開きます。このダイアログボックスでは、新しい IP アドレス プールを設定できます。
- [Edit]：[Edit IP Pool] ダイアログボックスが開きます。このダイアログボックスでは、選択した IP アドレス プールを変更できます。
- [Delete]：選択したアドレス プールを削除します。確認されず、やり直しもできません。
- [Assign]：インターフェイスに割り当てられているアドレス プール名を表示します。インターフェイスに追加する個々の未割り当てプールをダブルクリックします。[Assign] フィールドのプール割り当て一覧が更新されます。

Add or Edit an IP Address Pool

IP アドレス プールを設定または変更します。

- [Name]：IP アドレス プールに割り当てられている名前を指定します。

- [Starting IP Address]：プールの最初の IP アドレスを指定します。
- [Ending IP Address]：プールの最後の IP アドレスを指定します。
- [Subnet Mask]：プール内のアドレスに適用するサブネット マスクを選択します。

グループ ポリシー

グループ ポリシーは、ASA の内部（ローカル）または外部の RADIUS または LDAP サーバーに格納されているユーザー指向の属性と値のペアのセットです。VPN接続を確立する際に、グループポリシーによってクライアントに属性が割り当てられます。デフォルトでは、VPNユーザーにはグループ ポリシーが関連付けられません。グループ ポリシー情報は、VPN 接続プロファイル（トンネル グループ）およびユーザー アカウントで使用されます。

ASA には、DfltGrpPolicy という名前のデフォルト グループ ポリシーがあります。デフォルト グループパラメータは、すべてのグループおよびユーザーに共通であると考えられるパラメータで、コンフィギュレーションタスクの効率化に役立ちます。新しいグループはこのデフォルト グループからパラメータを「継承」でき、ユーザーは自身のグループまたはデフォルト グループからパラメータを「継承」できます。これらのパラメータは、グループおよびユーザーを設定するときに上書きできます。

内部グループポリシーと外部グループポリシーを設定できます。内部グループポリシーはローカルに保存され、外部グループは RADIUS サーバーまたは LDAP サーバーに外部で保存されます。

[Group Policy] ダイアログボックスで、次の種類のパラメータを設定します。

- 一般属性：名前、バナー、アドレスプール、プロトコル、フィルタリング、および接続の設定。
- サーバー：DNS およびWINS サーバー、DHCP スコープ、およびデフォルトドメイン名。
- 詳細属性：スプリットトンネリング、IEブラウザプロキシ、セキュアクライアント、および IPsec クライアント。

これらのパラメータを設定する前に、次の項目を設定する必要があります。

- アクセス時間（[General] > [More Options] > [Access Hours]）。
- フィルタ（[General] > [More Options] > [Filters]）。
- IPsec セキュリティ アソシエーション（[Configuration] > [Policy Management] > [Traffic Management] > [Security Associations]）。
- フィルタリングおよびスプリット トンネリング用のネットワーク リスト（[Configuration] > [Policy Management] > [Traffic Management] > [Network Lists]）。
- ユーザー認証サーバーと内部認証サーバー（[Configuration] > [System] > [Servers] > [Authentication]）。

次のタイプのグループ ポリシーを設定できます。

- 外部グループ ポリシー （72 ページ）：外部グループ ポリシーは、RADIUS または LDAP サーバーを ASA に示し、内部グループ ポリシーに設定されているようなポリシー情報の大部分を取得できるようにします。外部グループポリシーは、ネットワーク（クライアント）アクセス VPN 接続、およびサイト間 VPN 接続に対して同じ方法で設定されます。
- 内部グループ ポリシー （74 ページ）：これらの接続は、エンドポイントにインストールされている VPN クライアントによって開始されます。Secure Clientおよび Cisco IPsec VPN クライアントは、VPN クライアントの使用例です。VPN クライアントが認証されると、オンサイトの場合、リモートユーザーは企業ネットワークまたはアプリケーションにアクセスできます。リモート ユーザーと企業ネットワーク間のデータ トラフィックは、暗号化によってインターネットを通過する際に保護されます。
- セキュアクライアント内部グループポリシー （81 ページ）
- サイト間内部グループ ポリシー （111 ページ）

[Group Policy] ペイン フィールド

ASDM の [Configuration] > [Remote Access VPN] > [Network （Client） Access] > [Group Policies] ペインには、設定済みのグループ ポリシーが一覧表示されます。VPN グループ ポリシーを管理するための [Add]、[Edit]、および [Delete] ボタンを以下に示します。

- [Add]：ドロップダウン リストが表示され、内部または外部のグループ ポリシーを追加するかどうかを選択できます。単に [Add] をクリックする場合は、デフォルトにより内部グループ ポリシーを作成することになります。[Add] をクリックすると、[Add Internal Group Policy] ダイアログボックスまたは [Add External Group Policy] ダイアログボックスが開きます。これらのダイアログボックスを使用して、新しいグループ ポリシーを一覧に追加できます。このダイアログボックスには、3 つのメニュー セクションがあります。それぞれのメニュー項目をクリックすると、その項目のパラメータが表示されます。項目間を移動するとき、ASDM は設定を保持します。すべてのメニュー セクションでパラメータの設定が終了したら、[Apply] または [Cancel] をクリックします。
- [Edit]：[Edit Group Policy] ダイアログボックスを表示します。このダイアログボックスを使用して、既存のグループ ポリシーを編集できます。
- [Delete]：AAA グループ ポリシーをリストから削除します。確認されず、やり直しもできません。
- [Assign]：1 つ以上の接続プロファイルにグループ ポリシーを割り当てることができます。
- [Name]：現在設定されているグループ ポリシーの名前を一覧表示します。
- [Type]：現在設定されている各グループ ポリシーのタイプを一覧表示します。
- [Tunneling Protocol]：現在設定されている各グループ ポリシーが使用するトンネリング プロトコルを一覧表示します。
- [Connection Profiles/Users Assigned to]：このグループ ポリシーに関連付けられた ASA に直接設定された接続プロファイルとユーザーを示します。

外部グループ ポリシー

外部グループ ポリシーは、外部サーバーから認可および認証の属性値を取得します。このグループ ポリシーによって、ASA が属性を照会できる RADIUS または LDAP サーバー グループを特定し、それらの属性を取得するときに使用するパスワードを指定します。

ASA での外部グループ名は、RADIUS サーバーのユーザー名を参照しています。つまり、ASA に外部グループ X を設定した場合、RADIUS サーバーはクエリーをユーザー X に対する認証要求と見なします。したがって、外部グループは、ASA にとって特別な意味を持つ RADIUS サーバー上のユーザーアカウントにすぎません。外部グループ属性が認証する予定のユーザーと同じ RADIUS サーバーに存在する場合、それらの間で名前を重複させることはできません。

外部サーバーを使用するように ASA を設定する前に、適切な ASA 認可属性を指定してサーバーを設定し、それらの属性のサブセットから個々のユーザーに対する特定の許可を割り当てる必要があります。外部サーバーを設定するには、「認可および認証用の外部サーバー」の説明に従ってください。

これらの RADIUS 構成には、ローカル認証の RADIUS、Active Directory Windows DC の RADIUS、NT/4.0 ドメインの RADIUS、LDAP の RADIUS が含まれます。

外部グループ ポリシーのフィールド

- [Name]：追加または変更するグループ ポリシーを特定します。[Edit External Group Policy] の場合、このフィールドは表示専用です。
- [Server Group]：このポリシーの適用先として利用できるサーバー グループを一覧表示します。
- [New]：新しい RADIUS サーバー グループまたは新しい LDAP サーバー グループを作成するかどうかを選択できるダイアログボックスを開きます。どちらの場合も [Add AAA Server Group] ダイアログボックスが開きます。
- [Password]：このサーバー グループ ポリシーのパスワードを指定します。

AAA サーバーの作成および設定については、『*Cisco ASA Series General Operations ASDM Configuration Guide*』の「*AAA Servers and Local Database*」の章を参照してください。

AAA サーバーによるパスワード管理

ASA は、RADIUS および LDAP プロトコルのパスワード管理をサポートしています。「password-expire-in-days」オプションは、LDAP に対してのみサポートされます。その他のパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバー、LDAP サーバーなどの AAA サーバーで有効です。RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

（注） 現在のところ MS-CHAP をサポートしていても、MS-CHAPv2 はサポートしていない RADIUS サーバーもあります。この機能には MS-CHAPv2 が必要なため、ベンダーに確認してください。

ASA では、通常、LDAP による認証時または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

- の AnyConnect VPN モジュール
- IPsec VPN クライアント
- IPsec IKEv2 クライアント

パスワード管理は、Active Directory（Windows パスワード）または NT 4.0 ドメインではサポートされません。一部の RADIUS サーバー（Cisco ACS など）は、認証要求を別の認証サーバーにプロキシする場合があります。ただし、ASA からは RADIUS サーバーとだけ通信しているように見えます。

（注） LDAP でパスワードを変更するには、市販の LDAP サーバーごとに独自の方法が使用されています。現在、ASA では Microsoft Active Directory および Sun LDAP サーバーに対してのみ、独自のパスワード管理ロジックを実装しています。

ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。

セキュアクライアントによるパスワードのサポート

ASA では、セキュアクライアント の次のパスワード管理機能をサポートします。

- ユーザーが接続しようとしたときのパスワード期限切れの通知。
- パスワードの期限が切れる前のパスワード期限切れのリマインダ。
- パスワード期限切れの無効化。ASA は AAA サーバーからのパスワード期限切れの通知を無視し、ユーザーの接続を許可します。

パスワード管理を設定すると、ASA は、リモート ユーザーがログインしようとしたときに、現在のパスワードの期限が切れていること、または期限切れが近づいていることを通知します。それから ASA は、ユーザーがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザーはその古いパスワードを使用してログインし続けて、後でパスワードを変更することができます。

セキュアクライアント はパスワードの変更を開始できず、AAA サーバーからの変更要求に ASA を介して応答することしかできません。AAA サーバーは、AD にプロキシする RADIUS サーバー、または LDAP サーバーにする必要があります。

ASA は、次の条件下ではパスワード管理をサポートしません。

- ローカル（内部）認証を使用する場合
- LDAP 認証を使用する場合
- RADIUS 認証のみを使用しており、ユーザーが RADIUS サーバー データベースに存在する場合

パスワード期限切れの無効化を設定すると、ASA は AAA サーバーからの account-disabled インジケータを無視するようになります。これは、セキュリティ上のリスクになる可能性があります。たとえば、管理者のパスワードを変更しないようにする場合があります。

パスワード管理をイネーブルにすると、ASA は AAA サーバーに MS-CHAPv2 認証要求を送信します。

内部グループ ポリシー

内部グループ ポリシー、一般属性

[Configuration] > [Remote Access VPN] > [Network （Client） Access] > [Group Policies] ペインで、[Add or Edit Group Policy] ダイアログボックスを使用すると、追加または変更するグループ ポリシーのトンネリングプロトコル、フィルタ、接続設定、およびサーバーを指定できます。このダイアログボックスの各フィールドで、[Inherit] チェックボックスを選択すると、対応する設定の値をデフォルト グループ ポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

ASDM で [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [General] を選択して、内部グループ ポリシーの一般属性を設定します。次の属性は、SSL VPN セッションと IPsec セッションに適用されます。そのため、いくつかの属性は、1 つのタイプのセッションに表示され、他のタイプには表示されません。

- [Name]：このグループ ポリシーの名前を最大 64 文字で指定します（スペースの使用可）。Edit 機能の場合、このフィールドは読み取り専用です。
- [Banner]：ログイン時にユーザーに対して表示するバナー テキストを指定します。長さは最大 4000 文字です。デフォルト値はありません。

  IPsec VPN クライアントは、バナー用の完全な HTML をサポートしています。ただし、クライアントレスポータルおよび セキュアクライアント は部分的な HTML をサポートしています。バナーがリモート ユーザーに適切に表示されるようにするには、次のガイドラインに従います。

  - IPsec クライアント ユーザーの場合は、/n タグを使用します。
  - セキュアクライアント 用 ユーザーは
タグを使用してください。

- [SCEP forwarding URL]：CA のアドレス。クライアント プロファイルで SCEP プロキシを設定する場合に必要です。
- [Address Pools]：このグループ ポリシーで使用する 1 つ以上の IPv4 アドレス プールの名前を指定します。[Inherit] チェックボックスがオンの場合、グループ ポリシーはデフォルト グループ ポリシーで指定されている IPv4 アドレス プールを使用します。IPv4 アドレス プールを追加または編集する方法の詳細については、を参照してください。

（注） 内部グループ ポリシーで IPv4 と IPv6 両方のアドレス プールを指定できます。

[Select] —このボタンをアクティブにするには、[Inherit] チェックボックスをオフにします。[Select] をクリックして、[Address Pools] 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には、クライアント アドレス割り当てで選択可能なアドレス プールのプール名、開始アドレスと終了アドレス、およびサブネットマスクが表示され、そのリストからエントリを選択、追加、編集、削除、および割り当てできます。

- [IPv6 Address Pools]：このグループ ポリシーで使用する 1 つ以上の IPv6 アドレス プールの名前を指定します。

  [Select] —このボタンをアクティブにするには、[Inherit] チェックボックスをオフにします。[Select] をクリックすると、前述のような [Select Address Pools] ダイアログボックスが開きます。IPv6 アドレス プールを追加または編集する方法の詳細については、を参照してください。

- [More Options]：フィールドの右側にある下矢印をクリックすると、このグループ ポリシーのその他の設定可能なオプションが表示されます。
- [Tunneling Protocols]：このグループが使用できるトンネリング プロトコルを指定します。ユーザーは、選択されているプロトコルだけを使用できます。次の選択肢があります。
  - [Clientless SSL VPN]：SSL/TLS による VPN の使用を指定します。この VPN では、ソフトウェアやハードウェアのクライアントは必要なく、Web ブラウザを使用して ASA へのセキュアなリモートアクセス トンネルが確立されます。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
  - [SSL VPNクライアント（SSL VPN Client）]：Cisco Secure Client またはレガシー SSL VPN クライアントの AnyConnect VPN モジュールの使用を指定します。セキュアクライアントを使用している場合は、このプロトコルを選択して Mobile User Security（MUS）がサポートされるようにする必要があります。
  - [IPsec IKEv1]：IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピ

アツーピア）接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。

- [IPsec IKEv2]：Secure Clientによってサポートされています。IKEv2 を使用した IPsec を使用するセキュアクライアント接続では、ソフトウェアアップデート、クライアントプロファイル、GUI のローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
- [L2TP over IPsec]：一部の一般的 PC やモバイル PC のオペレーティング システムで提供される VPN クライアントを使用しているリモート ユーザーは、L2TP over IPSec によって、パブリック IP ネットワーク経由でセキュリティ アプライアンスやプライベート企業ネットワークへのセキュアな接続を確立できます。L2TP は、データのトンネリングに PPP over UDP（ポート 1701）を使用します。セキュリティ アプライアンスは、IPsec 転送モード用に設定する必要があります。

- [Filter]：IPv4 または IPv6 接続で使用するアクセス コントロール リストを指定するか、グループ ポリシーから値を継承するかどうかを指定します。フィルタは複数のルールから構成されています。これらのルールは、ASA を介して着信したトンネリング データ パケットを許可するか拒否するかを、送信元アドレス、宛先アドレス、プロトコルなどに基づいて決定します。VPN フィルタは初期接続にのみ適用されます。アプリケーション インスペクションのアクションによって開かれた SIP メディア接続などのセカンダリ接続には適用されません。フィルタおよびルールを設定するには、[Manage] をクリックします。
- [NAC Policy]：このグループ ポリシーに適用するネットワーク アドミッション コントロール ポリシーの名前を選択します。オプションの NAC ポリシーを各グループ ポリシーに割り当てることができます。デフォルト値は --None-- です。
- [Manage]：[Configure NAC Policy] ダイアログボックスが開きます。1 つ以上の NAC ポリシーを設定すると、[NAC Policy] 属性の横のドロップダウン リストに、設定した NAC ポリシー名がオプションとして表示されます。
- [Access Hours]：このユーザーに適用される既存のアクセス時間ポリシーがある場合はその名前を選択するか、または新しいアクセス時間ポリシーを作成します。デフォルトは [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルトは [--Unrestricted--] です。[Manage] をクリックして、[Browse Time Range] 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、時間範囲を追加、編集、または削除できます。
- [Simultaneous Logins]：このユーザーに許可する同時ログインの最大数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザー アクセスを禁止します。

（注） 最大数の制限はありませんが、複数の同時接続の許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼすおそれがあります。

- [Restrict Access to VLAN]：（オプション）「VLAN マッピング」とも呼ばれます。このパラメータにより、このグループ ポリシーが適用されるセッションの出力 VLAN インターフェイスを指定します。ASA は、このグループからのすべてのトラフィックを指定された VLAN に転送します。この属性を使用して VLAN をグループ ポリシーに割り当て、アクセス コントロールを簡素化します。この属性に値を割り当てる方法は、ACL を使用してセッションのトラフィックをフィルタリングする方法の代替方法です。ドロップダウン リストには、デフォルト値（[無制限（Unrestricted）]）の他に、この ASA で設定されている VLAN だけが表示されます。

（注） この機能は、HTTP 接続の場合には有効ですが、FTP および CIFS 接続では使用できません。

- [Connection Profile (Tunnel Group) Lock]：このパラメータを使用すると、選択された接続プロファイル（トンネル グループ）を使用する VPN アクセスのみを許可し、別の接続ファイルを使用するアクセスを回避できます。デフォルトの継承値は [None] です。
- Maximum Connect Time：[Inherit] チェックボックスがオフになっている場合、このパラメータで最大ユーザー接続時間を分単位で設定します。

  ここで指定した時間が経過すると、システムは接続を終了します。最小値は 1 分、最大値は 35791394 分です。制限なしの接続時間を許可するには、[Unlimited] をオンにします（デフォルト）。
- Idle Timeout：[Inherit] チェックボックスをオフにした場合、このパラメータでアイドル時間を分単位で設定します。

  この期間に接続で通信アクティビティがない場合、接続は終了します。最小時間は 1 分、最大時間は 10080 分であり、デフォルトは 30 分です。接続時間を無制限にするには、[Unlimited] をオンにします。
- [Security Group Tag (SGT)]：このグループ ポリシーで接続する VPN ユーザーに割り当てられる SGT タグの数値を入力します。
- [On smart card removal]：デフォルトのオプション [Disconnect] を選択した場合は、認証に使用されるスマート カードが取り外されると、クライアントは接続を切断します。接続の間、スマート カードをコンピュータに保持することをユーザーに要求しない場合は、[Keep the connection] をクリックします。

  スマート カードの取り外しに関する設定は、RSA スマート カードを使用する Microsoft Windows でのみ機能します。
- [同時セッションプリエンプションで遅延のないトンネル削除を無効にする（Disable Delete tunnel with no delay in Simultaneous Session preemt）]：特定のユーザーが許可された [同時ログイン（Simultaneous Logins）] の制限に達すると、ユーザーの次のログイン試行では、最も古いセッションを最初に削除する必要があります。この削除には数秒かかることがあり、ユーザーが新しいセッションをすぐに確立できない場合があります。最も古いセッ

ションの削除完了を待たずに新しいセッションを確立するようにシステムに指示するには、このオプションを選択します。

- Maximum Connection Time Alert Interval：ユーザーにメッセージを表示する、最大接続時間に達するまでの時間間隔。

  [Inherit] チェックボックスをオフにした場合、[Default] チェックボックスは自動的にオンになります。これにより、セッション アラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] をオフにし、1 ～ 30 分のセッション アラート間隔を指定します。

- Periodic Certificate Authentication Interval：証明書認証が定期的に再実行されるまでの時間間隔（時間単位）。

  [Inherit] チェックボックスがオフになっている場合、定期的な証明書検証の実行間隔を設定できます。範囲は 1 ～ 168 時間で、デフォルトは無効になっています。無制限の検証を許可するには、[Unlimited] をオンにします。

内部グループ ポリシーの設定、サーバー属性

[Group Policy] > [Servers] ウィンドウで、DNS サーバー、WINS サーバーおよび DNS スコープを設定します。DNS および WINS サーバーはフルトンネルクライアント（IPsec、セキュアクライアント、SVC、L2TP/IPsec）のみに適用され、名前解決に使用されます。DHCP スコープは、DHCP アドレス割り当てが設定されている場合に使用されます。

手順

ステップ 1 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [Servers]** を選択します。

ステップ 2 DefaultGroupPolicy を編集する場合を除き、[DNSサーバーの継承（DNS Servers Inherit）] チェックボックスをオフにして、このグループで使用する DNS サーバーの IPv4 または IPv6 アドレスを追加します。2 つの IPv4 アドレスと 2 つの IPv6 アドレスを指定できます。

複数の DNS サーバーを指定する場合、リモート アクセス クライアントは、このフィールドで指定された順序で DNS サーバーを使用しようとします。

ここで行った変更は、ASDM のこのグループ ポリシーを使用しているクライアントの [Configuration] > [Remote Access VPN] > [DNS] ウィンドウで設定された DNS 設定より優先されます。

ステップ 3 [WINSサーバーの継承（WINS Servers Inherit）] チェックボックスをオフにして、プライマリおよびセカンダリ WINS サーバの IP アドレスを入力します。最初に指定する IP アドレスがプライマリ WINS サーバーの IP アドレスです。2 番目（任意）の IP アドレスはセカンダリ WINS サーバーの IP アドレスです。。

ステップ 4 [More Options] バーの二重矢印をクリックして、[More Options] エリアを展開します。

ステップ 5 [DHCPスコープの継承（DHCP Scope Inherit）] をオフにして、DHCP スコープを定義します。

接続プロファイルのアドレスプールにDHCPサーバーを設定した場合、DHCPスコープはこのグループのプールに使用するサブネットを識別します。DHCPサーバーには、そのスコープによって識別される同じサブネット内のアドレスも設定されている必要があります。スコープを使用すると、この特定のグループに使用するDHCPサーバーで定義されているアドレスプールのサブセットを選択できます。

ネットワーク スコープを定義しない場合、DHCP サーバはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

スコープを指定するには、目的のプールと同じサブネット上にあり、そのプール内にはないルーティング可能なアドレスを入力します。DHCP サーバは、この IP アドレスが属するサブネットを判別し、そのプールからの IP アドレスを割り当てます。

ルーティングの目的で可能な場合は常に、インターフェイスの IP アドレスを使用することを推奨します。たとえば、プールが 10.100.10.2 ～ 10.100.10.254 で、インターフェイスアドレスが 10.100.10.1/24 の場合、DHCP スコープとして 10.100.10.1 を使用します。ネットワーク番号は使用しないでください。DHCP は IPv4 アドレス指定にのみ使用することができます。選択したアドレスがインターフェイスアドレスではない場合、スコープアドレスのスタティックルートを作成する必要があります。

ステップ 6 デフォルトドメインが **[設定（Configuration）]** > **[リモートアクセスVPN（Remote Access VPN）]**>**[DNS]** ウィンドウで指定されていない場合は、[デフォルトドメイン（Default Domain）] フィールドでデフォルトドメインを指定する必要があります。たとえば、example.com というドメイン名とトップ レベル ドメインを使用します。

ステップ 7 [OK] をクリックします。

ステップ 8 [適用（Apply）] をクリックします。

内部グループ ポリシー、ブラウザ プロキシ

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [Advanced] > [Browser Proxy]

このダイアログボックスでは、Microsoft Internet Explorer の設定を再構成するためにクライアントにプッシュダウンされる属性を設定します。

- [Proxy Server Policy]：クライアント PC の Microsoft Internet Explorer ブラウザのプロキシ アクション（「メソッド」）を設定します。
  - [Do not modify client proxy settings]：このクライアント PC の Internet Explorer の HTTP ブラウザ プロキシ サーバー設定を変更しません。
  - [Do not use proxy]：クライアント PC の Internet Explorer の HTTP プロキシ設定をディセーブルにします。
  - [Select proxy server settings from the following]：選択内容に応じて、[Auto detect proxy]、[Use proxy server settings given below]、および [Use proxy auto configuration (PAC) given below] のチェックボックスをオンにします。

- [Auto-detect proxy]：クライアント PC で、Internet Explorer の自動プロキシ サーバー検出の使用をイネーブルにします。
- [Use proxy server settings specified below]：[Proxy Server Name or IP Address] フィールドで設定された値を使用するように、Internet Explorer の HTTP プロキシ サーバー設定値を設定します。
- [Use proxy auto configuration (PAC) given below]：[Proxy Auto Configuration (PAC)] フィールドで指定したファイルを、自動コンフィギュレーション属性のソースとして使用するように指定します。

- [Proxy Server Settings]：Microsoft Internet Explorer を使用して、Microsoft クライアントのプロキシ サーバー パラメータを設定します。
  - [Server Address and Port]：このクライアント PC で適用される、Microsoft Internet Explorer サーバーの IP アドレスまたは名前、およびポートを指定します。
  - [Bypass Proxy Server for Local Addresses]：クライアント PC での Microsoft Internet Explorer ブラウザ プロキシ ローカル バイパス設定値を設定します。[Yes] を選択するとローカル バイパスがイネーブルになり、[No] を選択するとローカル バイパスがディセーブルになります。
  - [Exception List]：プロキシ サーバー アクセスから除外するサーバーの名前と IP アドレスを一覧表示します。プロキシサーバー経由のアクセスを行わないアドレスのリストを入力します。このリストは、[Internet Explorer の Proxy Settings] ダイアログボックスにある [Exceptions] リストに相当します。

- [Proxy Auto Configuration Settings]：PAC URL は自動設定ファイルの URL を指定します。このファイルには、ブラウザがプロキシ情報を探せる場所が記述されています。プロキシ自動コンフィギュレーション（PAC）機能を使用する場合、リモートユーザーは、Cisco Secure クライアントの AnyConnect VPN モジュール を使用する必要があります。

  多くのネットワーク環境が、Web ブラウザを特定のネットワーク リソースに接続する HTTP プロキシを定義しています。HTTP トラフィックがネットワーク リソースに到達できるのは、プロキシがブラウザに指定され、クライアントが HTTP トラフィックをプロキシにルーティングする場合だけです。SSLVPN トンネルにより、HTTP プロキシの定義が複雑になります。企業ネットワークにトンネリングするときに必要なプロキシが、ブロードバンド接続経由でインターネットに接続されるときや、サード パーティ ネットワーク上にあるときに必要なものとは異なることがあるためです。

  また、大規模ネットワークを構築している企業では、複数のプロキシサーバを設定し、一時的な状態に基づいてユーザがその中からプロキシサーバを選択できるようにすることが必要になる場合があります。.pac ファイルを使用すると、管理者は数多くのプロキシからどのプロキシを社内のすべてのクライアント コンピュータに使用するかを決定する単一のスクリプト ファイルを作成できます。

  次に、PAC ファイルを使用する例をいくつか示します。

  - ロード バランシングのためリストからプロキシをランダムに選択します。

- サーバのメンテナンス スケジュールに対応するために、時刻または曜日別にプロキシを交代で使用します。
- プライマリ プロキシで障害が発生した場合に備えて、使用するバックアップ プロキシ サーバを指定します。
- ローカルサブネットを元に、ローミングユーザ用に最も近いプロキシを指定します。

テキスト エディタを使用して、自分のブラウザにプロキシ自動コンフィギュレーション（.pac）ファイルを作成できます。.pac ファイルとは、URL のコンテンツに応じて、使用する 1 つ以上のプロキシ サーバを指定するロジックを含む JavaScript ファイルです。[PAC URL] フィールドを使用して、.pac ファイルの取得元 URL を指定します。ブラウザは、.pac ファイルを使用してプロキシ設定を判断します。

- Proxy Lockdown
  - [クライアントシステムのプロキシロックダウンを許可（Allow Proxy Lockdown for Client System）]：この機能をイネーブルにすると、セキュアクライアント VPN セッションの間、Microsoft Internet Explorer の [接続（Connections）] タブが非表示になります。また、Windows 10 バージョン 1703（以降）では、この機能を有効にすると、セキュアクライアント VPN セッションの間、設定アプリのシステムプロキシタブも非表示になります。この機能を無効にしても、Microsoft Internet Explorer の [Connections] タブと設定アプリのプロキシタブの表示は変わりません。これらのタブのデフォルト設定は、ユーザーのレジストリ設定に応じて表示または非表示になります。

（注） AnyConnect VPN セッションの間、設定アプリのシステムプロキシタブを非表示にするには、セキュアクライアント バージョン 4.7.03052 以降が必要です。

セキュアクライアント内部グループポリシー

内部グループポリシー、詳細、セキュアクライアント

- [Keep Installer on Client System]：リモート コンピュータ上で永続的なクライアントのインストールを可能にします。これをイネーブルにすることにより、クライアントの自動的なアンインストール機能がディセーブルになります。クライアントは、後続の接続のためにリモート コンピュータにインストールされたままなので、リモート ユーザーの接続時間が短縮されます。
- [Compression]：圧縮を行うと、転送されるパケットのサイズが減少するため、セキュリティ アプライアンスとクライアント間の通信パフォーマンスが向上します。

- [Datagram TLS]：Datagram Transport Layer Security により、一部の SSL 接続に関連する遅延と帯域幅の問題を回避し、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスを改善します。
- [Ignore Don't Defrag (DF) Bit]：この機能では、DF ビットが設定されているパケットを強制的にフラグメンテーションして、トンネルを通過させることができます。使用例として、TCP MSS ネゴシエーションに適切に応答しないネットワークのサーバーに対する使用などがあります。
- [クライアントバイパスプロトコル（Client Bypass Protocol）]：クライアント プロトコル バイパス機能を使用すると、ASA が IPv6 トラフィックだけを予期しているときの セキュアクライアント クライアントによる IPv4 トラフィックの管理方法や、IPv4 トラフィックだけを予期しているときの IPv6 トラフィックの管理方法を設定することができます。

  セキュアクライアント が ASA に VPN 接続するときに、ASA は IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ASA が セキュアクライアント 接続に IPv4 アドレスまたは IPv6 アドレスだけを割り当てた場合に、ASA が IP アドレスを割り当てなかったネットワークトラフィックについて、クライアント プロトコル バイパスによってそのトラフィックをドロップさせるか、または ASA をバイパスしてクライアントからの暗号化なし、つまり「クリアテキスト」としての送信を許可するかを設定できるようになりました。

  たとえば、ASA が セキュアクライアント 接続に IPv4 アドレスのみを割り当て、エンドポイントがデュアルスタックされているとします。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアントバイパスプロトコル機能がディセーブルの場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルがイネーブルの場合は、IPv6 トラフィックはクライアントからクリアテキストとして送信されます。

  SSL 接続ではなく IPsec トンネルを確立している場合は、クライアントで IPv6 が有効になっているかどうかが ASA に通知されないため、ASA は常にクライアント バイパス プロトコル設定をプッシュダウンします。

- [FQDN of This Device]：この情報は、VPN セッションの再確立で使用される ASA IP アドレスを解決するために、ネットワーク ローミングの後でクライアントに使用されます。この設定は、さまざまな IP プロトコルのネットワーク間のローミングをサポートするうえで重要です（IPv4 から IPv6 など）。

（注） セキュアクライアント プロファイルにある ASA FQDN を使用してローミング後に ASA IP アドレスを取得することはできません。アドレスがロード バランシング シナリオの正しいデバイス（トンネルが確立されているデバイス）と一致しない場合があります。

デバイスの FQDN がクライアントに配信されない場合、クライアントは、以前にトンネルが確立されている IP アドレスへの再接続を試みます。異なる IP プロトコル（IPv4 から IPv6）のネットワーク間のローミングをサポートするには、セキュアクライアントは、ト

ンネルの再確立に使用する ASA アドレスを決定できるように、ローミング後にデバイス FQDN の名前解決を行う必要があります。クライアントは、初期接続中にプロファイルに存在する ASA FQDN を使用します。以後のセッション再接続では、使用可能な場合は常に、ASA によってプッシュされた（また、グループ ポリシーで管理者が設定した）デバイス FQDN を使用します。FQDN が設定されていない場合、ASA は、[Device Setup] > [Device Name/Password and Domain Name] の設定内容からデバイス FQDN を取得（およびクライアントに送信）します。

デバイス FQDN が ASA によってプッシュされていない場合、クライアントは、異なる IP プロトコルのネットワーク間のローミング後に VPN セッションを再確立できません。

- [MTU]：SSL 接続の MTU サイズを調整します。256 ～ 1410 バイトの範囲で値を入力します。デフォルトでは、IP/UDP/DTLS のオーバーヘッド分を差し引き、接続で使用するインターフェイスの MTU に基づいて、自動的に MTU サイズが調整されます。

- [Keepalive Messages]：[Interval] フィールドに 15 秒から 600 秒までの数を入力することにより、接続がアイドルの時間がデバイスによって制限されている場合でも、キープアライブ メッセージの間隔をイネーブルおよび調整して、プロキシ、ファイアウォール、または NAT デバイスを通した接続を確実に開いたままにすることができます。また、間隔を調整することにより、リモート ユーザーが、Microsoft Outlook や Microsoft Internet Explorer などのソケットベースのアプリケーションを実際に実行していないときでも、クライアントが切断と再接続を行わないことが保証されます。

- **[ダウンロードするオプションのクライアントモジュール（Optional Client Modules to Download）]**：ダウンロード時間を短縮するために、セキュアクライアントは、サポートしている各機能に必要なモジュールだけを（ASA から）ダウンロードするように要求します。次のような他の機能をイネーブルにするモジュールの名前を指定する必要があります。セキュアクライアントには、次のモジュールが含まれています（一部の旧バージョンではモジュールの数が少なくなります）。

  - [セキュアクライアント DART]：Diagnostic セキュアクライアント Reporting Tool（DART）は、トラブルシューティング情報を簡単に Cisco TAC に送信できるように、システムログのスナップショットおよびその他の診断情報をキャプチャし、.zip ファイルをデスクトップに作成します。

  - セキュアクライアント ネットワーク アクセス マネージャ：以前は Cisco Secure Services Client と呼ばれていました。このモジュールは、有線とワイヤレスの両方のネットワークにアクセスするための 802.1X（レイヤ 2）とデバイス認証を備えています。

  - セキュアクライアント SBL：Start Before Logon（SBL）は、Windows のログインダイアログボックスが表示される前にセキュアクライアントを開始することにより、ユーザを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。

  - Secure Firewall ポスチャモジュール：以前は Cisco Secure Desktop HostScan 機能と呼ばれていました。このポスチャモジュールは セキュアクライアント に統合され、これにより セキュアクライアント は、ASA へのリモートアクセス接続を確立する前にポスチャアセスメントのクレデンシャルを収集できるようになります。

- ISE ポスチャ：OPSWAT v3 ライブラリを使用してポスチャ チェックを実行し、エンドポイントの適合性を評価します。その後、エンドポイントが適合するまでネットワーク アクセスを制限したり、ローカル ユーザーの権限を強化したりできます。
- AMP イネーブラ：エンドポイント向けの高度なマルウェア防御（AMP）を導入する手段として使用されます。社内でローカルにホストされているサーバーからエンドポイントのサブセットに AMP for Endpoints ソフトウェアをプッシュし、既存のユーザーベースに AMP サービスをインストールします。
- ネットワーク可視性モジュール：キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。NVM（ネットワーク可視性モジュール）は、エンドポイントのテレメトリを収集して、フローデータとファイル レピュテーションを syslog に記録し、さらに、ファイルの分析と UI インターフェイスの提供を行うコレクタ（サードパーティ ベンダー）にもフロー レコードをエクスポートします。
- Umbrella Roaming Security モジュール：アクティブな VPN がないときに DNS レイヤ セキュリティを提供します。Cisco Umbrella Roaming と OpenDNS Umbrella サービスのいずれかに対するサブスクリプションを提供し、Intelligent Proxy および IP レイヤ適用機能を追加します。Umbrella Security Roaming プロファイルは、対応するサービスと各展開を関連付けて、対応する保護レベルを自動的に有効にします（コンテンツ フィルタリング、複数のポリシー、強力なレポート、Active Directory 統合、または基本的な DNS レイヤ セキュリティ）。

- Always-On VPN：セキュアクライアント サービスプロファイルの常時接続 VPN フラグ設定をディセーブルにするか、または セキュアクライアント サービスプロファイル設定を使用する必要があるかを決定します。常時接続 VPN 機能により、ユーザーがコンピュータにログオンすると、AnyConnect は VPN セッションを自動的に確立します。VPN セッションは、ユーザーがコンピュータからログオフするまで維持されます。物理的な接続が失われてもセッションは維持され、セキュアクライアントは、適応型セキュリティアプライアンスとの物理的な接続の再確立を絶えず試行し、VPN セッションを再開します。

  常時接続 VPN によって、企業ポリシーを適用して、セキュリティ脅威からデバイスを保護できます。常時接続 VPN を使用して、エンドポイントが信頼ネットワーク内ではない場合にいつでも セキュアクライアント が VPN セッションを確立したことを確認できます。イネーブルにすると、接続が存在しない場合のネットワーク接続の管理方法を決定するポリシーが設定されます。

（注） また、常時接続 VPN にはセキュリティクライアント機能をサポートする セキュアクライアント リリースが必要です。

- [ダウンロードするクライアントプロファイル（Client Profiles to Download）]：プロファイルはコンフィギュレーション パラメータのグループであり、セキュアクライアントで VPN、ネットワーク アクセス マネージャ、Web セキュリティ、ISE ポスチャ、AMP イネーブラ、ネットワーク可視性モジュール、および Umbrella Roaming Security モジュール

の設定に使用されます。[追加（Add）]をクリックして[セキュアクライアントプロファイルの選択（Select AnyConnect Client Profiles）] ウィンドウを起動すると、以前グループポリシー用に作成されたプロファイルを指定できます。

セキュアクライアントトラフィックに対するスプリットトンネリングの設定

スプリットトンネリングは、一部の セキュアクライアント ネットワークトラフィックを VPN トンネルに誘導して通過させ（暗号化）、他のネットワークトラフィックを VPN トンネルの外に誘導します（非暗号化、つまり「クリアテキストの状態」）。

スプリット トンネリングを設定するには、スプリット トンネリング ポリシーを作成し、そのポリシーにアクセス コントロール リストを設定し、グループ ポリシーにスプリット トンネル ポリシーを追加します。グループ ポリシーをクライアントに送信する際に、クライアントはスプリット トンネリング ポリシーの ACL を使用してどこにネットワーク トラフィックを送信するかを決定します。

（注） スプリットトンネリングはセキュリティ機能ではなく、トラフィック管理機能です。最大限のセキュリティを確保するには、スプリットトンネリングをイネーブルにしないことを推奨します。

Windows クライアントでは、最初に ASA からのファイアウォール ルールが評価され、次にクライアントのファイアウォール ルールが評価されます。Mac OS X では、クライアントのファイアウォール ルールおよびフィルタ ルールは使用されません。Linux システムの AnyConnect バージョン 3.1.05149 以降では、circumvent-host-filtering という名前のカスタム属性をグループ プロファイルに追加して true に設定することで、クライアントのファイアウォールルールおよびフィルタルールを評価するように セキュアクライアント を設定できます。

アクセス リストを作成する場合：

- アクセス コントロール リストには IPv4 および IPv6 両方のアドレスを指定できます。
- 標準 ACL を使用すると、1 つのアドレスまたはネットワークのみが使用されます。
- 拡張 ACL を使用すると、ソース ネットワークがスプリット トンネリング ネットワークになります。この場合、宛先ネットワークは無視されます。
- any が設定されたアクセス リストや、split include または split exclude が 0.0.0.0/0.0.0.0 または ::/0 に設定されたアクセス リストは、クライアントに送信されません。すべてのトラフィックをトンネル経由で送信するには、スプリット トンネルの **Policy** に対して **Tunnel All Networks** を選択します。
- アドレス 0.0.0.0/255.255.255.255 または ::/128 は、スプリット トンネル ポリシーが **Exclude Network List Below** の場合にのみクライアントに送信されます。この設定は、トンネル トラフィックがローカル サブネット宛でないことをクライアントに通知します。
- セキュアクライアント では、スプリット トンネリング ポリシーで指定されたすべてのサイト、および ASA によって割り当てられた IP アドレスと同じサブネット内にあるすべて

のサイトにトラフィックが渡されます。たとえば、ASA によって割り当てられた IP アドレスが 10.1.1.1、マスクが 255.0.0.0 の場合、エンドポイント デバイスは、スプリット トンネリング ポリシーに関係なく、10.0.0.0/8 を宛先とするすべてのトラフィックを渡します。そのため、割り当てられた IP アドレスが、期待されるローカル サブネットを適切に参照するように、ネットマスクを使用します。

始める前に

- 適切な ACE でアクセス リストを作成する必要があります。
- スプリット トンネル ポリシーを IPv4 ネットワーク用と IPv6 ネットワーク用に作成した場合は、指定したネットワーク リストが両方のプロトコルで使用されます。このため、ネットワーク リストには、IPv4 および IPv6 の両方のトラフィックのアクセス コントロール エントリ（ACE）が含まれている必要があります。これらの ACL を作成していない場合は、一般的操作用コンフィギュレーション ガイドを参照してください。

次の手順では、フィールドの隣に [Inherit] チェックボックスがあるすべてのケースで、[Inherit] チェックボックスがオンのままの場合、設定しているグループ ポリシーは、そのフィールドについて、デフォルト グループ ポリシーと同じ値を使用することを意味します。[Inherit] チェックボックスをオフにすると、グループ ポリシーに固有の新しい値を指定できます。

手順

ステップ 1 ASDM を使用して ASA に接続し、**[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[Group Policies]** に移動します。

ステップ 2 [Add] をクリックして新しいグループ ポリシーを追加するか、既存のグループ ポリシーを選択して [Edit] をクリックします。

ステップ 3 **[Advanced]** > **[Split Tunneling]** を選択します。

ステップ 4 [DNS名（DNS Names）] フィールドに、トンネルを介して セキュアクライアント で解決するドメイン名を入力します。これらの名前は、プライベート ネットワーク上のホストに対応します。split-include トンネリングが設定されている場合は、指定された DNS サーバーがネットワーク リストに含まれている必要があります。フィールドには、完全修飾ドメイン名、IPv4 アドレス、または IPv6 アドレスを入力できます。

ダイナミック スプリット トンネリング ドメイン名には、トップレベルドメインの他に少なくとも 1 つのドメイン名ラベルが必要です。ダイナミック スプリット トンネリングは、特定のドメイン名に一致するフローをターゲットとするようになっているため、トップレベルドメイン（*org* など）だけを指定することはできないのです。トップレベルドメインと少なくとも 1 つのドメイン名ラベル（*domain.org* など）を入力する必要があります。

ステップ 5 スプリット トンネリングをディセーブルにするには、[Yes] をクリックして [Send All DNS Lookups Through Tunnel] をイネーブルにします。このオプションを設定すると、DNS トラフィックが物理アダプタに漏れず、クリアテキストで送信されるトラフィックが拒否されます。DNS 解決に失敗すると、アドレスは未解決のまま残ります。セキュアクライアントは、VPN外のアドレスを解決しようとはしません。

スプリット トンネリングをイネーブルにするには、[No] を選択します（デフォルト）。この設定では、クライアントはスプリット トンネル ポリシーに従ってトンネルを介して DNS クエリを送信します

ステップ 6 スプリット トンネリングを設定するには、[Inherit] チェックボックスをオフにして、スプリット トンネリング ポリシーを選択します。[Inherit] チェックボックスをオフにしない場合、グループ ポリシーでは、デフォルトのグループ ポリシー **DfltGrpPolicy** で定義されたスプリット トンネリング設定が使用されます。デフォルト グループ ポリシーのスプリット トンネリング ポリシーのデフォルト設定は [Tunnel All Networks] です。

スプリット トンネリング ポリシーを定義するには、ドロップダウン [Policy] および [IPv6 Policy] から選択します。[Policy] フィールドでは、IPv4 ネットワーク トラフィックのスプリット トンネリング ポリシーを定義します。[IPv6 Policy] フィールドでは、IPv6 ネットワーク トラフィックのスプリット トンネリング ポリシーを選択します。そうした違い以外は、これらのフィールドの目的は同じです。

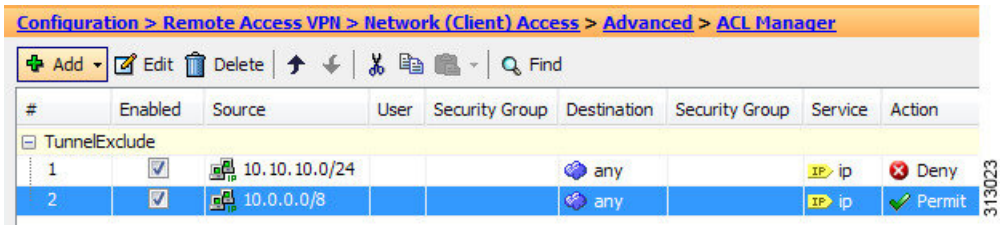
[Inherit] チェックボックスをオフにした場合は、次のいずれかのポリシー オプションを選択できます。

- [Exclude Network List Below]：クリア テキストで送信されるトラフィックの宛先ネットワークのリストを定義します。この機能は、社内ネットワークにトンネルを介して接続しながら、ローカル ネットワーク上のデバイス（プリンタなど）にアクセスするリモート ユーザーにとって役立ちます。

- [Tunnel Network List Below]：[Network List] で指定されたネットワーク間のすべてのトラフィックがトンネリングされます。インクルード ネットワーク リスト内のアドレスへのトラフィックがトンネリングされます。その他すべてのアドレスに対するデータは、クリア テキストで送信され、リモート ユーザーのインターネット サービス プロバイダーによってルーティングされます。

  ASA 9.1.4 以降のバージョンでは、インクルード リストを指定するときに、インクルード範囲内のサブネットにエクスクルード リストも指定できます。これらの除外されたサブネットはトンネリングされず、インクルードリストの残りのネットワークはトンネリングされます。インクルードリストのサブネットではないエクスクルージョン リスト内のネットワークは、クライアントで無視されます。Linux の場合、サブネットの除外をサポートするには、グループ ポリシーにカスタム属性を追加する必要があります。

  次に例を示します。



（注）
Split-Include ネットワークがローカル サブネットの完全一致（192.168.1.0/24 など）の場合、対応するトラフィックはトンネリングされています。Split-Include ネットワークがロー

カル サブネットのスーパーセット（192.168.0.0/16 など）の場合、対応するトラフィックは、ローカル サブネットを除き、トンネリングされています。ローカル サブネット トラフィックもトンネリングするには、一致する Split-Include ネットワーク（192.168.1.0/24 および 192.168.0.0/16 の両方を Split-Include ネットワークとして指定）を追加する必要があります。

Split-Include ネットワークが無効（0.0.0.0/0.0.0.0 など）の場合、スプリット トンネリングはディセーブルになります（すべてのトラフィックがトンネリングされます）。

- [Tunnel All Networks]：このポリシーは、すべてのトラフィックがトンネリングされるように指定します。この指定では、実質的にスプリット トンネリングは無効になります。リモート ユーザーは企業ネットワークを経由してインターネットにアクセスしますが、ローカル ネットワークにはアクセスできません。これがデフォルトのオプションです。

ステップ 7 [Network List] フィールドで、スプリット トンネリング ポリシーを適用するアクセス コントロール リストを選択します[Inherit] チェックボックスがオンの場合、グループ ポリシーはデフォルト グループ ポリシーで指定されているネットワーク リストを使用します。

[Manage] コマンドボタンを選択して [ACL Manager] ダイアログボックスを開きます。このボックスでは、ネットワーク リストとして使用するアクセス コントロール リストを設定できます。ネットワーク リストを作成または編集する方法の詳細については、一般的操作用コンフィギュレーション ガイドを参照してください。

拡張 ACL リストには IPv4 アドレスと IPv6 アドレスの両方を含めることができます。

ステップ 8 [Intercept DHCP Configuration Message from Microsoft Clients] は DHCP 代行受信に固有の追加パラメータを示します。DHCP 代行受信によって、Microsoft XP クライアントは ASA でスプリット トンネリングを使用できるようになります。

- [Intercept]：DHCP 代行受信を許可するかどうかを指定します。[Inherit] を選択しない場合、デフォルト設定は [No] です。
- [Subnet Mask]：使用するサブネット マスクを選択します。

ステップ 9 **[OK]** をクリックします。

ダイナミック スプリット トンネリングの設定

ダイナミック スプリット トンネリングでは、トンネルの確立後に、DNS ドメイン名に基づいて動的にスプリット除外トンネリングを行うことができます。ダイナミック スプリット トンネリングを設定するには、カスタム属性を作成し、グループ ポリシーに追加します。

始める前に

この機能を使用するには、AnyConnect リリース 4.5（またはそれ以降）が必要です。詳細については、「About Dynamic Split Tunneling」を参照してください。

手順

ステップ 1 **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [アドバンス（Advanced）] >** [セキュアクライアント**カスタム属性（Custom Attributes）]** 画面を参照します。

ステップ 2 [Add] をクリックし、`dynamic-split-exclude-domains` を属性タイプとして入力し、説明を入力します。

ステップ 3 この新しい属性をクリックして適用したら、UI 画面上部にある [セキュアクライアント custom attribute names] リンクをクリックします。

ステップ 4 VPN トンネル外部からのクライアントによるアクセスが必要な各クラウド/Web サービスについて、対応するカスタム属性名を追加します。たとえば、Google Web サービスに関する DNS ドメイン名のリストとして、Google_domains を追加します。これらのドメインは、[セキュアクライアントカスタム属性名（Custom Attribute Names）] 画面の [値（Value）] 部分で、ドメインをコンマ文字で区切るコンマ区切り値（CSV）形式を使用して定義します。セキュアクライアントでは、区切り文字（約 300 の通常サイズのドメイン名）を除く最初の 20,000 文字のみが考慮されます。その制限を超えるドメイン名は無視されます。

カスタム属性は 421 文字以内でなければなりません。大きな値が入力されると、ASDM は 421 文字を上限とする複数の値に分割されます。特定の属性タイプと名前のすべての名前は、設定がクライアントにプッシュされるときに ASA によって連結されます。

ステップ 5 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies]** を参照し、ダイナミック スプリット除外トンネリング属性を特定のグループ ポリシーに付加します。

ステップ 6 新しいグループ ポリシーを作成するか、[Edit] をクリックして既存のグループ ポリシーを管理することができます。

次のタスク

スプリットを含むトンネリングが設定されている場合、ダイナミック スプリット除外は、スプリットを含むネットワークに DNS 応答 IP アドレスが 1 つ以上含まれる場合のみ、実行されます。DNS 応答 IP アドレスとスプリットを含むネットワークのいずれかの間にまったく重なりがない場合、すべての DNS 応答 IP アドレスに一致するトラフィックはすでにトンネリングから除外されているため、ダイナミック スプリット除外の実行は不要です。

ダイナミック スプリット除外トンネリングの設定

ASDM を使用してダイナミック スプリット除外トンネリングを有効にするには、次の設定手順を実行します。ダイナミック スプリット除外ドメインとインクルード ドメインの両方が定義されている場合は、ドメイン名の一致による拡張ダイナミック スプリット除外トンネリングが有効になります。たとえば、管理者は example.com へのトラフィックを www.example.com 以外はすべて除外するように設定できます。*Example.com* はダイナミック スプリット除外ドメインであり、*www.example.com* はダイナミック スプリット インクルード ドメインです。

（注） ダイナミック スプリット除外トンネリングを使用するには、AnyConnect リリース 4.5（以降）が必要です。また、AnyConnect リリース 4.6（以降）で、両方のドメインが設定されている場合の拡張ダイナミック スプリット インクルードとスプリット除外のための改善が加えられました。ダイナミック スプリット除外は tunnel-all 設定、split-exclude 設定、および split-include 設定に適用されます。

始める前に

セキュアクライアント の要件については、「ダイナミック スプリット トンネリング」の項を参照してください。

手順

ステップ 1 **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [アドバンス（Advanced）] >** [セキュアクライアント**カスタム属性（Custom Attributes）]** 画面を参照します。

ステップ 2 [Add] をクリックし、`dynamic-split-exclude-domains` を属性タイプとして入力し、説明を入力します。

ステップ 3 この新しい属性をクリックして適用したら、UI 画面上部にある [セキュアクライアント custom attribute names] リンクをクリックします。

ステップ 4 VPN トンネル外部からのクライアントによるアクセスが必要な各クラウド/Web サービスについて、対応するカスタム属性名を追加します。たとえば、Google Web サービスに関する DNS ドメイン名のリストとして、Google_domains を追加します。これらのドメインは、[セキュアクライアントカスタム属性名（Custom Attribute Names）] 画面の [値（Value）] 部分で、ドメインをコンマ文字で区切るコンマ区切り値（CSV）形式を使用して定義します。セキュアクライアントでは、区切り文字（約 300 の通常サイズのドメイン名）を除く最初の 5000 文字のみが考慮されます。その制限を超えるドメイン名は無視されます。

カスタム属性は 421 文字以内でなければなりません。大きな値が入力されると、ASDM は 421 文字を上限とする複数の値に分割されます。特定の属性タイプと名前のすべての名前は、設定がクライアントにプッシュされるときに ASA によって連結されます。

ステップ 5 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies]** を参照し、ダイナミック スプリット除外トンネリング属性を特定のグループ ポリシーに付加します。

ステップ 6 新しいグループ ポリシーを作成するか、[Edit] をクリックして既存のグループ ポリシーを管理することができます。

ステップ 7 左側のメニューで、**[詳細設定（Advanced）]>**[セキュアクライアント]**>[カスタム属性（Custom Attributes）]** をクリックし、ドロップダウンから属性タイプを選択します。

ダイナミック スプリット包含トンネリングの設定

ASDM を使用してダイナミック スプリット インクルード トンネリングを有効にするには、次の設定手順を実行します。ダイナミック スプリット除外ドメインとインクルード ドメインの両方が定義されている場合は、ドメイン名の一致による拡張ダイナミック スプリット インクルード トンネリングが有効になります。たとえば、管理者は domain.com へのトラフィックを www.domain.com 以外はすべて含まれるように設定できます。*Domain.com* はダイナミック スプリット インクルード ドメインであり、*www.domain.com* はダイナミック スプリット除外ドメインです。

（注） AnyConnect リリース 4.6（以降）があり、ダイナミック スプリット インクルード トンネリングを使用する必要があります。また、AnyConnect リリース 4.6（以降）で、両方のドメインが設定されている場合の拡張ダイナミック スプリット インクルードとスプリット除外のための改善が加えられました。ダイナミック スプリット インクルードは split-include 設定にのみ適用されます。

始める前に

セキュアクライアント の要件については、「ダイナミック スプリット トンネリング」の項を参照してください。

手順

ステップ 1 **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [アドバンス（Advanced）] >** [セキュアクライアント**カスタム属性（Custom Attributes）]** 画面を参照します。

ステップ 2 [Add] をクリックし、属性タイプとして `dynamic-split-include-domains` と入力し、説明を入力します。

ステップ 3 この新しい属性をクリックして適用したら、UI 画面上部にある [セキュアクライアント custom attribute names] リンクをクリックします。

ステップ 4 VPN トンネル外部からのクライアントによるアクセスが必要な各クラウド/Web サービスについて、対応するカスタム属性名を追加します。たとえば、Google Web サービスに関する DNS ドメイン名のリストとして、Google_domains を追加します。これらのドメインは、[セキュアクライアントカスタム属性名（Custom Attribute Names）] 画面の [値（Value）] 部分で、ドメインをコンマ文字で区切るコンマ区切り値（CSV）形式を使用して定義します。セキュアクライアントでは、区切り文字（約 300 の通常サイズのドメイン名）を除く最初の 5000 文字のみが考慮されます。その制限を超えるドメイン名は無視されます。

カスタム属性は 421 文字以内でなければなりません。大きな値が入力されると、ASDM は 421 文字を上限とする複数の値に分割されます。特定の属性タイプと名前のすべての名前は、設定がクライアントにプッシュされるときに ASA によって連結されます。

ステップ 5 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies]** を参照して、ダイナミック スプリット インクルード トンネリング属性を特定のグループ ポリシーに追加します。

ステップ 6 新しいグループ ポリシーを作成するか、[Edit] をクリックして既存のグループ ポリシーを管理することができます。

ステップ 7 左側のメニューで、**[詳細設定（Advanced）]**>[セキュアクライアント]**>[カスタム属性（Custom Attributes）]** をクリックし、ドロップダウンから属性タイプを選択します。

管理 VPN トンネルの設定

管理 VPN トンネルにより、エンドユーザによって VPN 接続が確立されるときだけでなく、クライアント システムの電源が入るたびに社内ネットワークの接続が確保されます。オフィス ネットワークに VPN を介してユーザが頻繁に接続しないデバイスに対しては特に、外出中のオフィスのエンドポイントで Patch Management を行うことができます。この機能には、社内ネットワークの接続を必要とするエンドポイント OS ログイン スクリプトに対するメリットもあります。

管理 VPN トンネルはエンドユーザに対し透過的であるため、ユーザ アプリケーションによって開始されたネットワーク トラフィックはデフォルトで影響を受けませんが、代わりに管理 VPN トンネルの外部に転送されます。

ログインが低速であるとユーザーから報告された場合、管理トンネルが適切に設定されていない可能性があります。追加の要件、非互換性、制限、および管理 VPN トンネルのトラブルシューティングについては、『Cisco Secure Client Administration Guide』を参照してください。

始める前に

AnyConnect リリース 4.7（またはそれ以降）が必要

手順

ステップ 1 トンネルグループの認証方法は、**[設定（Configuration）]**>**[リモートアクセス（Remote Access）]** > **[ネットワーク（クライアント）アクセス（Network (Client) Access）]** > セキュアクライアント **[接続プロファイル（Connection Profiles）]** > **[追加/編集（Add/Edit）]**に移動し、[証明書のみ（certificate only）] として設定する必要があります。

ステップ 2 次に、同じウィンドウで、[Advanced] > [Group Alias/Group URL] を選択し、管理 VPN プロファイルで指定するグループ URL を追加します。

ステップ 3 このトンネル グループのグループ ポリシーには、トンネル グループで設定されたアドレス プールを使用するすべての IP プロトコルに対してスクリプト包含トンネリングが設定されている必要があります。**[Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Edit] > [Advanced] > [Split Tunneling]** から [Tunnel Network List Below] を選択します。

ステップ 4 （オプション）ユーザーが開始したネットワーク通信に影響しないように（管理 VPN トンネルは透過的であるため）スプリット包含トンネリングの設定がデフォルトで必要です。この動

作をオーバーライドするには、管理トンネル接続で使用されているグループポリシーにカスタム属性を設定します：セキュアクライアント カスタム属性 （184 ページ）。
両方の IP プロトコルに対するトンネル グループでアドレス プールが設定されていない場合、グループ ポリシーで [Client Bypass Protocol] をイネーブルにし、アドレス プールのない IP プロトコルと一致するトラフィックが管理 VPN トンネルで中断されないようにする必要があります。

ステップ 5 プロファイルを作成し、プロファイルの使用の管理 VPN トンネルを選択します：セキュアクライアント プロファイルの設定 （164 ページ）。

サブネットの除外をサポートするための Linux の設定

スプリット トンネリング用に [Tunnel Network List Below] を設定した場合、Linux ではサブネットの除外をサポートするために追加の設定が必要になります。circumvent-host-filtering という名前のカスタム属性を作成して true に設定し、スプリット トンネリング用に設定されたグループ ポリシーに関連付ける必要があります。

手順

ステップ 1 ASDM に接続し、**[設定（Configuration）]** > **[リモートアクセス VPN]** > **[Network (Client) Access]** > **[詳細設定（Advanced）]** > [セキュアクライアント**カスタム属性（Custom Attributes）]** に移動します。

ステップ 2 [Add] をクリックし、**circumvent-host-filtering** という名前のカスタム属性を作成して、その値を **true** に設定します。

ステップ 3 クライアントファイアウォールに対して使用予定のグループ ポリシーを編集し、**[詳細設定（Advanced）]** > [セキュアクライアント] > > **[カスタム属性（Custom Attributes）]** に移動します。

ステップ 4 作成したカスタム属性 **circumvent-host-filtering** をスプリット トンネリングに使用するグループ ポリシーに追加します。

内部グループポリシー、セキュアクライアント属性

[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループポリシー（Group Policies）] > [追加/編集（Add/Edit）] > [詳細設定（Advanced）] > [セキュアクライアント] には、このグループポリシーで設定可能なセキュアクライアントの属性が表示されます。

- [Keep Installer on Client System]：リモート コンピュータ上で永続的なクライアントのインストールを可能にします。これをイネーブルにすることにより、クライアントの自動的なアンインストール機能がディセーブルになります。クライアントは、後続の接続のためにリモート コンピュータにインストールされたままなので、リモート ユーザーの接続時間が短縮されます。

（注） [インストーラーをクライアントシステムに保持（Keep Installer on Client System）] は、セキュアクライアントのバージョン 2.5 以降でサポートされていません。

- [Datagram Transport Layer Security (DTLS)]：一部の SSL 接続に関連する遅延と帯域幅の問題を回避し、パケット遅延の影響を受けやすいリアルタイムアプリケーションのパフォーマンスを改善します。
- [DTLS Compression]：DTLS における圧縮を設定します。
- [SSL Compression]：SSL/TLS における圧縮を設定します。
- [Ignore Don't Defrag (DF) Bit]：この機能では、DF ビットが設定されているパケットを強制的にフラグメンテーションして、トンネルを通過させることができます。使用例として、TCP MSS ネゴシエーションに適切に応答しないネットワークのサーバーに対する使用などがあります。
- [クライアントバイパスプロトコル（Client Bypass Protocol）]：クライアント プロトコル バイパスでは、ASA が IPv6 トラフィックだけを予期しているときの セキュアクライアント クライアントによる IPv4 トラフィックの管理方法や、IPv4 トラフィックだけを予期しているときの IPv6 トラフィックの管理方法を設定します。

  セキュアクライアント が ASA に VPN 接続するときに、ASA は IPv4 と IPv6 の一方または両方のアドレスを割り当てます。クライアント バイパス プロトコルでは、ASA が IP アドレスを割り当てなかったトラフィックをドロップするか、または ASA をバイパスしてクライアントからの暗号化なし、つまり「クリアテキスト」としての送信を許可するかを決定します。

  たとえば、ASA が セキュアクライアント 接続に IPv4 アドレスのみを割り当て、エンドポイントがデュアルスタックされているとします。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアントバイパスプロトコル機能がディセーブルの場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルがイネーブルの場合は、IPv6 トラフィックはクライアントからクリアテキストとして送信されます。

- [FQDN of This Device]：この情報は、VPN セッションの再確立で使用される ASA IP アドレスを解決するために、ネットワーク ローミングの後でクライアントに使用されます。この設定は、さまざまな IP プロトコルのネットワーク間のローミングをサポートするうえで重要です（IPv4 から IPv6 など）。

（注） セキュアクライアント プロファイルにある ASA FQDN を使用してローミング後に ASA IP アドレスを取得することはできません。アドレスがロード バランシング シナリオの正しいデバイス（トンネルが確立されているデバイス）と一致しない場合があります。

デバイスのFQDNがクライアントに配信されない場合、クライアントは、以前にトンネルが確立されている IP アドレスへの再接続を試みます。異なる IP プロトコル（IPv4 から IPv6）のネットワーク間のローミングをサポートするには、セキュアクライアントは、トンネルの再確立に使用する ASA アドレスを決定できるように、ローミング後にデバイス FQDNの名前解決を行う必要があります。クライアントは、初期接続中にプロファイルに存在する ASA FQDN を使用します。以後のセッション再接続では、使用可能な場合は常に、ASA によってプッシュされた（また、グループ ポリシーで管理者が設定した）デバイス FQDN を使用します。FQDN が設定されていない場合、ASA は、[Device Setup] > [Device Name/Password and Domain Name] の設定内容からデバイス FQDN を取得（およびクライアントに送信）します。

デバイス FQDN が ASA によってプッシュされていない場合、クライアントは、異なる IP プロトコルのネットワーク間のローミング後に VPN セッションを再確立できません。

- [MTU]：SSL 接続の MTU サイズを調整します。256 ～ 1410 バイトの範囲で値を入力します。デフォルトでは、IP/UDP/DTLSのオーバーヘッド分を差し引き、接続で使用するインターフェイスの MTU に基づいて、自動的に MTU サイズが調整されます。
- [Keepalive Messages]：[Interval] フィールドに 15 秒から 600 秒までの数を入力することにより、接続がアイドルの時間がデバイスによって制限されている場合でも、キープアライブ メッセージの間隔をイネーブルおよび調整して、プロキシ、ファイアウォール、または NAT デバイスを通した接続を確実に開いたままにすることができます。また、間隔を調整することにより、リモート ユーザーが、Microsoft Outlook や Microsoft Internet Explorer などのソケットベースのアプリケーションを実際に実行していないときでも、クライアントが切断と再接続を行わないことが保証されます。
- [ダウンロードするオプションのクライアントモジュール（Optional Client Modules to Download）]：ダウンロード時間を短縮するために、セキュアクライアントは、サポートしている各機能に必要なモジュールだけを（ASAから）ダウンロードするように要求します。次のような他の機能をイネーブルにするモジュールの名前を指定する必要があります。セキュアクライアントのバージョン 4.0 には、次のモジュールが含まれています（旧バージョンではモジュールの数が少なくなります）。
  - [セキュアクライアント DART]：Diagnostic セキュアクライアント Reporting Tool（DART）は、トラブルシューティング情報を簡単にCisco TACに送信できるように、システムログのスナップショットおよびその他の診断情報をキャプチャし、.zip ファイルをデスクトップに作成します。
  - セキュアクライアント ネットワーク アクセス マネージャ：以前はCisco Secure Services Clientと呼ばれていました。このモジュールは、有線とワイヤレスの両方のネットワークにアクセスするための 802.1X（レイヤ 2）とデバイス認証を備えています。
  - セキュアクライアント SBL：Start Before Logon（SBL）は、Windows のログインダイアログボックスが表示される前にセキュアクライアントを開始することにより、ユーザを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。
  - セキュアクライアント Web セキュリティモジュール：以前は ScanSafe Hostscan と呼ばれていました。このモジュールは、セキュアクライアントに統合されています。ま

た、Web ページの要素を分解して、同時に各要素を分析できるようにします。その後、定義されているセキュリティポリシーに基づいて、受け入れ可能なコンテンツを許可し、悪意があるコンテンツや許容できないコンテンツをドロップします。

- セキュアクライアントテレメトリモジュール：悪意のあるコンテンツの発信元に関する情報を Cisco IronPort Web セキュリティアプライアンス（WSA）に送信します。WSA では、このデータを使用して、URL のフィルタリングルールを改善します。

（注） テレメトリは AnyConnect 4.0 ではサポートされません。

- ASA ポスチャモジュール：以前は Cisco Secure Desktop HostScan 機能と呼ばれていました。このポスチャモジュールは セキュアクライアント に統合され、これにより セキュアクライアント は、ASA へのリモートアクセス接続を確立する前にポスチャアセスメントのクレデンシャルを収集できるようになります。
- ISE ポスチャ：OPSWAT v3 ライブラリを使用してポスチャ チェックを実行し、エンドポイントの適合性を評価します。その後、エンドポイントが適合するまでネットワーク アクセスを制限したり、ローカル ユーザーの権限を強化したりできます。
- AMP イネーブラ：エンドポイント向けの高度なマルウェア防御（AMP）を導入する手段として使用されます。社内でローカルにホストされているサーバーからエンドポイントのサブセットに AMP for Endpoints ソフトウェアをプッシュし、既存のユーザーベースに AMP サービスをインストールします。
- ネットワーク可視性モジュール：キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。NVM（ネットワーク可視性モジュール）は、エンドポイントのテレメトリを収集して、フローデータとファイル レピュテーションを syslog に記録し、さらに、ファイルの分析と UI インターフェイスの提供を行うコレクタ（サードパーティ ベンダー）にもフロー レコードをエクスポートします。
- Umbrella Roaming Security モジュール：アクティブな VPN がないときに DNS レイヤ セキュリティを提供します。Cisco Umbrella Roaming と OpenDNS Umbrella サービスのいずれかに対するサブスクリプションを提供し、Intelligent Proxy および IP レイヤ適用機能を追加します。Umbrella Security Roaming プロファイルは、対応するサービスと各展開を関連付けて、対応する保護レベルを自動的に有効にします（コンテンツフィルタリング、複数のポリシー、強力なレポート、Active Directory 統合、または基本的な DNS レイヤ セキュリティ）。

- Always-On VPN：セキュアクライアント サービスプロファイルの常時接続 VPN フラグ設定をディセーブルにするか、または セキュアクライアント サービスプロファイル設定を使用する必要があるかを決定します。常時接続 VPN 機能により、ユーザーがコンピュータにログオンすると、AnyConnect は VPN セッションを自動的に確立します。VPN セッションは、ユーザーがコンピュータからログオフするまで維持されます。物理的な接続が失われてもセッションは維持され、セキュアクライアントは、適応型セキュリティアプライアンスとの物理的な接続の再確立を絶えず試行し、VPN セッションを再開します。

常時接続 VPN によって、企業ポリシーを適用して、セキュリティ脅威からデバイスを保護できます。常時接続 VPN を使用して、エンドポイントが信頼ネットワーク内ではない場合にいつでも セキュアクライアント が VPN セッションを確立したことを確認できます。イネーブルにすると、接続が存在しない場合のネットワーク接続の管理方法を決定するポリシーが設定されます。

（注） また、常時接続VPNにはセキュリティクライアント機能をサポートする セキュアクライアント リリースが必要です。

- [ダウンロードするクライアントプロファイル（Client Profiles to Download）]：プロファイルはコンフィギュレーション パラメータのグループであり、セキュアクライアントで VPN、ネットワーク アクセス マネージャ、Web セキュリティ、ISE ポスチャ、AMP イネーブラ、ネットワーク可視性モジュール、および Umbrella Roaming Security モジュールの設定に使用されます。[追加（Add）] をクリックして [セキュアクライアントプロファイルの選択（Select Profiles）] ウィンドウを起動すると、以前グループポリシー用に作成されたプロファイルを指定できます。

内部グループポリシー、セキュアクライアント ログイン設定

内部グループポリシーの **Advanced** > セキュアクライアント > **Login Setting** ペインでは、リモートユーザーにセキュアクライアントのダウンロードを求めるプロンプトを表示したり、クライアントレス SSL VPN のポータルページにダイレクト接続するように ASA を設定できます。

- [Post Login Setting]：ユーザーにプロンプトを表示して、デフォルトのポスト ログイン選択を実行するためのタイムアウトを設定する場合に選択します。
- [Default Post Login Selection]：ログイン後に実行するアクションを選択します。

クライアント ファイアウォールによる VPN でのローカル デバイス サポートの有効化

内部グループポリシーの **[詳細設定（Advanced）] > [セキュアクライアント] > [クライアントファイアウォール（Client Firewall）]** ペインでは、クライアントでのパブリックネットワークとプライベートネットワークの処理に影響するクライアントシステムのファイアウォールに送信するルールを設定できます。

リモートユーザーが ASA に接続すると、すべてのトラフィックがその VPN 接続を介してトンネリングされるため、ユーザーはローカル ネットワーク上のリソースにアクセスできなくなります。こうしたリソースには、ローカル コンピュータと同期するプリンタ、カメラ、Windows Mobile デバイス（テザー デバイス）などが含まれます。この問題は、クライアント プロファイルで [Local LAN Access] を有効にすることで解消されます。ただし、ローカル ネットワークへのアクセスが無制限になるため、一部の企業ではセキュリティやポリシーについて懸念が生じる可能性があります。プリンタやテザー デバイスなど特定タイプのローカル リソースに対するアクセスを制限するエンドポイントの OS のファイアウォール ルールを導入するように ASA を設定できます。

そのための操作として、印刷用の特定ポートに対するクライアント ファイアウォール ルールを有効にします。クライアントでは、着信ルールと発信ルールが区別されます。印刷機能の場合、クライアントでは発信接続に必要なポートは開放されますが、着信トラフィックはすべてブロックされます。

（注） 管理者としてログインしたユーザーは、ASA によりクライアントへ展開されたファイアウォール ルールを修正できることに注意が必要です。限定的な権限を持つユーザーは、ルールを修正できません。どちらのユーザーの場合も、接続が終了した時点でクライアントによりファイアウォール ルールが再適用されます。

クライアント ファイアウォールを設定している場合、ユーザーが Active Directory（AD）サーバーで認証されると、クライアントでは引き続き ASA のファイアウォール ポリシーが適用されます。ただし、AD グループ ポリシーで定義されたルールは、クライアント ファイアウォールのルールよりも優先されます。

ASA でクライアント ファイアウォール ルールが設定され、エンドポイントで VPN 接続が確立されている場合、

- ASA は、ファイアウォール ルール情報をクライアントに送信します。
- クライアントは、必要に応じてファイアウォール ルールを適用します。

以下の項では、次の処理を行うための手順について説明します。

- ローカル プリンタをサポートするためのクライアント ファイアウォールの展開 （99 ページ）
- VPN のテザー デバイス サポートの設定 （101 ページ）

ファイアウォールの動作に関する注意事項

以下は、セキュアクライアント でのファイアウォールの使用方法に関する注意事項です。

- ファイアウォール ルールには送信元 IP は使用されません。クライアントでは、ASA から送信されたファイアウォール ルール内の送信元 IP 情報は無視されます。送信元 IP は、ルールがパブリックかプライベートかに応じてクライアントが特定します。パブリック ルールは、クライアント上のすべてのインターフェイスに適用されます。プライベート ルールは、仮想アダプタに適用されます。
- ASA は、ACL ルールに対して数多くのプロトコルをサポートしています。ただし、セキュアクライアントのファイアウォール機能でサポートされているのは、TCP、UDP、ICMP、および IP のみです。クライアントでは、異なるプロトコルでルールが受信された場合、そのルールは無効なファイアウォール ルールとして処理され、さらにセキュリティ上の理由からスプリット トンネリングが無効となり、フル トンネリングが使用されます。
- ASA 9.0 から、パブリック ネットワーク ルールおよびプライベート ネットワーク ルールは、ユニファイド アクセス コントロール リストをサポートしています。これらのアクセ

ス コントロール リストは、同じルールで IPv4 および IPv6 トラフィックを定義する場合に使用できます。

ただし次のように、オペレーティング システムによって動作が異なるため注意が必要です。

- Windows コンピュータの場合、Windows Firewall では拒否ルールが許可ルールに優先します。ASA により許可ルールが セキュアクライアント にプッシュされても、ユーザーがカスタムの拒否ルールを作成している場合、セキュアクライアント ルールは適用されません。
- Windows Vista の場合、ファイアウォール ルールが作成されると、Windows Vista ではポート番号の範囲がカンマ区切りの文字列として認識されます。ポート範囲は、最大で 300 ポートです（1 ～ 300、5000 ～ 5300 など）。指定した範囲が 300 ポートを超える場合は、最初の 300 ポートに対してのみファイアウォール ルールが適用されます。
- ファイアウォールサービスが セキュアクライアント により開始される必要がある（システムにより自動的に開始されない）Windows ユーザーは、VPN 接続の確立時間が大幅に増える場合があります。
- Mac コンピュータの場合、セキュアクライアント では、ASA で適用された順序と同じ順序でルールが適用されます。グローバル ルールは必ず最後になるようにしてください。
- サードパーティ ファイアウォールの場合、セキュアクライアント ファイアウォールとサードパーティ ファイアウォールの両方で許可されているトラフィック タイプのトラフィックのみ通過できます。セキュアクライアント で許可されている特定のトラフィック タイプがサードパーティ ファイアウォールでブロックされる場合、そのタイプのトラフィックはクライアントでブロックされます。

ローカル プリンタをサポートするためのクライアント ファイアウォールの展開

ASA は、ASA バージョン 8.3(1) 以降および ASDM バージョン 6.3(1) 以降で、セキュアクライアント ファイアウォール機能をサポートします。この項では、ローカル プリンタへのアクセスが許可されるようにクライアント ファイアウォールを設定する方法、および VPN 接続の失敗時にファイアウォールを使用するようクライアント プロファイルを設定する方法について説明します。

クライアント ファイアウォールの制限事項

クライアント ファイアウォールを使用してローカル LAN アクセスを制限する場合には次の制限事項が適用されます。

- *deny ip any any* プライベート ルールは許可されません。
- OS の制限事項により、Windows XP が実行されているコンピュータのクライアント ファイアウォール ポリシーは、着信トラフィックに対してのみ適用されます。発信ルールおよび双方向ルールは無視されます。これには、「permit ip any any」などのファイアウォール ルールが含まれます。
- HostScan（現在の名前は Secure Firewall Posture）や一部のサードパーティ ファイアウォールは、ファイアウォールを妨害する可能性があります。

以下の表は、送信元ポートおよび宛先ポートの設定により影響を受けるトラフィックの方向をまとめたものです。

送信元ポート	宛先ポート	影響を受けるトラフィックの方向
特定のポート番号	特定のポート番号	着信および発信
範囲または「すべて」（値は 0）	範囲または「すべて」（値は 0）	着信および発信
特定のポート番号	範囲または「すべて」（値は 0）	着信のみ
範囲または「すべて」（値は 0）	特定のポート番号	発信のみ

ローカル印刷に関する ACL ルールの例

ACL セキュアクライアント_Local_Print は、クライアント ファイアウォールを設定しやすくするために、ASDM を備えています。グループ ポリシーの [Client Firewall] ペインのパブリック ネットワーク ルールのために ACL を選択する際は、一覧に次の ACE を含めます。

.

表 *3:* セキュアクライアント_*Local_Print* の *ACL* ルール

説明	権限	インターフェイス	プロトコル	送信元ポート	宛先アドレス	宛先ポート
すべて拒否	拒否	パブリック	すべて	デフォルト	任意	デフォルト
LPD	許可	パブリック	TCP	デフォルト	任意	515
IPP	許可	パブリック	TCP	デフォルト	任意	631
プリンタ	許可	パブリック	TCP	デフォルト	任意	9100
mDNS	許可	パブリック	UDP	デフォルト	224.0.0.251	5353
LLMNR	許可	パブリック	UDP	デフォルト	224.0.0.252	5355

説明	権限	インターフェイス	プロトコル	送信元ポート	宛先アドレス	宛先ポート
NetBios	許可	パブリック	TCP	デフォルト	任意	137
NetBios	許可	パブリック	UDP	デフォルト	任意	137
（注） デフォルトのポート範囲は 1 ～ 65535 です。						

（注） ローカル印刷を有効にするには、定義済み ACL ルール「allow Any Any」に対し、クライアント プロファイルの [Local LAN Access] 機能を有効にする必要があります。

VPN のローカル印刷サポートの設定

エンド ユーザーがローカル プリンタに出力できるようにするには、グループ ポリシーで標準 ACL を作成します。ASA はその ACL を VPN クライアントに送信し、VPN クライアントはクライアントのファイアウォール設定を変更します。

手順

ステップ 1 グループポリシーで、セキュアクライアントファイアウォールを有効にします。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。

ステップ 2 グループ ポリシーを選択して、[Edit] をクリックします。

ステップ 3 [詳細設定（Advanced）] > [セキュアクライアント] > [クライアントファイアウォール（Client Firewall）] を選択します。プライベート ネットワーク ルールに対応する [Manage] をクリックします。

ステップ 4 前述した ACE を含む ACL を作成します。この ACL をプライベート ネットワーク ルールとして追加します。

ステップ 5 常時接続の自動VPNポリシーを有効にし、かつクローズドポリシーを指定している場合、VPN障害が発生するとユーザーはローカルリソースにアクセスできません。このシナリオでは、プロファイル エディタの [Preferences (Part 2)] に移動し、[Apply last local VPN resource rules] をオンにすることによって、ファイアウォール ルールを適用できます。

VPN のテザー デバイス サポートの設定

テザー デバイスをサポートして企業ネットワークを保護する場合は、グループ ポリシーで標準的なACLを作成し、テザーデバイスで使用する宛先アドレスの範囲を指定します。さらに、

トンネリング VPN トラフィックから除外するネットワーク リストとしてスプリット トンネリング用の ACL を指定します。また、VPN 障害時には最後の VPN ローカル リソース ルールが使用されるようにクライアント プロファイルを設定することも必要です。

（注） セキュアクライアント を実行するコンピュータと同期する必要がある Windows モバイルデバイスについては、ACL で IPv4 宛先アドレスを 169.254.0.0、または IPv6 宛先アドレスを fe80::/64 と指定します。

手順

ステップ 1 ASDM で、[Group Policy] > [Advanced] > [Split Tunneling] を選択します。

ステップ 2 [Network List] フィールドの隣にある [Inherit] チェックボックスをオフにし、[Manage] をクリックします。

ステップ 3 [Extended ACL] タブをクリックします。

ステップ 4 [Add] > [Add ACL] を選択します。新しい ACL の名前を指定します。

ステップ 5 テーブルで新しい ACL を選択して、[Add] をクリックし、さらに [Add ACE] をクリックします。

ステップ 6 [Action] に対して [Permit] オプション ボタンを選択します。

ステップ 7 宛先条件エリアで、IPv4 宛先アドレスを 169.254.0.0、または IPv6 宛先アドレスを fe80::/64 と指定します。

ステップ 8 [Service] に対して IP を選択します。

ステップ 9 [OK] をクリックします。

ステップ 10 [OK] をクリックして、ACL を保存します。

ステップ 11 内部グループ ポリシーの [Split Tunneling] ペインで、ステップ 7 で指定した IP アドレスに応じて [Inherit for the Policy or IPv6 Policy] チェックボックスをオフにして、[Exclude Network List Below] を選択します。[Network List] で、作成した ACL を選択します。

ステップ 12 [OK] をクリックします。

ステップ 13 [適用（Apply）] をクリックします。

内部グループポリシー、セキュアクライアント キーの再生成

ASA とクライアントがキーを再生成し、暗号キーと初期ベクトルついて再ネゴシエーションするときに、キー再生成ネゴシエーションが実行され、接続のセキュリティが強化されます。

内部グループポリシーの [詳細設定（Advanced）] > [セキュアクライアント] > [キーの再生成（Key Regeneration）] ペインでは、キー再生成のパラメータを設定します。

- [Renegotiation Interval]：セッションの開始からキーの再生成が実行されるまでの分数を 1 ～ 10080（1 週間）の範囲で指定するには、[Unlimited] チェックボックスをオフにします。

- [Renegotiation Method]：[Inherit] チェックボックスをオフにして、デフォルトのグループポリシーとは異なる再ネゴシエーション方式を指定します。キー再生成をディセーブルにするには、[None] オプション ボタンを選択し、キー再生成時に新しいトンネルを確立するには、[SSL] または [New Tunnel] オプション ボタンを選択します。

（注） [Renegotiation Method] を [SSL] または [New Tunnel] に設定すると、キー再生成時に SSL 再ネゴシエーションが行われず、クライアントがキー再生成時に新規トンネルを確立することが指定されます。anyconnect ssl rekey コマンドの履歴については、コマンド リファレンスを参照してください。

内部グループポリシー、セキュアクライアント、デッドピア検出

Dead Peer Detection（DPD）により、ピアの応答がなく接続が失敗している場合には、ASA（ゲートウェイ）またはクライアント側で瞬時に検出できます。デッドピア検出（DPD）を有効にし、セキュアクライアントまたはASA ゲートウェイが DPD を実行する頻度を設定するには、以下の手順を実行します。

始める前に

- この機能は、ASA ゲートウェイと セキュアクライアント SSL VPN クライアント間の接続のみに適用されます。DPD は、埋め込みが許可されない標準実装に基づくため、IPsec とは併用できません。
- DTLS をイネーブルにすると、Dead Peer Detection（DPD）もイネーブルになります。DPD により、失敗した DTLS 接続の TLS へのフォールバックがイネーブルになります。それ以外の場合、接続は終了します。
- ASA で DPD が有効になっているとき、Optimal MTU（OMTU）機能を使用すると、クライアントが DTLS パケットを正常に渡すことができる最大のエンドポイント MTU を見つけることができます。最大 MTU までパディングされた DPD パケットを送信することによって、OMTU を実装します。ペイロードの正しいエコーをヘッドエンドから受信すると、MTU サイズが受け入れられます。受け入れられなかった場合、MTU は小さくされ、プロトコルで許可されている最小 MTU に到達するまで、繰り返しプローブが送信されます。

手順

ステップ 1 目的のグループ ポリシーに移動します。

- [設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループポリシー（Group Policies）] の順に移動し、目的のグループ ポリシーを追加（[追加（Add）]）または編集

（[編集（Edit）]）し、[詳細設定（Advanced）]>[セキュアクライアント]>[デッドピア検出（Dead Peer Detection）] ペインを開きます。

- または特定のユーザーポリシーに到達するには、[設定（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] > [ユーザーアカウント（User Accounts）] に移動し、目的のユーザーアカウントを追加（[追加（Add）]）または編集（[編集（Edit）]）し、[VPN ポリシー（VPN Policy）] > [セキュアクライアント] > [デッドピア検出（Dead Peer Detection）]ペインを開きます。

ステップ 2 ゲートウェイ側の検出を設定します。

DPD をセキュリティアプライアンス（ゲートウェイ）によって実行することを指定するには、[Disable] チェックボックスをオフにします。セキュリティ アプライアンスが DPD を実行する間隔を 30 秒（デフォルト）から 3600 秒の範囲で入力します。値 300 が推奨されます。

ステップ 3 クライアント側の検出を設定します。

DPD をクライアントが実行することを指定するには、[Disable] チェックボックスをオフにします。クライアントが DPD を実行する間隔を 30 秒（デフォルト）から 3600 秒の範囲で入力します。30 秒が推奨されます。

内部グループポリシー、クライアントレスポータルの セキュアクライアント カスタマイズ

内部グループポリシーの [詳細設定（Advanced）] > [セキュアクライアント] > [カスタマイズ（Customization）]ペインでは、グループポリシーのクライアントレスポータルのログインページをカスタマイズできます。

- [ポータルのカスタマイズ（Portal Customization）] : [セキュアクライアント/SSL VPN] ポータルページに適用するカスタマイゼーションを選択します。事前設定済みのポータル カスタマイゼーション オブジェクトを選択するか、またはデフォルト グループ ポリシーで定義されているカスタマイゼーションを受け入れることができます。デフォルトは DfltCustomization です。
  - [Manage]：[Configure GUI Customization object]s ダイアログボックスが開きます。このダイアログボックスでは、カスタマイゼーション オブジェクトの追加、編集、削除、インポート、またはエクスポートを指定できます。
- [Homepage URL](オプション)：グループ ポリシーに関連付けられたユーザーのクライアントレス ポータルに表示するホーム ページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。認証に成功すると、クライアントレス ユーザーにはすぐにこのページが表示されます。 VPN 接続が正常に確立されると、セキュアクライアント によってデフォルトの Web ブラウザが起動され、この URL が表示されます。

（注） セキュアクライアントは、Linux プラットフォーム、Android モバイルデバイス、および Apple iOS モバイルデバイスでこのフィールドを現在サポートしていません。設定されている場合、これらのセキュアクライアントは無視されます。

- [Use Smart Tunnel for Homepage]：ポート転送を使用する代わりにポータルに接続するスマート トンネルを作成します。
- [Access Deny Message]：アクセスを拒否するユーザーに表示するメッセージを作成するには、このフィールドに入力します。

内部グループポリシーの セキュアクライアントカスタム属性の設定

内部グループ ポリシーの [詳細設定（Advanced）] > [セキュアクライアント] > [カスタム属性（Custom Attributes）] ペインは、このポリシーに現在割り当てられているカスタム属性を示します。このダイアログボックスでは、すでに定義済みのカスタム属性をこのポリシーに関連付けるか、カスタム属性を定義してこのポリシーに関連付けることができます。

カスタム属性はセキュアクライアントに送信され、アップグレードの延期などの機能を設定するために使用されます。カスタム属性にはタイプと名前付きの値があります。まず属性のタイプを定義した後、このタイプの名前付きの値を 1 つ以上定義できます。機能に対して設定する固有のカスタム属性の詳細については、使用しているセキュアクライアントリリースの『*Cisco Secure Client Administrator Guide*』を参照してください。

カスタム属性は、[設定（Configuration）] > [リモートアクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [詳細設定（Advanced）] > [セキュアクライアントカスタム属性（Custom Attributes）] および [セキュアクライアントカスタム属性名（Custom Attribute Names）] で事前に定義することもできます。事前に定義したカスタム属性は、ダイナミック アクセス ポリシーとグループ ポリシーの両方で使用されます。

この手順を使用して、カスタム属性を追加または編集します。設定済みのカスタム属性を削除することもできますが、別のグループ ポリシーに関連付けられている場合は編集または削除できません。

手順

ステップ 1 **[設定（Configuration）] > [リモートアクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループポリシー（Group Policies）] > [追加/編集（ Add/Edit）] > [詳細設定（Advanced）]** > [セキュアクライアント] > **[カスタム属性（Custom Attributes）]**に移動します。

ステップ 2 [Add] をクリックして [Create Custom Attribute] ペインを開きます。

ステップ 3 ドロップダウン リストから事前に定義された属性タイプを選択するか、次の手順を実行して属性タイプを設定します。

a) [管理（Manage）] をクリックし、[カスタム属性タイプの設定（Configure Custom Attribute Types）] ペインで [追加（Add）] をクリックします。
b) [カスタム属性タイプの作成（Create Custom Attribute Type）] ペインで、新しい属性の [タイプ（Type）] と [説明（Description）] を入力します。どちらのフィールドも必須項目です。セキュアクライアント カスタム属性オプションについては、セキュアクライアント カスタム属性 （184 ページ）を参照してください。
c) [OK] をクリックしてこのペインを閉じ、もう一度 [OK] をクリックして、新しく定義したカスタム属性のタイプを選択します。

ステップ 4 [値の選択（Select Value）] を選択します。

ステップ 5 [値の選択（Select value）] ドロップダウン リストから事前に定義された名前付きの値を選択するか、次の手順を実行して新しい名前付きの値を設定します。

a) [管理（Manage）] をクリックし、[カスタム属性の設定（Configure Custom Attributes）] ペインで [追加（Add）] をクリックします。
b) [カスタム属性名の作成（Create Custom Attribute Name）] ペインで、前に選択または設定した属性タイプを選択し、新しい属性の [名前（Name）] と [値（Value）] を入力します。どちらのフィールドも必須項目です。

   値を追加するには、[追加（Add）] をクリックして値を入力し、[OK] をクリックします。値は 420 文字を超えてはなりません。値がこの長さを超える場合は、追加の値コンテンツ用の複数の値を追加します。設定値は セキュアクライアント に送信される前に連結されます。

c) [OK] をクリックしてこのペインを閉じ、もう一度 [OK] をクリックして、この属性の新しく定義した名前付きの値を選択します。

ステップ 6 [カスタム属性の作成（Create Custom Attribute）] ペインで [OK] をクリックします。

IPsec（IKEv1）クライアントの内部グループ ポリシー

内部グループ ポリシー、IPsec（IKEv1）クライアントの一般属性

[Configuration] > [Remote Access] > [Network （Client） Access] > [Group Policies] > [Advanced] > [IPsec (IKEv1) Client] で、[Add or Edit Group Policy] > [IPsec] ダイアログボックスを使用すると、追加または変更するグループポリシーのトンネリングプロトコル、フィルタ、接続設定、サーバーを指定できます。

- [Re-Authentication on IKE Re-key]：[Inherit] チェックボックスがオフである場合に、IKE キーの再生成が行われたときの再認証をイネーブルまたはディセーブルにします。ユーザーは、30 秒以内にクレデンシャルを入力する必要があります。また、約 2 分間で SA が期限切れになり、トンネルが終了するまでの間に、3 回まで入力を再試行できます。
- [Allow entry of authentication credentials until SA expires]：設定済み SA の最大ライフタイムまで、ユーザーは認証クレデンシャルをこの回数再入力できます。

- [IP Compression]：[Inherit] チェックボックスがオフである場合に、IP Compression をイネーブルまたはディセーブルにします。
- [Perfect Forward Secrecy]：[Inherit] チェックボックスがオフである場合に、完全転送秘密（PFS）をイネーブルまたはディセーブルにします。PFS は、特定の IPsec SA のキーが他のシークレット（他のキーなど）から導出されたものでないことを保証します。つまり、PFS では、攻撃者があるキーを突破しても、そこから他のキーを導出することはできないことが保証されます。PFS がイネーブルになっていない場合は、IKE SA の秘密キーが突破されると、その攻撃者は、IPsec のすべての保護データをコピーし、IKE SA のシークレットの知識を使用して、その IKE SA によって設定された IPsec SA のセキュリティを侵すことができると推測されます。PFS を使用すると、攻撃者が IKE を突破しても、直接 IPsec にはアクセスできません。その場合、攻撃者は各 IPsec SA を個別に突破する必要があります。
- [Store Password on Client System]：クライアント システムでのパスワードの保管をイネーブルまたはディセーブルにします。

（注） パスワードをクライアント システムで保管すると、潜在的なセキュリティ リスクが発生します。

- [IPsec over UDP]：IPsec over UDP の使用をイネーブルまたはディセーブルにします。
- [IPsec over UDP Port]：IPsec over UDP で使用する UDP ポートを指定します。
- [Tunnel Group Lock]：[Inherit] チェックボックスまたは値 [None] が選択されていない場合に、選択したトンネル グループをロックします。
- [IPsec Backup Servers]：[Server Configuration] フィールドと [Server IP Addresses] フィールドをアクティブにします。これによって、これらの値が継承されない場合に使用する UDP バックアップ サーバーを指定できます。
  - [Server Configuration]：IPsec バックアップ サーバーとして使用するサーバー設定オプションを一覧表示します。使用できるオプションは、[Keep Client Configuration]（デフォルト）、[Use Backup Servers Below]、および [Clear Client Configuration] です。
  - [Server Addresses（space delimited）]：IPsec バックアップ サーバーの IP アドレスを指定します。このフィールドは、[Server Configuration] で選択した値が Use Backup Servers Below である場合にだけ使用できます。

内部グループ ポリシーの IPsec（IKEv1）クライアントのアクセス ルールについて

このダイアログボックスの [Client Access Rules] テーブルには、クライアント アクセス ルールを 25 件まで表示できます。クライアント アクセス ルールを追加するときには次のフィールドを設定します。

- [Priority]：このルールの優先順位を選択します。

- [Action]：このルールに基づいてアクセスを許可または拒否します。
- [VPN Client Type]：このルールを適用する VPN クライアントのタイプ（ソフトウェアまたはハードウェア）を指定します。ソフトウェア クライアントの場合は、すべての Windows クライアントまたはサブセットを自由形式のテキストで指定します。
- [VPN Client Version]：このルールを適用する VPN クライアントのバージョンを指定します（複数可）。このカラムには、このクライアントに適用されるソフトウェアまたはファームウェア イメージのカンマ区切りリストが含まれます。エントリは自由形式のテキストで、***** はすべてのバージョンと一致します。

クライアント アクセス ルールの定義

- ルールを定義しない場合、ASA はすべての接続タイプを許可します。ただし、ユーザーがデフォルト グループ ポリシーに存在するルールを継承する場合があります。
- クライアントがいずれのルールにも一致しない場合、ASA は接続を拒否します。拒否ルールを定義する場合は、許可ルールも 1 つ以上定義する必要があります。許可ルールを定義しないと、ASA はすべての接続を拒否します。
- ***** 文字はワイルドカードです。ワイルドカードは各ルールで複数回入力することができます。
- ルール セット全体に対して 255 文字の制限があります。
- クライアントのタイプまたはバージョン（あるいはその両方）を送信しないクライアントには、**n/a** を入力できます。

内部グループ ポリシー、IPsec（IKEv1）クライアントのクライアント ファイアウォール

[Add or Edit Group Policy] の [Client Firewall] ダイアログボックスでは、追加または変更するグループ ポリシーに対して VPN クライアントのファイアウォール設定を行うことができます。これらのファイアウォール機能を使用できるのは、Microsoft Windows 上で動作している VPN クライアントだけです。現在、ハードウェア クライアントまたは他（Windows 以外）のソフトウェア クライアントでは、これらの機能は使用できません。

VPN クライアントを使用して ASA に接続しているリモート ユーザーは、適切なファイアウォール オプションを選択できます。

最初のシナリオでは、リモート ユーザーの PC 上にパーソナル ファイアウォールがインストールされています。VPN クライアントは、ローカル ファイアウォールで定義されているファイアウォール ポリシーを適用し、そのファイアウォールが実行されていることを確認するためにモニターします。ファイアウォールの実行が停止すると、VPN クライアントは ASA への通信をドロップします（このファイアウォール適用メカニズムは Are You There（AYT）と呼ばれます。VPN クライアントが定期的に「are you there?」メッセージを送信することによってファイアウォールをモニターするからです。応答が返されない場合、VPN クライアントは、ファイアウォールがダウンしたため ASA への接続が終了したと認識します。）ネットワーク管理者がこれらの PC ファイアウォールを独自に設定する場合もありますが、この方法を使用すれば、ユーザーは各自の設定をカスタマイズできます。

第 2 のシナリオでは、VPN クライアント PC のパーソナル ファイアウォールに中央集中型ファイアウォール ポリシーを適用することが選択されることがあります。一般的な例としては、スプリット トンネリングを使用してグループのリモート PC へのインターネット トラフィックをブロックすることが挙げられます。この方法は、トンネルが確立されている間、インターネット経由の侵入から PC を保護するので、中央サイトも保護されます。このファイアウォールのシナリオは、プッシュ ポリシーまたは Central Protection Policy（CPP）と呼ばれます。ASA では、VPN クライアントに適用するトラフィック管理ルールのセットを作成し、これらのルールをフィルタに関連付けて、そのフィルタをファイアウォール ポリシーとして指定します。ASA はこのポリシーを VPN クライアントまで配信します。その後、VPN クライアントはポリシーをローカル ファイアウォールに渡し、そこでポリシーが適用されます。

[Configuration] > [Remote Access] > [Network (Client) Access] > [Group Policies] > [Advanced] > [IPsec (IKEv1) Client] > [Client Firewall]

フィールド

- [Inherit]：グループ ポリシーがデフォルト グループ ポリシーからクライアントのファイアウォール設定を取得するかどうかを決めます。このオプションはデフォルト設定です。設定すると、このダイアログボックスにある残りの属性がその設定によって上書きされ、名前がグレー表示になります。
- [Client Firewall Attributes]：（実装されている場合）実装されているファイアウォールのタイプやファイアウォール ポリシーなど、クライアントのファイアウォール属性を指定します。
- [Firewall Setting]：ファイアウォールが存在するかどうかを一覧表示します。存在する場合には、そのファイアウォールが必須かオプションかも示します。[No Firewall]（デフォルト）を選択すると、このダイアログボックスにある残りのフィールドは、いずれもアクティブになりません。このグループのユーザーをファイアウォールで保護する場合は [Firewall Required] または [Firewall Optional] 設定を選択します。

  [Firewall Required] を選択した場合は、このグループのユーザー全員が指定されたファイアウォールを使用する必要があります。指定されたサポート対象のファイアウォールがインストールされておらず、実行されていない場合、ASA は接続を試行したセッションをすべてドロップします。この場合、ASA は、ファイアウォール設定が一致しないことを VPN クライアントに通知します。

（注） グループでファイアウォールを必須にする場合には、そのグループに Windows VPN クライアント以外のクライアントが存在しないことを確認してください。グループ内のその他のクライアント（クライアント モードの ASA 5505 を含む）は接続できません。

このグループに、まだファイアウォールに対応していないリモート ユーザーがいる場合は、[Firewall Optional] を選択します。Firewall Optional 設定を使用すると、グループ内のすべてのユーザーが接続できるようになります。ファイアウォールに対応しているユーザーは、ファイアウォールを使用できます。ファイアウォールなしで接続するユーザーに

は、警告メッセージが表示されます。この設定は、一部のユーザーがファイアウォールをサポートしており、他のユーザーがサポートしていないグループを作成するときに役立ちます。たとえば、移行途中のグループでは、一部のメンバはファイアウォール機能を設定し、別のユーザーはまだ設定していないことがあります。

- [Firewall Type]：シスコを含む複数のベンダーのファイアウォールを一覧表示します。[Custom Firewall] を選択すると、[Custom Firewall] の下のフィールドがアクティブになります。指定したファイアウォールが、使用できるファイアウォール ポリシーと相関している必要があります。設定したファイアウォールにより、サポートされるファイアウォール ポリシー オプションが決まります。
- [Custom Firewall]：カスタム ファイアウォールのベンダー ID、製品 ID、および説明を指定します。
  - [Vendor ID]：このグループ ポリシーのカスタム ファイアウォールのベンダーを指定します。
  - [Product ID]：このグループ ポリシー用に設定するカスタム ファイアウォールの製品名またはモデル名を指定します。
  - [Description]：（任意）カスタム ファイアウォールについて説明します。
- [Firewall Policy]：カスタム ファイアウォール ポリシーのタイプとソースを指定します。
  - [Policy defined by remote firewall (AYT)]：ファイアウォール ポリシーをリモート ファイアウォール（Are You There）によって定義するように指定します。Policy defined by remote firewall（AYT）は、このグループのリモートユーザーのファイアウォールが、各自の PC に存在することを意味しています。このローカル ファイアウォールが、VPN クライアントにファイアウォール ポリシーを適用します。ASA は、指定されたファイアウォールがインストールされ、実行している場合にのみ、このグループの VPN クライアントが接続できるようにします。指定されたファイアウォールが実行されていない場合、接続は失敗します。接続が確立すると、VPN クライアントがファイアウォールを 30 秒ごとにポーリングして、そのファイアウォールが実行されていることを確認します。ファイアウォールの実行が停止すると、VPN クライアントはセッションを終了します。
  - [Policy pushed (CPP)]：ポリシーがピアからプッシュされるように指定します。このオプションを選択する場合は、[Inbound Traffic Policy] および [Outbound Traffic Policy] リストと [Manage] ボタンがアクティブになります。ASA は、[Policy Pushed (CPP)] ドロップダウン リストで選択されたフィルタによって定義されるトラフィック管理ルールを、このグループの VPN クライアントに適用します。メニューで選択できるのは、デフォルト フィルタを含めて、この ASA で定義されているフィルタです。ASA がこれらのルールを VPN クライアントにプッシュすることに注意してください。ASA ではなく VPN クライアントに対してこれらのルールを作成して定義する必要があります。たとえば、「in」と「out」はそれぞれ、VPN クライアントに着信するトラフィックと、VPN クライアントから発信されるトラフィックです。VPN クライアントにローカル ファイアウォールもある場合、ASA からプッシュされたポリシーはローカル ファ

イアウォールのポリシーと連携して機能します。いずれかのファイアウォールのルールでブロックされたすべてのパケットがドロップされます。

- [Inbound Traffic Policy]：着信トラフィックに対して使用できるプッシュ ポリシーを一覧表示します。
- [Outbound Traffic Policy]：発信トラフィックに対して使用できるプッシュ ポリシーを一覧表示します。
- [Manage]：[ACL Manager] ダイアログボックスを表示します。このダイアログボックスで、アクセス コントロール リスト（ACL）を設定できます。

サイト間内部グループ ポリシー

サイト間 VPN 接続のグループ ポリシーでは、トンネリング プロトコル、フィルタ、および接続設定を指定します。このダイアログボックスの各フィールドで、[Inherit] チェックボックスを選択すると、対応する設定の値をデフォルト グループ ポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

フィールド

[Add Internal Group Policy] > [General] ダイアログボックスには、次の属性が表示されます。これらの属性は、SSL VPN と IPsec セッションに適用されます。そのため、いくつかの属性は、1 つのタイプのセッションに表示され、他のタイプには表示されません。

- [Name]：このグループ ポリシーの名前を指定します。Edit機能の場合、このフィールドは読み取り専用です。
- [Tunneling Protocols]：このグループが許可するトンネリング プロトコルを指定します。ユーザーは、選択されているプロトコルだけを使用できます。次の選択肢があります。
  - [Clientless SSL VPN]：SSL VPN（SSL/TLS を利用する VPN）を使用することを指定します。この VPN では、ソフトウェアやハードウェアのクライアントは必要なく、Web ブラウザを使用して ASA へのセキュアなリモートアクセス トンネルが確立されます。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
  - [SSL VPNクライアント（SSL VPN Client）]：Cisco Secure Client またはレガシー SSL VPN クライアントの AnyConnect VPN モジュールの使用を指定します。セキュアクライアントを使用している場合は、このプロトコルを選択して MUS がサポートされるようにする必要があります。
  - [IPsec IKEv1]：IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピアツーピア）接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。

- [IPsec IKEv2]：Secure Clientによってサポートされています。IKEv2 を使用した IPsec を使用するセキュアクライアント接続では、ソフトウェアアップデート、クライアントプロファイル、GUIのローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
- [L2TP over IPsec]：一部の一般的 PC やモバイル PC のオペレーティング システムで提供される VPN クライアントを使用しているリモート ユーザーは、L2TP over IPSec によって、パブリック IP ネットワーク経由でセキュリティ アプライアンスやプライベート企業ネットワークへのセキュアな接続を確立できます。L2TP は、データのトンネリングに PPP over UDP（ポート 1701）を使用します。セキュリティ アプライアンスは、IPsec 転送モード用に設定する必要があります。

- [フィルター（Filter）]：（Network (Client) Access 専用）使用するアクセス コントロール リストを指定するか、またはグループポリシーから値を継承するかどうかを指定します。フィルタは複数のルールから構成されています。これらのルールは、ASA を介して着信したトンネリング データ パケットを許可するか拒否するかを、送信元アドレス、宛先アドレス、プロトコルなどに基づいて決定します。VPN フィルタは初期接続にのみ適用されます。アプリケーションインスペクションのアクションによって開かれた SIP メディア接続などのセカンダリ接続には適用されません。フィルタおよびルールを設定する方法については、[Group Policy] ダイアログボックスを参照してください。ACL を表示および設定できる [ACL Manager] を開くには、[Manage] をクリックします。
- Idle Timeout：[Inherit] チェックボックスをオフにした場合、このパラメータでアイドル時間を分単位で設定します。

  この期間に接続で通信アクティビティがない場合、接続は終了します。最小時間は 1 分、最大時間は 10080 分であり、デフォルトは 30 分です。接続時間を無制限にするには、[Unlimited] をオンにします。
- Maximum Connect Time：[Inherit] チェックボックスがオフになっている場合、このパラメータで最大ユーザー接続時間を分単位で設定します。

  ここで指定した時間が経過すると、システムは接続を終了します。最小値は 1 分、最大値は 35791394 分です。制限なしの接続時間を許可するには、[Unlimited] をオンにします（デフォルト）。
- Periodic Certificate Authentication Interval：証明書認証が定期的に再実行されるまでの時間間隔（時間単位）。

  [Inherit] チェックボックスがオフになっている場合、定期的な証明書検証の実行間隔を設定できます。範囲は 1 ～ 168 時間で、デフォルトは無効になっています。無制限の検証を許可するには、[Unlimited] をオンにします。

ローカル ユーザーの VPN ポリシー属性の設定

この手順では、既存のユーザーを編集する方法について説明します。ユーザーを追加するには、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] を選択し、[Add]

をクリックします。詳細については、一般的操作用コンフィギュレーション ガイドを参照してください。

始める前に

デフォルトで、ユーザー アカウントはデフォルト グループ ポリシー DfltGrpPolicy から設定値を継承します。各設定内容を上書きする場合は、[Inherit] チェックボックスをオフにし、新しい値を入力します。

手順

ステップ 1 ASDM を開始し、**[Configuration]** > **[Remote Access VPN]** > **[AAA/Local Users]** > **[Local Users]** の順に選択します。

ステップ 2 設定するユーザーを選択し、[Edit] をクリックします。

ステップ 3 左側のペインで、[VPN Policy] をクリックします。

ステップ 4 ユーザーのグループ ポリシーを指定します。ユーザー ポリシーは、このグループ ポリシーの属性を継承します。この画面にデフォルト グループ ポリシーの設定を**継承するよう**設定されている他のフィールドがある場合、このグループ ポリシーで指定された属性がデフォルト グループ ポリシーで設定された属性より優先されます。

ステップ 5 ユーザーが使用できるトンネリング プロトコルを指定するか、グループ ポリシーから値を継承するかどうかを指定します。

目的の [Tunneling Protocols] チェックボックスをオンにし、次のトンネリング プロトコルのいずれかを選択します。

- SSL VPN クライアントは、セキュアクライアント アプリケーションのダウンロード後にユーザーが接続できるようにします。ユーザーは、最初にクライアントレス SSL VPN 接続を使用してこのアプリケーションをダウンロードします。ユーザーが接続するたびに、必要に応じてクライアント アップデートが自動的に行われます。
- [IPsec IKEv1]：IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピアツーピア）接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
- [IPsec IKEv2]：セキュアクライアント によってサポートされています。IKEv2 を使用した IPsec を使用する セキュアクライアント 接続では、ソフトウェアアップデート、クライアントプロファイル、GUI のローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張機能が提供されます。
- 一部の一般的 PC やモバイル PC のオペレーティング システムで提供される VPN クライアントを使用しているリモート ユーザーは、L2TP over IPSec によって、パブリック IP ネットワーク経由で ASA およびプライベート企業ネットワークへのセキュアな接続を確立できます。

（注）

プロトコルを選択しなかった場合は、エラー メッセージが表示されます。

ステップ 6 使用するフィルタ（IPv4 または IPv6）を指定するか、またはグループ ポリシーの値を継承するかどうかを指定します。

フィルタは複数のルールから構成されています。これらのルールは、ASA を介して着信したトンネリング データ パケットを許可するか拒否するかを、送信元アドレス、宛先アドレス、プロトコルなどに基づいて決定します。VPN フィルタは初期接続にのみ適用されます。アプリケーションインスペクションのアクションによって開かれた SIP メディア接続などのセカンダリ接続には適用されません。

a) フィルタとルールを設定するには、**[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[Group Policies]** > **[Add/Edit]** > **[General]** > **[More Options]** > **[Filter]** の順に選択します。

b) [Manage] をクリックして、ACL と ACE を追加、編集、および削除できる [ACL Manager] ペインを表示します。

ステップ 7 接続プロファイル（トンネル グループ ロック）がある場合、それを継承するかどうか、または選択したトンネル グループ ロックを使用するかどうかを指定します。

特定のロックを選択すると、ユーザーのリモート アクセスはこのグループだけに制限されます。[Tunnel Group Lock] では、VPN クライアントで設定されたグループと、そのユーザーが割り当てられているグループが同じかどうかをチェックすることによって、ユーザーが制限されます。一致していない場合、ASA はユーザーが接続できないようにします。[Inherit] チェックボックスがオフの場合、デフォルト値は [None] です。

ステップ 8 [Store Password on Client System] 設定をグループから継承するかどうかを指定します。

[Inherit] チェックボックスをオフにすると、[Yes] および [No] のオプション ボタンが有効になります。[Yes] をクリックすると、ログイン パスワードがクライアント システムに保存されます（セキュリティが低下するおそれのあるオプションです）。接続ごとにユーザーにパスワードの入力を求めるようにするには、[No] をクリックします（デフォルト）。セキュリティを最大限に確保するためにも、パスワードの保存を許可しないことを推奨します。

ステップ 9 [Connection Settings] を設定します。

a) このユーザーに適用するアクセス時間ポリシーを指定する、そのユーザーの新しいアクセス時間ポリシーを作成する、または [Inherit] チェックボックスをオンのままにします。デフォルトは [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルトは [Unrestricted] です。

[Manage] をクリックして、[Add Time Range] 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アクセス時間の新規セットを指定できます。

b) ユーザーによる同時ログイン数を指定します。Simultaneous Logins パラメータは、このユーザーに指定できる最大同時ログイン数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザー アクセスを禁止します。

（注）

最大値を設定て制限しておかない同時に多数の接続が許可されるため、セキュリティとパフォーマンスの低下を招くおそれがあります。

c) VPN 接続の [Maximum Connect Time] を分単位で指定します。ここで指定した時間が経過すると、システムは接続を終了します。

[Inherit] チェックボックスがオフになっている場合、このパラメータで最大ユーザー接続時間を分単位で指定します。最小値は 1 分、最大値は 35791394 分（4000 年超）です。制限なしの接続時間を許可するには、[Unlimited] をオンにします（デフォルト）。

d) VPN 接続の [Idle Timeout] を分単位で指定します。この期間に接続で通信アクティビティがない場合、接続は終了します。

[Inherit] チェックボックスがオフになっている場合、このパラメータで出アイドル タイムアウトを分単位で指定します。最小時間は 1 分、最大時間は 10080 分であり、デフォルトは 30 分です。接続時間を無制限にするには、[Unlimited] をオンにします。

ステップ 10 [Timeout Alerts] を設定します。

a) [Maximum Connection Time Alert Interval] を指定します。

[Inherit] チェックボックスをオフにした場合、[Default] チェックボックスは自動的にオンになります。これにより、最大接続アラート間隔は 30 分に設定されます。新しい値を指定する場合は、[Default] をオフにし、1 ～ 30 分のセッション アラート間隔を指定します。

b) [Idle Alert Interval] を指定します。

[Inherit] チェックボックスをオフにした場合、[Default] チェックボックスは自動的にオンになります。これにより、アイドル アラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] をオフにし、1 ～ 30 分のセッション アラート間隔を指定します。

ステップ 11 このユーザーに対して専用の IPv4 アドレスを設定する場合は、[Dedicated IPv4 Address (Optional)] 領域で、IPv4 アドレスとサブネット マスクを入力します。

ステップ 12 このユーザーに専用の IPv6 アドレスを設定するには、[Dedicated IPv6 Address (Optional)] 領域に IPv6 プレフィックスを含む IPv6 アドレスを入力します。IPv6 プレフィックスは、IPv6 アドレスが常駐するサブネットを示します。

ステップ 13 特定のセキュアクライアントを設定します。これは、左側ペインでこれらのオプションをクリックすることにより行います。各設定内容を上書きする場合は、[Inherit] チェックボックスをオフにし、新しい値を入力します。

ステップ 14 実行コンフィギュレーションに変更を適用するには、[OK] をクリックします。

接続プロファイル

接続プロファイル（トンネル グループとも呼ばれる）では、VPN 接続の接続属性を設定します。これらの属性は、Cisco Secure Clientの AnyConnect VPN モジュール、クライアントレス SSL VPN 接続、および IKEv1 と IKEv2 のサードパーティ VPN クライアントに適用されます。

セキュアクライアント 接続プロファイル、メインペイン

セキュアクライアント接続プロファイルのメインペインでは、インターフェイス上のクライアントアクセスを有効にして、接続プロファイルを追加、編集、および削除できます。ログイン時にユーザーが特定の接続を選択できるようにするかどうかも指定できます。

- [Access Interfaces]：アクセスをイネーブルにするインターフェイスをテーブルから選択できます。このテーブルのフィールドには、インターフェイス名やチェックボックスが表示され、アクセスを許可するかどうかを指定します。
  - [インターフェイス（Interface）] テーブルの セキュアクライアント 接続に設定するインターフェイスの行で、インターフェイスでイネーブルにするプロトコルをオンにします。SSL アクセス、IPSec アクセス、またはその両方を許可できます。

    SSL をオンにすると、DTLS（Datagram Transport Layer Security）がデフォルトでイネーブルになります。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

    IPsec（IKEv2）アクセスをオンにすると、クライアント サービスがデフォルトでイネーブルになります。クライアントサービスには、ソフトウェア更新、クライアントプロファイル、GUI のローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張 セキュアクライアント 機能が含まれています。クライアントサービスを無効にしても、セキュアクライアント では IKEv2 との基本的な IPsec 接続が確立されます。
  - [Device Certificate]：RSA キーまたは ECDSA キーの認証の証明書を指定できます。デバイス証明書の指定 （117 ページ）を参照してください。
  - [Port Setting]：HTTPS および DTLS（RA クライアントのみ）接続のポート番号を設定します。接続プロファイル、ポート設定 （118 ページ）を参照してください。
  - [Bypass interface access lists for inbound VPN sessions]：[Enable inbound VPN sessions to bypass interface ACLs] がデフォルトでオンになっています。セキュリティ アプライアンスが、すべての VPN トラフィックのインターフェイス ACL の通過を許可します。たとえば、外部インターフェイス ACL が復号化されたトラフィックの通過を許可しない場合でも、セキュリティ アプライアンスはリモート プライベート ネットワークを信頼し、復号化されたパケットの通過を許可します。このデフォルトの動作を変更できます。インターフェイス ACL に VPN 保護対象トラフィックの検査を行わせるためには、このチェックボックスをオフにします。

- Login Page Setting
  - ユーザーはそのエイリアスで識別される接続プロファイルをログインページで選択できます。このチェックボックスをオンにしない場合、デフォルト接続プロファイルは DefaultWebVPNGroup です。
  - [Shutdown portal login page.]：ログインがディセーブルの場合に Web ページを表示します。

- [Connection Profiles]：接続（トンネル グループ）のプロトコル固有属性を設定します。
  - [Add/Edit]：接続プロファイル（トンネル グループ）を追加または編集します。
  - [Name]：接続プロファイルの名前。
  - [Aliases]：接続プロファイルの別名。
  - [SSL VPN Client Protocol]：SSL VPN クライアントにアクセス権を与えるかどうかを指定します。
  - [Group Policy]：この接続プロファイルのデフォルト グループ ポリシーを表示します。
  - [Allow user to choose connection, identified by alias in the table above, at login page]：[Login] ページでの接続プロファイル（トンネル グループ）エイリアスの表示をイネーブルにする場合はオンにします。
- [Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used.]：このオプションでは、接続プロファイルの選択プロセス時にグループ URL および証明書の値の相対的プリファレンスを指定します。ASA で、推奨される値と一致する値が見つからない場合は、別の値に一致する接続プロファイルが選択されます。VPN エンドポイントで指定したグループ URL を、同じグループ URL を指定する接続プロファイルと照合するために、多数の古い ASA ソフトウェア リリースで使用されるプリファレンスを利用する場合にのみ、このオプションをオンにします。このオプションは、デフォルトではオフになっています。オフにした場合、ASA は接続プロファイルで指定した証明書フィールド値を、エンドポイントで使用する証明書のフィールド値と照合して、接続プロファイルを割り当てます。

デバイス証明書の指定

[Specify Device Certificate] ペインを使用すると、接続を試みたときに、クライアントに対して ASA を識別する証明書を指定できます。この画面は、セキュアクライアント 接続プロファイルおよびクライアントレス接続プロファイル用です。Alway-on IPsec/IKEv2 などの特定の セキュアクライアント 機能では、有効で信頼できるデバイスの証明書を ASA で利用できる必要があります。

ASA リリース 9.4.1 以降では、ECDSA 証明書を（セキュアクライアント とクライアントレス SSL の両方からの）SSL 接続に使用できます。このリリース以前は、セキュアクライアント IPsec 接続用の ECDSA 証明書だけがサポートされ、設定されました。

手順

ステップ 1 （VPN 接続のみ）[Certificate with RSA Key] 領域で、次のいずれかのタスクを実行します。

- 1 つの証明書を選択して、両方のプロトコルを使用してクライアントを認証する場合、[Use the same device certificate for SSL and IPsec IKEv2] チェックボックスをオンのままにします。

リスト ボックスで使用できる証明書を選択したり、[Manage] をクリックして、使用する ID 証明書を作成したりできます。

- [Use the same device certificate for SSL and IPsec IKEv2] チェックボックスをオフにして、SSL 接続または IPSec 接続の別個の証明書を指定します。

ステップ 2 [Device Certificate] リスト ボックスから証明書を選択します。

必要な証明書が表示されない場合は、[Manage] ボタンをクリックして、ASA の ID 証明書を管理します。

ステップ 3 （VPN 接続のみ）[ECDSA key] フィールドの [Certificate] で、リスト ボックスから ECDSA の証明書を選択するか、[Manage] をクリックして、ECDSA の ID 証明書を作成します。

ステップ 4 **[OK]** をクリックします。

接続プロファイル、ポート設定

ASDM の接続プロファイル ペインで SSL および DTLS 接続（リモート アクセスのみ）のポート番号を設定します。

[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [セキュアクライアント接続プロファイル（Connection Profiles）]

フィールド

- [HTTPS Port]：HTTPS（ブラウザベース）SSL 接続用にイネーブルにするポート。範囲は 1 ～ 65535 です。デフォルトはポート 443 です。
- [DTLS Port]：DTLS 接続用にイネーブルにする UDP ポート。範囲は 1 ～ 65535 です。デフォルトはポート 443 です。

セキュアクライアント 接続プロファイル、基本属性

Cisco Secure Client 接続の AnyConnect VPN モジュールの基本属性を設定するには、[セキュアクライアント接続プロファイル（Connection Profiles）] セクションで [追加（Add）] または [編集（Edit）] を選択します。[セキュアクライアント接続プロファイルの追加/編集（Add/Edit Connection Profile）] > [基本（Basic）] ダイアログボックスが開きます。

- [Name]：[Add] の場合、追加する接続プロファイルの名前を指定します。[Edit] の場合、このフィールドは編集できません。
- [Aliases]：（任意）この接続の代替名を 1 つ以上入力します。名前は、スペースまたは句読点で区切ることができます。
- [Authentication]：認識の方法を、次の中から 1 つ選択し、認証処理で使用する AAA サーバー グループを指定します。

- [Method]：複数証明書認証のためのプロトコル交換を定義し、両方のセッションタイプでこれを利用するために認証プロトコルが拡張されています。セキュアクライアント SSL クライアントプロトコルと IKEv2 クライアントプロトコルを使用して、セッションごとに複数の認証を検証できます。使用する認証タイプを、AAA、AAA と証明書、証明書のみ、SAML、複数証明書および AAA、複数の証明書、SAML と証明書、またはSAML と複数証明書から選択します。選択に応じて、接続するために証明書を提供する必要がある場合があります。
- [AAA Server Group]：ドロップダウン リストから AAA サーバー グループを選択します。デフォルトの設定はLOCAL です。その場合、ASA が認証を処理するように指定されます。選択する前に、[Manage] をクリックして、このダイアログボックスの上に別のダイアログボックスを開き、AAA サーバー グループの ASA コンフィギュレーションを表示したり変更することができます。
  - LOCAL 以外のグループを選択すると、[Use LOCAL if Server Group Fails] チェックボックスが選択できるようになります。
  - [Use LOCAL if Server Group fails]：Authentication Server Group 属性によって指定されたグループに障害が発生したときに、LOCAL データベースをイネーブルにする場合はオンにします。

- [SAML ID プロバイダー（SAML Identity Provider）]：シングルサインオン（SSO）認証用の SAML IdP サーバーを選択します。
  - [SAMLサーバー（SAML Server）]：セキュアクライアント シングルサインオン認証用にドロップダウンから SAML サーバーを選択するか、**[管理（Manage）]** をクリックして SSO サーバーを追加し、次のパラメータを設定します。
    - **[IDPエンティティID（IDP Entity ID）]**：SAML Idp のエンティティ ID。
    - [Sign In URL]：IdP にサインインするための URL。url value は 4 ～ 500 文字の範囲で指定します。
    - [Sign Out URL]（オプション）：IdP からサインインするときのリダイレクト先 URL。url value は 4 ～ 500 文字の範囲で指定します。
    - [Base URL]（オプション）：エンドユーザーを ASA にリダイレクトするために、サードパーティ製 IdP に提供されます。

      base-url が設定されている場合、その URL は **show saml metadata** の AssertionConsumerService と SingleLogoutService 属性のベース URL として使用されます。

      base-url が設定されていない場合、URL は ASA のホスト名とドメイン名から決定されます。たとえば、ホスト名が `ssl-vpn`、ドメイン名が `cisco.com` の場合は、`https://ssl-vpn.cisco.com` が使用されます。

      base-url もホスト名/ドメイン名も設定されていない場合は、**show saml metadata** を入力するとエラーが発生します。

- **ローカルベース URL**：（オプション）DNS ロードバランシングクラスタでは、SAML 認証を ASA で設定するときに、設定が適用されるデバイスに一意に解決されるベース URL を指定できます。
- [Identity Provider Certificate]：ASA が SAML アサーションを検証するための IdP 証明書を含むトラストポイントを指定します。すでに設定されているトラストポイントを選択します。
- [Service Provider Certificate]（オプション）：IdP が ASA（SP）の署名や暗号化 SAML アサーションを検証するための ASA（SP）証明書含むトラストポイントを指定します。すでに設定されているトラストポイントを選択します。
- [Request Signature]：ドロップダウンを使用して、SAML IdP サーバーに対して希望する署名方法を選択します。rsa-sha1、rsa-sha256、rsa-sha384、rsa-sha512 から選択できます。
- **[要求タイムアウト（Request Timeout）]**：（オプション）SAML 要求のタイムアウト（秒）。範囲は 1 ～ 7200 です。

  指定した場合、NotBefore と timeout-in-seconds の合計が NotOnOrAfter よりも早い場合は、この設定が NotOnOrAfter に優先します。

  指定しない場合は、セッションの NotBefore と NotOnOrAfter が有効期間の確認に使用されます。
- **[内部ネットワークでアクセス可能な場合のみIDPを有効化（Enable IDP only accessible on internal network）]**：内部ネットワークでアクセス可能な場合にのみ IDP を有効にするには、このチェックボックスをオンにします。
- **[ログイン時にIDP再認証を要求（Request IDP reauthentication at login）]**：ログイン時の IDP 再認証を有効にするには、このチェックボックスをオンにします。
- **[クロックスキュー（Clock-skew）]**：NotBefore アサーションと NotOnOrAfter SAML アサーションを許容するクロックスキュー。デフォルトでは、クロックスキューは無効にする必要があります。デフォルト値は 1 秒で、範囲は 1 ～ 180 秒です。

- [SAML IDP TrustPoint]：シングルサインオン（SSO）認証用の SAML IdP TrustPoint を選択します。
  - [IDP TrustPoint]：ASA が SAML アサーションを検証するための IdP 証明書を含む SAML IdP トラストポイントを選択します。
- [SAMLログインエクスペリエンス（SAML Login Experience）]：シングルサインオン（SSO）認証用の SAML IdP TrustPoint を選択します。
  - [VPNクライアント組み込みブラウザ（VPN Client Embedded Browser）]：VPN クライアントは Web 認証に組み込みブラウザを使用するため、認証は VPN 接続にのみ適用されます。

- [デフォルトOSブラウザ（Default OS Browser）]：VPN クライアントは、Web 認証にシステムのデフォルトブラウザを使用します。このオプションは、シングルサインオン（SSO）と、組み込みブラウザでは実行できない Web 認証方式（生体認証など）のサポートを有効にします。

  SSO 認証にデフォルトの OS ブラウザを選択する場合は、デフォルトのブラウザを使用するようにセキュアクライアントの外部ブラウザパッケージを設定する必要があります。セキュアクライアント外部ブラウザ SAML パッケージ（162 ページ）を参照してください。

- [SAMLユーザー名の一致（SAML UserName Match）]：証明書のユーザー名を SAML ユーザー名に一致させる場合に選択します。
- [Client Address Assignment]：使用する DHCP サーバー、クライアント アドレス プール、クライアント IPv6 アドレス プールを選択します。
- [Client Address Assignment]：使用する DHCP サーバー、クライアント アドレス プール、クライアント IPv6 アドレス プールを選択します。
  - [DHCP Servers]：使用する DHCP サーバーの名前または IP アドレスを入力します。
  - [Client Address Pools]：クライアント アドレス割り当てで使用する、選択可能な設定済みの IPv4 アドレス プールの名前を入力します。選択する前に、[Select] をクリックして、このダイアログボックスに重ねてダイアログボックスを開き、アドレス プールを表示したり、変更を加えたりすることができます。IPv4 アドレス プールを追加または編集する方法の詳細については を参照してください。
  - [Client IPv6 Address Pools]：クライアント アドレス割り当てで使用する、選択可能な設定済みの IPv6 アドレス プールの名前を入力します。選択する前に、[Select] をクリックして、このダイアログボックスに重ねてダイアログボックスを開き、アドレス プールを表示したり、変更を加えたりすることができます。IPv6 アドレス プールを追加または編集する方法の詳細については を参照してください。
-
- [Default Group Policy]：使用するグループ ポリシーを選択します。
  - [Group Policy]：この接続のデフォルト グループ ポリシーとして割り当てる VPN グループ ポリシーを選択します。VPN グループ ポリシーは、ユーザー指向属性値のペアの集合で、デバイスで内部に、または RADIUS サーバーで外部に保存できます。デフォルト値は DfltGrpPolicy です。[Manage] をクリックして別のダイアログボックスを重ねて開き、グループ ポリシー コンフィギュレーションに変更を加えることができます。
  - [Enable SSL VPN client protocol]：VPN 接続の SSL をイネーブルにする場合にオンにします。
  - [Enable IPsec (IKEv2) client protocol]：接続で IKEv2 を使用する IPsec をイネーブルにする場合にオンにします。

- [DNS Servers]：ポリシーの DNS サーバーの IP アドレスを入力します（1 つまたは複数）。
- [WINS Servers]：ポリシーの WINS サーバーの IP アドレスを入力します（1 つまたは複数）。
- [Domain]：デフォルトのドメイン名を入力します。

- [Find]：検索文字列として使用する GUI ラベルまたは CLI コマンドを入力し、[Next] または [Previous] をクリックして検索を開始します。

接続プロファイル、詳細属性

[Advanced] メニュー項目とそのダイアログボックスでは、この接続に関する次の特性を設定できます。

- 一般属性
- クライアント アドレス指定属性
- 認証属性
- 認可属性
- アカウンティング属性
- ネーム サーバー属性

（注） SSL VPN 属性および 2 次認証属性は、SSL VPN 接続プロファイルにだけ適用されます。

セキュアクライアント 接続プロファイル、一般属性

- [Enable Simple Certificate Enrollment (SCEP) for this Connection Profile]
- [Strip the realm from username before passing it on to the AAA server]
- [Strip the group from username before passing it on to the AAA server]
- [Group Delimiter]
- [Enable Password Management]：ユーザーへのパスワード期限切れ通知に関するパラメータを設定できます。
  - [Notify user __ days prior to password expiration]：パスワードが期限切れになるまでの特定の日数を指定し、その日数だけ前の日のログイン時に ASDM がユーザーに通知するよう指定します。デフォルトでは、パスワードが期限切れになるより 14 日前にユーザーへの通知を開始し、以後、ユーザーがパスワードを変更するまで毎日通知するように設定されています。範囲は 1 ～ 180 日です。

- [Notify user on the day password expires]：パスワードが期限切れになる当日にユーザーに通知します。

  いずれの場合でも、変更されずにパスワードが期限切れになったとき、ASA ではユーザーによるパスワードの変更が可能です。現在のパスワードの期限が切れていなければ、ユーザーはそのパスワードで引き続きログインできます。

  この処理によってパスワードの期限が切れるまでの日数が変わるのではなく、通知がイネーブルになるだけであるという点に注意してください。このオプションを選択する場合は、日数も指定する必要があります。

- [Translate Assigned IP Address to Public IP Address]：まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく、VPN ピアの実際の IP アドレスを使用する場合があります。VPN では通常、内部ネットワークにアクセスするために、割り当てられたローカル IP アドレスがピアに指定されます。ただし、内部サーバおよびネットワーク セキュリティがピアの実際の IP アドレスに基づく場合などに、ローカル IP アドレスを変換してピアの実際のパブリック IP アドレスに戻す場合があります。この機能は、トンネル グループごとに 1 つのインターフェイスでイネーブルにすることができます。

  - [Enable the address translation on interface]：アドレス変換を可能にし、アドレスが表示されるインターフェイスを選択することができます。*outside* は セキュアクライアント が接続するインターフェイスであり、*inside* は新しいトンネルグループに固有のインターフェイスです。

（注） ルーティングの問題および他の制限事項のため、この機能が必要でない場合は、この機能の使用は推奨しません。

- [Find]：検索文字列として使用する GUI ラベルまたは CLI コマンドを入力し、[Next] または [Previous] をクリックして検索を開始します。

接続プロファイル、クライアント アドレス指定

接続プロファイルの [Client Addressing] ペインでは、この接続プロファイルで使用するために特定のインターフェイスに IP アドレス プールを割り当てます。[Client Addressing] ペインはすべてのクライアント接続プロファイルに共通で、次の ASDM パスからアクセスできます。

- [設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [Secure Client AnyConnect接続プロファイル（Secure Client Connection Profiles）]
- **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv1) Connection Profiles]**
- **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv2) Connection Profiles]**

ここで設定するアドレス プールは、接続プロファイルの [Basic] ペインでも設定できます。

セキュアクライアント 接続プロファイルでは、IPv4 アドレスプールだけでなく IPv6 アドレス プールも割り当てることができます。

クライアント アドレス指定を設定するには、リモート アクセス クライアント接続プロファイル（セキュアクライアント、IKEv1 または IKEv2）を開き、[詳細設定（Advanced）] > [クライアントアドレッシング（Client Addressing）] を選択します。

- アドレスプールのコンフィギュレーションを表示または変更するには、ダイアログボックスの [Add] または [Edit] をクリックします。[Assign Address Pools to Interface] ダイアログボックスが開きます。このダイアログボックスでは、ASA で設定されたインターフェイスに IP アドレス プールを割り当てることができます。[Select] をクリックします。このダイアログボックスを使用して、アドレス プールのコンフィギュレーションを表示します。アドレス プールのコンフィギュレーションを変更するには、次の手順を実行します。
  - ASA にアドレス プールを追加するには、[Add] をクリックします。[Add IP Pool] ダイアログボックスが開きます。
  - ASA のアドレス プールのコンフィギュレーションを変更するには、[Edit] をクリックします。プール内のアドレスが使用されていない場合には、[Edit IP Pool] ダイアログボックスが開きます。

    使用中の場合はアドレス プールを変更できません。[Edit] をクリックしたときにアドレス プールが使用中であった場合、ASDM は、エラー メッセージとともに、プール内のそのアドレスを使用している接続名およびユーザー名の一覧を表示します。
  - ASA 上のアドレス プールを削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。

    使用中の場合はアドレス プールを削除できません。[Delete] をクリックしたときにアドレス プールが使用中であった場合、ASDM は、エラー メッセージとともに、プール内のそのアドレスを使用している接続名の一覧を表示します。
- アドレス プールをインターフェイスに割り当てるには、[Add] をクリックします。[Assign Address Pools to Interface] ダイアログボックスが開きます。アドレス プールを割り当てるインターフェイスを選択します。[Address Pools] フィールドの横にある [Select] をクリックします。[Select Address Pools] ダイアログボックスが開きます。インターフェイスに割り当てる個々の未割り当てプールをダブルクリックするか、または個々の未割り当てプールを選択して [Assign] をクリックします。隣のフィールドにプール割り当ての一覧が表示されます。[OK] をクリックして、これらのアドレス プールの名前を [Address Pools] フィールドに取り込み、もう一度 [OK] をクリックして割り当てのコンフィギュレーションを完了します。
- インターフェイスに割り当てられているアドレス プールを変更するには、そのインターフェイスをダブルクリックするか、インターフェイスを選択して [Edit] をクリックします。[Assign Address Pools to Interface] ダイアログボックスが開きます。アドレス プールを削除するには、各プール名をダブルクリックし、キーボードの [Delete] キーを押します。インターフェイスにその他のフィールドを割り当てる場合は、[Address Pools] フィールドの横にある [Select] をクリックします。[Select Address Pools] ダイアログボックスが開きま

す。[Assign] フィールドには、インターフェイスに割り当てられているアドレス プール名が表示されます。インターフェイスに追加する個々の未割り当てプールをダブルクリックします。[Assign] フィールドのプール割り当て一覧が更新されます。[OK] をクリックして、これらのアドレス プールの名前で [Address Pools] フィールドを確認し、もう一度 [OK] をクリックして割り当てのコンフィギュレーションを完了します。

- エントリを削除するには、そのエントリを選択して [Delete] をクリックします。

関連トピック

接続プロファイル、クライアント アドレス指定、追加または編集 （125 ページ）
接続プロファイル、アドレス プール （125 ページ）
接続プロファイル、詳細、IP プールの追加または編集 （126 ページ）

接続プロファイル、クライアント アドレス指定、追加または編集

接続プロファイルにアドレス プールを割り当てるには、[Advanced] > [Client Addressing] を選択し、[Add] または [Edit] を選択します。

- [Interface]：アドレス プールの割り当て先インターフェイスを選択します。デフォルトは DMZ です。
- [Address Pools]：指定したインターフェイスに割り当てるアドレス プールを指定します。
- [Select]：[Select Address Pools] ダイアログボックスが開きます。このダイアログボックスでは、このインターフェイスに割り当てるアドレス プールを 1 つ以上選択できます。選択内容は、[Assign Address Pools to Interface] ダイアログボックスの [Address Pools] フィールドに表示されます。

接続プロファイル、アドレス プール

[Connection Profile] > [Advanced] の [Select Address Pools] ダイアログボックスに、クライアント アドレス割り当てに使用可能なアドレス プールのプール名、開始アドレスと終了アドレス、およびサブネット マスクが表示されます。そのリストを使って接続プロファイルを追加、編集、または削除できます。

- [Add]：[Add IP Pool] ダイアログボックスが開きます。このダイアログボックスでは、新しい IP アドレス プールを設定できます。
- [Edit]：[Edit IP Pool] ダイアログボックスが開きます。このダイアログボックスでは、選択した IP アドレス プールを変更できます。
- [Delete]：選択したアドレス プールを削除します。確認されず、やり直しもできません。
- [Assign]：インターフェイスに割り当てられているアドレス プール名を表示します。インターフェイスに追加する個々の未割り当てプールをダブルクリックします。[Assign] フィールドのプール割り当て一覧が更新されます。

接続プロファイル、詳細、IP プールの追加または編集

[Connection Profile] > [Advanced] の [Add or Edit IP Pool] ダイアログボックスを使用すれば、クライアント アドレス割り当て用の IP アドレスの範囲を指定または変更できます。

- [Name]：IP アドレス プールに割り当てられている名前を指定します。
- [Starting IP Address]：プールの最初の IP アドレスを指定します。
- [Ending IP Address]：プールの最後の IP アドレスを指定します。
- [Subnet Mask]：プール内のアドレスに適用するサブネット マスクを選択します。

セキュアクライアント接続プロファイル、認証属性

[Connection Profile] > [Advanced] > [Authentication] タブで、次のフィールドを設定できます。

- [Interface-specific Authentication Server Groups]：指定のインターフェイスに対する認証サーバー グループの割り当てを管理します。
  - [Add or Edit]：[Assign Authentication Server Group to Interfac]e ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスとサーバー グループを指定するとともに、選択したサーバー グループで障害が発生した場合に LOCAL データベースへのフォールバックを許可するかどうかを指定できます。このダイアログボックスの [Manage] ボタンをクリックすると、[Configure AAA Server Groups] ダイアログボックスが開きます。[Interface/Server Group] テーブルに選択内容が表示されます。
  - [Delete]：選択したサーバー グループをテーブルから削除します。確認されず、やり直しもできません。
- [Username Mapping from Certificate]：ユーザー名を抽出する方法およびデジタル証明書のフィールドを指定できます。

（注） この機能はマルチ コンテキスト モードではサポートされません。

  - [Pre-fill Username from Certificate]：指定した証明書のフィールドからユーザー名を抽出し、このパネルの後に続くオプションに従って、ユーザー名/パスワード認証および認可に使用します。
  - [Hide username from end user]：抽出したユーザー名はエンド ユーザーに表示されません。
  - [Use script to choose username]：デジタル証明書からユーザー名を選択する場合に使用するスクリプト名を指定します。デフォルトは [None] です。
  - [Add or Edit]：[Opens the Add or Edit Script Content] ダイアログボックスが開き、証明書のユーザー名のマッピングに使用するスクリプトを定義できます。

- [Delete]：選択したスクリプトを削除します。確認されず、やり直しもできません。
- [Use the entire DN as the username]：証明書の [Distinguished Name] フィールド全体をユーザー名として使用する場合に指定します。
- [Specify the certificate fields to be used as the username]：ユーザー名に結合する 1 つ以上のフィールドを指定します。

  プライマリ属性およびセカンダリ属性の有効値は、次のとおりです。

属性	定義
C	Country（国名）：2 文字の国名略語。国名コードは、ISO 3166 国名語に準拠しています。
CN	Common Name（一般名）：人、システム、その他のエンティティの前。セカンダリ属性としては使用できません。
DNQ	ドメイン名修飾子。
EA	E-mail Address（電子メール アドレス）。
GENQ	Generational Qualifier（世代修飾子）。
GN	Given Name（名）。
I	Initials（イニシャル）。
L	Locality（地名）：組織が置かれている市または町。
N	名前
O	Organization（組織）：会社、団体、機関、連合、その他のエンティテの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	State/Province（州または都道府県）：組織が置かれている州または都府県。
T	Title（タイトル）。
UID	User Identifier（ユーザ ID）。
UPN	User Principal Name（ユーザ プリンシパル名）。

- [Primary Field]：ユーザー名に使用する証明書の最初のフィールドを選択します。この値が指定されている場合、[Secondary Field] は無視されます。

- [Secondary Field]：[Primary Field] が指定されていない場合、使用するフィールドを選択します。

- [Certificate Mapping for Multi-Certificate Authentication]：プライマリ認証に使用する証明書の割り当てを管理します。
  - [First Certificate]：マシンが発行した証明書をプライマリ認証に使用する場合は、このオプションをクリックします。
  - [Second Certificate]：クライアントから発行されたユーザー証明書をプライマリ認証に使用する場合は、このオプションをクリックします。

- [Find]：検索文字列として使用する GUI ラベルまたは CLI コマンドを入力し、[Next] または [Previous] をクリックして検索を開始します。

接続プロファイル、2 次認証属性

[Connection Profile] > [Advanced] の下の [Secondary Authentication] を使用すれば、二重認証としても知られる 2 次認証を設定することができます。2 次認証が有効になっている場合は、エンドユーザーがログオンするときに有効な認証クレデンシャルを 2 セット入力する必要があります。証明書のユーザー名の事前入力と 2 次認証を組み合わせて使用できます。このダイアログボックスのフィールドは、1 次認証で設定するフィールドと似ていますが、これらのフィールドは 2 次認証にだけ関連します。

二重認証がイネーブルになっている場合、これらの属性はユーザー名として使用する 1 つ以上のフィールドを証明書から選択します。証明書属性からセカンダリ ユーザー名を設定すると、セキュリティ アプライアンスは、指定された証明書フィールドを、2 次ユーザー名/パスワード認証処理に 2 つ目のユーザー名を使用するよう強制されます。

（注） 証明書のセカンダリ ユーザー名とともに 2 次認証サーバー グループも指定する場合でも、認証処理にはプライマリ ユーザー名だけが使用されます。

- [Secondary Authorization Server Group]：セカンダリ クレデンシャルを抽出する認証サーバー グループを指定します。
  - [Server Group]：セカンダリ サーバー AAA グループとして使用する認証サーバー グループを選択します。デフォルトは none です。SDI サーバー グループはセカンダリ サーバー グループにできません。
  - [Manage]：[Configure AAA Server Group] ダイアログボックスが開きます。
  - [Use LOCAL if Server Group fails]：指定したサーバー グループに障害が発生した場合の LOCAL データベースへのフォールバックを指定します。
  - [Use primary username]：ログイン ダイアログがユーザー名を 1 つだけ要求するよう指定します。

- [Attributes Server]：プライマリ属性サーバーかセカンダリ属性サーバーかを選択します。

（注） この接続プロファイルにも認証サーバーを指定すると、その認証サーバーの設定が優先されます。ASA はセカンダリ認証サーバーを無視します。

- [Session Username Server]：プライマリ セッション ユーザー名サーバーかセカンダリ セッション ユーザー名サーバーかを指定します。

- [Interface-Specific Authorization Server Groups]：指定のインターフェイスに対する認可サーバー グループの割り当てを管理します。
  - [Add or Edit]：[Assign Authentication Server Group to Interfac]e ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスとサーバー グループを指定するとともに、選択したサーバー グループで障害が発生した場合に LOCAL データベースへのフォールバックを許可するかどうかを指定できます。このダイアログボックスの [Manage] ボタンをクリックすると、[Configure AAA Server Groups] ダイアログボックスが開きます。[Interface/Server Group] テーブルに選択内容が表示されます。
  - [Delete]：選択したサーバー グループをテーブルから削除します。確認されず、やり直しもできません。

- [Username Mapping from Certificate]：ユーザー名を抽出するデジタル証明書のフィールドを指定できます。
- [Pre-fill Username from Certificate]：このパネルで指定されている最初のフィールドおよび 2 番目のフィールドから、2 次認証に使用される名前を抽出する場合にオンにします。この属性をオンにする前に、AAA および証明書の認証方式を設定する必要があります。これを行うには、同じウィンドウの [Basic] パネルに戻り、[Method] の横の [Both] をオンにします。
- [Hide username from end user]：2 次認証に使用されるユーザー名を VPN ユーザーに非表示にする場合にオンにします。
- [Fallback when a certificate is unavailable]：この属性は、[Hide username from end user] がオンの場合にのみ使用可能です。証明書が使用不可な場合は、HostScan（現在は Secure Firewall ポスチャと呼ばれています） データを使用して、2 次認証のユーザー名を事前入力します。
- [Password]：2 次認証に使用されるパスワードの取得方式として次のいずれかを選択します。
  - [Prompt]：ユーザーにパスワードを入力するようプロンプトを表示します。
  - [Use Primary]：すべての 2 次認証に 1 次認証のパスワードを再利用します。
  - [Use]：すべての 2 次認証の共通セカンダリ パスワードを入力します。

- [Specify the certificate fields to be used as the username]：ユーザー名として一致する 1 つ以上のフィールドを指定します。セカンダリ ユーザー名/パスワード認証または認可に証明書のユーザー名事前入力機能でこのユーザー名を使用するには、ユーザー名事前入力およびセカンダリ ユーザー名事前入力も設定する必要があります。
  - [Primary Field]：ユーザー名に使用する証明書の最初のフィールドを選択します。この値が指定されている場合、[Secondary Field] は無視されます。
  - [Secondary Field]：[Primary Field] が指定されていない場合、使用するフィールドを選択します。

最初のフィールドおよび 2 番目のフィールドの属性には、次のオプションがあります。

属性	定義
C	Country（国名）：2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
CN	Common Name（一般名）：人、システム、その他のエンティティの名前。セカンダリ属性としては使用できません。
DNQ	ドメイン名修飾子。
EA	E-mail Address（電子メール アドレス）。
GENQ	Generational Qualifier（世代修飾子）。
GN	Given Name（名）。
I	Initials（イニシャル）。
L	Locality（地名）：組織が置かれている市または町。
N	名前
O	Organization（組織）：会社、団体、機関、連合、その他のエンティティの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	State/Province（州または都道府県）：組織が置かれている州または都道府県。
T	Title（タイトル）。
UID	User Identifier（ユーザ ID）。

属性	定義
UPN	User Principal Name（ユーザ プリンシパル名）。

- [Use the entire DN as the username]：完全なサブジェクト DN（RFC1779）を使用して、デジタル証明書から認可クエリーの名前を取得します。
- [Use script to select username]：デジタル証明書からユーザー名を抽出するスクリプトを指定します。デフォルトは [None] です。
  - [Add or Edit]：[Opens the Add or Edit Script Content] ダイアログボックスが開き、証明書のユーザー名のマッピングに使用するスクリプトを定義できます。
  - [Delete]：選択したスクリプトを削除します。確認されず、やり直しもできません。
- [Certificate Mapping for Multi-Certificate Authentication]：セカンダリ認証に使用する証明書の割り当てを管理します。
  - [First Certificate]：マシンが発行した証明書をセカンダリ認証に使用する場合は、このオプションをクリックします。
  - [Second Certificate]：クライアントから発行されたユーザー証明書をセカンダリ認証に使用する場合は、このオプションをクリックします。

セキュアクライアント 接続プロファイル、認可属性

セキュアクライアント 接続プロファイルの [認証（Authorization）] ダイアログボックスを使用すれば、インターフェイス固有の認可サーバーグループを表示、追加、編集、または削除することができます。このダイアログボックスのテーブルの各行には、インターフェイス固有サーバー グループのステータスが表示されます。表示されるのは、インターフェイス名、それに関連付けられたサーバー グループ、および選択したサーバー グループで障害が発生したときにローカル データベースへのフォールバックがイネーブルになっているかどうかです。

このペインのフィールドは、セキュアクライアント、IKEv1、IKEv2、およびクライアントレス SSL 接続プロファイルで共通です。

- [Authorization Server Group]：認可パラメータを記述する認可サーバー グループを指定します。
  - [Server Group]：使用する認可サーバー グループを選択します。デフォルトは none です。
  - [Manage]：[Configure AAA Server Group] ダイアログボックスが開きます。
  - [Users must exist in the authorization database to connect]：ユーザーがこの基準を満たす必要がある場合は、このチェックボックスをオンにします。
- [Interface-specific Authorization Server Groups]：指定のインターフェイスに対する認可サーバー グループの割り当てを管理します。

- [Add or Edit]：[Assign Authentication Server Group to Interfac]e ダイアログボックスが開きます。このダイアログボックスでは、インターフェイスとサーバー グループを指定するとともに、選択したサーバー グループで障害が発生した場合に LOCAL データベースへのフォールバックを許可するかどうかを指定できます。このダイアログボックスの [Manage] ボタンをクリックすると、[Configure AAA Server Groups] ダイアログボックスが開きます。[Interface/Server Group] テーブルに選択内容が表示されます。
- [Delete]：選択したサーバー グループをテーブルから削除します。確認されず、やり直しもできません。

- [Username Mapping from Certificate]：ユーザー名を抽出するデジタル証明書のフィールドを指定できます。
  - [Use script to select username]：デジタル証明書からユーザー名を選択する場合に使用するスクリプト名を指定します。デフォルトは [None] です。証明書フィールドからユーザー名を選択するスクリプトを作成する方法については、を参照してください。
  - [Add or Edit]：[Opens the Add or Edit Script Content] ダイアログボックスが開き、証明書のユーザー名のマッピングに使用するスクリプトを定義できます。
  - [Delete]：選択したスクリプトを削除します。確認されず、やり直しもできません。
  - [Use the entire DN as the username]：証明書の [Distinguished Name] フィールド全体をユーザー名として使用する場合に指定します。
  - [Specify the certificate fields to be used as the username]：ユーザー名に結合する 1 つ以上のフィールドを指定します。
  - [Primary Field]：ユーザー名に使用する証明書の最初のフィールドを選択します。この値が指定されている場合、[Secondary Field] は無視されます。
  - [Secondary Field]：[Primary Field] が指定されていない場合、使用するフィールドを選択します。

- [Find]：検索文字列として使用する GUI ラベルまたは CLI コマンドを入力し、[Next] または [Previous] をクリックして検索を開始します。

セキュアクライアント接続プロファイル、認可、ユーザー名を選択するためのスクリプトの内容の追加

セキュアクライアントの [認証（Authorization）] ペインで [ユーザー名選択にスクリプトを使用（use a script to select username）] を選択し、[追加（Add）] または [編集（Edit）] ボタンをクリックすると、次のフィールドが表示されます。

スクリプトでは、他のマッピング オプションでは表示されない認可用の証明書フィールドを使用できます。

（注） スクリプトを使用した証明書からのユーザー名事前入力でクライアント証明書のユーザー名が見つからない場合、セキュアクライアント およびクライアントレス WebVPN に「不明（Unknown）」と表示されます。

- [Script Name]：スクリプトの名前を指定します。認証および認可のスクリプト名は同じでなければなりません。ここでスクリプトを定義し、CLI は、この機能を実行するために同じスクリプトを使用します。
- [Select script parameters]：スクリプトの属性および内容を指定します。
- [Value for Username]：ユーザー名として使用する一般的な DN 属性のドロップダウン リスト（Subject DN）から属性を選択します。
- [No Filtering]：指定した DN 名全体を使用するよう指定します。
- [Filter by substring]：開始インデックス（一致する最初の文字の文字列内の位置）および終了インデックス（検索する文字列数）を指定します。このオプションを選択する場合、開始インデックスは、空白にはできません。終了インデックスを空白にするとデフォルトは -1 となり、文字列全体が一致するかどうか検索されます。

  たとえば、ホスト/ユーザーの値を含む DN 属性の Common Name（CN）を選択したとします。次の表に、さまざまな戻り値を実現する部分文字列を使用してこの値をフィルタする方法を示します。戻り値は、ユーザー名として実際に事前入力される値です。

  表 *4:* 部分文字列によるフィルタリング

開始インデックス	終了インデックス	戻り値
1	5	host/
6	10	user
6	-1	user

  この表の 3 行目のようにマイナスのインデックスを使用して、文字列の最後から部分文字列の最後まで（この場合は「user」の「r」）カウントするよう指定します。

  部分文字列によるフィルタリングを使用する場合、検索する部分文字列の長さがわかっていることが必要です。次の例では、正規表現照合または Lua 形式のカスタム スクリプトを使用します。

- 例 1：[Regular Expression Matching]：[Regular Expression] フィールドに検索に適用する正規表現を入力します。一般的な正規表現の演算子が適用されます。「Email Address (EA)」DN 値の @ 記号までのすべての文字列をフィルタリングするために正規表現を使用するとします。^[^@]* がこれを実行できる正規表現の 1 つです。この例では、DN 値に user1234@example.com が含まれている場合、正規表現の後の戻り値は user1234 となります。

- 例 2：[Use custom script in LUA format]：検索フィールドを解析するために、LUA プログラム言語で記述されたカスタム スクリプトを指定します。このオプションを選択すると、カスタム LUA スクリプトをフィールドに入力できるようになります。スクリプトは次のようになります。

```
return cert.subject.cn..'/'..cert.subject.l
```

1 つのユーザー名として使用する 2 つの DN フィールド、ユーザー名（cn）および地域（l）を結合し、2 つのフィールド間にスラッシュ（/）文字を挿入します。

次の表に LUA スクリプトで使用可能な属性名と説明を示します。

（注） LUA では、大文字と小文字が区別されます。

表 *5:* 属性名と説明

属性名	説明
cert.subject.c	Country
cert.subject.cn	Common Name
cert.subject.dnq	DN 修飾子
cert.subject.ea	電子メール アドレス
cert.subject.genq	世代修飾子
cert.subject.gn	名
cert.subject.i	イニシャル
cert.subject.l	地名
cert.subject.n	名前
cert.subject.o	マニュアルの構成
cert.subject.ou	組織単位
cert.subject.ser	サブジェクト シリアル番号
cert.subject.sn	姓
cert.subject.sp	州/県
cert.subject.t	Title
cert.subject.uid	ユーザー ID
cert.issuer.c	Country

cert.issuer.cn	Common Name
cert.issuer.dnq	DN 修飾子
cert.issuer.ea	電子メール アドレス
cert.issuer.genq	世代修飾子
cert.issuer.gn	名
cert.issuer.i	イニシャル
cert.issuer.l	地名
cert.issuer.n	名前
cert.issuer.o	マニュアルの構成
cert.issuer.ou	組織単位
cert.issuer.ser	発行元シリアル番号
cert.issuer.sn	姓
cert.issuer.sp	州/県
cert.issuer.t	Title
cert.issuer.uid	ユーザー ID
cert.serialnumber	証明書シリアル番号
cert.subjectaltname.upn	ユーザー プリンシパル名

トンネル グループ スクリプトをアクティブにしているときにエラーが発生し、スクリプトがアクティブにならなかった場合、管理者のコンソールにエラー メッセージが表示されます。

接続プロファイル、アカウンティング

[Connection Profile] > [Advanced] の [Accounting] ペインでは、ASA 全体のアカウンティング オプションを設定します。

- [Accounting Server Group]：アカウンティングに使用するすでに定義済みのサーバー グループを選択します。
- [Manage]：AAA サーバー グループを作成できる [Configure AAA Server Groups] ダイアログ ボックスが開きます。

接続プロファイル、グループ エイリアスとグループ URL

[Connection Profile] > [Advanced] の [GroupAlias/Group Group URL] ダイアログボックスで、リモート ユーザーのログイン時に表示される内容に影響を与える属性を設定します。

接続プロファイルのタブの名前は、セキュアクライアントでは、[グループURL/グループエイリアス（Group URL/Group Alias）] です。

- [Login and Logout (Portal) Page Customization (Clientless SSL VPN only)]：適用する事前設定されたカスタマイズ属性を指定することにより、ユーザー ログイン ページの外観を設定します。デフォルトは DfltCustomization です。新しいカスタマイゼーション オブジェクトを作成するには、[Manage] をクリックします。
- [Enable the display of Radius Reject-Message on the login screen]：認証が拒否されたときにログイン ダイアログボックスに RADIUS-reject メッセージを表示するには、このチェックボックスをオンにします。
- [Enable the display of SecurId message on the login screen]：ログイン ダイアログボックスに SecurID メッセージを表示するには、このチェックボックスをオンにします。
- [Connection Aliases]：接続エイリアスとそのステータス。ログイン時にユーザーが特定の接続（トンネル グループ）を選択できるように接続が設定されている場合は、ユーザーのログイン ページに接続エイリアスが表示されます。エイリアスを追加または削除するには、[Add] または [Delete] ボタンをクリックします。エイリアスを編集するには、テーブルでそのエイリアスをダブルクリックし、エントリを編集します。イネーブルになっているステータスを変更するには、テーブル内のチェックボックスをオンまたはオフにします。
- [Group URLs]：グループ URL とそのステータス。ログイン時にユーザーが特定のグループを選択できるように接続が設定されている場合は、ユーザーのログイン ページにグループ URL が表示されます。URL を追加または削除するには、[Add] または [Delete] ボタンをクリックします。URL を編集（[Edit]）するには、テーブル内の URL をダブルクリックしてエントリを編集します。イネーブルになっているステータスを変更するには、テーブル内のチェックボックスをオンまたはオフにします。

IKEv1 接続プロファイル

IKEv1 接続プロファイルは、L2TP IPsec などのネイティブ VPN クライアントとサードパーティ VPN クライアントの認証ポリシーを定義します。IKEv1 接続プロファイルは、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv1) Connection Profiles] ペインで設定します。

- [Access Interfaces]：IPsec アクセスでイネーブルにするインターフェイスを選択します。デフォルトでは、アクセス方式は何も選択されていません。
- [Connection Profiles]：既存の IPsec 接続の設定済みパラメータを表形式で表示します。[Connections] テーブルには、接続ポリシーを決定するレコードが表示されます。1 つのレ

コードによって、その接続のデフォルト グループ ポリシーが識別されます。レコードにはプロトコル固有の接続パラメータが含まれています。テーブルには、次のカラムがあります。

- [Name]：IPsec IKEv1 接続の名前または IP アドレスを指定します。
- [IPsec Enabled]：IPsec プロトコルがイネーブルになっているかどうかを示します。このプロトコルは、[Add or Edit IPsec Remote Access Connection] の [Basic] ダイアログボックスでイネーブルにします。
- [L2TP/IPsec Enabled]：L2TP/IPsec プロトコルがイネーブルになっているかどうかを示します。このプロトコルは、[Add or Edit IPsec Remote Access Connection] の [Basic] ダイアログボックスでイネーブルにします。
- [Authentication Server Group]：認証を提供できるサーバー グループの名前。
- [Group Policy]：この IPsec 接続のグループ ポリシーの名前を示します。

（注） [Delete]：選択したサーバー グループをテーブルから削除します。確認されず、やり直しもできません。

IPsec リモート アクセス接続プロファイル、[Basic] タブ

[Configuration] > [Remote Access VPN] > [Network （Client） Access] > [IPSec（IKEv1） Connection Profiles] > [Add/Edit] > [Basic] の [Add or Edit IPsec Remote Access Connection Profile Basic] ダイアログボックスを使用すると、L2TP-IPsec を含めて、IPsec IKEv1 VPN 接続用の共通属性を設定できます。

- [Name]：接続プロファイルの名前。
- [IKE Peer Authentication]：IKE ピアを設定します。
  - [Pre-shared key]：接続用の事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Identity Certificate]：ID 証明書が設定され、登録されている場合は、ID 証明書の名前を選択します。[Manage]：[Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、選択した証明書の詳細を追加、編集、削除、エクスポート、表示できます。
- [User Authentication]：ユーザー認証で使用するサーバーの情報を指定します。詳細な認証情報は [Advanced] セクションで設定できます。
  - [Server Group]：ユーザー認証で使用するサーバー グループを選択します。デフォルトは LOCAL です。LOCAL 以外のサーバー グループを選択すると、[Fallback] チェックボックスが選択できるようになります。サーバー グループを追加するには、[Manage] ボタンをクリックします。

- [Fallback]：指定したサーバー グループで障害が発生した場合に、ユーザー認証で LOCAL を使用するかどうかを指定します。

- [Client Address Assignment]：クライアント属性の割り当てに関連する属性を指定します。
  - [DHCP Servers]：使用する DHCP サーバーの IP アドレスを指定します。最大で 10 台までのサーバーをスペースで区切って追加できます。
  - [Client Address Pools]：事前定義済みのアドレス プールを 6 個まで指定します。アドレス プールを定義するには、[Select] ボタンをクリックします。

- [Default Group Policy]：デフォルト グループ ポリシーに関連する属性を指定します。
  - [Group Policy]：この接続で使用するデフォルト グループ ポリシーを選択します。デフォルトは DfltGrpPolicy です。このグループ ポリシーに関連付ける新しいグループ ポリシーを定義するには、[**Manage**] をクリックします。
  - [Enable IPsec protocol] と [Enable L2TP over IPsec protocol]：この接続で使用するプロトコルを選択します。

[Add/Edit Remote Access Connections] > [Advanced] > [General]

このダイアログボックスを使用して、AAA サーバーに渡す前にユーザー名からレルムとグループを除去するかどうかを指定し、パスワード管理パラメータを指定します。

- [Strip the realm from the username before passing it on to the AAA server]：ユーザー名を AAA サーバーに渡す前に、レルム（管理ドメイン）をユーザー名から除去する処理をイネーブルまたはディセーブルにします。認証時にユーザー名のレルム修飾子を削除するには、[Strip Realm] チェックボックスをオンにします。レルム名は、AAA（認証、許可、アカウンティング）のユーザー名に追加できます。レルムに対して有効なデリミタは @ だけです。形式は、username@realm です。たとえば、JaneDoe@example.com です。この [Strip Realm] チェックボックスをオンにすると、認証はユーザー名のみに基づいて行われます。オフにした場合は、username@realm 文字列全体に基づいて認証が行われます。サーバーでデリミタを解析できない場合は、このチェックボックスをオンにする必要があります。

（注） レルムとグループの両方をユーザー名に追加できます。その場合、ASA は、AAA 機能に対してグループ用とレルム用に設定されたパラメータを使用します。このオプションの形式は、ユーザー名[@realm][<# または !>グループ] となります（例：JaneDoe@example.com#VPNGroup）。このオプションを選択した場合は、グループ デリミタとして # または ! を使用する必要があります。これは、@がレルムデリミタとしても使用されている場合、ASA が @ をグループ デリミタと解釈できないからです。

Kerberos レルムは特殊事例です。Kerberos レルムの命名規則として、Kerberos レルムと関連付けられている DNS ドメイン名を大文字で表記します。たとえば、ユーザーが example.com ドメインに存在する場合には、Kerberos レルムを EXAMPLE.COM と表記します。

ASA には、user@grouppolicy のサポートは含まれません。L2TP/IPsec クライアントだけが、user@tunnelgroup を介したトンネル スイッチングをサポートしています。

- [Strip the group from the username before passing it on to the AAA server]：ユーザー名を AAA サーバーに渡す前に、レルム（管理ドメイン）をユーザー名から除去する処理をイネーブルまたはディセーブルにします。認証時にユーザー名のグループ名を削除するには、[Strip Group] チェックボックスをオンにします。このオプションは、[Enable Group Lookup] ボックスをオンにした場合にだけ有効です。デリミタを使用してグループ名をユーザー名に追加し、Group Lookup をイネーブルにすると、ASA は、デリミタの左側にある文字をすべてユーザー名と解釈し、右側の文字をすべてグループ名と解釈します。有効なグループ デリミタは @、#、および ! で、@ が Group Lookup のデフォルトです。ユーザー名<デリミタ>グループの形式でグループをユーザー名に追加します（例：JaneDoe@VPNGroup、JaneDoe#VPNGroup や JaneDoe!VPNGroup）。
- [Password Management]：AAA サーバーからの account-disabled インジケータの上書きに関するパラメータと、ユーザーに対するパスワード期限切れ通知に関するパラメータを設定できます。
  - [Enable notification upon password expiration to allow user to change password]：このチェックボックスをオンにすると、次の 2 つのパラメータが利用できるようになります。パスワードが期限切れになるまでの特定の日数を指定し、その日数だけ前の日のログイン時にユーザーに通知するか、またはパスワードが期限切れになる当日にユーザーに通知するかを選択できます。デフォルトでは、パスワードが期限切れになるより 14 日前にユーザーへの通知を開始し、以後、ユーザーがパスワードを変更するまで毎日通知するように設定されています。範囲は 1 ～ 180 日です。

（注） この処理によってパスワードの期限が切れるまでの日数が変わるのではなく、通知がイネーブルになるだけであるという点に注意してください。このオプションを選択する場合は、日数も指定する必要があります。

いずれの場合でも、変更されずにパスワードが期限切れになったとき、ASA ではユーザーによるパスワードの変更が可能です。現行のパスワードが失効していない場合、ユーザーはそのパスワードを使用してログインし続けることができます。

このパラメータは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバー、LDAP サーバーなどの AAA サーバーで有効です。RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

この機能では、MS-CHAPv2 を使用する必要があります。

IKEv1 クライアント アドレス指定

クライアント アドレス指定の設定はすべてのクライアント接続プロファイルに共通です。詳細については、接続プロファイル、クライアント アドレス指定（123 ページ）を参照してください。

IKEv1 接続プロファイル、認証

このダイアログボックスは、IPsec on Remote Access および Site-to-Site トンネル グループの場合に表示されます。このダイアログボックスでの設定は、ASA 全体に渡ってこの接続プロファイル（トンネル グループ）に適用されます。インターフェイスごとに認証サーバー グループを設定するには、[Advanced] をクリックします。このダイアログボックスでは、次の属性を設定できます。

- [Authentication Server Group]：LOCAL グループ（デフォルト）などの利用可能な認証サーバー グループを一覧表示します。None も選択可能です。None または Local 以外を選択すると、[Use LOCAL if Server Group Fails] チェックボックスが利用できるようになります。
- [Use LOCAL if Server Group fails]：Authentication Server Group 属性によって指定されたグループで障害が発生した場合に、LOCAL データベースへのフォールバックをイネーブルまたはディセーブルにします。

  [Enable Group Lookup] ボックスをオフにすると、ユーザー名のみに基づく認証を設定できます。[Enable Group Lookup] ボックスと [Strip Group] の両方をオンにすると、AAA サーバーでグループ名が付加されたユーザーのデータベースを維持しながら、同時にユーザー名のみに基づいてユーザーを認証することができます。

IKEv1 接続プロファイル、認可

認可の設定はすべてのクライアント接続プロファイルに共通です。詳細については、セキュアクライアント接続プロファイル、認証属性 （126 ページ）を参照してください。

IKEv1 接続プロファイル、アカウンティング

アカウンティングの設定はすべてのクライアント接続プロファイルに共通です。詳細については、接続プロファイル、アカウンティング （135 ページ）を参照してください。

IKEv1 接続プロファイル、IPsec

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec(IKEv1) Connection Profiles] > [Add/Edi] > [Advanced] > [IPsec]

- [Send certificate chain]：証明書チェーン全体の送信をイネーブルまたはディセーブルにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。
- [IKE Peer ID Validation]：IKE ピア ID 検証を無視するか、必須とするか、あるいは証明書によってサポートされている場合にだけチェックするかを選択します。
- [IKE Keep Alive]：ISAKMP キープアライブ モニタリングをイネーブルにして設定します。
  - [Disable Keep Alives]：ISAKMP キープアライブをイネーブルまたはディセーブルにします。
  - [Monitor Keep Alives]：ISAKMP キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、[Confidence Interval] フィールドと [Retry Interval] フィールドが利用できるようになります。
  - [Confidence Interval]：ISAKMP キープアライブの信頼間隔を指定します。これは、ASA がキープアライブ モニタリングを開始するまでに、ピアがアイドル状態を継続できる秒数です。最小 10 秒、最大 300 秒です。リモート アクセス グループのデフォルトは 300 秒です。
  - [Retry Interval]：ISAKMP キープアライブのリトライ間の待機秒数を指定します。デフォルト値は 2 秒です。
  - [Head end will never initiate keepalive monitoring]：中央サイトの ASA がキープアライブ モニタリングを開始しないように指定します。

IKEv1 接続プロファイル、IPsec、IKE 認証

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec(IKEv1) Connection Profiles] > [Add/Edi] > [Advanced] > [IPsec] > [IKE Authentication]

- [Default Mode]：上記の none、xauth、または hybrid からデフォルトの認証モードを選択できます。

- [Interface-Specific Mode]：認証モードをインターフェイスごとに指定します。
  - [Add/Edit/Delete]：[Interface/Authentication Modes] テーブルに対して、選択したインターフェイスと認証モードのペアを追加/編集/削除します。
  - [Interface]：名前付きインターフェイスを選択します。 デフォルトのインターフェイスは inside と outside ですが、別のインターフェイス名を設定した場合には、その名前がリストに表示されます。
  - [Authentication Mode]：上記の none、xauth、または hybrid から認証モードを選択できます。

IKEv1 接続プロファイル、IPsec、クライアント ソフトウェアの更新

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec(IKEv1) Connection Profiles] > [Add/Edi] > [Advanced] > [IPsec] > [Client Software Update]

[Client VPN Software Update Table]：インストールされている各クライアント VPN ソフトウェアパッケージについて、クライアントタイプ、VPN クライアントのリビジョン、およびイメージ URL を一覧表示します。クライアント タイプごとに、許可されるクライアント ソフトウェア リビジョンと、必要に応じて、ソフトウェア アップグレードをダウンロードする URL または IP アドレスを指定できます。クライアント アップデート メカニズム（Client Update ダイアログボックスに詳細説明があります）は、この情報を使用して、各 VPN クライアントが適切なリビジョン レベルで実行されているかどうか、適切であれば、通知メッセージとアップデートメカニズムを、旧式のソフトウェアを実行しているクライアントに提供するかどうかを判断します。

- [Client Type]：VPN クライアント タイプを識別します。
- [VPN Client Revisions]：許容される VPN クライアントのリビジョン レベルを指定します。
- [Location URL]：適切な VPN クライアント ソフトウェア イメージをダウンロードできる URL または IP アドレスを指定します。ダイアログボックスベースの VPN クライアントの場合、URL は http:// または https:// という形式です。クライアント モードの ASA 5505 では、URL は tftp:// 形式である必要があります。

IKEv1 接続プロファイル、PPP

この IKEv1 接続プロファイルを使用して PPP 接続で許可される認証プロトコルを設定するには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv1) Connection Profiles] > [Add/Edit] > [Advanced] > [PPP] を開きます。

このダイアログボックスは、IPsec IKEv1 リモートアクセス接続プロファイルにだけ適用されます。

- [CHAP]：PPP 接続で CHAP プロトコルの使用をイネーブルにします。
- [MS-CHAP-V1]：PPP 接続で MS-CHAP-V1 プロトコルの使用をイネーブルにします。

- [MS-CHAP-V2]：PPP 接続で MS-CHAP-V2 プロトコルの使用をイネーブルにします。
- [PAP]：PPP 接続で PAP プロトコルの使用をイネーブルにします。
- [EAP-PROXY]：PPP 接続で EAP-PROXY プロトコルの使用をイネーブルにします。EAP は、Extensible Authentication protocol（拡張認証プロトコル）を意味します。

IKEv2 接続プロファイル

IKEv2 接続プロファイルでは、Cisco Secure Client の AnyConnect VPN モジュールに対する EAP、証明書ベース、および事前共有キー ベースの認証を定義します。ASDM の設定パネルは、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPsec (IKEv2) Connection Profiles] です。

- [Access Interfaces]：IPsec アクセスでイネーブルにするインターフェイスを選択します。デフォルトでは、アクセス方式は何も選択されていません。
- [Bypass interface access lists for inbound VPN sessions]：着信 VPN セッションのインターフェイス アクセス リストをバイパスするには、このチェックボックスをオンにします。グループ ポリシーおよびユーザー ポリシーのアクセス リストはすべてのトラフィックに常に適用されます。
- [Connection Profiles]：既存の IPsec 接続の設定済みパラメータを表形式で表示します。[Connection Profiles] テーブルには、接続ポリシーを決定するレコードが表示されます。1 つのレコードによって、その接続のデフォルト グループ ポリシーが識別されます。レコードにはプロトコル固有の接続パラメータが含まれています。テーブルには、次のカラムがあります。
  - [Name]：IPsec 接続の名前または IP アドレスを指定します。
  - [IKEv2 Enabled]：オンになっている場合は、IKEv2 プロトコルがイネーブルになっていることを示します。
  - [Authentication Server Group]：認証に使用するサーバー グループの名前を指定します。
  - [Group Policy]：この IPsec 接続のグループ ポリシーの名前を示します。

（注） [Delete]：選択したサーバー グループをテーブルから削除します。確認されず、やり直しもできません。

IPsec IKEv2 接続プロファイル：[Basic] タブ

[Add or Edit IPsec Remote Access Connection Profile Basic] ダイアログボックスでは、IPsec IKEv2 接続の共通属性を設定します。

- [Name]：接続名を特定します。
- [IKE Peer Authentication]：IKE ピアを設定します。
  - [Pre-shared key]：接続用の事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Enable Certificate Authentication]：オンにすると、認証に証明書を使用できます。
  - [Enable peer authentication using EAP]：オンにすると、認証に EAP を使用できます。このチェックボックスをオンにした場合は、ローカル認証に証明書を使用する必要があります。
  - [Send an EAP identity request to the client]：リモート アクセス VPN クライアントに EAP 認証要求を送信できます。
- [ポスト量子キー（Post Quantum Key）]：ポスト量子事前共有キー（PPK）を指定するには、このチェックボックスをオンにします。PPK は 256 ビット、64 文字の 16 進文字列で、量子コンピュータ攻撃からセッションを保護します。
  - [ポスト量子キー識別子（Post Quantum Key Identity）]：PPK の ID を指定します。
- [Mobike RRC]：Mobike RRC を有効/無効にします。
  - [Enable Return Routability Check for mobike]：Mobike が有効になっている IKE/IPSEC セキュリティ アソシエーションにおけるダイナミック IP アドレスの変更をチェックする Return Routability を有効/無効にします。
- [User Authentication]：ユーザー認証で使用するサーバーの情報を指定します。詳細な認証情報は [Advanced] セクションで設定できます。
  - [Server Group]：ユーザー認証で使用するサーバー グループを選択します。デフォルトは LOCAL です。LOCAL 以外のサーバー グループを選択すると、[Fallback] チェックボックスが選択できるようになります。
  - [Manage]：[Configure AAA Server Group] ダイアログボックスが開きます。
  - [Fallback]：指定したサーバー グループで障害が発生した場合に、ユーザー認証で LOCAL を使用するかどうかを指定します。
- [Client Address Assignment]：クライアント属性の割り当てに関連する属性を指定します。
  - [DHCP Servers]：使用する DHCP サーバーの IP アドレスを指定します。最大で 10 台までのサーバーをスペースで区切って追加できます。
  - [Client Address Pools]：事前定義済みのアドレス プールを 6 個まで指定します。[Select] をクリックすると、[Address Pools] ダイアログボックスが開きます。
- [Default Group Policy]：デフォルト グループ ポリシーに関連する属性を指定します。
  - [Group Policy]：この接続で使用するデフォルト グループ ポリシーを選択します。デフォルトは DfltGrpPolicy です。

- [Manage]：[Configure Group Policies] ダイアログボックスが開きます。このダイアログボックスでは、グループ ポリシーを追加、編集、または削除できます。
- [Client Protocols]：この接続で使用するプロトコルを選択します。デフォルトでは、IPsec と L2TP over IPsec の両方が選択されています。
- [Enable IKEv2 Protocol]：リモート アクセス接続プロファイルで使用する IKEv2 プロトコルをイネーブルにします。これは、先ほど選択したグループ ポリシーの属性です。

IPsec リモート アクセス接続プロファイル：[Advanced] > [IPsec] タブ

IPsec（IKEv2）接続プロファイルの [IPsec] テーブルに次のフィールドがあります。

- [Send certificate chain]：証明書チェーン全体の送信をイネーブルまたはディセーブルにする場合にオンにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。
- [IKE Peer ID Validation]：IKE ピア ID の有効性をチェックしないか、必須とするか、あるいは証明書によってサポートされている場合にチェックするかをドロップダウン リストから選択します。

IPsec または SSL VPN 接続プロファイルへの証明書のマッピング

ASA は、クライアント証明書認証による IPsec 接続要求を受信すると、設定されているポリシーに従って接続に接続プロファイルを割り当てます。そのポリシーは、設定したルールを使用でき、証明書 OU フィールド、IKE ID（ホスト名、IP アドレス、キー ID など）、ピア IP アドレス、またはデフォルト接続プロファイルを使用できます。SSL 接続の場合、ASA は設定されているルールだけを使用します。

ルールを使用する IPsec 接続または SSL 接続の場合、ASA は一致するものが見つかるまでルールに対して証明書の属性を評価します。一致するルールが見つかると、そのルールに関連付けられた接続プロファイルを接続に割り当てます。一致するルールが見つからない場合、ASA は、デフォルトの接続プロファイル（IPsec の場合は DefaultRAGroup、SSL VPN の場合は DefaultWEBVPNGroup）を接続に割り当てます。ユーザーは、接続プロファイルがイネーブルになっていれば、ポータル ページに表示されるドロップダウン リストからその接続プロファイルを選択できます。この接続プロファイルの接続を 1 回試みた場合の結果は、証明書が有効かどうか、そして接続プロファイルの認証設定によって異なります。

ポリシーに一致する証明書グループは、証明書ユーザーの権限グループを特定するために使用する方法を定義します。

[Policy] ペインで照合するポリシーを設定します。照合するルールを選択する場合は、[Rules] ペインに移動してルールを指定します。

証明書/接続プロファイル マップ、ポリシー

IPsec 接続において、ポリシーに一致する証明書グループは、証明書ユーザーの権限グループを特定するために使用する方法を定義します。これらのポリシーの設定項目は、[Configuration] > [Remote Access VPN] > [Network （Client） Access] > [Advanced] > [IPsec] > [Certificate to Connection Profile Maps] > [Policy] で設定します。

- [Use the configured rules to match a certificate to a group]：[Rules] で定義したルールを使用できます。
- [Use the certificate OU field to determine the group]：組織ユニット フィールドを使用して、証明書に一致するグループを決定できます。この設定は、デフォルトでオンになっています。
- [Use the IKE identity to determine the group]：[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [IKE Parameters] で定義した ID を使用できます。IKE ID は、IP アドレス、キー ID により、または自動で指定されます。
- [Use the peer IP address to determine the group]：ピアの IP アドレスを使用できます。この設定は、デフォルトでオンになっています。
- [Default to Connection Profile]：どの方法にも一致しなかった場合に使用する、証明書ユーザーのデフォルト グループを選択できます。この設定は、デフォルトでオンになっています。[Default] にあるデフォルト グループをクリックして、リストをグループ化します。設定にはグループが必要です。リスト内にグループがない場合は、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] でグループを定義する必要があります。

証明書/接続プロファイル マップのルール

IPsec 接続において、ポリシーに一致する証明書グループは、証明書ユーザーの権限グループを特定するために使用する方法を定義します。プロファイルマップは、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Certificate to Connection Profile Maps] > [Rules] で作成します。

このペインには、証明書/接続プロファイルマップのリストとマッピング基準が表示されます。

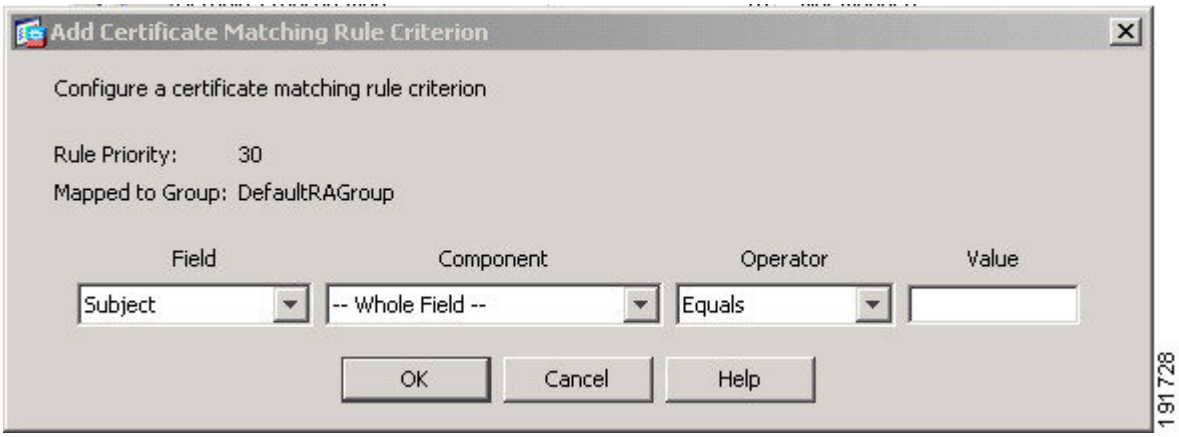
証明書/接続プロファイル マップ、証明書照合ルール基準の追加

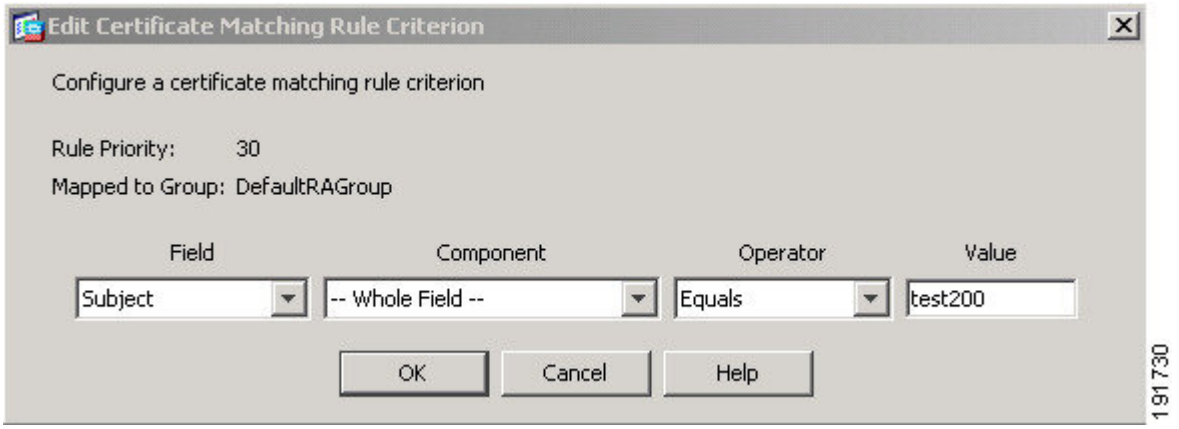
接続プロファイルをマッピング ルールにマップするマップ プロファイルを作成します。

- [Map]：次のいずれかを選択します。
  - [Existing]：ルールを含めるマップの名前を選択します。
  - [New]：ルールの新しいマップ名を入力します。

- [Priority]：10 進数を入力して、接続要求を受け取ったときに ASA がマップを評価する順序を指定します。定義されている最初のルールのデフォルト プライオリティは 10 です。ASA は各接続を評価する際に、優先順位番号が最も小さいマップから評価します。
- [Mapped to Connection Profile]：以前は「トンネル グループ」と呼んでいた接続プロファイルを選択して、このルールにマッピングします。

次の項で説明するマップへのルール基準の割り当てを行わない場合、ASA はそのマップ エントリを無視します。





証明書照合ルール基準の追加/編集

このダイアログボックスは、接続プロファイルにマッピング可能な証明書照合ルール基準を設定するために使用します。

- [Rule Priority]：（表示専用）接続要求を受け取ったときに ASA がマップを評価する順序。ASA は各接続を評価する際に、優先順位番号が最も小さいマップから評価します。
- [Mapped to Group]：（表示専用）ルールが割り当てられている接続プロファイル。
- [Field]：ドロップダウン リストから、評価する証明書の部分を選択します。

- [Subject]：証明書を使用するユーザーまたはシステム。CA のルート証明書の場合は、Subject と Issuer が同じです。
- [Alternative Subject]：サブジェクト代替名拡張により、追加する ID を証明書のサブジェクトにバインドできます。
- [Issuer]：証明書を発行した CA または他のエンティティ（管轄元）。
- [Extended Key Usage]：一致の候補として選択できる、より高度な基準を提供するクライアント証明書の拡張。

- [Component]：（[Subject of Issuer] が選択されている場合にのみ適用されます）。ルールで使用する識別名コンポーネントを次の中から選択します。

DN フィールド	定義
Whole Field	DN 全体。
Country（C）	2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
Common Name（CN）	ユーザー、システム、その他のエンティティの名前。これは、ID 階層の最下位（最も固有性の高い）レベルです。
DN Qualifier（DNQ）	特定の DN 属性。
E-mail Address（EA）	証明書を所有するユーザー、システム、またはエンティティの電子メール アドレス。
Generational Qualifier（GENQ）	Jr.、Sr.、または III などの世代修飾子。
Given Name（GN）	証明書所有者の名前（名）。
Initials（I）	証明書所有者の姓と名の最初の文字。
Locality（L）	組織が所在する市町村。
Name（N）	証明書所有者の名前。
Organization（O）	会社、団体、機関、協会、その他のエンティティの名前。
Organizational Unit（OU）	組織内のサブグループ。
Serial Number（SER）	証明書のシリアル番号。
Surname（SN）	証明書所有者の姓。
State/Province（S/P）	組織が所在する州や県。
Title（T）	証明書所有者の役職（Dr. など）。

DN フィールド	定義
User ID（UID）	証明書所有者の ID 番号。
Unstructured Name（UNAME）	unstructuredName 属性タイプは、サブジェクトの名前を非構造化 ASCII 文字列として指定します。
IP Address（IP）	IP アドレス フィールド。

- [Operator]：ルールで使用する演算子を選択します。
  - [Equals]：認定者名フィールドが値に完全一致する必要があります。
  - [Contains]：認定者名フィールドに値が含まれている必要があります。
  - [Does Not Equal]：認定者名フィールドが値と一致しないようにします。
  - [Does Not Contain]：認定者名フィールドに値が含まれないようにします。
- [Value]：255 文字までの範囲で演算子のオブジェクトを指定します。Extended Key Usage 機能の場合、ドロップダウン リストで事前定義された値のいずれかを選択するか、他の拡張の OID を入力できます。事前定義された値は次のとおりです。

選択項目	キー使用の目的	OID 文字列
clientauth	**クライアント認証**	**1.3.6.1.5.5.7.3.2**
codesigning	コード署名	1.3.6.1.5.5.7.3.3
emailprotection	安全な電子メール保護	1.3.6.1.5.5.7.3.4
ocspsigning	OCSP 署名	1.3.6.1.5.5.7.3.9
serverauth	サーバー認証	1.3.6.1.5.5.7.3.1
timestamping	タイム スタンプ	1.3.6.1.5.5.7.3.8

Site-to-Site 接続プロファイル

[Connection Profiles] ダイアログボックスには、現在設定されている Site-to-Site 接続プロファイル（トンネル グループ）の属性が表示されます。このダイアログボックスを使用すれば、接続プロファイル名を解析するときに使用するデリミタを選択したり、接続プロファイルを追加、変更、または削除したりすることもできます。

ASA では、IPv4 または IPv6 の IPsec LAN-to-LAN VPN 接続は IKEv1 または IKEv2 を使用してサポートされ、内部ネットワークと外部ネットワークは内部および外部 IP ヘッダーを使用してサポートされます。

[Site to Site Connection Profile] ペインのフィールド

- [Access Interfaces]：インターフェイスのリモート ピア デバイスによってアクセスできるデバイス インターフェイスのテーブルが表示されます。
  - [Interface]：アクセスをイネーブルまたはディセーブルにするデバイス インターフェイス。
  - [Allow IKEv1 Access]：ピア デバイスによる IPsec IKEv1 アクセスをイネーブルにする場合にオンにします。
  - [Allow IKEv2 Access]：ピア デバイスによる IPsec IKEv2 アクセスをイネーブルにする場合にオンにします。
- [Connection Profiles]：プロファイルを追加、編集、または削除できる接続プロファイルのテーブルを表示します。
  - [Add]：[Add IPsec Site-to-Site connection profile] ダイアログボックスが開きます。
  - [Edit]：[Edit IPsec Site-to-Site connection profile] ダイアログボックスが開きます。
  - [Delete]：選択した接続プロファイルを削除します。確認されず、やり直しもできません。
  - [Name]：接続プロファイルの名前。
  - [Interface]：接続プロファイルがイネーブルになっているインターフェイス。
  - [Local Network]：ローカル ネットワークの IP アドレスを指定します。
  - [Remote Network]：リモート ネットワークの IP アドレスを指定します。
  - [IKEv1 Enabled]：接続プロファイルに対してイネーブルになっている IKEv1 を表示します。
  - [IKEv2 Enabled]：接続プロファイルに対してイネーブルになっている IKEv2 を表示します。
  - [Group Policy]：接続プロファイルのデフォルト グループ ポリシーを表示します。

Site-to-Site 接続プロファイルの追加または編集

[Add or Edit IPsec Site-to-Site Connection] ダイアログボックスでは、IPsec Site-to-Site 接続を作成または変更できます。このダイアログボックスでは、IP アドレス（IPv4 または IPv6）の指定、接続名の指定、インターフェイスの選択、IKEv1 ピアおよび IKEv2 ピアとユーザー認証パラメータの指定、保護されたネットワークの指定、および暗号化アルゴリズムの指定を行うことができます。

（注） サイト間 VPN 接続プロファイルを作成する場合、接続プロファイルを開き、構成を変更せずにキャンセルします。[Apply] ボタンが強調表示されている場合は、変更を破棄します。

2 つのピアの内部および外部ネットワークが IPv4 の場合（内部および外部インターフェイス上のアドレスが IPv4 の場合）、ASA では、シスコまたはサードパーティのピアとの LAN-to-LAN VPN 接続がサポートされます。

IPv4 アドレッシングと IPv6 アドレッシングが混在した、またはすべて IPv6 アドレッシングを使用する LAN-to-LAN 接続については、両方のピアが ASA の場合、および両方の内部ネットワークのアドレッシング方式が一致している場合（両方が IPv4 または両方が IPv6 の場合）は、セキュリティアプライアンスで VPN トンネルがサポートされます。

具体的には、両方のピアが ASA の場合、次のトポロジがサポートされます。

- ASA の内部ネットワークが IPv4 で、外部ネットワークが IPv6（内部インターフェイス上のアドレスが IPv4 で、外部インターフェイス上のアドレスが IPv6）
- ASA の内部ネットワークが IPv6 で、外部ネットワークが IPv4（内部インターフェイス上のアドレスが IPv6 で、外部インターフェイス上のアドレスが IPv4）
- ASA の内部ネットワークが IPv6 で、外部ネットワークが IPv6（内部および外部インターフェイス上のアドレスが IPv6）

[Basic] パネルのフィールド

- [Peer IP Address]：IP アドレス（IPv4 または IPv6）を指定し、そのアドレスをスタティックにするかどうかを指定できます。
- [Connection Name]：この接続プロファイルに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示専用です。接続名が、[Peer IP Address] フィールドで指定される IP アドレスと同じになるように指定できます。
- [Interface]：この接続で使用するインターフェイスを選択します。
- [Protected Networks]：この接続で保護されているローカルおよびリモート ネットワークを選択または指定します。
  - [IP Address Type]：アドレスが IPv4 アドレスまたは IPv6 アドレスのいずれであるかを指定します。
  - [Local Network]：ローカル ネットワークの IP アドレスを指定します。
  - [...]：[Browse Local Network] ダイアログボックスが開きます。このダイアログボックスでは、ローカル ネットワークを選択できます。
  - [Remote Network]：リモート ネットワークの IP アドレスを指定します。
- [IPsec Enabling]：この接続プロファイルのグループ ポリシー、およびそのポリシーで指定したキー交換プロトコルを指定します。

- [Group Policy Name]：この接続プロファイルに関連付けられているグループ ポリシーを指定します。
- [Manage]：[Browse Remote Network] ダイアログボックスが開きます。このダイアログボックスでは、リモート ネットワークを選択できます。
- [Enable IKEv1]：指定したグループ ポリシーでキー交換プロトコル IKEv1 をイネーブルにします。
- [Enable IKEv2]：指定したグループ ポリシーでキー交換プロトコル IKEv2 をイネーブルにします。

- [IKEv1 Settings] タブ：IKEv1 の次の認証設定および暗号化設定を指定します。
  - [Pre-shared Key]：トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Device Certificate]：認証で使用する ID 証明書がある場合は、その名前を指定します。
  - [Manage]：[Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
  - [IKE Policy]：IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
  - [Manage]：[Configure IKEv1 Proposals] ダイアログボックスが開きます。
  - [IPsec Proposal]：IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。

- [IKEv2 Settings] タブ：IKEv2 の次の認証設定および暗号化設定を指定します。
  - [Local Pre-shared Key]：トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Local Device Certificate]：認証で使用する ID 証明書がある場合は、その名前を指定します。
  - [Manage]：[Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
  - [Remote Peer Pre-shared Key]：トンネル グループのリモート ピア事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [リモート ピア ポスト量子キー（Remote Peer Post Quantum Key）]：IKEv2 セッション用のポスト量子事前共有キー（PPK）を指定するには、このチェックボックスをオンにします。PPK は 256 ビット、64 文字の 16 進文字列で、量子コンピュータ攻撃から IKEv2 セッションを保護します。IKEv2 セッションでは、事前共有キー ベースの認証とともに PPK を使用できます。

- [パスワードの表示（Show Password）]：このチェックボックスをオンにすると、PPK キーが表示されます。
- [リモートピアポスト量子キーID（Remote Peer Post Quantum Key Identity）]：PPK の ID を指定します。
- [Remote Peer Certificate Authentication]：この接続プロファイルの IKEv2 接続用の証明書認証を許可するには、[Allowed] をオンにします。
- [Manage]：証明書の表示や新規証明書の追加を実行できる [Manage CA Certificates] ダイアログが開きます。
- ダイナミック VTI の場合：
  - [IKEv2ルートですべてを許可（IKEv2 Route Accept Any）]：ASA が IKEv2 交換中に受信したトンネルインターフェイスの IP アドレスを受け入れるには、このチェックボックスをオンにします。デフォルトで、このオプションは有効になっています。
  - [IKEv2ルートでのインターフェイスの設定（IKEv2 Route Set Interface）]：IKEv2 交換中にトンネルインターフェイスの IP アドレスを送信するには、このチェックボックスをオンにします。このオプションでは、ピアのトンネルインターフェイスへのダイナミックルートを構成し、トンネルを介してハブとスポークの間でダイナミック ルーティング プロトコルを実行します。
- [RSA署名ハッシュを有効にする（Enable RSA Signature Hash）]：RSA 署名ハッシュを有効にするには、このチェックボックスをオンにします。RSA は暗号化の一種です。
- [IKE Policy]：IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
- [Manage]：[Configure IKEv1 Proposals] ダイアログボックスが開きます。
- [IPsec Proposal]：IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
- [Select]：IKEv2 接続の接続プロファイルにプロポーザルを割り当てることができる [Select IPsec Proposals (Transform Sets)] ダイアログボックスが開きます。

この接続プロファイルには、次のパラメータもあります。

- [詳細（Advanced）] > [クリプトマップエントリ（Crypto Map Entry）]。詳細については、Site-to-Site 接続プロファイル、暗号マップ エントリ （157 ページ）を参照してください。
- [詳細（Advanced）] > [トンネルグループ（Tunnel Group）]。詳細については、「サイト間接続プロファイルのトンネルグループ （158 ページ）」を参照してください。

Site-to-Site トンネル グループ

ASDM ペインの [設定（Configuration）] > [サイト間 VPN（Site-to-Site VPN）] > [詳細（Advanced）] > [トンネルグループ（Tunnel Groups）] では、IPsec サイト間接続プロファイル（トンネルグループ）の属性を指定します。また、IKE ピアとユーザー認証パラメータの選択、IKE キープアライブ モニタリングの設定、およびデフォルト グループ ポリシーの選択も行うことができます。

- [Name]：このトンネル グループに割り当てられた名前を指定します。Edit 機能の場合、このフィールドは表示専用です。
- [IKE Authentication]：IKE ピアの認証で使用する事前共有キーおよび ID 証明書パラメータを指定します。
  - [Pre-shared Key]：トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Identity Certificate]：認証で使用する ID 証明書がある場合は、その名前を指定します。
  - [Manage]：[Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
  - [IKE Peer ID Validation]：IKE ピア ID の有効性をチェックするかどうかを指定します。デフォルトは Required です。
- [IPsec Enabling]：この接続プロファイルのグループ ポリシー、およびそのポリシーで指定したキー交換プロトコルを指定します。
  - [Group Policy Name]：この接続プロファイルに関連付けられているグループ ポリシーを指定します。
  - [Manage]：[Browse Remote Network] ダイアログボックスが開きます。このダイアログボックスでは、リモート ネットワークを選択できます。
  - [Enable IKEv1]：指定したグループ ポリシーでキー交換プロトコル IKEv1 をイネーブルにします。
  - [Enable IKEv2]：指定したグループ ポリシーでキー交換プロトコル IKEv2 をイネーブルにします。
- [IKEv1 Settings] タブ：IKEv1 の次の認証設定および暗号化設定を指定します。
  - [Pre-shared Key]：トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Device Certificate]：認証で使用する ID 証明書がある場合は、その名前を指定します。

（注） 一部のプロファイルは、エンドポイントがリモートアクセスまたはLAN-かどうかを判別できないことがあります。トンネル グループを判別できない場合、デフォルトで

```
tunnel-group-map default-group <tunnel-group-name>
```

に設定されます（デフォルト値は *DefaultRAGroup* です）。

- [Manage]：[Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
- [IKE Policy]：IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
- [Manage]：[Configure IKEv1 Proposals] ダイアログボックスが開きます。
- [IPsec Proposal]：IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。

- [IKEv2 Settings] タブ：IKEv2 の次の認証設定および暗号化設定を指定します。
  - [Local Pre-shared Key]：トンネル グループの事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Local Device Certificate]：認証で使用する ID 証明書がある場合は、その名前を指定します。
  - [Manage]：[Manage Identity Certificates] ダイアログボックスが開きます。このダイアログボックスでは、すでに設定されている証明書の表示、新しい証明書の追加、証明書の詳細の表示、および証明書の編集または削除を行うことができます。
  - [Remote Peer Pre-shared Key]：トンネル グループのリモート ピア事前共有キーの値を指定します。事前共有キーの最大長は 128 文字です。
  - [Remote Peer Certificate Authentication]：この接続プロファイルの IKEv2 接続用の証明書認証を許可するには、[Allowed] をオンにします。
  - [Manage]：証明書の表示や新規証明書の追加を実行できる [Manage CA Certificates] ダイアログが開きます。
  - [IKE Policy]：IKE プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。
  - [Manage]：[Configure IKEv1 Proposals] ダイアログボックスが開きます。
  - [IPsec Proposal]：IPsec IKEv1 プロポーザルで使用する暗号化アルゴリズムを 1 つ以上指定します。

- [Select]：IKEv2 接続の接続プロファイルにプロポーザルを割り当てることができる [Select IPsec Proposals (Transform Sets)] ダイアログボックスが開きます。
- [リモート ピア ポスト量子キー（Remote Peer Post Quantum Key）]：IKEv2 セッション用のポスト量子事前共有キー（PPK）を指定するには、このチェックボックスをオンにします。PPK は 256 ビット、64 文字の 16 進文字列で、量子コンピュータ攻撃から IKEv2 セッションを保護します。IKEv2 セッションでは、事前共有キー ベースの認証とともに PPK を使用できます。
- [パスワードの表示（Show Password）]：このチェックボックスをオンにすると、PPK キーが表示されます。
- [リモートピアポスト量子キーID（Remote Peer Post Quantum Key Identity）]：PPK の ID を指定します。
- ダイナミック VTI の場合：
  - [IKEv2ルートですべてを許可（IKEv2 Route Accept Any）]：ASA が IKEv2 交換中に受信したトンネルインターフェイスの IP アドレスを受け入れるには、このチェックボックスをオンにします。デフォルトで、このオプションは有効になっています。
  - [IKEv2ルートでのインターフェイスの設定（IKEv2 Route Set Interface）]：IKEv2 交換中にトンネルインターフェイスの IP アドレスを送信するには、このチェックボックスをオンにします。このオプションでは、ピアのトンネルインターフェイスへのダイナミックルートを構成し、トンネルを介してハブとスポークの間でダイナミック ルーティング プロトコルを実行します。

- [IKE Keepalive]：IKE キープアライブ モニタリングをイネーブルにし、設定を行います。次の属性の中から 1 つだけ選択できます。
  - [Disable Keep Alives]：IKE キープアライブをイネーブルまたはディセーブルにします。
  - [Monitor Keep Alives]：IKE キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、[Confidence Interval] フィールドと [Retry Interval] フィールドが利用できるようになります。
  - [Confidence Interval]：IKE キープアライブの信頼間隔を指定します。これは、ASA がキープアライブ モニタリングを開始するまでに、ピアがアイドル状態を継続できる秒数です。最小 10 秒、最大 300 秒です。リモート アクセス グループのデフォルトは 10 秒です。
  - [Retry Interval]：IKE キープアライブのリトライ間の待機秒数を指定します。デフォルト値は 2 秒です。
  - [Head end will never initiate keepalive monitoring]：中央サイトの ASA がキープアライブ モニタリングを開始しないように指定します。

- [ダイナミックVTIの場合（For Dynamic VTI）]：トンネルグループに仮想テンプレートを適用します。
  - [仮想テンプレート（Virtual Template）]：ドロップダウンリストから仮想テンプレートを選択します。同じ仮想テンプレートを複数のトンネルグループに適用することができます。ASA は、仮想テンプレートを使用して、VPN セッションごとに個別の仮想アクセスインターフェイスを作成します。

    仮想テンプレートの設定を正常に完了するには、次の DVTI インターフェイスパラメータを設定する必要があります（[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [追加（Add）] > [DVTIインターフェイスの追加（Add DVTI Interface）]。
    - DVTI インターフェイス名
    - [Enable Interface]
    - IPSec（IPv4 または IPv6）のトンネルモード IP オーバーレイのイネーブル化
    - IPsec プロファイルによるトンネル保護

Site-to-Site 接続プロファイル、暗号マップ エントリ

このダイアログボックスでは、現在の Site-to-Site 接続プロファイルの暗号パラメータを指定します。

- [Priority]：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）。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。
- [Perfect Forward Secrecy]：特定の IPsec SA のキーが他の秘密情報（他のキーなど）から導出されたものでないことを保証します。PFS により、攻撃者がキーを突破できたとしても、そのキーから他のキーを導出できないようにします。PFS をイネーブルにすると、Diffie-Hellman Group リストがアクティブになります。
  - [Diffie-Hellman Group]：2 つの IPsec ピアが、相互に共有秘密情報を転送することなく共有秘密情報を導出するために使用する ID。Group 1（768 ビット）、Group 2（1024 ビット）、および Group 5（1536 ビット）の中から選択します。
- [Enable NAT-T]：このポリシーの NAT Traversal（NAT-T）をイネーブルにします。これにより IPsec ピアは、NAT デバイスを介してリモート アクセスと LAN-to-LAN の両方の接続を確立できます。
- [Enable Reverse Route Injection]：リモート トンネルのエンドポイントによって保護されているネットワークとホストのルーティング プロセスに、スタティック ルートが自動的に挿入されるようにすることができます。

- [Security Association Lifetime]：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 Crypto Map Entry Parameters]：ピア IP アドレスが Static に指定されている場合に、次の追加パラメータを指定します。
  - [Connection Type]：許可されるネゴシエーションを、bidirectional、answer-only、または originate-only として指定します。
  - [Send ID Cert. Chain]：証明書チェーン全体の送信をイネーブルにします。
  - [IKE Negotiation Mode]：SA、Main、または Aggressive の中から、セットアップでキー情報を交換するとき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も設定されます。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]：2 つの IPsec ピアが、相互に共有秘密情報を転送することなく共有秘密情報を導出するために使用する ID。Group 1（768 ビット）、Group 2（1024 ビット）、および Group 5（1536 ビット）の中から選択します。

サイト間接続プロファイルのトンネルグループ

このダイアログボックスでは、現在の Site-to-Site 接続プロファイルのトンネルグループパラメータを指定します。

- [証明書チェーンの送信（Send Certificate Chain）]：証明書チェーン全体の送信をイネーブルまたはディセーブルにします。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。
- [IKE Peer ID Validation]：IKE ピア ID 確認要求を無視するか、必須とするか、あるいは証明書によってサポートされている場合にだけチェックするかを選択します。
- [IKEキープアライブ（IKE Keepalive）]：IKE キープアライブモニタリングをイネーブルにし、設定を行います。次の属性の中から 1 つだけ選択できます。

- [Disable Keep Alives]：IKE キープアライブをイネーブルまたはディセーブルにします。
- [Monitor Keep Alives]：IKE キープアライブ モニタリングをイネーブルまたはディセーブルにします。このオプションを選択すると、[Confidence Interval] フィールドと [Retry Interval] フィールドが利用できるようになります。
- [Confidence Interval]：IKE キープアライブの信頼間隔を指定します。これは、ASA がキープアライブモニタリングを開始するまでに、ピアがアイドル状態を継続できる秒数です。最小 10 秒、最大 300 秒です。リモートアクセスグループのデフォルトの間隔は 10 秒です。
- [Retry Interval]：IKE キープアライブのリトライ間の待機秒数を指定します。デフォルト値は 2 秒です。
- [Head end will never initiate keepalive monitoring]：中央サイトの ASA がキープアライブモニタリングを開始しないように指定します。

- [ダイナミックVTIの場合（For Dynamic VTI）]：トンネルグループに仮想テンプレートを適用します。
  - [仮想テンプレート（Virtual Template）]：ドロップダウンリストから仮想テンプレートを選択します。同じ仮想テンプレートを複数のトンネルグループに適用することができます。ASA は、仮想テンプレートを使用して、VPN セッションごとに個別の仮想アクセスインターフェイスを作成します。

    仮想テンプレートの設定を正常に完了するには、次の DVTI インターフェイスパラメータを設定する必要があります（[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [追加（Add）] > [DVTIインターフェイスの追加（Add DVTI Interface）]。
    - DVTI インターフェイス名
    - [Enable Interface]
    - IPSec（IPv4 または IPv6）のトンネルモード IP オーバーレイのイネーブル化
    - IPsec プロファイルによるトンネル保護

-

CA 証明書の管理

CA 証明書の管理は、リモート アクセス VPN とサイト間 VPN に適用されます。

- Site-to_site の場合：[IKE Peer Authentication] の [Manage] をクリックすると、[Manage CA Certificates] ダイアログボックスが開きます。

- リモート アクセス VPN では、**[Certificate Management]** > **[CA Certificates]** をクリックします。

このダイアログボックスを使用して、IKE ピア認証で使用可能な CA 証明書のリストのエントリを、表示、追加、編集、および削除します。[Manage CA Certificates] ダイアログボックスには、証明書の発行先、証明書の発行元、証明書の有効期限、および利用データなど、現在設定されている証明書の情報が一覧表示されます。

- [Add or Edit]：[Install Certificate] ダイアログボックスまたは [Edit Certificate] ダイアログボックスが開きます。これらのダイアログボックスでは、証明書の情報を指定し、証明書をインストールできます
- [Show Details]：テーブルで選択する証明書の詳細情報を表示します。
- [Delete]：選択した証明書をテーブルから削除します。確認されず、やり直しもできません。

Site-to-Site 接続プロファイル、証明書のインストール

このダイアログボックスを使用して、新しい CA 証明書をインストールします。次のいずれかの方法で証明書を取得できます。

- 証明書ファイルを参照してファイルからインストールします。
- 事前取得済みの PEM 形式の証明書テキストをこのダイアログボックス内のボックスに貼り付けます。
- [Use SCEP]：Simple Certificate Enrollment Protocol（SCEP）の使用を指定します。証明書サービスのアドオンは、Windows Server 2003 ファミリで実行されます。SCEP プロトコルのサポートを提供し、これによりシスコのルータおよび他の中間ネットワーク デバイスは、証明書を取得できます。
  - [SCEP URL: http://]：SCEP 情報のダウンロード元の URL を指定します。
  - [Retry Period]：SCEP クエリー間の必須経過時間を分数で指定します。
  - [Retry Count]：リトライの最大許容回数を指定します。
- [More Options]：[Configure Options for CA Certificate] ダイアログボックスが開きます。

このダイアログボックスを使用して、この IPsec リモート アクセス接続の CA 証明書の取得に関する詳細を指定します。このダイアログボックスに含まれるダイアログボックスは、[Revocation Check]、[CRL Retrieval Policy]、[CRL Retrieval Method]、[OCSP Rules]、および [Advanced] です。

[Revocation Check] ダイアログボックスは、CA 証明書失効確認に関する情報を指定するために使用します。

- オプション ボタンにより、失効状態について証明書をチェックするかどうかを指定します。[Do not check certificates for revocation] または [Check Certificates for revocation] を選択します。
- [Revocation Methods area]：失効チェックに使用する方法（CRL または OCSP）、およびそれらの方法を使用する順序を指定できます。いずれか一方または両方の方法を選択できます。

Cisco Secure Client イメージの AnyConnect VPN モジュール

[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）]>[セキュアクライアントソフトウェア（Client Software）] ペインに、ASDM で設定された セキュアクライアントイメージが一覧表示されます。

[セキュアクライアントイメージ（AnyConnect Client Image）] テーブル：ASDM で設定されたパッケージファイルが表示されます。ASA がリモート PC にイメージをダウンロードする順序を設定できます。

- [追加（Add）] : [セキュアクライアントイメージの追加（Add AnyConnect Client Image）] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュメモリ内のファイルをクライアントイメージファイルとして指定したり、フラッシュメモリから、クライアントイメージとして指定するファイルを参照したりできます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。
- [置換（Replace）] : [セキュアクライアントイメージの置換（Replace Image）] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュメモリ内のファイルをクライアントイメージとして指定して、[SSL VPNクライアントイメージ（SSL VPN Client Image）] テーブルで選択したイメージと置換できます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。
- [Delete]：テーブルからイメージを削除します。イメージを削除しても、パッケージ ファイルはフラッシュから削除されません。
- [Move Up] および [Move Down]：上矢印と下矢印を使用して、ASA がリモート PC にクライアントイメージをダウンロードする順序を変更します。テーブルの一番上にあるイメージを最初にダウンロードします。このため、最もよく使用するオペレーティング システムで使用されるイメージを一番上に移動する必要があります。

Cisco Secure Client イメージの AnyConnect VPN モジュール、追加/置換

このペインでは、ASA フラッシュメモリ上のファイルの名前を指定して、そのファイルを セキュアクライアントイメージとして追加したり、テーブルにすでに記載されているイメージと

置換することができます。また、識別するファイルをフラッシュ メモリから参照したり、ローカル コンピュータからファイルをアップロードしたりすることもできます。

- [Flash SVC Image]：SSL VPN クライアント イメージとして識別する、フラッシュ メモリ内のファイルを指定します。
- [Browse Flash]：フラッシュ メモリに格納されているすべてのファイルを参照できる [Browse Flash Dialog] ダイアログボックスを表示します。
- [Upload]：[Upload Image] ダイアログボックスが表示されます。このダイアログボックスでは、クライアント イメージとして指定するファイルをローカル PC からアップロードできます。
- [Regular expression to match user-agent]：ASA が、ブラウザから渡された User-Agent 文字列との照合に使用する文字列を指定します。モバイルユーザーの場合、この機能を使用してモバイルデバイスの接続時間を短縮できます。ブラウザは ASA に接続するときに、HTTP ヘッダーに User-Agent 文字列を含めます。ASA が文字列を受信し、その文字列がいずれかのイメージ用に設定された式と一致すると、他のクライアント イメージはテストされず、一致したイメージがただちにダウンロードされます。

Cisco Secure Client イメージの AnyConnect VPN モジュール、イメージのアップロード

このペインでは、ローカルコンピュータまたはセキュリティアプライアンスのフラッシュメモリに格納されている、セキュアクライアントイメージとして識別するファイルのパスを指定できます。ローカルコンピュータまたはセキュリティアプライアンスのフラッシュメモリから、識別するファイルを参照できます。

- [Local File Path]：ローカル コンピュータに格納されている、SSL VPN クライアントイメージとして識別するファイルの名前を指定します。
- [Browse Local Files]：[Select File Path] ダイアログボックスが表示されます。このダイアログボックスでは、ローカル コンピュータ上のすべてのファイルを表示し、クライアント イメージとして識別するファイルを選択できます。
- [Flash File System Path]：セキュリティ アプライアンスのフラッシュ メモリに格納されている、SSL VPN クライアント イメージとして識別するファイルの名前を指定します。
- [Browse Flash]：[Browse Flash] ダイアログボックスが表示されます。このダイアログボックスでは、セキュリティ アプライアンスのフラッシュ メモリに格納されているすべてのファイルを表示し、クライアント イメージとして識別するファイルを選択できます。
- [Upload File]：ファイルのアップロードを開始します。

セキュアクライアント外部ブラウザ SAML パッケージ

[設定（Configuration）] > [アクセスVPNの削除（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [セキュアクライアント（Secure Client）] ペ

インには、セキュアクライアント SAML シングルサインオン（SSO）認証に使用できるセキュアクライアント 外部ブラウザパッケージが一覧表示されます。

セキュアクライアント 外部ブラウザパッケージイメージ：ASDM で設定された外部ブラウザパッケージファイルを表示します。

- [追加（Add）]：[セキュアクライアント外部ブラウザイメージの追加（Add AnyConnect External Browser Image）] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュメモリ内のファイルを外部パッケージイメージファイルとして指定したり、フラッシュメモリから、外部ブラウザパッケージファイルとして指定するファイルを参照したりできます。
- [置き換え（Replace）]：[セキュアクライアント外部ブラウザパッケージの置き換え（Replace AnyConnect External Browser Package）] ダイアログボックスが表示されます。ここでは、フラッシュメモリ内のファイルを外部ブラウザパッケージとして指定して、既存のパッケージファイルを置き換えることができます。
- [削除（Delete）]：外部ブラウザパッケージファイルをテーブルから削除します。イメージを削除しても、パッケージ ファイルはフラッシュから削除されません。
- [上に移動（Move Up）] および [下に移動（Move Down）]：上矢印と下矢印を使用して、ASA がリモート PC に外部ブラウザパッケージをダウンロードする順序を変更します。

[セキュアクライアント外部ブラウザSAMLパッケージイメージ、追加/置き換え（AnyConnect Client External Browser SAML Package Images, Add/Replace）]

このペインでは、ASA フラッシュメモリ上のファイルの名前を指定して、そのファイルを セキュアクライアント外部ブラウザパッケージイメージとして追加したり、テーブルにすでに記載されているイメージと置換したりすることができます。また、識別するファイルをフラッシュ メモリから参照したり、ローカル コンピュータからファイルをアップロードしたりすることもできます。

- [セキュアクライアント外部ブラウザパッケージ（AnyConnect Client External Browser Package）]：外部ブラウザパッケージイメージとして識別するフラッシュメモリ内のファイルを指定します。
- [フラッシュの参照（Browse Flash）]：フラッシュメモリ上のすべてのファイルを参照できる [フラッシュの参照（Browse Flash）] ダイアログボックスが表示されます。
- [アップロード（Upload）]：[イメージのアップロード（Upload Image）] ダイアログボックスが表示されます。このダイアログボックスでは、外部ブラウザパッケージイメージとして指定するファイルをローカル PC からアップロードできます。

[セキュアクライアント外部ブラウザSAMLパッケージイメージ、イメージのアップロード（AnyConnect External Browser SAML Package Images, Upload Image）]

このペインでは、ローカルコンピュータまたはセキュリティアプライアンスのフラッシュメモリに格納されている、セキュアクライアントイメージとして識別するファイルのパスを指定で

きます。ローカルコンピュータまたはセキュリティアプライアンスのフラッシュメモリから、識別するファイルを参照できます。

- [ローカルファイルパス（Local File Path）]：ローカルコンピュータに格納されている、外部ブラウザパッケージイメージとして識別するファイルの名前を指定します。
- [ローカルファイルの参照（Browse Local Files）]：[ファイルパスの選択（Select File Path）]ダイアログボックスが表示されます。このダイアログボックスでは、ローカルコンピュータ上のすべてのファイルを表示し、外部ブラウザパッケージイメージとして識別するファイルを選択できます。
- [フラッシュファイルのシステムパス（Flash File System Path）]：セキュリティアプライアンスのフラッシュメモリに格納されている、外部ブラウザパッケージイメージとして識別するファイルの名前を指定します。
- [フラッシュの参照（Browse Flash）]：[フラッシュの参照（Browse Flash）]ダイアログボックスが表示されます。このダイアログボックスでは、セキュリティアプライアンスのフラッシュメモリに格納されているすべてのファイルを表示し、外部ブラウザパッケージイメージとして識別するファイルを選択できます。
- [ファイルのアップロード（Upload File）]：ファイルのアップロードを開始します。

セキュアクライアントVPN 接続の設定

セキュアクライアント接続の注意事項と制約事項

セッショントークンの推奨事項

ASA がセキュアクライアントからの VPN 接続要求を認証すると、セキュリティを強化するためにセッショントークンがクライアントに返されます。AnyConnect 4.9（MR1）以降、ASA とセキュアクライアントは、セッショントークンのセキュリティを強化するメカニズムをサポートします。トークンセキュリティをサポートしていないセキュアクライアントバージョンからの接続試行を拒否するように DAP ルールを設定できます。「DAP を使用してセッショントークンのセキュリティを確認する （241 ページ）」を参照してください。

セキュアクライアント プロファイルの設定

ASA は、すべてのセキュアクライアントユーザーにグローバルにセキュアクライアントプロファイルを展開するか、ユーザーのグループポリシーに基づいて展開するように設定できます。通常、ユーザーは、インストールされている セキュアクライアント モジュールごとに 1 つのクライアントプロファイルを持ちます。ユーザーに複数のプロファイルを割り当てることもできます。たとえば、複数の場所で作業するユーザーには、複数のプロファイルが必要になることがあります。一部のプロファイル設定（SBL など）は、グローバル レベルで接続を制

御します。その他の設定は、特定のホストに固有であり、選択されたホストにより異なります。

セキュアクライアントプロファイルの作成と展開、およびクライアント機能の制御の詳細については、『AnyConnect VPN module of Cisco Secure Client Administrator Guide』を参照してください。

クライアントプロファイルは、[設定（Configuration）> [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [セキュアクライアントプロファイル（Profile）] で設定します。

[追加/インポート（Add/Import）] : [セキュアクライアントプロファイルの追加（Add AnyConnect Profiles] ダイアログボックスが表示されます。このダイアログボックスでは、フラッシュメモリ内のファイルをプロファイルとして指定したり、フラッシュメモリを参照してプロファイルとして指定するファイルを検索したりできます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。

- [プロファイル名（Profile Name）] : グループポリシーの セキュアクライアント プロファイルを指定します。
- [Profile Usage]：最初に作成されたときにプロファイルに割り当てられた用途（VPN、ネットワーク アクセス マネージャ、Web セキュリティ、ISE ポスチャ、AMP イネーブラ、ネットワーク可視性モジュール、Umbrella Roaming Security、または管理 VPN トンネル）を表示します。ASDM が、XML ファイルで指定された用途を認識しない場合、ドロップダウン リストが選択可能になり、用途タイプを手動で選択できます。
- [Profile Location]：ASA のフラッシュ メモリ内のプロファイル ファイルへのパスを指定します。このファイルが存在しない場合、ASA はプロファイルテンプレートに基づいてファイルを作成します。
- [Group Policy]：プロファイルのグループ ポリシーを指定します。プロファイルは、セキュアクライアントとともにこのグループポリシーに属しているユーザーにダウンロードされます。

[編集（Edit）] : [SSL VPNクライアントプロファイルの編集（Edit SSL VPN Client Profiles）] ウィンドウが表示されます。このウィンドウでは、プロファイルに含まれているセキュアクライアント 機能の設定を変更できます。

[エクスポート（Export）]

- [Device Profile Path]：プロファイル ファイルのパスおよびファイル名を表示します。
- [Local Path]：パスとファイル名を指定してプロファイル ファイルをエクスポートします。
- [Browse Local]：ローカル デバイス ファイル システムを参照するには、これをクリックしてウィンドウを起動します。

[Delete]：テーブルからプロファイルを削除します。プロファイルを削除しても、XML ファイルはフラッシュから削除されません。

[セキュアクライアントプロファイル（AnyConnect Profiles）] テーブル：セキュアクライアント プロファイルとして指定された XML ファイルを表示します。

セキュアクライアントトラフィックに対するネットワークアドレス変換の免除

ネットワークアドレス変換（NAT）を実行するように ASA を設定した場合は、セキュアクライアント、内部ネットワーク、およびDMZの企業リソースが相互に接続を開始できるように、リモートアクセスセキュアクライアントトラフィックを変換の対象外にする必要があります。セキュアクライアントトラフィックを変換の対象外にできないと、セキュアクライアントおよび他の企業リソースが通信できなくなります。

「アイデンティティ NAT」（「NAT 免除」とも呼ばれている）によりアドレスを自らに変換できます。これにより効果的に NAT が回避されます。アイデンティティ NAT は 2 つのアドレス プール、アドレス プールとサブネットワーク、または 2 つのサブネットワーク間で適用できます。

この手順は、例にあるネットワーク トポロジの次の仮定のネットワーク オブジェクト間でアイデンティティ NAT を設定する方法を示しています。それらは、Engineering VPN アドレス プール、Sales VPN アドレス プール、ネットワーク内、DMZ ネットワーク、およびインターネットです。アイデンティティ NAT 設定ではそれぞれ、NAT 規則が 1 つ必要です。

表 *6 : VPN* クライアントのアイデンティティ *NAT* を設定するネットワーク アドレス アドレッシング

ネットワークまたはアドレス プール	ネットワーク名またはアドレス プール名	アドレス範囲
内部ネットワーク	inside-network	10.50.50.0 - 10.50.50.255
Engineering VPN アドレス プール	Engineering-VPN	10.60.60.1 - 10.60.60.254
Sales VPN アドレス プール	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ ネットワーク	DMZ-network	192.168.1.0 - 192.168.1.255

手順

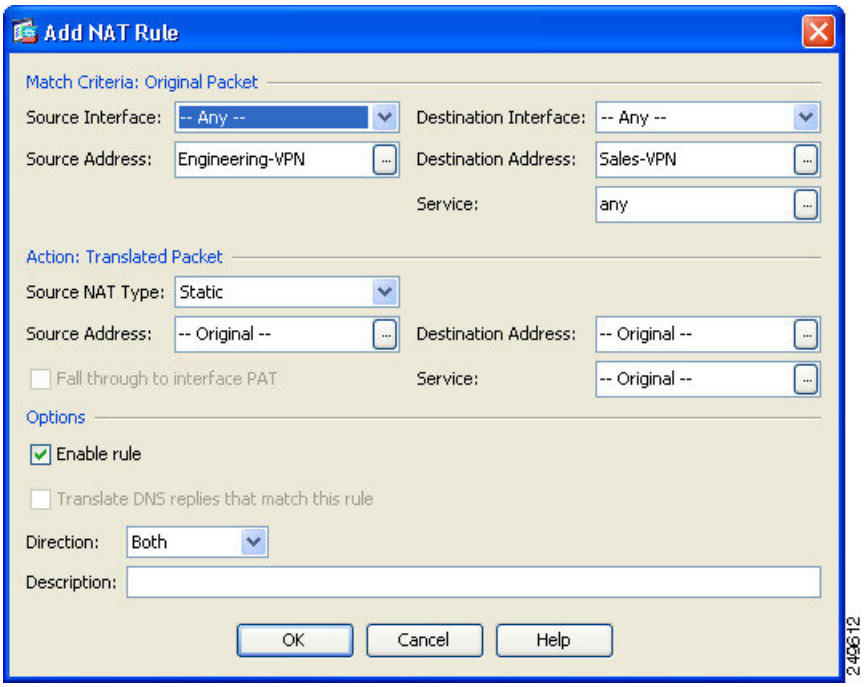
ステップ 1 ASDM にログインし、[Configuration] > [Firewall] > [NAT Rules] に移動します。

ステップ 2 Engineering VPN アドレス プールのホストが Sales VPN アドレス プールのホストに接続できるよう、NAT 規則を作成します。ASA が Unified NAT テーブルの他の規則よりも先にこの規則を評価するように、[NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] に移動します。

（注）

NAT ルールはトップダウン方式で最初に一致したルールから順に適用されます。ASA によりいったんパケットが特定の NAT 規則と一致すると、それ以上評価は行われません。ASA が NAT 規則を早まって広範な NAT 規則に一致しないよう、Unified NAT テーブルの先頭に最も固有の NAT 規則を配置することが重要です。

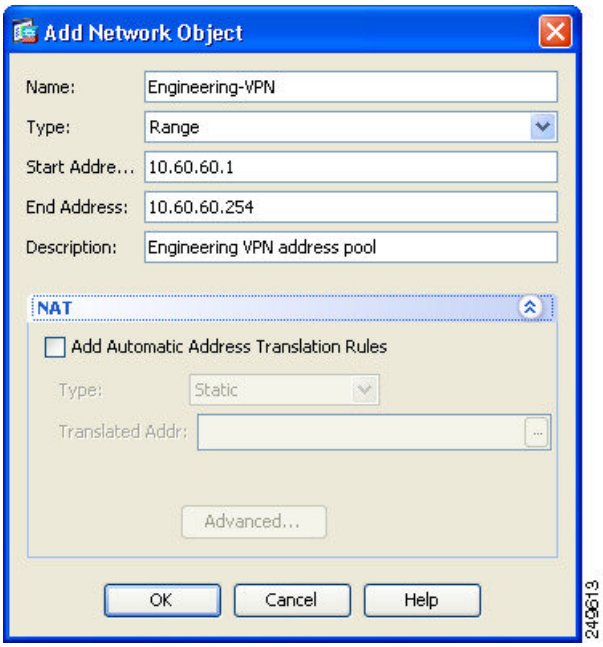
図 *2 : [Add NAT Rule]* ダイアログ ボックス



a) [Match criteria: Original Packet] エリアで、次のフィールドを設定します。

- [Source Interface:] Any
- [Destination Interface:] Any
- [Source Address:] [Source Address] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを作成します。オブジェクト タイプをアドレスの [Range] として定義します。自動アドレス トランスレーション ルールは追加しないでください。
- [Destination Address:] [Destination Address] ブラウズ ボタンをクリックし、Sales VPN アドレス プールを表すネットワーク オブジェクトを作成します。オブジェクト タイプをアドレスの [Range] として定義します。自動アドレス トランスレーション ルールは追加しないでください。

図 *3 : VPN* アドレス プールのネットワーク オブジェクトの作成



b) [Action Translated Packet] エリアで、次のフィールドを設定します。

- [Source NAT Type:] Static
- [Source Address:] Original
- [Destination Address:] Original
- [Service:] Original

c) [Options] エリアで、次のフィールドを設定します。

- [Enable rule] をオンにします。
- [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
- [Direction:] Both
- [Description:] 規則の説明を入力します。

d) [OK] をクリックします。

e) [Apply] をクリックします。

CLI の例：

```
nat source static Engineering-VPN Engineering-VPN destination static Sales-VPN
Sales-VPN
```

f) [Send] をクリックします。

ステップ 3 ASA が NAT を実行しているときに、同じ VPN プール内の 2 つのホストが互いに接続できるように、またはそれらのホストが VPN トンネル経由でインターネットに接続できるように、[Enable traffic between two or more hosts connected to the same interface] オプションをイネーブルにする必要があります。これを行うには、ASDM で [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] を選択します。[Interface] パネルの下の [Enable traffic between two or more hosts connected to the same interface] をオンにして、[Apply] をクリックします。

CLI の例：

```
same-security-traffic permit inter-interface
```

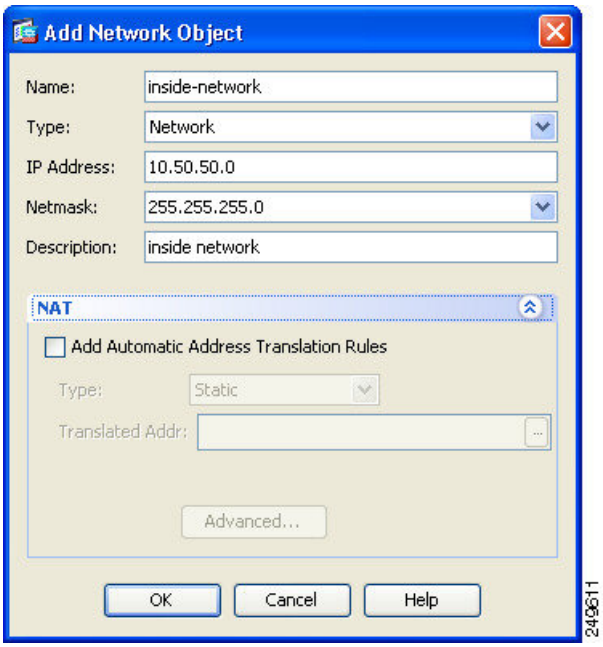
ステップ 4 Engineering VPN アドレス プールのホストが Engineering VPN アドレス プールの他のホストに接続できるよう、NAT 規則を作成します。上記で規則を作成したときと同様にこの規則を作成します。ただし、[Match criteria: Original Packet] エリアで、Engineering VPN アドレス プールを送信元と宛先の両方のアドレスとして指定します。

ステップ 5 Engineering VPN リモート アクセス クライアントが「内部」ネットワークに到達できるよう NAT 規則を作成します。この規則が他の規則よりも先に処理されるように、[NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] を選択します。

a) [Match criteria: Original Packet] エリアで、次のフィールドを設定します。

- [Source Interface:] Any
- [Destination Interface:] Any
- [Source Address:] [Source Address] ブラウズ ボタンをクリックし、内部ネットワークを表すネットワーク オブジェクトを作成します。オブジェクト タイプをアドレスの [Network] として定義します。自動アドレス トランスレーション ルールは追加しないでください。
- [Destination Address:] [Destination Address] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを選択します。

図 *4 : inside-network* オブジェクトの追加



b) [Action Translated Packet] エリアで、次のフィールドを設定します。

- [Source NAT Type:] Static
- [Source Address:] Original
- [Destination Address:] Original
- [Service:] Original

c) [Options] エリアで、次のフィールドを設定します。

- [Enable rule] をオンにします。
- [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
- [Direction:] Both
- [Description:] 規則の説明を入力します。

d) [OK] をクリックします。

e) [Apply] をクリックします。

CLI の例

```
nat source static inside-network inside-network destination static Engineering-VPN
Engineering-VPN
```

ステップ 6 **ステップ 5** の方法に従って新しい規則を作成し、Engineering VPN アドレス プールと DMZ ネットワーク間の接続のアイデンティティ NAT を設定します。DMZ ネットワークを送信元アドレス、Engineering VPN アドレス プールを宛先アドレスとして使用します。

ステップ 7 新しい NAT 規則を作成し、Engineering VPN アドレス プールがトンネル経由でインターネットにアクセスできるようにします。この場合、アイデンティティ NAT は使用しません。送信元アドレスをプライベート アドレスからインターネット ルーティング可能なアドレスに変更するためです。この規則を作成するには、次の手順に従います。

a) この規則が他の規則よりも先に処理されるように、[NAT Rules] ペインで、[Add] > [Add NAT Rule Before "Network Object" NAT rules] を選択します。

b) [Match criteria: Original Packet] エリアで、次のフィールドを設定します。

- [Source Interface:] Any
- [Destination Interface:] Any。[Action: Translated Packet] エリアの [Source Address] で [outside] を選択すると、このフィールドに自動的に「outside」が入力されます。
- [Source Address]：[Source Address] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを選択します。
- [Destination Address:] Any

c) [Action Translated Packet] エリアで、次のフィールドを設定します。

- [Source NAT Type:] Dynamic PAT (Hide)
- [Source Address:] [Source Address] ブラウズ ボタンをクリックして、outside インターフェイスを選択します。
- [Destination Address:] Original
- [Service:] Original

d) [Options] エリアで、次のフィールドを設定します。

- [Enable rule] をオンにします。
- [Translate DNS replies that match this rule] をオフにするか、空にしておきます。
- [Direction:] Both
- [Description:] 規則の説明を入力します。

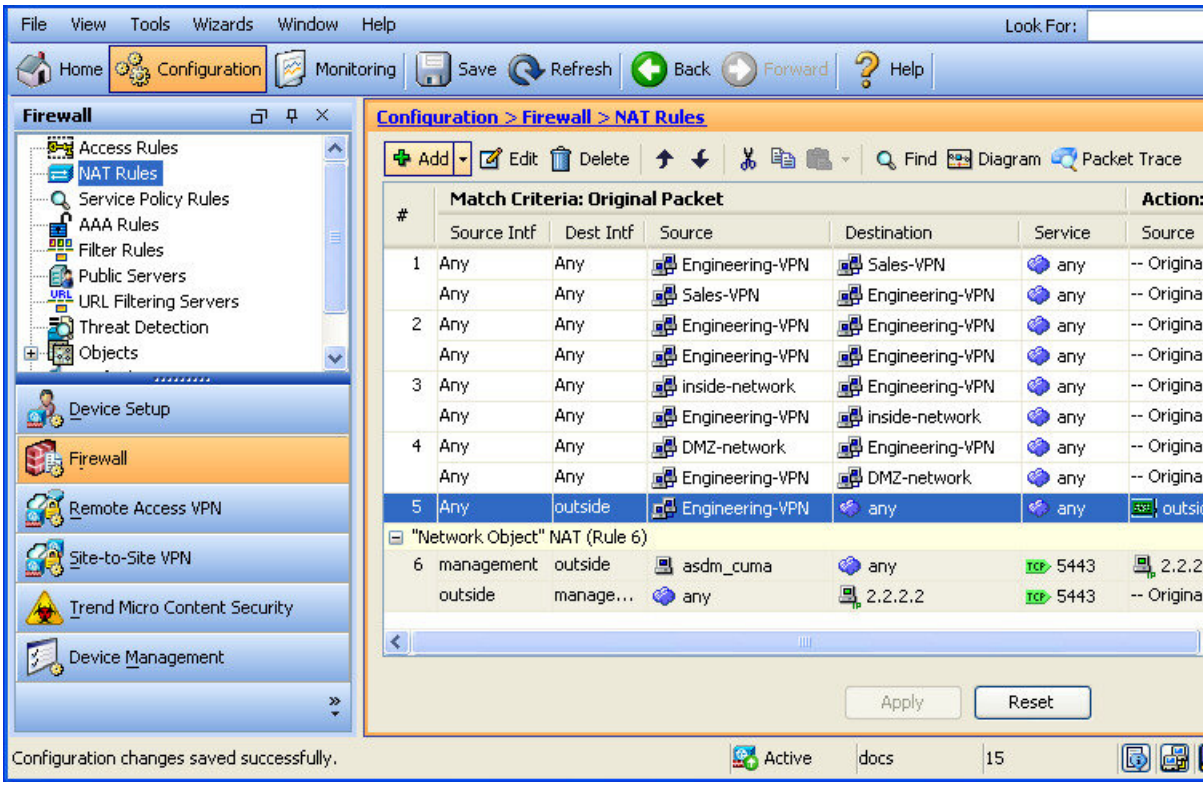
e) [OK] をクリックします。

f) [Apply] をクリックします。

CLI の例：

```
nat (any,outside) source dynamic Engineering-VPN interface
```

図 *5 : Unified NAT* テーブル



ステップ 8 Engineering VPN アドレス プールがそのプール自体、Sales VPN アドレス プール、内部ネットワーク、DMZ ネットワーク、およびインターネットに到達するように設定した後に、Sales VPN アドレス プールについて同じプロセスを繰り返す必要があります。アイデンティティ NAT を使用して、Sales VPN アドレス プール トラフィックが、Sales VPN アドレス プール、内部ネットワーク、DMZ ネットワーク、およびインターネット間のネットワーク アドレス変換の対象外となるようにします。

ステップ 9 ASA の [File] メニューで [Save Running Configuration to Flash] を選択し、アイデンティティ NAT 規則を実装します。

セキュアクライアント HostScan

セキュアクライアント HostScan（現在は Cisco Secure Firewall ポスチャと呼ばれています）により、Secure Client）はホストにインストールされているオペレーティングシステム、マルウェア対策、ファイアウォールの各ソフトウェアを識別できます。この情報は、Cisco Secure Firewall ポスチャ/HostScan アプリケーションによって収集されます。ポスチャアセスメントでは、ホストに Secure Firewall ポスチャ/HostScan がインストールされている必要があります。

ASDM UI は動的であり、HostScan がロードされている場合は HostScan が反映されます。Secure Firewall ポスチャがロードされると、Secure Firewall ポスチャが反映されます。実行しているバージョンによって名前は異なります。

HostScan/Secure Firewall ポスチャの前提条件

セキュアクライアント を Secure Firewall Posture/HostScan モジュールとともに使用するには、最低でも次のような ASA コンポーネントが必要です。

- ASA 8.4
- ASDM 6.4

SCEP 認証機能を使用するには、Secure Firewall Posture/HostScan をインストールする必要があります。

Secure Firewall Posture/HostScan のインストールでサポートされるオペレーティングシステムについては、『Supported VPN Platforms, Cisco ASA Series』を参照してください。

セキュアクライアントHostScan/Secure Firewall ポスチャのライセンス

Secure Firewall ポスチャ/HostScan のライセンス要件は次のとおりです。

- 基本的な HostScan/Secure Firewall ポスチャのセキュアクライアントの利点（Apex）。
- 修復には、Advanced Endpoint Assessment ライセンスが必要です。

HostScan パッケージ

HostScan パッケージを ASA にスタンドアロン パッケージ **hostscan-version.pkg** としてロードすることができます。このファイルには、HostScan ソフトウェアとともに、HostScan ライブラリおよびサポート表が含まれています。

HostScan/Secure Firewall ポスチャのインストールまたはアップグレード

この手順では、ASDM を使用して、HostScan/Secure Firewall ポスチャパッケージをインストールまたはアップグレードし、有効にします。ASDM UI は動的であり、HostScan がロードされている場合は HostScan が反映されます。Secure Firewall ポスチャがロードされると、Secure Firewall ポスチャが反映されます。実行しているバージョンによって名前は異なります。

始める前に

（注） HostScan バージョン 4.3.x 以前から 4.6.x 以降にアップグレードしようとしている場合、以前に確立した既存の AV/AS/FW DAP ポリシーおよび LUA スクリプトがすべて HostScan 4.6.x 以降と非互換であるという事実に起因するエラー メッセージが表示されます。

設定を適応させるために実行する必要があるワンタイム移行手順が存在します。この手順では、このダイアログボックスを閉じて、この設定を保存する前に HostScan 4.4.x と互換になるように設定を移行します。この手順を中止し、『セキュアクライアント HostScan 4.3.x to 4.6.x Migration Guide』で詳細な手順を参照してください。つまり、移行するには ASDM DAP のポリシーページに移動して、互換性のない AV/AS/FW 属性を確認して手動で削除してから、LUA スクリプトを確認し、書き換える必要があります。

手順

ステップ 1 バージョン 5 を使用している場合は、secure-firewall-posture-version-k9.pkg ファイルをコンピュータにダウンロードします。バージョン 4.x の場合、ファイルは hostscan_version-k9.pkg です。

ステップ 2 ASDM を開いて **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [Cisco Secure Firewall用ポスチャ（Posture (for Secure Firewall)）] > [ポスチャイメージ（Posture Image）] を選択します**。HostScan 4.x バージョンを使用している場合、パスは **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [Secure Desktop Manager] > [ホストスキャンイメージ（Host Scan Image）]** になります。

ステップ 3 [アップロード（Upload）] をクリックして、HostScan/Secure Firewall ポスチャパッケージのコピーをコンピュータから ASA のドライブに転送する準備を行います。

ステップ 4 [イメージのアップロード（Upload Image）] ダイアログボックスで [ローカルファイルの参照（Browse Local Files）] をクリックして、ローカルコンピュータ上の HostScan/Secure Firewall ポスチャパッケージを検索します。

ステップ 5 先ほどダウンロードした hostscan_version-k9.pkg ファイル、または secure-firewall-posture-version-k9.pkg ファイルを選択し、[選択（Select）] をクリックします。[ローカルファイルパス（Local File Path）] フィールドと [フラッシュファイルシステムパス（Flash File System Path）] フィールドで選択したファイルのパスは、HostScan/Secure Firewall パッケージのアップロード先のパスを反映しています。ASA に複数のフラッシュ ドライブがある場合は、別のフラッシュ ドライブを示すように [Flash File System Path] を編集できます。

ステップ 6 [Upload File] をクリックします。ASDM によって、ファイルのコピーがフラッシュ カードに転送されます。情報ダイアログボックスに、ファイルがフラッシュに正常にダウンロードされたことが表示されます。

ステップ 7 [OK] をクリックします。

ステップ 8 [アップロードしたイメージの使用（Use Uploaded Image）] ダイアログで [OK] をクリックして、現在のイメージとしてアップロードした HostScan/Secure Firewall ポスチャパッケージファイルを使用します。

ステップ 9 [HostScanを有効化（Enable HostScan）] または [ポスチャイメージを有効化（Enable Posture Image）] がオンになっていない場合はオンにします。

ステップ 10 [Apply] をクリックします。

ステップ 11 [File] メニューから [Save Running Configuration To Flash] を選択します。

ポスチャ設定の構成

デバイスごとに、ポスチャ設定を構成できます。

始める前に

HostScan/Secure Firewall Posture パッケージがあることを確認します。

手順

ステップ 1 **[構成（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ポスチャ（Secure Firewall 用）（Posture（for Secure Firewall））] > [ポスチャ設定（Posture Settings）]** を選択します。

ステップ 2 左側のペインのデバイス リストから、デバイスを選択します。

デバイスごとに、**[基本ポスチャ（Basic Posture）]** 属性と **[ポスチャ拡張（Posture Extensions）]** 属性を表示できます。

ステップ 3 デフォルトでは、Endpoint Detection and Response（EDR）セキュリティ ソフトウェアが、それぞれのサーバーと通信して情報を取得します。EDR 更新に対して次の設定を構成することができます。

- VPN トンネルがアクティブなときには EDR にインターネット接続チェックをスキップするようにさせたい場合は、**[EDR 更新で、VPN がアクティブになった後はインターネット接続チェックをスキップする（For EDR update, Skip Internet Check after VPN is active）]** チェックボックスをオンにします。
- セキュリティ ソフトウェアが最新かどうかを確認せずにホットスキャン/セキュア ファイアウォール ポスチャ評価を有効にするには、**[EDR 更新で、VPN がアクティブになる前でもインターネット接続チェックをスキップする（For EDR update, Skip Internet Check before VPN is active）]** チェックボックスをオンにします。このチェックボックスをオフにすると、接続が存在しないためポスチャ評価が失敗し、ポリシーによってはネットワーク アクセスが拒否される場合があります。ポスチャ評価の前には、インターネット接続を確認することを推奨します。

HostScan/Secure Firewall ポスチャのアンインストール

HostScan/Secure Firewall ポスチャパッケージをアンインストールすると、ASDM インターフェイス上のビューから削除されます。これにより、HostScan/Secure Firewall ポスチャが有効になっている場合でも ASA による HostScan/Secure Firewall ポスチャパッケージの展開が回避されます。HostScan/Secure Firewall ポスチャをアンインストールしても、HostScan/Secure Firewall ポスチャパッケージはフラッシュドライブから削除されません。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ポスチャ（Secure Firewall用）（Posture (for Secure Firewall)）] > [ポスチャイメージ（Posture Image）]** に移動して、Secure Firewall ポスチャをアンインストールします。AnyConnect バージョン4.xを使用していて、HostScanをアンインストールする場合は、**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [Secure Desktop Manager] > [ホストスキャンイメージ（Host Scan Image）]** に移動します。

ステップ 2 [Uninstall] をクリックし、確認のために [Yes] をクリックします。

ステップ 3 [Uninstall] をクリックします。

グループポリシーへの セキュアクライアント 機能モジュールの割り当て

次の手順で、セキュアクライアント機能モジュールとグループポリシーを関連付けます。VPN ユーザーが ASA に接続するときに、ASA はこれらの セキュアクライアント 機能モジュールをエンドポイントコンピュータにダウンロードしてインストールします。

始める前に

ASA にログオンし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は hostname(config)# プロンプトを表示します。

手順

ステップ 1 ネットワーク クライアント アクセス用の内部グループ ポリシーを追加します。

group-policy *name* **internal**

例：

```
hostname(config)# group-policy PostureModuleGroup internal
```

ステップ 2 新しいグループ ポリシーを編集します。このコマンドを入力した後は、グループ ポリシー コンフィギュレーション モードのプロンプト hostname(config-group-policy)# が表示されます。

group-policy *name* **attributes**

例：

```
hostname(config)# group-policy PostureModuleGroup attributes
```

ステップ 3 グループ ポリシー webvpn コンフィギュレーション モードを開始します。このコマンドを入力した後は、次に示す ASA のプロンプトが表示されます。hostname(config-group-webvpn)#

webvpn

ステップ 4 グループ内のすべてのユーザーに セキュアクライアント 機能モジュールがダウンロードされるように、グループポリシーを設定します。

anyconnect modules value Secure Firewall モジュール 名

anyconnect module コマンドの value には、次の値の 1 つ以上を指定することができます。複数のモジュールを指定する場合は、値をカンマで区切ります。

値	Secure Firewall モジュール/機能名
dart	Secure Client DART（診断およびレポートツール）
vpngina	Secure Client SBL（ログイン前の起動）
ポスチャ	Secure Firewall ポスチャ/HostScan
nam	Secure Client ネットワーク アクセス マネージャ
none	グループ ポリシーからすべての AnyConnect モジュールを削除する場合に使用します。
profileMgmt	Secure Client 管理トンネル VPN

例：

```
hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture
```

モジュールの 1 つを削除するには、保持したいモジュールの値だけを指定したコマンドを再送信します。たとえば、このコマンドは Web セキュリティ モジュールを削除します。

```
hostname(config-group-webvpn)# anyconnect modules value telemetry,posture
```

ステップ 5 実行コンフィギュレーションをフラッシュ メモリに保存します。

新しいコンフィギュレーションが正常にフラッシュ メモリに保存されると、[OK] というメッセージが表示され、次に示す ASA のプロンプトが表示されます。hostname(config-group-webvpn)#

write memory

ディスク暗号化

Windows、MacOS、および Linux の場合、[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ポスチャ（Cisco Secure Firewall向け）（Posture (for Secure Firewall)）] > [ポスチャ設定（Posture Settings）] > [設定（Configure）] > [高度なエンドポイントアセスメント（Advanced Endpoint Assessment）] ウィンドウの **[エンドポイントで暗号化されたディスクを識別する（Identify Encrypted Disks on Endpoint）]** チェックボックスをクリックすると、エンドポイントでインストールされたディスク暗号化製品のレポートが有効になります。csc_cscan ログで、ディスクのバージョンの詳細と暗号化の状態を確認できます。

この機能は、Secure Client 5.0.02075 以降および ASDM 7.19.1 以降でのみ使用できます。

HostScan/Secure Firewall ポスチャ関連資料

HostScan/Secure Firewall ポスチャがエンドポイントコンピュータからポスチャクレデンシャルを収集した後は、情報を活用するために、ダイナミック アクセス ポリシーの設定、Lua の式の使用などのサブジェクトを理解する必要があります。

これらのトピックの詳細については、『Cisco Adaptive Security Device Manager Configuration Guides』を参照してください。また、セキュアクライアント での HostScan/Secure Firewall ポスチャの動作の詳細については、『Cisco *Secure Client (including AnyConnect) Administrator Guide*』を参照してください。

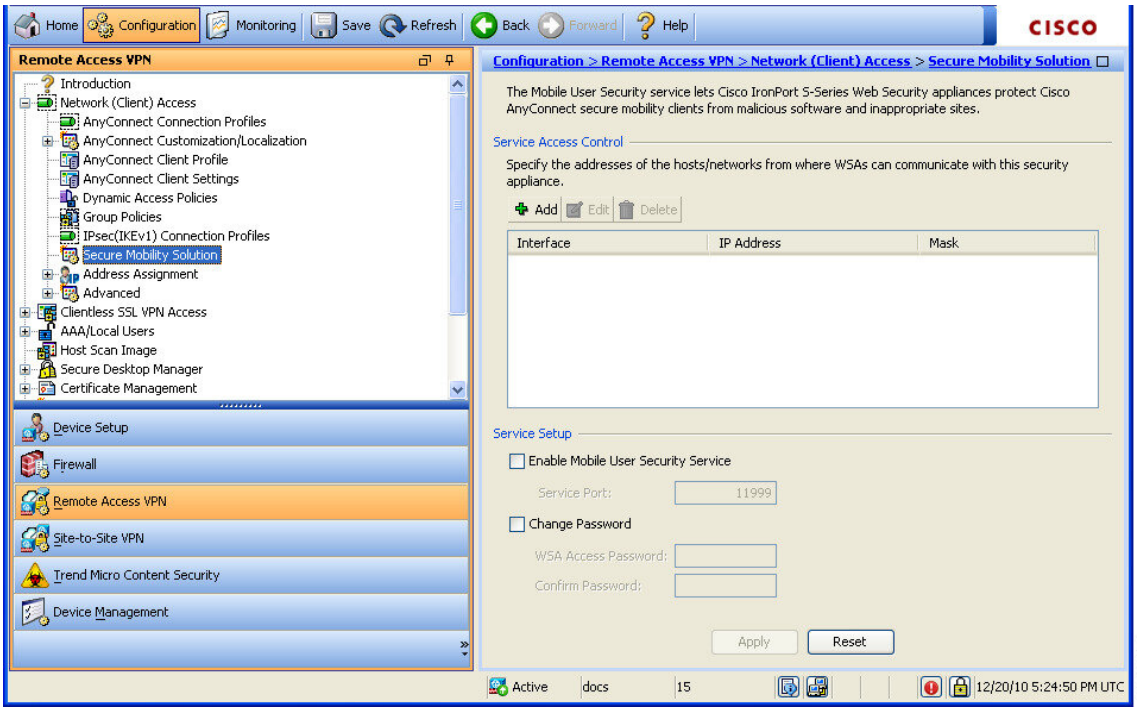
Secure Client ソリューション

セキュアクライアントは、従業員の移動時に企業の利益と資産をインターネットの脅威から保護します。セキュアクライアントにより Cisco IronPort S シリーズ Web セキュリティアプライアンスはセキュアクライアントをスキャンでき、クライアントを悪意あるソフトウェアや不適切なサイトから確実に保護します。クライアントは、Cisco IronPort S シリーズ Web セキュリティ アプライアンス保護がイネーブルになっているか定期的に確認します。

（注） この機能には、セキュアクライアント Secure Client ライセンス サポートを提供する Cisco IronPort Web セキュリティアプライアンスのリリースが必要です。また、 セキュリティクライアント機能をサポートする セキュアクライアント リリースが必要です。AnyConnect 3.1 以降はこの機能をサポートしていません。

セキュア モビリティ ソリューションを設定するには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Secure Mobility Solution] の順に選択します。

図 *6 : [Mobile User Security]* ウィンドウ



- [Service Access Control]：WSA の通信元となるホストまたはネットワーク アドレスを指定します。
  - [Add]：選択した接続の [Add MUS Access Control Configuration] ダイアログボックスが開きます。
  - [Edit]：選択した接続の [Edit MUS Access Control Configuration] ダイアログボックスが開きます。
  - [Delete]：選択した接続をテーブルから削除します。確認されず、やり直しもできません。
- [Enable Mobile User Security Service]：VPN を介したクライアントとの接続を開始します。イネーブルにすると、ASA への接続時に WSA によって使用されるパスワードを入力する必要があります。WSA が存在しない場合、ステータスは disabled になります。
- [Service Port]：サービスをイネーブルにする場合、サービスのどのポート番号を使用するかを指定します。ポートの範囲は 1 ～ 65535 で、管理システムにより WSA にプロビジョニングされた対応する値と一致させる必要があります。デフォルトは 11999 です。
- [Change Password]：WSA アクセス パスワードを変更できます。
- [WSA Access Password]：ASA と WSA の間の認証で必要となる共有シークレット パスワードを指定します。このパスワードは、管理システムにより WSA にプロビジョニングされた対応するパスワードと一致させる必要があります。
- [Confirm Password]：指定したパスワードを再入力します。

- [Show WSA Sessions]：ASA に接続された WSA のセッション情報を表示できます。接続されている（または接続された）WSA のホスト IP アドレスおよび接続時間がダイアログボックスに返されます。

Add or Edit MUS Access Control

[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network （Client） Access）] > [セキュアモビリティソリューション（Secure Mobility Solution）] の下の [MUS アクセス制御の追加または編集（Add or Edit MUS Access Control）] ダイアログボックスで、セキュアクライアントの Mobile User Security（MUS）アクセスを設定します。

- [Interface Name]：ドロップダウン リストを使用して、追加または編集しているインターフェイス名を選択します。
- [IP Address]：IPv4 アドレスまたは IPv6 アドレスを入力できます。
- [Mask]：ドロップダウン リストを使用して、該当のマスクを選択します。

セキュアクライアントのカスタマイズとローカリゼーション

Cisco Secure ClientのAnyConnect VPN モジュールをカスタマイズして、リモートユーザーに、会社のイメージを表示できます。[セキュアクライアントのカスタマイズ/ローカライズ（AnyConnect Client Customization/Localization）] のフィールドを使用すれば、次のタイプのカスタマイズされたファイルをインポートすることができます。

- **Resources**：セキュアクライアントの変更された GUI アイコン。
- **Binary**：セキュアクライアントインストーラに代わる実行可能ファイル。これには、GUI ファイルのほか、VPN クライアント プロファイル、スクリプト、その他のクライアントファイルが含まれます。
- **Script**：セキュアクライアントが VPN 接続を確立する前または後に実行するスクリプト。
- **GUI Text and Messages**：セキュアクライアントが使用するタイトルとメッセージ。
- **Customized Installer**：クライアントのインストールを変更するトランスフォーム。
- **Localized Installer**：クライアントで使用される言語を変更するトランスフォーム。

各ダイアログでは次のアクションを実行できます。

- [インポート（Import）] をクリックすると、[セキュアクライアントのカスタマイズオブジェクトをインポート（Import AnyConnect Client Customization Objects）] ダイアログが起動します。このダイアログでは、オブジェクトとしてインポートするファイルを指定できます。

- [エクスポート（Export）] をクリックすると、[セキュアクライアントのカスタマイズオブジェクトをエクスポート（Export Customization Objects）] ダイアログが起動します。このダイアログでは、オブジェクトとしてエクスポートするファイルを指定できます。
- [Delete] をクリックすると、選択したオブジェクトが削除されます。

（注） この機能はマルチ コンテキスト モードではサポートされません。

セキュアクライアントのカスタマイズとローカリゼーション、リソース

インポートするカスタムコンポーネントのファイル名は、セキュアクライアント GUI で使用されるファイル名と一致している必要があります。これはオペレーティングシステムによって異なり、Mac および Linux では大文字と小文字が区別されます。たとえば、Windows クライアント用の企業ロゴを置き換えるには、独自の企業ロゴを company_logo.png としてインポートする必要があります。別のファイル名でインポートすると、セキュアクライアントインストーラはそのコンポーネントを変更しません。ただし、独自の実行ファイルを展開して GUI をカスタマイズする場合は、その実行ファイルから任意のファイル名のリソース ファイルを呼び出すことができます。

イメージをソース ファイルとして（たとえば、company_logo.bmp）インポートする場合、インポートしたイメージは、同じファイル名を使用して別のイメージを再インポートするまで、セキュアクライアント をカスタマイズします。たとえば、company_logo.bmp をカスタム イメージに置き換えて、このイメージを削除する場合、同じファイル名を使用して新しいイメージ（または元のシスコ ロゴ イメージ）をインポートするまで、クライアントはこのイメージの表示を継続します。

セキュアクライアントのカスタマイズとローカリゼーション、バイナリとスクリプト

セキュアクライアントカスタマイゼーション/ローカリゼーション、バイナリ

Windows、Linux、または Mac（PowerPC または Intel ベース）コンピュータの場合、セキュアクライアント API を使用する独自のクライアントを展開できます。クライアントのバイナリ ファイルを置き換えることによって、セキュアクライアント GUI および セキュアクライアント CLI を置き換えます。

[**Import**] ダイアログのフィールドは次のとおりです。

- **Name** 置き換える セキュアクライアント ファイルの名前を入力します。
- **Platform** ファイルを実行する OS プラットフォームを選択します。

- **Select a file** ファイル名は、インポートするファイルの名前と同じにする必要はありません。

セキュアクライアントカスタマイゼーション/ローカリゼーション、スクリプト

スクリプトの展開およびスクリプトの制限事項の詳細については、『AnyConnect VPN module of Cisco Secure Client Administrators Guide』を参照してください。

[**Import**] ダイアログのフィールドは次のとおりです。

- **Name**：スクリプトの名前を入力します。名前には正しい拡張子を指定してください。例：myscript.bat.
- **Script Type**：スクリプトを実行するタイミングを選択します。

  ASA でファイルをスクリプトとして識別できるように、セキュアクライアントによって、プレフィックス scripts_ とプレフィックス OnConnect または OnDisconnect がユーザーのファイル名に追加されます。クライアントが接続すると、ASA は、リモート コンピュータ上の適切なターゲット ディレクトリにスクリプトをダウンロードします。その際、scripts_ プレフィックスは削除され、OnConnect または OnDisconnect プレフィックスはそのまま残ります。たとえば、myscript.bat スクリプトをインポートした場合、ASA 上では、スクリプトは scripts_OnConnect_myscript.bat となります。リモート コンピュータ上では、スクリプトは OnConnect_myscript.bat となります。

  スクリプトの実行の信頼性を確保するために、すべての ASA で同じスクリプトを展開するように設定します。スクリプトを修正または置換する場合は、旧バージョンと同じ名前を使用し、ユーザーが接続する可能性のあるすべての ASA に置換スクリプトを割り当てます。ユーザーが接続すると、新しいスクリプトにより同じ名前のスクリプトが上書きされます。

- **Platform**：ファイルを実行する OS プラットフォームを選択します。
- **Select a file**：ファイル名は、スクリプトに対して指定した名前と同じである必要はありません。

ASDM によってファイルがソース ファイルからインポートされ、[Name] に対して指定した新しい名前が作成されます。

セキュアクライアントのカスタマイズとローカリゼーション、GUI テキストとメッセージ

デフォルトの変換テーブルを編集するか、または新しいテーブルを作成して、セキュアクライアント GUI に表示されるテキストとメッセージを変更できます。このペインは、[Language Localization] ペインと同じ機能を持ちます。より高度な言語変換については、[Configuration] > [Remote Access VPN] > [Language Localization] に移動します。

上部ツールバーにある通常のボタンに加えて、このペインには [**Add**] ボタンと、追加のボタンを備えた [Template] エリアがあります。

Add：[Add] ボタンをクリックするとデフォルトの変換テーブルのコピーが開き、直接編集したり保存することができます。保存ファイルの言語を選択し、ファイル内のテキストの言語を後で編集することができます。

変換テーブルのメッセージをカスタマイズする場合、msgid は変更しないでください。msgstr 内のテキストを変更します。

テンプレートの言語を指定します。テンプレートはキャッシュメモリ内の変換テーブルになり、指定した名前が付きます。ブラウザの言語オプションと互換性のある短縮形を使用してください。たとえば、中国語のテーブルを作成するときに IE を使用している場合は、IE によって認識される *zh* という略語を使用します。

[Template] セクション

- テンプレート領域を展開してデフォルトの英語変換テーブルにアクセスするには、[Template] をクリックします。
- デフォルトの英語変換テーブルを表示し、必要に応じて保存するには、[**View**] をクリックします。
- デフォルトの英語変換テーブルのコピーを表示せずに保存するには、[**Export**] をクリックします。

セキュアクライアントのカスタマイズとローカリゼーション、カスタマイズされたインストーラ トランスフォーム

作成した独自のトランスフォームを、クライアント インストーラ プログラムを使用して展開することによって、セキュアクライアント GUI を大幅にカスタマイズすることができます（Windows のみ）。トランスフォームを ASA にインポートすると、インストーラ プログラムを使用して展開されます。

トランスフォームの適用先として選択できるのは Windows だけです。トランスフォームの詳細については、『*Cisco Secure Client Administration Guide*』を参照してください。

セキュアクライアントのカスタマイズとローカリゼーション、ローカライズされたインストーラ トランスフォーム

トランスフォームを使用して、クライアント インストーラ プログラムに表示されるメッセージを翻訳できます。トランスフォームによってインストレーションが変更されますが、元のセキュリティ署名 MSI は変化しません。これらのトランスフォームではインストーラ画面だけが翻訳され、クライアント GUI 画面は翻訳されません。

セキュアクライアント カスタム属性

カスタム属性は セキュアクライアント に送信され、以下に示すような機能を設定するために使用されます。カスタム属性にはタイプと名前付きの値があります。事前に定義したカスタム属性は、ダイナミック アクセス ポリシーとグループ ポリシーの両方で使用されます。これらのカスタム属性の設定については、『Configure Secure Client Custom Attributes in an Internal Group Policy』を参照してください。多数のさまざまな用途のカスタム属性を作成および設定します。

- **DSCPPreservationAllowed**：（DSCP の保存を有効化）このカスタム属性を設定すると、Windows または Mac のオペレーティング システム プラットフォームで DTLS 接続の Differentiated Services Code Point（DSCP）が制御されます。この属性を使用すると、デバイスは、遅延の影響を受けやすいトラフィックを優先順位付けし、優先順位付けされたトラフィックにマークを付けてアウトバウンド接続の質を改善することができます。詳細については、『Cisco Secure Client Administration Guide』の「*Enable DSCP Preservation*」セクションを参照してください。

  値は True または False です。デフォルトでは、セキュアクライアント は DSCP の保存を実行します（True）。無効にするには、ヘッドエンドでカスタム属性値を false に設定し、接続を再初期化します。

- **DeferredUpdateAllowed または DeferredUpdateAllowed_ComplianceModule**：（ASA で更新の延期を有効化）これらのカスタム属性が設定されている場合に、クライアントの更新が利用可能になると、セキュアクライアント は更新を実行するか延期するかをユーザーに尋ねるダイアログを開きます。詳細については、『Cisco Secure Client Administration Guide』の「Enable セキュアクライアント Deferred Upgrade」または「*Configure Deferred Update on an ASA*」を参照してください。

  値は True または False です。True の場合、更新の延期が有効になります。更新の延期が無効（False）の場合、下記の設定は無視されます。

  - **DeferredUpdateMinimumVersion_ComplianceModule または DeferredUpdateMinimumVersion**：更新を延期できるようにするためにインストールする必要がある最小バージョンの セキュアクライアント。

    値は x.x.x で、デフォルトは 0.0.0 です。

  - **DeferredUpdateDismissTimeout**：更新の延期を確認するダイアログが表示されてから、自動的に閉じるまでの秒数。更新の延期を確認するダイアログが表示される場合にのみ適用されます。

    値は 0 ー 300 秒です。デフォルトは 150 秒です。

  - **DeferredUpdateDismissResponse**：DeferredUpdateDismissTimeout の発生時に実行するアクション。

    値は defer（延期）または update（更新）です。デフォルトは update です。

- **dynamic-split-exclude-domains <属性名> <ドメインのリスト> または dynamic-split-include-domains <属性名> <ドメインのリスト>**：（ダイナミック スプリット

トンネリングを有効化）このカスタム属性を作成することにより、トンネルの確立後に、ホストの DNS ドメイン名に基づいて動的にスプリット除外トンネリングを行うことができます。dynamic-split-exclude-domains を追加することにより、VPN トンネルの外部のクライアントによるアクセスが必要なクラウドまたは Web サービスを入力できます。詳細については、『Cisco Secure Client Administration Guide』の「*About Dynamic Split Tunneling*」を参照してください。

値の属性名には、任意の名前を指定できます。たとえば、anyconnect-custom-data dynamic-split-exclude-domains excludedomains webex.com, ciscospark.com のようにします。

- **managementTunnelAllAllowed**：（管理 VPN トンネルを有効化）ユーザーが開始したネットワーク通信に影響しないように（管理 VPN トンネルは透過的であるため）スプリット包含トンネリングの設定がデフォルトで必要です。

  値は true または false です。この動作をオーバーライドする場合は、属性名と値の両方を *true* に設定します。そのように設定すると、両方の IP プロトコルの設定が tunnel-all、split-exclude、split-include、または bypass のいずれかの場合、セキュアクライアント は管理トンネルの接続に進みます。

- **UseLocalProfileAsAlternative**：Cisco Secure Firewall ASA で Cisco Secure Client プロファイル（旧名は AnyConnect）を設定せずに、アウトオブバンドで（SCCM、MDM、SecureX Cloud Management などを使用して）プロファイルを配布する場合は、*UseLocalProfileAsAlternative* カスタム属性を使用できます。このカスタム属性を設定すると、クライアントは設定とプリファレンスに(通常のデフォルトではなく)ローカル（ディスク上）の Cisco Secure Client プロファイルを使用します。詳細については、アドミニストレーション ガイドの「Predeploying Cisco Secure Client」を参照してください。

  ローカルプロファイルを使用したセッションの確立は、1) UseLocalProfileAsAlternative が有効に設定されている場合、および 2) ASA グループ ポリシー プロファイルが設定されていない場合にのみ発生します。このカスタム属性を設定し、ASA のグループポリシー構成から Cisco Secure Client プロファイルを元に戻したり削除したりしない場合、グループポリシーで構成された Cisco Secure Client プロファイルが維持され、カスタム属性の設定が無視される各接続で使用されます。

  名前：無効/有効

  値：true/false

- **no-dhcp-server-route**：（パブリック DHCP サーバールートの設定）このカスタム属性により、Tunnel All Network が設定されている場合にローカル DHCP トラフィックがクリアテキストで流れるようになります。セキュアクライアント は、セキュアクライアント の接続時にローカル DHCP サーバーに特定のルートを追加し、ホストマシンの LAN アダプターに暗黙的なフィルタを適用して、DHCP トラフィックを除く当該ルートのすべてのトラフィックをブロックします。詳細については、『Cisco Secure Client Administration Guide』の「*Set Public DHCP Server Route*」セクションを参照してください。

  値は true または false です。トンネル確立時のパブリック DHCP サーバー ルート作成を避けるために、no-dhcp-server-route カスタム属性が存在し、true に設定されている必要があります。

- **circumvent-host-filtering**：（サブネットの除外をサポートするようにLinuxを設定）[Tunnel Network List Below] がスプリットトンネリング用に設定されている場合はサブネットの除外をサポートするように、Linux を設定します。詳細については、サブネットの除外をサポートするための Linux の設定 （93 ページ）を参照してください。

  値は true または false です。true に設定します。

- **tunnel-from-any-source**：（Linuxのみ）セキュアクライアント は、Split-Include または Split-Exclude トンネルモードの任意の送信元アドレスを持つパケットを許可します。VM インスタンスまたは Docker コンテナ内のネットワークアクセスを許可できます。

（注） VM/Docker で使用されるネットワークは、最初にトンネルから除外する必要があります。

- **perapp**：モバイルデバイス（Android または Apple iOS のみ）上の特定のアプリケーションセットで VPN 接続が使用されます。詳細については、『*Cisco Secure Client Administration Guide*』の「Create Per App Custom Attributes」セクションを参照してください。

  値を指定する際は、ポリシーツールから BASE64 形式をコピーしてここに貼り付けて、1 つ以上の値を追加します。

これらの機能の使用をさらに完全にするには、**[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Polices]** > メニューで、定義済みカスタム属性のほとんどを特定のグループ ポリシーに関連付ける必要があります。

IPsec VPN クライアント ソフトウェア

（注） **VPN クライアントは耐用年数末期で、サポートが終了しています。**VPN クライアントの設定については、ASA バージョン 9.2 に関する ASDM のマニュアルを参照してください。Secure Client**にアップグレードすることを推奨します。**

Zone Labs Integrity Server

[Configuration] > [Remote Access VPN] > [Network （Client） Access] > [Advanced] > [IPsec] > [Zone Labs Integrity Server] パネルでは、Zone Labs Integrity Server をサポートするように ASA を設定できます。このサーバーは、プライベート ネットワークにアクセスするリモート クライアントでセキュリティ ポリシーを適用する目的で設計された Integrity System というシステムの一部です。実質的には、ASA がファイアウォール サーバーに対するクライアント PC のプロキシとして機能し、Integrity クライアントと Integrity サーバー間で必要なすべての Integrity 情報をリレーします。

（注） 現在のリリースのセキュリティ アプライアンスでは同時に 1 台の Integrity サーバーのみがサポートされていますが、ユーザー インターフェイスでは最大 5 台の Integrity サーバーの設定がサポートされています。アクティブなサーバーに障害が発生した場合は、ASA 上で別の Integrity サーバーを設定して、クライアント VPN セッションを再確立してください。

- [Server IP address]：Integrity サーバーの IP アドレスを入力します。ドット付き 10 進数を使用します。
- [Add]：新しいサーバー IP アドレスを Integrity サーバーのリストに追加します。このボタンは、Server IP アドレス フィールドにアドレスが入力されるとアクティブになります。
- [Delete]：選択したサーバーを Integrity サーバーのリストから削除します。
- [Move Up]：選択したサーバーを Integrity サーバーのリスト内で上に移動します。このボタンは、リストにサーバーが 1 台以上存在する場合にだけ使用できます。
- [Move Down]：選択したサーバーを Integrity サーバーのリスト内で下に移動します。このボタンは、リストにサーバーが 1 台以上存在する場合にだけ使用できます。
- [Server Port]：アクティブな Integrity サーバーをリッスンする ASA のポート番号を入力します。このフィールドは、Integrity Server のリストにサーバーが少なくとも 1 台以上存在する場合にだけ使用できます。デフォルト ポート番号は 5054、範囲は 10 ～ 10000 です。このフィールドは、Integrity Server リスト内にサーバーが存在する場合にだけ使用できます。
- [Interface]：アクティブな Integrity サーバーと通信する ASA インターフェイスを選択します。このインターフェイス名メニューは、Integrity Server リスト内にサーバーが存在する場合にだけ使用できます。
- [Fail Timeout]：ASA がアクティブな Integrity サーバーに到達できないことを宣言するまでの待機秒数を入力します。デフォルトは 10 で、範囲は、5 ～ 20 です。
- [SSL Certificate Port]：SSL 認証で使用する ASA のポートを指定します。デフォルトのポートは 80 です。
- [Enable SSL Authentication]：ASA によるリモート クライアントの SSL 証明書の認証をイネーブルにする場合にオンにします。デフォルトでは、クライアント SSL 認証はディセーブルになっています。
- [Close connection on timeout]：タイムアウト時に ASA と Integrity サーバー間の接続を終了する場合にオンにします。デフォルトでは、接続が維持されます。
- [Apply]：設定を実行している ASA に Integrity サーバーの設定を適用します。
- [Reset]：まだ適用されていない Integrity サーバーの設定の変更を削除します。

ISE ポリシーの適用

Cisco Identity Services Engine（ISE）は、セキュリティ ポリシー管理および制御プラットフォームです。有線、ワイヤレス、VPN 接続のアクセス制御とセキュリティ コンプライアンスを自動化し、シンプルにします。Cisco ISE は主に、Cisco TrustSec と連携してセキュア アクセスとゲスト アクセスを提供し、個人所有デバイス持ち込み（BYOD）イニシアティブをサポートし、使用ポリシーを適用するために使用されます。

ISE Change of Authorization（CoA）機能は、認証、認可、およびアカウンティング（AAA）セッションの属性を、セッション確立後に変更するためのメカニズムを提供します。AAA のユーザまたはユーザ グループのポリシーを変更すると、ISE から ASA へ CoA パケットを直接送信して認証を再初期化し、新しいポリシーを適用できます。インライン ポスチャ実施ポイント（IPEP）は、ASA によって確立された各 VPN セッションにアクセス コントロール リスト（ACL）を適用する必要はありません。

ISE ポリシーの実施は、次の VPN クライアントでサポートされています。

- IPSec
- セキュアクライアント
- L2TP/IPSec

システム フローは次のとおりです。

1. エンド ユーザーが VPN 接続を要求します。
2. ASA は、ISE に対してユーザーを認証し、ネットワークへの限定アクセスを提供するユーザー ACL を受け取ります。
3. アカウンティング開始メッセージが ISE に送信され、セッションが登録されます。
4. ポスチャ アセスメントが NAC エージェントと ISE 間で直接行われます。このプロセスは、ASA に透過的です。
5. ISE が CoA の「ポリシー プッシュ」を介して ASA にポリシーの更新を送信します。これにより、ネットワーク アクセス権限を高める新しいユーザ ACL が識別されます。

（注） 後続の CoA 更新を介し、接続のライフタイム中に追加のポリシー評価が ASA に透過的に行われる場合があります。

ISE 許可変更の設定

ISE 認可変更を設定するには、ISE RADIUS サーバーを含むサーバー グループを作成し、リモート アクセス VPN 設定プロファイル（トンネル）でそのサーバー グループを使用します。

手順

ステップ 1 ISE サーバーの RADIUS AAA サーバー グループを設定します。

次の手順は、最小限の設定を示しています。必要に応じて、グループの他の設定を調整できます。大部分の設定には、ほとんどのネットワークに適したデフォルト設定があります。RADIUS AAA サーバー グループの設定の詳細については、一般的なコンフィギュレーション ガイドを参照してください。

a) **[Configuration]** > **[Remote Access VPN]** > **[AAA/Local Users]** > **[AAA Server Groups]** を選択します。

b) [AAA Server Group] 領域で、[Add] をクリックします。

c) [Server Group] フィールドにグループの名前を入力します。

d) [Protocol] ドロップダウン リストから RADIUS サーバー タイプを選択します。

e) [Enable interim accounting update] と [Update Interval] を選択し、RADIUS 中間アカウンティング更新メッセージが定期的に生成されるようにします。

ISE は、ASA などの NAS デバイスから受信するアカウンティング レコードに基づいて、アクティブ セッションのディレクトリを保持します。ただし、セッションがアクティブであるという通知（アカウンティング メッセージまたはポスチャ トランザクション）を 5 日間受信しなかった場合、ISE はデータベースからそのセッションのレコードを削除します。存続時間の長い VPN 接続が削除されないようにするには、すべてのアクティブ セッションについて ISE に定期的に中間アカウンティング更新メッセージを送信するように、グループを設定します。

これらの更新を送信する間隔を時間単位で変更できます。デフォルトは 24 時間で、指定できる範囲は 1 ～ 120 です。

f) [Enable dynamic authorization] を選択します。

このオプションは、AAA サーバー グループの RADIUS の動的認可（ISE 許可変更、CoA）サービスをイネーブルにします。VPN トンネルでサーバー グループを使用すると、対応する RADIUS サーバー グループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー更新用ポートをリッスンします。別のポートを使用するように ISE サーバーが設定されていない限り、ポート（1700）を変更しないでください。有効な範囲は 1024 ～ 65535 です。

g) 認証に ISE を使用しない場合は、[Use authorization only mode] を選択します。

このオプションは、サーバー グループを認可に使用するときに、RADIUS アクセス要求メッセージが、AAA サーバー用に設定されているパスワード方式に反して、「認可専用」要求として構築されることを示しています。RADIUS サーバーの共通パスワードを設定すると、そのパスワードは無視されます。

たとえば、認証にこのサーバー グループではなく証明書を使用する場合には、認可専用モードを使用します。VPN トンネルでの認可とアカウンティングにこのサーバー グループを使用する可能性があるからです。

h) [OK] をクリックして、サーバー グループを保存します。

i) サーバー グループを選択したら、[Servers in the Selected Group] リストで [Add] をクリックし、ISE RADIUS サーバーをグループに追加します。

キー属性を以下に示します。必要に応じて、他の設定用にデフォルトを調整できます。

- [Interface Name]：ISE サーバーに到達するためのインターフェイス。
- [Server Name or IP Address]：ISE サーバーのホスト名または IP アドレス。
- （任意）[Server Secret Key]：接続を暗号化するキー。キーを設定しないと、接続は暗号化されません（プレーン テキスト）。このキーは 127 文字までの英数字から構成され、大文字と小文字の区別があり、RADIUS サーバー上のキーと同じ値になります。

j) [OK] をクリックして、サーバーをグループに追加します。

サーバー グループに別の ISE サーバーを追加します。

ステップ 2 リモート アクセス VPN で ISE サーバー グループを使用するために、設定プロファイルを更新します。

以下の手順は、ISE 関連の設定オプションにのみ該当します。機能的なリモート アクセス VPN を作成するには、その他のオプションも設定する必要があります。リモート アクセス VPN の実装については、このマニュアルの他の箇所の説明に従ってください。

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

b) [Connection Profiles] テーブルで、プロファイルを追加または編集します。

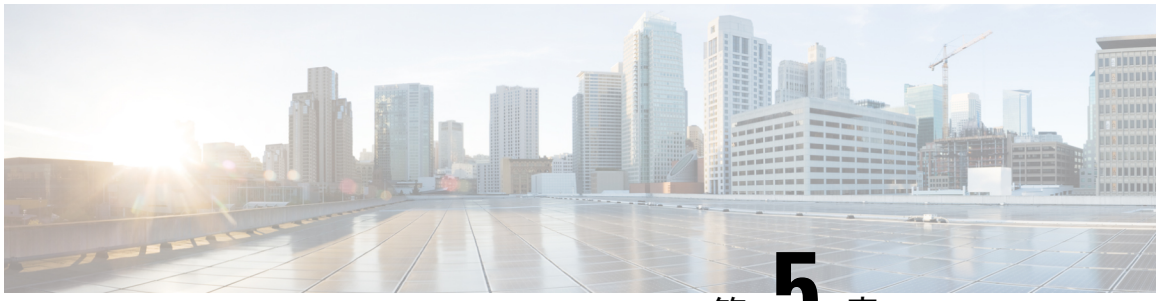
c) [Basic] ページで、認証方式を設定します。

- 認証に ISE サーバーを使用する場合は、**[Authentication] > [Method]** に対して [AAA] を選択し、次に ISE AAA サーバー グループを選択します。
- 許可用にのみ ISE サーバー グループを設定する場合は、別の認証方式（[Certificate] など）を選択します。

d) **[Advanced] > [Authorization]** ページで、[Authorization Server Group] に対して ISE サーバー グループを選択します。

e) **[Advanced] > [Accounting]** ページで、ISE サーバー グループを選択します。

f) **[OK]** をクリックして変更を保存します。



第 5 章

VPN の IP アドレス

IP アドレス割り当てポリシーの設定

ASA では、リモート アクセス クライアントに IP アドレスを割り当てる際に、次の 1 つ以上の方式を使用できます。複数のアドレス割り当て方式を設定すると、ASA は IP アドレスが見つかるまで各オプションを検索します。デフォルトでは、すべての方式がイネーブルになっています。

- [Use authentication server]：ユーザー単位で外部認証、認可、アカウンティング サーバーからアドレスを取得します。IP アドレスが設定された認証サーバーを使用している場合は、この方式を使用することをお勧めします。AAA サーバーは、[Configuration] > [AAA Setup] ペインで設定できます。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。

- [Use DHCP]：DHCP サーバーから IP アドレスを取得します。DHCP を使用する場合は、DHCP サーバーを設定する必要があります。また、DHCP サーバーで使用可能な IP アドレスの範囲も定義する必要があります。DHCP を使用する場合は、[Configuration] > [Remote Access VPN] > [DHCP Server] ペインでサーバーを設定します。この方法は IPv4 の割り当てポリシーに使用できます。

- [Use an internal address pool]：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。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。

  - [Allow the reuse of an IP address so many 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。遅延時間を設定する場合は、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。この設定要素は、IPv4 割り当てポリシーで使用できます。

次のいずれかの方式を使用して、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指定します。

IP アドレス割り当てオプションの設定

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[Address Assignment]** > **[Assignment Policy]** を選択します。

ステップ 2 [IPv4 Policy] エリアで、アドレス割り当て方式をオンにして有効にするか、オフにして無効にします。次の方法は、デフォルトで有効になっています。

- [Use Authentication server]: IP アドレスを提供するために設定した認証、許可、アカウンティング（AAA）サーバーを使用できるようにします。
- [Use DHCP]: IP アドレスを提供するために設定したダイナミック ホスト コンフィギュレーション プロトコル（DHCP）サーバーを使用できるようにします。
- [Use internal address pools]：ASA で設定されたローカル アドレス プール設定を使用できるようにします。

[Use internal address pools] を有効にする場合、IPv4 アドレスが解放された後、そのアドレスの再利用を有効にできます。You can specify a range of minutes from 0-480 after which the IP v4 address can be reused.

ステップ 3 [IPv6 Policy] エリアで、アドレス割り当て方式をオンにして有効にするか、オフにして無効にします。次の方法は、デフォルトで有効になっています。

- [Use Authentication server]: IP アドレスを提供するために設定した認証、許可、アカウンティング（AAA）サーバーを使用できるようにします。
- [Use internal address pools]：ASA で設定されたローカル アドレス プール設定を使用できるようにします。

ステップ 4 [Apply] をクリックします。

ステップ 5 **[OK]** をクリックします。

アドレス割り当て方式の表示

手順

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] の順に選択します。

ローカル IP アドレス プールの設定

VPN リモート アクセス トンネルに対して IPv4 または IPv6 アドレス プールを設定するには、ASDM を開き、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Management] > [Address Pools] > [Add/Edit IP Pool] を選択します。アドレス プールを削除するには、ASDM を開き、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Management] > [Address Pools] を選択します。削除するアドレス プールを選択し、[Delete] をクリックします。

ASA は、接続用の接続プロファイルまたはトンネル グループに基づいてアドレス プールを使用します。プールの指定順序は重要です。接続プロファイルまたはグループ ポリシーに複数のアドレス プールを設定すると、ASA は追加された順でそれらのプールを使用します。

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お勧めします。

ローカル IPv4 アドレス プールの設定

[IP Pool] エリアには、設定されたアドレス 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、エリアは空です。ASA 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。最初のプール内のアドレスがすべて割り当てられると、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お勧めします。

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[Address Assignment]** > **[Address Pools]** を選択します。

ステップ 2 IPv4 アドレスを追加するには、**[Add]** > **[IPv4 Address pool]** をクリックします。既存のアドレス プールを編集するには、アドレス プール テーブルで、[Edit] をクリックします。

ステップ 3 [Add/Edit IP Pool] ダイアログボックスで、次の情報を入力します。

- [Pool Name]：アドレス プールの名前を入力します。最大 64 文字を指定できます。
- [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。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 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。たとえば 10.10.147.177 のように、ドット付き 10 進数表記を使用します。
- [Subnet Mask]：この IP アドレスが常駐するサブネットを指定します。

ステップ 4 [Apply] をクリックします。

ステップ 5 **[OK]** をクリックします。

ローカル IPv6 アドレス プールの設定

[IP Pool] エリアには、設定されたアドレス プールが、名前ごとに、開始 IP アドレス範囲、アドレスプレフィックス、プールに設定できるアドレス数とともに表示されます。プールが存在しない場合、エリアは空です。ASA 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。最初のプール内のアドレスがすべて割り当てられると、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お勧めします。

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[Address Assignment]** > **[Address Pools]** を選択します。

ステップ 2 IPv6 アドレスを追加するには、**[Add]** > **[IPv6 Address pool]** をクリックします。既存のアドレス プールを編集するには、アドレス プール テーブルで、[Edit] をクリックします。

ステップ 3 [Add/Edit IP Pool] ダイアログボックスで、次の情報を入力します。

- [Name]：設定された各アドレス プールの名前を表示します。

  [Starting IP Address]：設定された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、2001:DB8::1 となります。

- [Prefix Length]：IP アドレス プレフィックス長をビット単位で入力します。たとえば、32 は CIDR 表記で /32 を表します。プレフィックス長は、IP アドレスが常駐するプールのサブネットを定義します。

- [Number of Addresses]：開始 IP アドレスから始まる、プールにある IPv6 アドレスの数を指定します。

ステップ 4 [Apply] をクリックします。

ステップ 5 **[OK]** をクリックします。

グループ ポリシーへの内部アドレス プールの割り当て

[Add or Edit Group Policy] ダイアログボックスでは、追加または編集している内部ネットワーク（クライアント）アクセス グループ ポリシーのアドレス プール、トンネリング プロトコル、フィルタ、接続設定、およびサーバーを指定できます。このダイアログボックスの各フィールドで、[Inherit] チェックボックスを選択すると、対応する設定の値をデフォルト グループ ポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

同じグループ ポリシーで IPv4 と IPv6 両方のアドレス ポリシーを設定できます。同じグループ ポリシーに両方のバージョンの IP アドレスが設定されている場合、IPv4 に設定されたクライアントは IPv4 アドレス、IPv6 に設定されたクライアントは IPv6 アドレスを取得し、IPv4 アドレスと IPv6 アドレス両方に設定されたクライアントは IPv4 アドレスと IPv6 アドレス両方を取得します。

手順

ステップ 1 ASDM を使用して ASA に接続し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。

ステップ 2 新しいグループ ポリシーを作成するか、内部アドレス プールを設定するグループ ポリシーを作成し、[Edit] をクリックします。

[General attributes] ペインは [group policy] ダイアログで、デフォルトで選択されています。

ステップ 3 [Address Pools] フィールドを使用して、このグループ ポリシーの IPv4 アドレス プールを指定します。[Select] をクリックし、IPv4 アドレス プールを追加または編集します。

ステップ 4 [IPv6 Address Pools] フィールドを使用して、このグループ ポリシーに使用する IPv6 アドレス プールを指定します。[Select] をクリックし、IPv6 アドレス プールを追加または編集します。

ステップ 5 [OK] をクリックします。

ステップ 6 [適用（Apply）] をクリックします。

DHCP アドレス指定の設定

DHCP を使用して VPN クライアントのアドレスを割り当てるには、まず DHCP サーバー、およびその DHCP サーバーで使用可能な IP アドレスの範囲を設定する必要があります。その後、接続プロファイル単位で DHCP サーバーを定義します。また、オプションとして、該当の接続プロファイルまたはユーザー名に関連付けられたグループ ポリシー内に、DHCP ネットワーク スコープも定義できます。

次の例では、firstgroup という名前の接続プロファイルに、172.33.44.19 の DHCP サーバーを定義しています。この例では、remotegroup というグループポリシーに対して、10.100.10.1 の DHCP ネットワークスコープも定義しています。（remotegroup というグループ ポリシーは、firstgroup という接続プロファイルに関連付けられています）。ネットワーク スコープを定義しない場合、DHCP サーバはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

始める前に

IPv4 アドレスを使用して、クライアント アドレスを割り当てる DHCP サーバーを識別できます。また、DHCP オプションはユーザーに転送されず、ユーザーはアドレス割り当てのみを受信します。

手順

ステップ 1 DHCP サーバーを設定します。

DHCP サーバーを使用して IPv6 アドレスを セキュアクライアント に割り当てることはできません。

a) **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）]> > [アドレス割り当て（Address Assignment）] > [割り当てポリシー（Assignment Policy）]** で DHCP が有効になっていることを確認します。

b) **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [DHCPサーバー（DHCP Server）]** を選択して、DHCP サーバーを設定します。

ステップ 2 接続プロファイルで DHCP サーバーを定義します。

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

b) [Connection Profiles] エリアで [Add] または [Edit] をクリックします。

c) 接続プロファイルの設定ツリーで、[Basic] をクリックします。

d) [Client Address Assignment] エリアで、クライアントに IP アドレスを割り当てるために使用する DHCP サーバーの IPv4 アドレスを入力します。たとえば、**172.33.44.19** と指定します。

ステップ 3 DHCPスコープを定義するために、接続プロファイルに関連付けられたグループ ポリシーを編集します。

a) **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループポリシー（Group Policies）]** を選択します。
b) 編集するグループ ポリシーをダブルクリックします。
c) 設定ツリーで、[Server] をクリックします。
d) 下矢印をクリックして、[More Options] エリアを拡大表示します。
e) [DHCPスコープの継承（DHCP Scope Inherit）] をオフにして、DHCP スコープを定義します。

接続プロファイルのアドレスプールに DHCP サーバーを設定した場合、DHCP スコープはこのグループのプールに使用するサブネットを識別します。DHCP サーバーには、そのスコープによって識別される同じサブネット内のアドレスも設定されている必要があります。スコープを使用すると、この特定のグループに使用する DHCP サーバーで定義されているアドレスプールのサブセットを選択できます。

ネットワーク スコープを定義しない場合、DHCP サーバはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

スコープを指定するには、目的のプールと同じサブネット上にあり、そのプール内にはないルーティング可能なアドレスを入力します。DHCP サーバは、この IP アドレスが属するサブネットを判別し、そのプールからの IP アドレスを割り当てます。

ルーティングの目的で可能な場合は常に、インターフェイスの IP アドレスを使用することを推奨します。たとえば、プールが 10.100.10.2 ～ 10.100.10.254 で、インターフェイスアドレスが 10.100.10.1/24 の場合、DHCP スコープとして 10.100.10.1 を使用します。ネットワーク番号は使用しないでください。DHCP は IPv4 アドレス指定にのみ使用することができます。選択したアドレスがインターフェイスアドレスではない場合、スコープアドレスのスタティックルートを作成する必要があります。

f) [OK] をクリックします。
g) [Apply] をクリックします。

ローカル ユーザーへの IP アドレスの割り当て

グループポリシーを使用するようにローカルユーザーアカウントを設定し、またセキュアクライアント属性を設定することもできます。IP アドレスの他のソースに障害が発生した場合に、これらのユーザーアカウントがフォールバックを提供するので、管理者は引き続きアクセスできます。

始める前に

ユーザーを追加または編集するには、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] の順に選択し、[Add] または [Edit] をクリックします。

デフォルトでは、[Edit User Account] 画面の設定ごとに [Inherit] チェックボックスがオンになっています。つまり、ユーザー アカウントは、デフォルト グループ ポリシー DfltGrpPolicy のその設定の値を継承するということです。

各設定内容をオーバーライドする場合は、[Inherit] チェックボックスをオフにし、新しい値を入力します。次の詳細な手順では IP アドレスの設定について説明します。設定の完全な詳細についてはローカルユーザーの VPN ポリシー属性の設定（112 ページ）を参照してください。

手順

ステップ 1 ASDM を開始し、**[Configuration]** > **[Remote Access VPN]** > **[AAA/Local Users]** > **[Local Users]** の順に選択します。

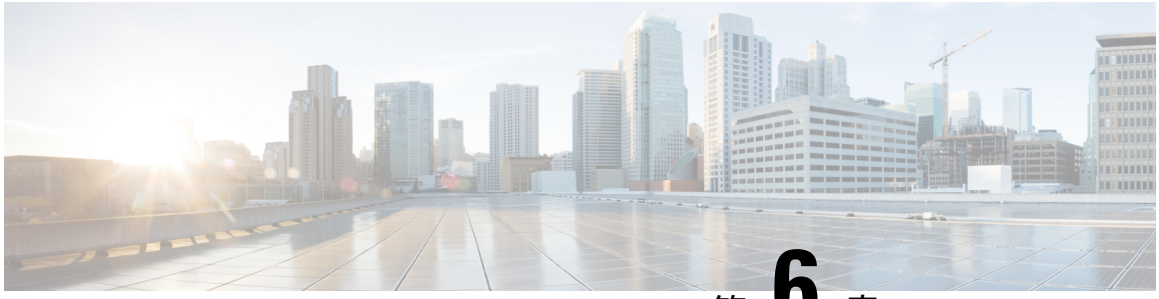
ステップ 2 設定するユーザーを選択し、[Edit] をクリックします。

ステップ 3 左側のペインで、[VPN Policy] をクリックします。

ステップ 4 このユーザーに対して専用の IPv4 アドレスを設定する場合は、[Dedicated IPv4 Address (Optional)] 領域で、IPv4 アドレスとサブネット マスクを入力します。

ステップ 5 このユーザーに専用の IPv6 アドレスを設定するには、[Dedicated IPv6 Address (Optional)] 領域に IPv6 プレフィックスを含む IPv6 アドレスを入力します。IPv6 プレフィックスは、IPv6 アドレスが常駐するサブネットを示します。

ステップ 6 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。



第 6 章

ダイナミック アクセス ポリシー

この章では、ダイナミック アクセス ポリシーを設定する方法を説明します。

ダイナミック アクセス ポリシーについて

VPN ゲートウェイは動的な環境で動作します。個々の VPN 接続には、頻繁に変更されるイントラネット設定、組織内の各ユーザーが持つさまざまなロール、および設定とセキュリティ レベルが異なるリモート アクセス サイトからのログインなど、複数の変数が影響する可能性があります。VPN環境でのユーザー認可のタスクは、スタティックな設定のネットワークでの認可タスクよりもかなり複雑です。

ASA ではダイナミック アクセス ポリシー（DAP）によって、これらのさまざまな変数に対処する認可機能を設定できます。ダイナミック アクセス ポリシーは、特定のユーザー トンネルまたはユーザー セッションに関連付ける一連のアクセス コントロール属性を設定して作成します。これらの属性により、複数のグループ メンバーシップやエンドポイント セキュリティの問題に対処します。つまり、ASA では、定義したポリシーに基づき、特定のセッションへのアクセス権が特定のユーザーに付与されます。ASA は、ユーザーが接続した時点で、DAP レコードからの属性を選択または集約することによって DAP を生成します。DAP レコードは、リモート デバイスのエンドポイント セキュリティ情報および認証されたユーザーの AAA 認可情報に基づいて選択されます。選択された DAP レコードは、ユーザー トンネルまたはセッションに適用されます。

DAP システムには、注意を必要とする次のコンポーネントがあります。

- DAP 選択コンフィギュレーション ファイル：セッション確立中に DAP レコードを選択して適用するために ASA が使用する、基準が記述されたテキスト ファイル。ASA 上に保存されます。ASDM を使用して、このファイルを変更したり、XML データ形式で ASA にアップロードしたりできます。DAP選択設定ファイルには、ユーザーが設定するすべての属性が記載されています。これには、AAA 属性、エンドポイント属性、およびネットワーク ACL と Web タイプ ACL のフィルタ、ポート転送、URL のリストとして設定されたアクセス ポリシーなどがあります。
- DfltAccess ポリシー：常に DAP サマリー テーブルの最後のエントリで、プライオリティは必ず0。デフォルトアクセスポリシーのアクセスポリシー属性を設定できますが、AAA 属性またはエンドポイント属性は含まれておらず、これらの属性は設定できません。DfltAccessPolicy は削除できません。また、サマリー テーブルの最後のエントリになっている必要があります。

詳細については、『*Dynamic Access Deployment Guide*』（https://supportforums.cisco.com/docs/DOC-1369）を参照してください。

DAP によるリモート アクセス プロトコルおよびポスチャ評価ツールのサポート

ASA は、管理者が設定したポスチャ評価ツールを使用してエンドポイント セキュリティ属性を取得します。このポスチャ評価ツールには、 Secure Firewall ポスチャモジュール、独立した HostScan/Secure Firewall ポスチャパッケージ、および NAC が含まれます。

次の表に、DAP がサポートしている各リモート アクセス プロトコル、その方式で使用可能なポスチャ評価ツール、およびそのツールによって提供される情報を示します。

サポートされるリモート アクセス プロトコル	**Secure Firewall ポスチャモジュール** **ホスト スキャン パッケージ** **Secure Firewall ポスチャ**	**Secure Firewall ポスチャモジュール** **Hostscan パッケージ** **Secure Firewall ポスチャ**	**NAC**	**Cisco NAC アプライアンス**
	ファイル情報、レジストリ キーの値、実行プロセス、オペレーティング システムを返す	マルウェア対策およびパーソナル ファイアウォール ソフトウェアの情報を返す	NAC ステータスを返す	VLAN タイプと VLAN ID を返す
IPsec VPN	いいえ	非対応	はい	はい

サポートされるリモート アクセス プロトコル	Secure Firewall ポスチャモジュール ホスト スキャン パッケージ Secure Firewall ポスチャ	Secure Firewall ポスチャモジュール Hostscan パッケージ Secure Firewall ポスチャ	NAC	Cisco NAC アプライアンス
Cisco AnyConnect VPN	はい	はい	はい	はい
クライアントレス（ブラウザベース）SSL VPN	はい	はい	非対応	非対応
PIX カットスループロキシ（ポスチャ評価は使用不可）	いいえ	非対応	非対応	非対応

DAP によるリモート アクセス接続のシーケンス

次のシーケンスに、標準的なリモート アクセス接続を確立する場合の概要を示します。

1. リモート クライアントが VPN 接続を試みます。
2. ASA は、設定された NAC 値と HostScan/Secure Firewall ポスチャ値を使用してポスチャ評価を実行します。
3. ASA は、AAA を介してユーザーを認証します。AAA サーバーは、ユーザーの認可属性も返します。
4. ASA は AAA 認可属性をそのセッションに適用し、VPN トンネルを確立します。
5. ASA は、AAA 認可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。
6. ASA は選択した DAP レコードから DAP 属性を集約し、その集約された属性が DAP ポリシーになります。
7. ASA はその DAP ポリシーをセッションに適用します。

ダイナミック アクセス ポリシーのライセンス

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

ダイナミックアクセスポリシー（DAP）には、次のいずれかのライセンスが必要です。

- Secure Client Premier：すべての DAP 機能を使用する場合。
- Secure Client Advantage：オペレーティングシステムおよびオペレーティングシステムまたは セキュアクライアント のバージョンチェック専用。

関連トピック

DAP への セキュアクライアント エンドポイント属性の追加 （213 ページ）

ダイナミック アクセス ポリシーの設定

始める前に

- 特に記載のない限り、DAP エンドポイント属性を設定する前に、HostScan/Secure Firewall ポスチャをインストールする必要があります。
- HostScan 4.3.x から HostScan 4.6.x 以降にアップグレードする場合は、アップグレードの前に、既存の AV/AS/FW エンドポイント属性を対応する代替 AM/FW エンドポイント属性に移行する必要があります。アップグレードおよび移行の完全な手順については、『AnyConnect HostScan 4.3.x to 4.6.x Migration Guide』を参照してください。
- Java Web Start セキュリティの問題のため、デバイスで webvpn ベースの設定を使用する場合は、設定した値を高度なエンドポイント属性に入力できないことがあります。この問題を解決するには、ASDM デスクトップアプリケーションを使用するか、または Java セキュリティの例外として AEA 関連の URL を追加します。
- ファイル、プロセス、レジストリのエンドポイント属性を設定する前に、ファイル、プロセス、レジストリの基本HostScan/Secure Firewall ポスチャ属性を設定する必要があります。手順については、ASDM 内で適切な UI 画面に移動し、[ヘルプ（Help）] をクリックしてください。
- DAP は、ASCII 文字のみサポートされます。

手順

ステップ 1 ASDM を起動し、**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [ダイナミックアクセスポリシー（Dynamic Access Policies）]** を選択します。

（注）
[Add]、[Edit]、および [Delete] アクションの下に [Incompatible] アクションボタンが表示される場合は、内部ライブラリの更新により既存 DAP ポリシー（HostScan 4.3.x 以前を使用して作成）と互換性がなくなったバージョン（4.6.x 以降）に HostScan をアップグレードしようとしています。ワンタイム移行手順を実行して、設定を適応させる必要があります。

[Incompatible] アクションが表示される場合は、HostScan のアップグレードが開始され、設定の移行が必要になったことを示しています。詳細な手順については、『AnyConnect Hostscan 4.3.x to 4.6.x Migration Guide』を参照してください。

ステップ 2 特定のマルウェア対策またはパーソナルファイアウォールのエンドポイント属性を含めるには、ペインの最上部近くの [設定（configuration）] リンクをクリックします。このリンクは、これら両方の機能をすでにイネーブルにしている場合には表示されません。

ステップ 3 設定済みの DAP のリストを表示します。

テーブルには次のフィールドが表示されます。

- [ACL Priority]：DAP レコードのプライオリティを表示します。

  ASA は、複数の DAP レコードからネットワーク ACL と Web タイプ ACL を集約するときに、この値を使用して ACL を論理的に順序付けします。ASA は、最上位のプライオリティ番号から最下位のプライオリティ番号の順にレコードを並べ、最下位のプライオリティをテーブルの一番下に配置します。番号が大きいほどプライオリティが高いことを意味します。たとえば、値が 4 の DAP レコードは値が 2 のレコードよりも高いプライオリティを持つことになります。プライオリティは、手動での並べ替えはできません。

- [Name]：DAP レコードの名前を表示します。
- [Network ACL List]：セッションに適用されるファイアウォール ACL の名前を表示します。
- [Web-Type ACL List]：セッションに適用される SSL VPN ACL の名前を表示します。
- [Description]：DAP レコードの目的を説明します。

ステップ 4 [Add] または [Edit] をクリックして、ダイナミック アクセス ポリシーの追加または編集 （204 ページ）を実行します。

ステップ 5 [Apply] をクリックして DAP 設定を保存します。

ステップ 6 [Find] フィールドを使用して、ダイナミック アクセス ポリシー（DAP）を検索します。

このフィールドへの入力を開始すると、DAP テーブルの各フィールドの先頭部分の文字が検索され、一致するものが検出されます。ワイルドカードを使用すると、検索範囲が広がります。

たとえば、[Find] フィールドに「**sal**」と入力した場合は、`Sales` という名前の DAP とは一致しますが、`Wholesalers` という名前の DAP とは一致しません。[Find] フィールドに ***sal** と入力すると、テーブル内の **Sales** または **Wholesalers** のうち、最初に出現したものが検出されます。

ステップ 7 ダイナミック アクセス ポリシーのテスト （206 ページ）を実行して設定を確認します。

ダイナミック アクセス ポリシーの追加または編集

手順

ステップ 1 ASDM を起動し、**[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** または **[Clientless SSL VPN Access]** > **[Dynamic Access Policies]** > **[Add]** または [Edit] を選択します。

ステップ 2 このダイナミック アクセス ポリシーの名前（必須）と説明（オプション）を入力します。

- [Policy Name] は、4 ～ 32 文字の文字列で、スペースは使用できません。
- DAP の [Description] フィールドには 80 文字まで入力できます。

ステップ 3 [ACL Priority] フィールドで、そのダイナミック アクセス ポリシーのプライオリティを設定します。

セキュリティ アプライアンスは、ここで設定した順序でアクセス ポリシーを適用します。数が大きいほどプライオリティは高くなります。有効値の範囲は 0 ～ 2147483647 です。デフォルト値は 0 です

ステップ 4 この DAP の選択基準を指定します。

a) [Selection Criteria] ペインのドロップダウン リスト（ラベルなし）で、ユーザーがこのダイナミック アクセス ポリシーを使用するには、すべてのエンドポイント属性を満たすことに加えて、ここで設定される AAA 属性値のいずれか（[ANY]）またはすべて（[ALL]）が必要となるのか、それとも一切不要（[NONE]）であるのかを選択します。

重複するエントリは許可されません。AAA 属性やエンドポイント属性を指定せずに DAP レコードを設定すると、レコードがすべての選択基準を満たしていることになるので、ASA は常にそのレコードを選択します。

b) [AAA Attributes] フィールドの [Add] または [Edit] をクリックして、DAP の AAA 属性選択基準の設定 （206 ページ）を実行します。

c) [Endpoint Attributes] 領域で [Add] または [Edit] をクリックして、DAP のエンドポイント属性選択基準の設定 （210 ページ）を実行します。

d) [Advanced] フィールドをクリックして、#unique_179を実行します。この機能を使用するには、Lua プログラミング言語の知識が必要です。

- [AND/OR]：基本的な選択ルールと、ここで入力する論理式との関係を定義します。つまり、すでに設定されている AAA 属性およびエンドポイント属性に新しい属性を追加するのか、またはそれら設定済みの属性に置き換えるのかを指定します。デフォルトは AND です。
- [Logical Expressions]：それぞれのタイプのエンドポイント属性のインスタンスを複数設定できます。新しい AAA 選択属性またはエンドポイント選択属性（あるいはその両方）を定義するフリー形式の LUA テキストを入力します。ASDM は、ここで入力されたテキストを検証せず、テキストを DAP XML ファイルにコピーするだけです。処理は ASA によって行われ、解析不能な式は破棄されます。

dap.xml ファイルのインポート/エクスポートについては、2 つの ASA 間で DAP XML ファイルをインポートおよびエクスポート （205 ページ）を参照してください。

ステップ 5 この DAP のアクセス/許可ポリシー属性を指定します。

ここで設定する属性値は、既存のユーザー、グループ、トンネル グループ、およびデフォルトのグループ レコードを含め、AAA システムの認可値を上書きします。DAP アクセスと許可ポリシー属性の設定 （232 ページ）を参照してください。

ステップ 6 **[OK]** をクリックします。

2 つの ASA 間で DAP XML ファイルをインポートおよびエクスポート

ASA のダイナミック アクセス ポリシー（DAP）設定は、ASA のフラッシュメモリ上の *dap.xml* というファイルに保存されます。このファイルには、DAP ポリシーの選択属性が含まれています。

（注） *dap.xml* ファイルをエクスポートして編集し（xml 構文を知っている場合）、再度インポートして戻すことはできますが、設定に誤りがあると、ASDM が DAP レコードの処理を停止する可能性があるため、十分に注意してください。構成のこの部分を操作する CLI はありません。

次の手順を使用して、2 つの ASA 間で *dap.xml* ファイルをインポートおよびエクスポートします。

手順では、ASA#1 から *dap.xml* ファイルをエクスポートし、ASA#2 にインポートする例を使用します。

ASDM を使用した ASA でのファイル処理については、『*Cisco ASA Series General Operations ASDM Configuration Guide*』の「*Managing Files*」の項を参照してください。

手順

ステップ 1 ASA#2 の *dap.xml* ファイルをクリアします。

a) ASA#2 の設定と *dap.xml* を外部の tftp または ftp サーバーに保存します。

b) ASA#2 の ASDM を終了します。

（注）
ASDM > **[ツール（Tools）]** > **[バックアップの設定（BackUp Configurations）]** > **[DAP 設定（DAP Configurations）]** オプションを使用して、*dap.xml* ファイルを保存することもできます。

ASA#2 フラッシュメモリ上の *dap.xml* ファイルの名前を変更または削除することもできます。

ステップ 2 ASA#2 コマンドプロンプトで、**clear configure dynamic-access-policy-record** コマンドを入力して、DAP レコードの構成を削除します。

ステップ 3 *dap.xml* ファイルを ASA#1 フラッシュからエクスポートし、ASA#2 フラッシュにインポートします。

ステップ 4 **dynamic-access-policy-record** コマンドを使用して、ASA#2 の ASA#1 からの DAP レコードエントリを設定します。

ステップ 5 ASA#2 で、**dynamic-access-policy-config activate** コマンドを使用して DAP を有効にします。

（注）
ASA#2 の ASDM を再起動して、DAP 設定をアクティブにすることもできます。

ステップ 6 ASA#2 で ASDM を再起動します。
新しい DAP ポリシーは ASA#2 で設定されます。

ダイナミック アクセス ポリシーのテスト

このペインでは、認可属性値のペアを指定することによって、デバイスで設定される DAP レコード セットが取得されるかどうかをテストできます。

手順

ステップ 1 属性値のペアを指定するには、[AAA Attribute] テーブルと [Endpoint Attribute] テーブルに関連付けられた [Add/Edit] ボタンを使用します。

[Add/Edit] ボタンをクリックすると表示されるダイアログは、[Add/Edit AAA Attributes] ウィンドウと [Add/Edit Endpoint Attributes] ダイアログボックスに表示されるダイアログに似ています。

ステップ 2 [Test] ボタンをクリックします。

デバイス上の DAP サブシステムは、各レコードの AAA およびエンドポイント選択属性を評価するときに、これらの値を参照します。結果は、[Test Results] 領域に表示されます。

DAP の AAA 属性選択基準の設定

DAP は AAA サービスを補完します。用意されている認可属性のセットは限られていますが、それらの属性によって AAA で提供される認可属性を無効にできます。AAA 属性は、Cisco AAA 属性階層から指定するか、ASA が RADIUS または LDAP サーバーから受信する応答属性一式から指定できます。ASA は、ユーザーの AAA 認可情報とセッションのポスチャ評価情報に基

づいて DAP レコードを選択します。ASA は、この情報に基づいて複数の DAP レコードを選択でき、それらのレコードを集約して DAP 認可属性を作成します。

手順

DAP レコードの選択基準として AAA 属性を設定するには、[Add/Edit AAA Attributes] ダイアログボックスで、使用する Cisco、LDAP、または RADIUS 属性を設定します。これらの属性は、入力する値に対して「=」または「!=」のいずれかに設定できます。各 DAP レコードに設定可能な AAA 属性の数に制限はありません。AAA 属性の詳細については、AAA 属性の定義（209 ページ）を参照してください。

[AAA Attributes Type]：ドロップダウン リストを使用して、Cisco、LDAP、または RADIUS 属性を選択します。

- [Cisco]：AAA 階層モデルに保存されているユーザー認可属性を参照します。DAP レコードの AAA 選択属性に、これらのユーザー認可属性の小規模なサブセットを指定できます。次の属性が含まれます。
  - [Group Policy]：VPN ユーザー セッションに関連付けられているグループ ポリシー名を示します。セキュリティ アプライアンスでローカルに設定するか、IETF クラス（25）属性として RADIUS/LDAP から送信します。最大 64 文字です。
  - [Assigned IP Address]：ポリシーに指定する IPv4 アドレスを入力します。
  - [Assigned IPv6 Address]：ポリシーに指定する IPv6 アドレスを入力します。
  - [Connection Profile]：コネクションまたはトネリングのグループ名。最大 64 文字です。
  - [Username]：認証されたユーザーのユーザー名。最大 64 文字です。ローカル認証、RADIUS 認証、LDAP 認証のいずれかを、またはその他の認証タイプ（RSA/SDI、NT Domain などのいずれかを使用している場合に適用されます。
  - [=/!=]：と等しい/と等しくない
- [LDAP]：LDAP クライアントは、ユーザーの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ LDAP 応答属性値のペアを保存します。LDAP クライアントでは、受信した順に応答属性をデータベースに書き込みます。その名前の後続の属性はすべて廃棄されます。ユーザー レコードとグループ レコードの両方が LDAP サーバーから読み込まれると、このシナリオが発生する場合があります。ユーザー レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

  Active Directory グループ メンバーシップをサポートするために、AAA LDAP クライアントでは、LDAP memberOf 応答属性に対する特別な処理が行われます。AD memberOf 属性は、AD 内のグループ レコードの DN 文字列を指定します。グループの名前は、DN 文字列内の最初の CN 値です。LDAP クライアントでは、DN 文字列からグループ名を抽出して、AAA memberOf 属性として格納し、応答属性データベースに LDAP memberOf 属性として格納します。LDAP 応答メッセージ内に追加の memberOf 属性が存在する場合、それらの属性からグループ名が抽出され、前の AAA memberOf 属性と結合されて、グループ名

がカンマで区切られた文字列が生成されます。この文字列は応答属性データベース内で更新されます。

LDAP 認証/認可サーバーへの VPN リモート アクセス セッションが次の 3 つの Active Directory グループ（memberOf 列挙）のいずれかを返す場合は、次の通りとなります。

cn=Engineering,ou=People,dc=company,dc=com

cn=Employees,ou=People,dc=company,dc=com

cn=EastCoastast,ou=People,dc=company,dc=com

ASA は、Engineering、Employees、EastCoast の 3 つの Active Directory グループを処理します。これらのグループは、aaa.ldap の選択基準としてどのような組み合わせでも使用できます。

LDAP 属性は、DAP レコード内の属性名と属性値のペアで構成されています。LDAP 属性名は、構文に従う必要があり、大文字、小文字を区別します。たとえば、AD サーバーが部門として返す値の代わりに、LDAP 属性の Department を指定した場合、DAP レコードはこの属性設定に基づき一致しません。

（注）
[Value] フィールドに複数の値を入力するには、セミコロン（;）をデリミタとして使用します。次に例を示します。

eng;sale; cn=Audgen VPN,ou=USERS,o=OAG

- [RADIUS]：RADIUS クライアントは、ユーザーの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ RADIUS 応答属性値のペアを保存します。RADIUS クライアントは、受け取った順序で応答属性をデータベースに書き込みます。その名前の後続の属性はすべて廃棄されます。ユーザー レコードおよびグループ レコードの両方が RADIUS サーバーから読み込まれた場合、このシナリオが発生する可能性があります。ユーザー レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

  RADIUS 属性は、DAP レコード内の属性番号と属性値のペアで構成されています。

  （注）
  RADIUS 属性について、DAP は Attribute ID = 4096 + RADIUS ID と定義します。

  次に例を示します。

  RADIUS 属性「Access Hours」の Radius ID は 1 であり、したがって DAP 属性値は 4096 + 1 = 4097 となります。

  RADIUS 属性「Member Of」の Radius ID は 146 であり、したがって DAP 属性値は 4096 + 146 = 4242 となります。

- LDAP および RADIUS 属性には、次の値があります。
  - [Attribute ID]：属性の名前/番号。最大 64 文字です。
  - [Value]：属性名（LDAP）または数値（RADIUS）。

[Value] フィールドに複数の値を入力するには、セミコロン（;）をデリミタとして使用します。例：`eng;sale; cn=Audgen VPN,ou=USERS,o=OAG`

- [=/!=]：と等しい/と等しくない

- LDAP には、[Get AD Groups] ボタンが含まれます。「Active Directory グループの取得（209 ページ）」を参照してください。

Active Directory グループの取得

Active Directory サーバーにクエリーを実行し、このペインで利用可能な AD グループを問い合わせることができます。この機能は、LDAP を使用している Active Directory サーバーだけに適用されます。このボタンは、Active Directory LDAP サーバーに対して、ユーザーが属するグループのリスト（memberOf 列挙）の問い合わせを実行します。このグループ情報を使用し、ダイナミック アクセス ポリシーの AAA 選択基準を指定します。

AD グループは、バックグランドで CLI の **how-ad-groups** コマンドを使用することで LDAP サーバーから取得されます。ASA がサーバーの応答を待つデフォルト時間は 10 秒です。aaa-server ホスト コンフィギュレーション モードで **group-search-timeout** コマンドを使用し、時間を調整できます。

[Edit AAA Server] ペインで Group Base DN を変更し、Active Directory 階層の中で検索を開始するレベルを変更できます。このウィンドウでは、ASA がサーバーの応答を待つ時間も変更できます。これらの機能を設定するには、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups] > [Edit AAA Server] を選択します。

（注） Active Directory サーバーに多数のグループが存在する場合は、サーバーが応答パケットに含めることのできるデータ量の制限に従って、取得した AD グループのリスト（または **show ad-groups** コマンドの出力）が切り詰められることがあります。この問題を回避するには、フィルタ 機能を使用し、サーバーが返すグループ数を減らしてください。

[AD Server Group]：AD グループを取得する AAA サーバー グループの名前。

[Filter By]：表示されるグループ数を減らすために、グループ名またはグループ名の一部を指定します。

[Group Name]：サーバーから取得された AD グループのリスト。

AAA 属性の定義

次の表に、DAP で使用できる AAA 選択属性名の定義を示します。属性名フィールドは、LUA 論理式での各属性名の入力方法を示しており、[Add/Edit Dynamic Access Policy] ペインの [Advanced] セクションで使用します。

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
Cisco	aaa.cisco.grouppolicy	AAA	string	64	ASA 上のグループ ポリシー名、または RADIUS/LDAP サーバーから IETF-CLass (25) 属性として送信されたグループ ポリシー名
	aaa.cisco.ipaddress	AAA	number	-	フルトンネル VPN クライアントに割り当てられた IP アドレス（IPsec、L2TP/IPsec、SSL VPN Anyconnect モジュール）
	aaa.cisco.tunnelgroup	AAA	string	64	接続プロファイル（トンネルグループ）の名前
	aaa.cisco.username	AAA	string	64	認証されたユーザーの名前（ローカル認証や認可を使用している場合に適用）
LDAP	aaa.ldap.<*label*>	LDAP	string	128	LDAP 属性値ペア
RADIUS	aaa.radius.<number>	RADIUS	string	128	RADIUS 属性値ペア

DAP のエンドポイント属性選択基準の設定

エンドポイント属性には、エンドポイント システム環境、ポスチャ評価結果、およびアプリケーションに関する情報が含まれています。ASA は、セッション確立時にエンドポイント属性の集合を動的に生成し、セッションに関連付けられているデータベースにそれらの属性を保存します。各 DAP レコードには、ASA がセッションの DAP レコードを選択するために満たす必要があるエンドポイント選択属性が指定されています。ASA は、設定されている条件をすべて満たす DAP レコードだけを選択します。

始める前に

- DAP レコードの選択基準としてエンドポイント属性を設定することは、ダイナミック アクセス ポリシーの設定（202 ページ）のための大きなプロセスの一部です。DAP の選択基準としてエンドポイント属性を設定する前に、この手順を確認します。
- エンドポイント属性の詳細については、「エンドポイント属性の定義（221 ページ）」を参照してください。
-

- メモリ常駐型のマルウェア対策、およびパーソナル ファイアウォール プログラムを HostScan/Secure Firewall ポスチャがチェックする方法の詳細については、DAP とマルウェア対策およびパーソナル ファイアウォール プログラム （220 ページ）を参照してください。

手順

ステップ 1 [Add] または [Edit] をクリックして、次のいずれかのエンドポイント属性を選択基準として追加します。

各タイプのエンドポイント属性のインスタンスを複数作成できます。各 DAP レコードに設定可能なエンドポイント属性の数に制限はありません。

- DAP へのマルウェア対策エンドポイント属性の追加 （212 ページ）
- DAP へのアプリケーション属性の追加 （212 ページ）
- DAP への セキュアクライアント エンドポイント属性の追加 （213 ページ）
- DAP へのファイル エンドポイント属性の追加 （215 ページ）
- DAP へのデバイス エンドポイント属性の追加 （215 ページ）
- DAP への NAC エンドポイント属性の追加 （216 ページ）
- DAP へのオペレーティング システム エンドポイント属性の追加 （217 ページ）
- DAP へのパーソナル ファイアウォール エンドポイント属性の追加 （217 ページ）
- DAP へのポリシー エンドポイント属性の追加 （218 ページ）
- DAP へのプロセス エンドポイント属性の追加 （218 ページ）
- DAP へのレジストリ エンドポイント属性の追加 （219 ページ）
- DAP への複数証明書認証属性の追加 （219 ページ）

ステップ 2 条件に一致する DAP ポリシーを指定します。

これらのエンドポイント属性のタイプごとに、ユーザーがあるタイプのインスタンスのすべてを持つように DAP ポリシーで要求する（Match all = AND、デフォルト）のか、またはそれらのインスタンスを 1 つだけ持つように要求する（Match Any = OR）のかを決定します。

a) [Logical Op] をクリックします。
b) エンドポイント属性のタイプごとに、[Match Any]（デフォルト）または [Match All] を選択します。
c) [OK] をクリックします。

ステップ 3 ダイナミック アクセス ポリシーの追加または編集 （204 ページ）に戻ってください。

DAP へのマルウェア対策エンドポイント属性の追加

始める前に

HostScan 4.3.x から HostScan 4.6.x 以降にアップグレードする場合は、アップグレードの前に、既存の AV/AS/FW エンドポイント属性を対応する代替 AM/FW エンドポイント属性に移行する必要があります。アップグレードおよび移行の完全な手順については、『AnyConnect HostScan 4.3.x to 4.6.x Migration Guide』を参照してください。

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Anti-Malware] を選択します。

ステップ 2 適切なボタン [Installed] または [Not Installed] をクリックして、選択したエンドポイント属性とそれに付随する修飾子（[Name]/[Operation]/[Value] 列の下のフィールド）をインストールするか、またはインストールしないかを指定します。

ステップ 3 リアルタイム スキャンを有効または無効のどちらにするかを決定します。

ステップ 4 [Vendor] リスト ボックスで、テスト対象のマルウェア対策ベンダーの名前をクリックします。

ステップ 5 [Product Description] チェックボックスをオンにして、テストするベンダーの製品名をリスト ボックスから選択します。

ステップ 6 [Version] チェックボックスをオンにして、操作フィールドを、[Version] リスト ボックスで選択した製品バージョン番号に等しい（=）、等しくない（!=）、より小さい（<）、より大きい（>）、以下（<=）、または以上（>=）に設定します。

リスト ボックスで選択したバージョンに x が付いている場合（たとえば 3.x）は、この x を具体的なリリース番号で置き換えます（たとえば 3.5）。

ステップ 7 [Last Update] チェックボックスをオンにします。最後の更新からの日数を指定します。更新を、ここで入力した日数よりも早く（[<]）実行するか、遅く（[>]）実行するかを指定できます。

ステップ 8 **[OK]** をクリックします。

DAP へのアプリケーション属性の追加

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Application] を選択します。

ステップ 2 [Client Type] の操作フィールドで、[=]（等しい）または [!=]（等しくない）を選択します。

ステップ 3 [Client type] リスト ボックスで、テスト対象のリモート アクセス接続のタイプを指定します。

ステップ 4 **[OK]** をクリックします。

DAP への セキュアクライアント エンドポイント属性の追加

セキュアクライアント エンドポイント属性（モバイルポスチャまたは AnyConnect アイデンティティ拡張機能（ACIDex）とも呼ばれる）は、Cisco Secure Clientの AnyConnect VPN モジュールが ASA にポスチャ情報を伝えるために使用されます。ダイナミック アクセス ポリシーでは、ユーザーの認証にこれらのエンドポイント属性が使用されます。

モバイルポスチャ属性をダイナミック アクセス ポリシーに組み込むと、エンドポイントに HostScan/Secure Firewall ポスチャがエンドポイントにインストールされていなくても適用できます。

一部のモバイルポスチャ属性は、モバイルデバイス上で実行しているセキュアクライアントにのみ関連します。その他のモバイルポスチャ属性は、モバイルデバイス上で実行している セキュアクライアントと セキュアクライアント デスクトップクライアント上で実行している AnyConnect クライアントの両方に関連します。

始める前に

モバイルポスチャを活用するには、セキュアクライアント Mobile ライセンスと、セキュアクライアント Premium ライセンスが ASA にインストールされている必要があります。これらのライセンスをインストールする企業は、DAP 属性および他の既存のエンドポイント属性に基づいてサポートされているモバイル デバイスの DAP ポリシーを適用できます。これには、モバイル デバイスからのリモート アクセスの許可または拒否が含まれます。

手順

ステップ 1 [エンドポイント属性タイプ（Endpoint Attribute Type）] リストボックスで セキュアクライアント を選択します。

ステップ 2 [クライアントバージョン（Client Version）] チェックボックスをオンにして、等しい（=）、等しくない（!=）、より小さい（<）、より大きい（>）、以下（<=）、または以上（>=）を操作フィールドで選択してから、[クライアントバージョン（Client Version）] フィールドで セキュアクライアントバージョン番号を指定します。

このフィールドを使用すると、モバイルデバイス（携帯電話やタブレットなど）のクライアント バージョンを評価できるほか、デスクトップやラップトップ デバイスのクライアント バージョンも評価できます。

ステップ 3 [Platform] チェックボックスをオンにして、等しい（=）または等しくない（!=）を操作フィールドで選択してから、[Platform] リスト ボックスでオペレーティング システムを選択します。

このフィールドを使用すると、モバイル デバイス（携帯電話やタブレットなど）のオペレーティング システムを評価できるほか、デスクトップやラップトップ デバイスのオペレーティ

ングシステムも評価できます。プラットフォームを選択すると、追加の属性フィールドである [Device Type] と [Device Unique ID] が使用可能になります。

ステップ 4 [Platform Version] チェックボックスをオンにして、等しい（=）、等しくない（!=）、より小さい（<）、より大きい（>）、以下（<=）、または以上（>=）を操作フィールドで選択してから、[Platform Version] フィールドでオペレーティング システム バージョン番号を指定します。

作成する DAP レコードにこの属性も含まれるようにするには、前の手順でプラットフォームも必ず指定してください。

ステップ 5 [Platform] チェックボックスをオンにした場合は、[Device Type] チェックボックスをオンにすることができます。等しい（=）または等しくない（!=）を操作フィールドで選択してから、デバイスを [Device Type] フィールドで選択するか入力します。

サポートされるデバイスであるにもかかわらず、[Device Type] フィールドのリストに表示されていない場合は、[Device Type] フィールドに入力できます。デバイスタイプ情報を入手する最も確実な方法は、セキュアクライアントをエンドポイントにインストールして ASA に接続し、DAP トレースを実行することです。DAP トレースの結果の中で、**endpoint.anyconnect.devicetype** の値を見つけます。この値を [Device Type] フィールドに入力する必要があります。

ステップ 6 [Platform] チェックボックスをオンにした場合は、[Device Unique ID] チェックボックスをオンにすることができます。等しい（=）または等しくない（!=）を操作フィールドで選択してから、デバイスの一意の ID を [Device Unique ID] フィールドに入力します。

[Device Unique ID] によって個々のデバイスが区別されるので、特定のモバイル デバイスに対するポリシーを設定できます。デバイスの一意の ID を取得するには、そのデバイスを ASA に接続して DAP トレースを実行し、**endpoint.anyconnect.deviceuniqueid** の値を見つける必要があります。この値を [Device Unique ID] フィールドに入力する必要があります。

ステップ 7 [Platform] をオンにした場合は、[MAC Addresses Pool] フィールドに MAC アドレスを追加できます。等しい（=）または等しくない（!=）を操作フィールドで選択してから、MAC アドレスを指定します。各 MAC アドレスのフォーマットは xx-xx-xx-xx-xx-xx であることが必要です。x は有効な 16 進数文字（0 ～ 9、A ～ F、または a ～ f）です。MAC アドレスは、1 つ以上の空白スペースで区切る必要があります。

MAC アドレスによって個々のシステムが区別されるので、特定のデバイスに対するポリシーを設定できます。システムの MAC アドレスを取得するには、そのデバイスを ASA に接続して DAP トレースを実行し、**endpoint.anyconnect.macaddress** の値を見つける必要があります。この値を [MAC Address Pool] フィールドに入力する必要があります。

ステップ 8 **[OK]** をクリックします。

DAP へのファイル エンドポイント属性の追加

始める前に

ファイルエンドポイント属性を設定する前に、どのファイルをスキャンするかを[HostScan/Secure Firewall ポスチャ（HostScan/Secure Firewall Posture）] ウィンドウで定義します。

HostScan バージョン 4.x の場合、ASDM で [設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [Secure Desktop Manager] > [HostScan] を選択します。Secure Firewall ポスチャバージョン 5.x の場合、ASDM で [設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ポスチャ（Secure Firewall用）（Posture (for Secure Firewall)）] > [ポスチャ設定（Posture Settings）] を選択します。

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [File] を選択します。

ステップ 2 [Exists] と [Does not exist] のオプション ボタンでは、選択したエンドポイント属性とそれに付随する修飾子（[Exists]/[Does not exist] ボタンの下にあるフィールド）が存在する必要があるかどうかに応じて、該当するものを選択します。

ステップ 3 [Endpoint ID] リスト ボックスで、スキャン対象のファイル エントリに等しいエンドポイント ID をドロップダウン リストから選択します。

ファイルの情報が [Endpoint ID] リスト ボックスの下に表示されます。

ステップ 4 [Last Update] チェックボックスをオンにしてから、更新日からの日数が指定の値よりも小さい（<）と大きい（>）のどちらを条件とするかを操作フィールドで選択します。更新日からの日数を [days] フィールドに入力します。

ステップ 5 [Checksum] チェックボックスをオンにしてから、テスト対象ファイルのチェックサム値と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 6 [Compute CRC32 Checksum**]** をクリックすると、テスト対象のファイルのチェックサム値が計算されます。

ステップ 7 **[OK]** をクリックします。

DAP へのデバイス エンドポイント属性の追加

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Device] を選択します。

ステップ 2 [Host Name] チェックボックスをオンにしてから、テスト対象デバイスのホスト名と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。完全修飾ドメイン名（FQDN）ではなく、コンピュータのホスト名のみを使用します。

ステップ 3 [MAC address] チェックボックスをオンにしてから、テスト対象のネットワーク インターフェイス カードの MAC アドレスと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。1 つのエントリにつき MAC アドレスは 1 つだけです。アドレスのフォーマットは xxxx.xxxx.xxxx であることが必要です。x は 16 進数文字です。

ステップ 4 [BIOS Serial Number] チェックボックスをオンにしてから、テスト対象のデバイスの BIOS シリアル番号と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。数値フォーマットは、製造業者固有です。フォーマット要件はありません。

ステップ 5 [TCP/UDP Port Number] チェックボックスをオンにしてから、テスト対象のリスニング状態の TCP ポートと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

TCP/UDP コンボ ボックスでは、テスト対象（TCP（IPv4）、UDP（IPv4）、TCP（IPv6）、または UDP（IPv6））のポートの種類を選択します。複数のポートをテストする場合は、DAP の個々のエンドポイント属性のルールをいくつか作成し、それぞれに 1 個のポートを指定します。

ステップ 6 [Version of Secure Desktop (CSD)] チェックボックスをオンにしてから、エンドポイント上で実行される HostScan/Secure Firewall ポスチャ イメージのバージョンと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 7 [Version of Endpoint Assessment] チェックボックスをオンにしてから、テスト対象のエンドポイント アセスメント（OPSWAT）のバージョンと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 8 **[OK]** をクリックします。

DAP への NAC エンドポイント属性の追加

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [NAC] を選択します。

ステップ 2 [Posture Status] チェックボックスをオンにしてから、ACS によって受信されるポスチャ トークン文字列と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。ポスチャ トークン文字列を [Posture Status] テキスト ボックスに入力します。

ステップ 3 **[OK]** をクリックします。

DAP へのオペレーティング システム エンドポイント属性の追加

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Operating System] を選択します。

ステップ 2 [OS Version] チェックボックスをオンにしてから、[OS Version] リスト ボックスで設定するオペレーティング システム（Windows、Mac、または Linux）と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 3 [OS Update] チェックボックスをオンにしてから、[OS Update] テキスト ボックスに入力する Windows、Mac、または Linux オペレーティング システムのサービス パックと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 4 **[OK]** をクリックします。

DAP へのパーソナル ファイアウォール エンドポイント属性の追加

始める前に

HostScan 4.3.x から HostScan 4.6.x 以降にアップグレードする場合は、アップグレードの前に、既存の AV/AS/FW エンドポイント属性を対応する代替 AM/FW エンドポイント属性に移行する必要があります。アップグレードおよび移行の完全な手順については、『AnyConnect HostScan 4.3.x to 4.6.x Migration Guide』を参照してください。

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Operating System] を選択します。

ステップ 2 適切なボタン [Installed] または [Not Installed] をクリックして、選択したエンドポイント属性とそれに付随する修飾子（[Name]/[Operation]/[Valud] 列の下のフィールド）をインストールするか、またはインストールしないかを指定します。

ステップ 3 [Vendor] リスト ボックスで、テスト対象のパーソナル ファイアウォール ベンダーの名前をクリックします。

ステップ 4 [Product Description] チェックボックスをオンにして、テストするベンダーの製品名をリスト ボックスから選択します。

ステップ 5 [Version] チェックボックスをオンにして、操作フィールドを、[Version] リスト ボックスで選択した製品バージョン番号に等しい（=）、等しくない（!=）、より小さい（<）、より大きい（>）、以下（<=）、または以上（>=）に設定します。

[Version] リスト ボックスで選択したバージョンに x が付いている場合（たとえば 3.x）は、この x を具体的なリリース番号で置き換えます（たとえば 3.5）。

ステップ 6 [Last Update] チェックボックスをオンにします。最後の更新からの日数を指定します。更新を、ここで入力した日数よりも早く（[<]）実行するか、遅く（[>]）実行するかを指定できます。

ステップ 7 [OK] をクリックします。

DAP へのポリシー エンドポイント属性の追加

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Policy] を選択します。

ステップ 2 [Location] チェックボックスをオンにしてから、Cisco Secure Desktop Microsoft Windows ロケーション プロファイルと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。Cisco Secure Desktop Microsoft Windows ロケーション プロファイル文字列を [Location] テキスト ボックスに入力します。

ステップ 3 **[OK]** をクリックします。

DAP へのプロセス エンドポイント属性の追加

始める前に

プロセスエンドポイント属性を設定する前に、どのプロセスをスキャンするかを Cisco Secure Desktop の [HostScan/Secure Firewallポスチャ（HostScan/Secure Firewall Posture）] ウィンドウで定義します。

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Process] を選択します。

ステップ 2 [Exists] または [Does not exist] のボタンでは、選択したエンドポイント属性とそれに付随する修飾子（[Exists]/[Does not exist] ボタンの下にあるフィールド）が存在する必要があるかどうかに応じて、該当するものをクリックします。

ステップ 3 [Endpoint ID] リスト ボックスで、スキャン対象のエンドポイント ID をドロップダウン リストから選択します。

エンドポイント ID プロセス情報がリスト ボックスの下に表示されます。

ステップ 4 **[OK]** をクリックします。

DAP へのレジストリ エンドポイント属性の追加

レジストリ エンドポイント属性のスキャンは Windows オペレーティング システムにのみ適用されます。

始める前に

レジストリエンドポイント属性を設定する前に、どのレジストリキーをスキャンするかを [HostScan/Secure Firewall ポスチャ（HostScan/Secure Firewall Posture）] ウィンドウで定義します。

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Registry] を選択します。

ステップ 2 [Exists] または [Does not exist] のボタンでは、レジストリ エンドポイント属性とそれに付随する修飾子（[Exists]/[Does not exist] ボタンの下にあるフィールド）が存在する必要があるかどうかに応じて、該当するものをクリックします。

ステップ 3 [Endpoint ID] リスト ボックスで、スキャン対象のレジストリ エントリに等しいエンドポイント ID をドロップダウン リストから選択します。

レジストリの情報が [Endpoint ID] リスト ボックスの下に表示されます。

ステップ 4 [Value] チェックボックスをオンにしてから、操作フィールドで等しい（=）または等しくない（!=）を選択します。

ステップ 5 最初の [Value] リスト ボックスで、レジストリ キーが dword か文字列かを指定します。

ステップ 6 2 つ目の [Value] 操作リスト ボックスに、スキャン対象のレジストリ キーの値を入力します。

ステップ 7 スキャン時にレジストリ エントリの大文字と小文字の違いを無視するには、チェックボックスをオンにします。検索時に大文字と小文字を区別するには、チェックボックスをオフにしてください。

ステップ 8 **[OK]** をクリックします。

DAP への複数証明書認証属性の追加

受信した証明書のいずれかを設定されたルールで参照できるように各証明書をインデックス化できます。これらの証明書フィールドに基づいて、接続試行を許可または拒否する DAP ルールを設定できます。

手順

ステップ 1 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] > [Add Endpoint Attribute]** の順に移動します。

ステップ 2 [Endpoint Attribute Type] としてドロップダウン メニューの [Multiple Certificate Authentication] を選択します。

ステップ 3 必要に応じて次のいずれかまたはすべてを設定します。

- Subject Name
- 発行元名
- Subject Alternate Name
- Serial Number

ステップ 4 証明書ストアをデフォルトの [None] のままにしていずれのストアからの証明書も許可するか、ユーザーのみまたはマシンのみを許可するように選択します。[User] または [Machine] を選択する場合、証明書の元のストアを入力する必要があります。この情報は、プロトコルでクライアントによって送信されます。

DAP とマルウェア対策およびパーソナル ファイアウォール プログラム

セキュリティ アプライアンスは、ユーザー属性が、設定済みの AAA 属性およびエンドポイント属性に一致する場合に DAP ポリシーを使用します。プリログイン評価モジュールおよび HostScan/Secure Firewall ポスチャは、設定済みエンドポイント属性の情報をセキュリティアプライアンスに返し、DAP サブシステムでは、その情報に基づいてそれらの属性値に一致する DAP レコードを選択します。

マルウェア対策およびパーソナルファイアウォールプログラムのほとんど（すべてではなく）は、アクティブ スキャンをサポートしています。つまり、それらのプログラムはメモリ常駐型であり、常に動作しています。HostScan/Secure Firewall ポスチャは、エンドポイントにプログラムがインストールされているかどうか、およびそのプログラムがメモリ常駐型かどうかを、次のようにしてチェックします。

- インストールされているプログラムがアクティブスキャンをサポートしない場合、HostScan/Secure Firewall ポスチャはそのソフトウェアの存在をレポートします。DAP システムは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブスキャンをサポートしており、そのプログラムでアクティブスキャンがイネーブルになっている場合、HostScan/Secure Firewall ポスチャはそのソフトウェアの存在をレポートします。この場合も、セキュリティアプライアンスは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブスキャンをサポートしており、そのプログラムでアクティブスキャンが無効になっている場合、HostScan/Secure Firewall ポスチャはそのソフトウェアの存在を無視します。セキュリティアプライアンスは、そのプログラムを指定する DAP レコードを選択しません。さらに、プログラムがインストールされている場合でも、DAP に関する多数の情報が含まれる **debug trace** コマンドの出力にはプログラムの存在が示されません。

（注） HostScan 4.3.x から HostScan 4.6.x 以降にアップグレードする場合は、アップグレードの前に、既存の AV/AS/FW エンドポイント属性を対応する代替 AM/FW エンドポイント属性に移行する必要があります。アップグレードおよび移行の完全な手順については、『AnyConnect HostScan 4.3.x to 4.6.x Migration Guide』を参照してください。

エンドポイント属性の定義

次に、DAP で使用できるエンドポイント選択属性を示します。[Attribute Name] フィールドは、LUA 論理式での各属性名の入力方法を示しており、[Dynamic Access Policy Selection Criteria] ペインの [Advanced] 領域で使用します。*label* 変数は、アプリケーション、ファイル名、プロセス、またはレジストリ エントリを示します。

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
マルウェア対策	endpoint.am["*label*"].exists	Host ScanSecure Firewall ポスチャ	true	—	マルウェア対策プログラムが存在する
	endpoint.am["*label*"].version		string	32	Version
	endpoint.am["*label*"].description		string	128	マルウェア対策の説明
	endpoint.am["*label*"].lastupdate		整数	—	マルウェア対策定義を更新してからの経過時間（秒）
Personal Firewall	endpoint.pfw["*label*"].exists	Host ScanSecure Firewall ポスチャ	true	—	パーソナルファイアウォールが存在する
	endpoint.pfw["*label*"].version		string	string	Version
	endpoint.pfw["*label*"].description		string	128	パーソナルファイアウォールの説明

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
AnyConnect（HostScan/Secure Firewall ポスチャは不要）	endpoint.anyconnect.clientversion	エンドポイント	version	—	セキュアクライアント バージョン
	endpoint.anyconnect.platform		string	—	セキュアクライアントがインストールされているオペレーティングシステム
	endpoint.anyconnect.platformversion		version	64	セキュアクライアントがインストールされているオペレーティングシステムのバージョン
	endpoint.anyconnect.devicetype		string	64	セキュアクライアントがインストールされているモバイルデバイスのタイプ
	endpoint.anyconnect.deviceuniqueid			64	セキュアクライアントがインストールされているモバイルデバイスの一意の ID
	endpoint.anyconnect.macaddress		string	—	セキュアクライアントがインストールされているデバイスの MAC アドレス。 フォーマットは xx-xx-xx-xx-xx-xx であることが必要です。x は有効な 16 進数文字です。
アプリケーション	endpoint.application.clienttype	アプリケーション	string	—	クライアント タイプ： CLIENTLESS ANYCONNECT IPSEC L2TP

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
デバイス	endpoint.device. hostname	エンドポイント	string	64	ホスト名のみ。FQDN ではありません
	endpoint.device.MAC		string	—	ネットワーク インターフェイス カードの MAC アドレス。1 つのエントリにつき MAC アドレスは 1 つだけです フォーマットは xxxx.xxxx.xxxx であることが必要です。x は 16 進数文字です。
	endpoint.device.id		string	64	BIOS シリアル番号。数値フォーマットは、製造業者固有です。フォーマット要件はありません
	endpoint.device.port		string	—	リスニング状態の TCP ポート 1 回線ごとに 1 つのポートを定義できます 1 ～ 65535 の範囲の整数
	endpoint.device. protection_version		string	64	実行される HostScan/Secure Firewall ポスチャイメージのバージョン
	endpoint.device. protection_extension		string	64	Endpoint Assessment（OPSWAT）のバージョン

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
ファイル	endpoint.file["*label*"].exists		true	—	ファイルが存在する
	endpoint.file[“label”].endpointid				
	endpoint.file["*label*"].lastmodified		整数	—	ファイルが最後に変更されてからの経過時間（秒）
	endpoint.file["*label*"].crc.32		整数	—	ファイルの CRC32 ハッシュ
NAC	endpoint.nac.status	NAC	string	—	ユーザー定義ステータス ストリング
オペレーティング システム	endpoint.os.version		string	32	オペレーティング システム
	endpoint.os.servicepack		整数	—	Windows のサービス パック
ポリシー（Policy）	endpoint.policy.location		string	64	
プロセス	endpoint.process["*label*"].exists		true	—	プロセスが存在する
	endpoint.process["*label*"].path		string	255	プロセスのフルパス
Registry	endpoint.registry["*label*"].type		*dword string*	—	dword
	endpoint.registry["*label*"].value		string	255	レジストリ エントリの値
VLAN	endoint.vlan.type	CNA	string	—	VLAN タイプ： ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

LUA を使用した DAP における追加の DAP 選択基準の作成

このセクションでは、AAA またはエンドポイント属性の論理式の作成方法について説明します。これを行うには、LUA に関する高度な知識が必要です。LUA のプログラミングの詳細情報については、http://www.lua.org/manual/5.1/manual.html を参照してください。

[Advanced] フィールドに、AAA またはエンドポイント選択論理演算を表す自由形式の LUA テキストを入力します。ASDM は、ここで入力されたテキストを検証せず、テキストを DAP ポリシー ファイルにコピーするだけです。処理は ASA によって行われ、解析不能な式は破棄されます。

このオプションは、上の説明にある AAA およびエンドポイントの属性領域で指定可能な基準以外の選択基準を追加する場合に有効です。たとえば、指定された条件のいずれかを満たす、すべてを満たす、またはいずれも満たさない AAA 属性を使用するように ASA を設定できます。エンドポイント属性は累積され、そのすべてを満たす必要があります。セキュリティ アプライアンスが任意のエンドポイント属性を使用できるようにするには、LUA で適切な論理式を作成し、ここでその式を入力する必要があります。

次のセクションでは、LUA EVAL 式作成の詳細と例を示します。

- LUA EVAL 式を作成する構文 （225 ページ）
- DAP EVAL 式の例 （230 ページ）
- 追加の LUA 関数 （227 ページ）

LUA EVAL 式を作成する構文

（注） [Advanced] モードを使用する必要がある場合は、プログラムを直接的に検証することが可能になり、明確になるため、できるだけ EVAL 式を使用することをお勧めします。

EVAL(<*attribute*> , <comparison>, {<*value*> | <*attribute*>}, [<type>])

<attribute>	AAA 属性または Cisco Secure Desktop から返された属性。属性の定義については、エンドポイント属性の定義 （221 ページ）を参照してください。

<comparison>	次の文字列のいずれか（引用符が必要）	
	“EQ”	等しい
	“NE”	等しくない
	“LT”	より小さい
	“GT”	より大きい
	“LE”	以下
	“GE”	以上
<value>	引用符で囲まれ、属性と比較する値を含む文字列	
<type>	次の文字列のいずれか（引用符が必要）	
	“string”	大文字、小文字を区別する文字列の比較
	“”	大文字、小文字を区別しない文字列の比較
	“integer”	数値比較で、文字列値を数値に変換
	“hex”	16 進数を用いた数値比較で、16 進数の文字列を 16 進数に変換
	“version”	X.Y.Z. 形式（X、Y、Z は数字）のバージョンを比較

HostScan 4.6（およびそれ以降）および Secure Firewall ポスチャバージョン 5 の LUA 手順

'ANY' のウイルス対策（endpoint.am）用 LUA スクリプト（最終更新済み）

次の LUA スクリプトを使用して、'ANY' のウイルス対策製品/ベンダー（endpoint.am）を確認します。異なる最終更新の間隔に対応するため、修正が適用される場合があります。次の例は、30 日（2592000 秒と記載）以内に実行されたものとする最終更新の方法を示しています。

```
assert(function()
  for k,v in pairs(endpoint.am) do
    if(EVAL(v.activescan, "EQ", "ok", "string")and EVAL (v.lastupdate, "LT", "2592000",
 "integer"))
     then
             return true
         end
  end
  return false
end)()
```

'ANY' のパーソナル ファイアウォール用 LUA スクリプト

次の LUA スクリプトを使用して、'ANY' のファイアウォール製品/ベンダー（endpoint.pfw）を確認します。

```
assert(function()
    for k,v in pairs(endpoint.pfw) do
         if (EVAL(v.enabled, "EQ", "ok", "string")) then
              return true
         end
    end
    return false
end)()
```

追加の LUA 関数

ダイナミック アクセス ポリシーで作業している場合、一致基準に高度な柔軟性が必要とされることが考えられます。たとえば、以下に従い別の DAP を適用しなければならない場合があります。

- CheckAndMsg は、DAP がコールするように設定可能な LUA 関数です。条件に基づきユーザー メッセージを生成します。
- 組織ユニット（OU）またはユーザー オブジェクトの他の階層のレベル。
- 命名規則に従ったグループ名に多くの一致候補がある場合、ワイルドカードの使用が必要になることがあります。

ASDM の [DAP] ペイン内の [Advanced] セクションで LUA 論理式を作成し、この柔軟性を実現できます。

DAP CheckAndMsg 関数

ASA は、LUA CheckAndMsg 関数を含む DAP レコードが選択され、それによって接続が終了する結果になる場合にのみ、ユーザーにメッセージを表示します。

CheckAndMsg 関数の構文は以下の通りです。

```
CheckAndMsg(value, "<message string if value is true>", "<message string if value if
false>")
```

CheckAndMsg 関数の作成時には、以下の点に注意してください。

- CheckAndMsg は、最初の引数として渡された値を返します。
- 文字列比較を使用したくない場合、EVAL 関数を最初の引数として使用してください。次に例を示します。

```
(CheckAndMsg((EVAL(...)) , "true msg", "false msg"))
```

CheckandMsg は EVAL 関数の結果を返し、セキュリティ アプライアンスはその結果を使用して、DAP レコードを選択すべきかどうかを判断します。レコードが選択された結果、ターミネーションとなった場合、セキュリティアプライアンスは適切なメッセージを表示します。

OU ベースの照合の例

DAP は、論理式で LDAP サーバーから返される多数の属性を使用できます。DAP トレースの項で出力例を参照するか、debug dap トレースを実行してください。

LDAP サーバーはユーザーの認定者名（DN）を返します。これは、ディレクトリ内のどの部分にユーザー オブジェクトがあるかを暗黙的に示します。たとえば、ユーザーの DN が CN=Example User、OU=Admins、dc=cisco、dc=com である場合、このユーザーは OU=Admins,dc=cisco,dc=com に存在します。すべての管理者がこの OU（または、このレベル以下のコンテナ）に存在する場合、以下のように、この基準に一致する論理式を使用できます。

```
assert(function()
   if ( (type(aaa.ldap.distinguishedName) == "string") and
        (string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$") ~= nil)
) then
       return true
   end
   return false
end)()
```

この例では、string.find 関数で正規表現を使用できます。この文字列を distinguishedName フィールドの最後にアンカーするには、文字列の最後に $ を使用します。

グループ メンバーシップの例

AD グループ メンバーシップのパターン照合のために、基本論理式を作成できます。ユーザーが複数のグループのメンバーであることが考えられるため、DAP は LDAP サーバーからの応答を表内の別々のエントリへと解析します。以下を実行するには、高度な機能が必要です。

- memberOf フィールドを文字列として比較する（ユーザーが 1 つのグループだけに所属している場合）。
- 返されたデータが「table」タイプである場合、返されたそれぞれの memberOf フィールドを繰り返し処理する。

そのために記述し、テストした関数を以下に示します。この例では、ユーザーが「-stu」で終わるいずれかのグループのメンバーである場合、この DAP に一致します。

```
assert(function()
   local pattern = "-stu$"
   local attribute = aaa.ldap.memberOf
   if ((type(attribute) == "string") and
       (string.find(attribute, pattern) ~= nil)) then
       return true
   elseif (type(attribute) == "table") then
       local k, v
```

```
       for k, v in pairs(attribute) do
           if (string.find(v, pattern) ~= nil) then
               return true
           end
       end
   end
   return false
end)()
```

アクセス拒否の例

マルウェア対策プログラムが存在しない場合のアクセスを拒否するために、次の関数を使用できます。ターミネーションを実行するためのアクションが設定されているDAPで使用します。

```
assert(
    function()
for k,v in pairs(endpoint.am) do

        if (EVAL(v.exists, "EQ", "true", "string")) then

            return false

        end
    end
    return CheckAndMsg(true, "Please install antimalware software before connecting.",
nil)
end)()
```

マルウェア対策プログラムがないユーザーがログインしようとすると、DAPは次のメッセージを表示します。

```
Please install antimalware software before connecting.
```

マルチ証明書認証の例

DAP ルールで複数の証明書認証を使用して、ワイルドカード発行者の CN を定義できます。

2 つの異なる認証局（abc.cisco.com と xyz.cisco.com など）によって 2 つの異なるマシンに発行された2つの証明書を設定した場合、DAPルールには、発行者CNが*.cisco.comまたはcisco.comである複数の証明書認証の条件が必要です。

次の関数を使用して、ユーザーおよびマシンの証明書にワイルドカード issuer_cn cisco.com を使用して証明書の DAP ルールを定義できます。

```
assert(
 function()
  if ((string.find(endpoint.cert[1].issuer.cn[0], "cisco.com") ~= nil) and
   (string.find(endpoint.cert[2].issuer.cn[0], "cisco.com") ~= nil)) then
     return true;
 end
 return false;
end)()
```

DAP EVAL 式の例

LUA で論理式を作成する場合は、次の例を参考にしてください。

説明	例
Windows 10 用エンドポイント LUA チェック	`(EVAL(endpoint.os.version,"EQ","Windows 10","string"))`
CLIENTLESS または CVC クライアントタイプに一致するかどうかのエンドポイント LUA チェック。	`(EVAL(endpoint.application.clienttype,"EQ","CLIENTLESS") or EVAL(endpoint.application.clienttype, "EQ","CVC"))`
単一マルウェア対策プログラム Symantec Enterprise Protection がユーザーの PC にインストールされているかどうかのエンドポイント LUA チェック。インストールされていない場合はメッセージを表示します。	`(CheckAndMsg(EVAL(endpoint.am["538"].description,"NE","Symantec Endpoint Protection","string"),"Symantec Endpoint Protection was not found on your computer", nil))`
McAfee Endpoint Protection バージョン 10 から 10.5.3 およびバージョン 10.6 以降用のエンドポイント LUA チェック。	`(EVAL(endpoint.am["1637"].version,"GE","10","version") and EVAL(endpoint.am["1637"].version,"LT","10.5.4","version") or EVAL(endpoint.am["1637"].version,"GE","10.6","version"))`
McAfee マルウェア対策定義が過去 10 日（864000 秒）以内に更新されたかどうかのエンドポイント LUA チェック。更新が必要な場合はメッセージを表示します。	`(CheckAndMsg(EVAL(endpoint.am["1637"].lastupdate,"GT","864000","integer"),"Update needed! Please wait for McAfee to load the latest dat file.", nil))`
debug dap trace で `endpoint.os.windows.hotfix["KB923414"] = "true";` が返された後に特定のホットフィックスがあるかどうかのチェック。	`(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"), "The required hotfix is not installed on your PC.",nil))`

マルウェア対策プログラムのチェックとメッセージの表示

マルウェア対策ソフトウェアにより、エンドユーザーが問題に気づいて修正できるようにメッセージを設定できます。アクセスが許可された場合、ASA はポータル ページの DAP 評価プロセスで生成されたすべてのメッセージを表示します。アクセスが拒否された場合、ASAは「ター

ミネーション」状態の原因となったすべてのメッセージを DAP から収集して、ブラウザのログイン ページに表示します。

次の例は、この機能を使用して Symantec Endpoint Protection のステータスをチェックする方法を示します。

1. 次の LUA 式をコピーし、[Add/Edit Dynamic Access Policy] ペインの [Advanced] フィールドに貼り付けます（右端にある二重矢印をクリックして、フィールドを展開します）。

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
Protection","string") and EVAL(endpoint.am["538"].activescan,"NE","ok","string")
"Symantec Endpoint Protection is disabled. You must enable before being granted
access", nil))
```

2. 同じ [Advanced] フィールドで、[OR] ボタンをクリックします。
3. 下の [Access Attributes] セクションの一番左の [Action] タブで、[Terminate] をクリックします。
4. Symantec Endpoint Protection がインストールされているものの無効になっている PC から接続します。想定される結果は、接続は許可されず、ユーザーに次のメッセージが表示されるというものです。「Symantec Endpoint Protection is disabled. You must enable before being granted access」。

マルウェア対策プログラムと 2 日以上経過した定義のチェック

この例では、Symantec または McAfee のマルウェア対策プログラムが存在するかどうか、また、ウイルス定義が 2 日（172,800 秒）以内のものであるかどうかを確認します。定義が 2 日以上経過している場合、ASA はセッションを終了し、メッセージと修正用リンクを表示します。このタスクを完了するには、次の手順を実行します。

1. 次の LUA 式をコピーし、[Add/Edit Dynamic Access Policy] ペインの [Advanced] フィールドに貼り付けます。

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
Protection","string") and EVAL(endpoint.am["538"].lastupdate,"GT","172800","integer"),
 "Symantec Endpoint Protection Virus Definitions are Out of Date. You must run
LiveUpdate before being granted access", nil)) or
(CheckAndMsg(EVAL(endpoint.am["1637"].description,"EQ","McAfee Endpoint
Security","string") and EVAL(endpoint.am["1637"].lastupdate,"GT","172800","integer"),
 "McAfee Endpoint Security Virus Definitions are Out of Date. You must update your
McAfee Virus Definitions before being granted access", nil))
```

2. 同じ [Advanced] フィールドで、[AND] をクリックします。
3. 下の [Access Attributes] セクションの一番左の [Action] タブで、[Terminate] をクリックします。
4. Symantec または McAfee のマルウェア対策プログラムがインストールされており、バージョンが 2 日以上前のものである PC から接続します。

   結果として、接続は許可されず、ユーザーに「virus definitions are out of date」というメッセージが表示されることが予測されます。

DAP アクセスと許可ポリシー属性の設定

各タブをクリックして、タブ内のフィールドを設定します。

手順

ステップ 1 特定の接続またはセッションに適用される特別な処理を指定するには、[Action] タブを選択します。

- [Continue]：（デフォルト）セッションにアクセス ポリシー属性を適用します。
- [Quarantine]：検疫を使用すると、VPN 経由ですでにトンネルを確立している特定のクライアントを制限できます。ASAは、制限付きACLをセッションに適用して制限付きグループを形成します。この基になるのは、選択された DAP レコードです。エンドポイントが管理面で定義されているポリシーに準拠していない場合でも、ユーザーはサービスにアクセスして修復できますが、ユーザーに制限がかけられます。修復後、ユーザーは再接続できます。この再接続により、新しいポスチャアセスメントが起動されます。このアセスメントに合格すると、接続されます。このパラメータを使用するには、セキュアクライアント機能をサポートしている セキュアクライアント リリースが必要です。
- [Terminate]：セッションを終了します。
- [User Message]：この DAP レコードが選択されるときに、ポータル ページに表示するテキスト メッセージを入力します。最大 490 文字を入力できます。ユーザー メッセージは、黄色のオーブとして表示されます。ユーザがログインすると、メッセージは3回点滅してから静止します。数件の DAP レコードが選択され、それぞれにユーザー メッセージがある場合は、ユーザー メッセージがすべて表示されます。

  URL やその他の埋め込みテキストを含めることができます。この場合は、正しい HTML タグを使用する必要があります。例：すべてのコントラクタは、ご使用のマルウェア対策ソフトウェアのアップグレード手順について、Instructions を参照してください。

ステップ 2 [Network ACL Filters] タブを選択し、この DAP レコードに適用されるネットワーク ACL を設定します。

DAP の ACL には、許可ルールまたは拒否ルールを含めることができますが、両方を含めることはできません。ACLに許可ルールと拒否ルールの両方が含まれている場合、ASAはそのACLを拒否します。

- [Network ACL] ドロップダウン リスト：この DAP レコードに追加する、すでに設定済みのネットワーク ACL を選択します。ACL には、許可ルールと拒否ルールの任意の組み合わせを指定できます。このフィールドは、IPv4 および IPv6 ネットワーク トラフィックのアクセス ルールを定義できる統合 ACL をサポートしています。
- [Manage]：ネットワーク ACL を追加、編集、および削除するときにクリックします。

- [Network ACL] リスト：この DAP レコードのネットワーク ACL が表示されます。
- [Add]：ドロップダウン リストで選択したネットワーク ACL が右側の [Network ACLs] リストに追加されます。
- [Delete]：クリックすると、強調表示されているネットワーク ACL が [Network ACLs] リストから削除されます。ASA から ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。

ステップ 3 [Web-Type ACL Filters (clientless)] タブを選択し、この DAP レコードに適用される Web タイプ ACL を設定します。DAP の ACL には、許可または拒否ルールだけを含めることができます。ACL に許可ルールと拒否ルールの両方が含まれている場合、ASA はその ACL を拒否します。

- [Web-Type ACL] ドロップダウン リスト：この DAP レコードに追加する、設定済みの Web-type ACL を選択します。ACL には、許可ルールと拒否ルールの任意の組み合わせを指定できます。
- [Manage]：Web タイプ ACL を追加、編集、削除するときにクリックします。
- [Web-Type ACL] リスト：この DAP レコードの Web-type ACL が表示されます。
- [Add]：ドロップダウン リストで選択した Web タイプ ACL が右側の [Web-Type ACLs] リストに追加されます。
- [Delete]：クリックすると、Web-type ACL の 1 つが [Web-Type ACLs] リストから削除されます。ASA から ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。

ステップ 4 [Functions] タブを選択し、ファイル サーバー エントリとブラウジング、HTTP プロキシ、および DAP レコードの URL エントリを設定します。

- [File Server Browsing]：ファイル サーバーまたは共有機能の CIFS ブラウジングをイネーブルまたはディセーブルにします。

  ブラウズには、NBNS（マスター ブラウザまたは WINS）が必要です。NBNS に障害が発生した場合や、NBNS が設定されていない場合は、DNS を使用します。CIFS ブラウズ機能では、国際化がサポートされていません。

- [File Server Entry]：ポータル ページでユーザーがファイル サーバーのパスおよび名前を入力できるようにするかどうかを設定します。イネーブルになっている場合、ポータル ページにファイル サーバー エントリのドロワが配置されます。ユーザは Windows ファイルのパス名を直接入力できます。ユーザは、ファイルをダウンロード、編集、削除、名前変更、および移動できます。また、ファイルおよびフォルダを追加することもできます。適用可能な Windows サーバーでユーザー アクセスに対して共有を設定する必要もあります。ネットワークの要件によっては、ユーザーがファイルへのアクセス前に認証を受ける必要があることもあります。
- [HTTP Proxy]：クライアントへの HTTP アプレット プロキシの転送に関与します。このプロキシは、適切なコンテンツ変換に干渉するテクノロジー（Java、ActiveX、Flash など）に対して有用です。このプロキシによって、セキュリティ アプライアンスの使用を継続し

ながら、マングリングを回避できます。転送されたプロキシは、自動的にブラウザの古いプロキシ コンフィギュレーションを変更して、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。

- [URL Entry]：ポータル ページでユーザーが HTTP/HTTPS URL を入力できるようにするかどうかを設定します。この機能がイネーブルになっている場合、ユーザーは URL エントリ ボックスに Web アドレスを入力できます。

SSL VPN を使用しても、すべてのサイトとの通信が必ずしもセキュアになるとはかぎりません。SSL VPN は、企業ネットワーク上のリモートユーザーの PC やワークステーションと ASA との間のデータ転送のセキュリティを保証するものです。したがって、ユーザーが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるリソース）にアクセスする場合、企業の ASA から目的の Web サーバーまでの通信はセキュアではありません。

クライアントレス VPN 接続では、ASA はエンド ユーザーの Web ブラウザとターゲット Web サーバーとの間のプロキシとして機能します。ユーザーが SSL 対応 Web サーバーに接続すると、ASA はセキュアな接続を確立し、サーバーの SSL 証明書を検証します。エンド ユーザー ブラウザでは提示された証明書を受信しないため、証明書を調査して検証することはできません。SSL VPN の現在の実装では、期限切れになった証明書を提示するサイトとの通信は許可されません。また、ASA は信頼できる CA 証明書の検証も実行しません。このため、ユーザーは、SSL 対応の Web サーバーと通信する前に、そのサーバーにより提示された証明書を分析することはできません。

ユーザーのインターネット アクセスを制限するには、[Disable for the URL Entry] フィールドを選択します。これにより、SSL VPN ユーザーがクライアントレス VPN 接続中に Web サーフィンできないようにします。

- [Unchanged]：（デフォルト）クリックすると、このセッションに適用されるグループ ポリシーからの値が使用されます。
- [Enable/Disable]：機能をイネーブルにするかディセーブルにするかを指定します。
- [Auto-start]：クリックすると HTTP プロキシがイネーブルになり、これらの機能に関連付けられたアプレットが DAP レコードによって自動的に起動するようになります。

ステップ 5 [Port Forwarding Lists] タブを選択し、ユーザー セッションのポート転送リストを設定します。

ポート転送によりグループ内のリモート ユーザーは、既知の固定 TCP/IP ポートで通信するクライアント/サーバー アプリケーションにアクセスできます。リモート ユーザーは、ローカル PC にインストールされたクライアント アプリケーションを使用して、そのアプリケーションをサポートするリモート サーバーに安全にアクセスできます。シスコでは、Windows Terminal Services、Telnet、Secure FTP（FTP over SSH）、Perforce、Outlook Express、および Lotus Notes についてテストしています。その他の TCP ベースのアプリケーションの一部も機能すると考えられますが、シスコではテストしていません。

（注）
ポート転送は、一部の SSL/TLS バージョンでは使用できません。

注意
ポート転送（アプリケーション アクセス）およびデジタル証明書をサポートするために、リモート コンピュータに Sun Microsystems Java ランタイム環境（JRE）がインストールされていることを確認します。

- [Port Forwarding]：この DAP レコードに適用されるポート転送リストのオプションを選択します。このフィールドのその他の属性は、[Port Forwarding] を [Enable] または [Auto-start] に設定した場合にだけイネーブルになります。
- [Unchanged]：クリックすると、属性が実行コンフィギュレーションから削除されます。
- [Enable/Disable]：ポート転送をイネーブルにするかディセーブルにするかを指定します。
- [Auto-start]：クリックするとポート転送がイネーブルになり、DAP レコードのポート転送リストに関連付けられたポート転送アプレットが自動的に起動するようになります。
- [Port Forwarding List] ドロップダウン リスト：DAP レコードに追加する、設定済みのポート転送リストを選択します。
- **[New...]**：新規のポート転送リストを設定するときにクリックします。
- [Port Forwarding Lists]（ラベルなし）：DAP レコードのポート転送リストが表示されます。
- [Add]：クリックすると、ドロップダウン リストで選択したポート転送リストが右側のポート転送リストに追加されます。
- [Delete]：クリックすると、選択されているポート転送リストがポート転送リストから削除されます。 ASA からポート転送リストを削除するには、まず DAP レコードからそのリストを削除する必要があります。

ステップ 6 [Bookmarks] タブを選択し、特定のユーザー セッション URL のブックマークを設定します。

- [Enable bookmarks]：クリックするとイネーブルになります。 このチェックボックスがオフのときは、接続のポータル ページにブックマークは表示されません。
- [Bookmark] ドロップダウン リスト：DAP レコードに追加する、設定済みのブックマークを選択します。
- **[Manage...]**：ブックマークを追加、インポート、エクスポート、削除するときにクリックします。
- **[Bookmarks]**（ラベルなし）：この DAP レコードの URL リストが表示されます。
- [Add>>]：クリックすると、ドロップダウン リストで選択したブックマークが右側の URL 領域に追加されます。
- [Delete]：クリックすると、選択されているブックマークが URL リスト領域から削除されます。ASA からブックマークを削除するには、まず DAP レコードからそのブックマークを削除する必要があります。

ステップ 7 [Access Method] タブを選択し、許可するリモート アクセスのタイプを設定します。

- [Unchanged]：現在のリモート アクセス方式を引き続き使用します。
- **セキュアクライアント**：Cisco Secure Client AnyConnect VPN クライアントの AnyConnect VPN モジュールを使用して接続する

  .
- [Web-Portal]：クライアントレス VPN で接続します。
- **Both-default-Web-Portal**：クライアントレスまたはセキュアクライアントを介して接続します。デフォルトはクライアントレスです。
- **Both-default-セキュアクライアント**：クライアントレスまたはセキュアクライアントを介して接続します。セキュアクライアントのデフォルトはクライアントレスです。

ステップ 8 [**セキュアクライアント**] タブを選択し、Always-on VPN フラグのステータスを選択します。

- Always-On VPN for セキュアクライアント：セキュアクライアント サービスプロファイル内の Always-on VPN フラグ設定を未変更にするか、ディセーブルにするか、セキュアクライアント プロファイル設定を使用するかを指定します。

  このパラメータを使用するには、Cisco Web セキュリティ アプライアンスのリリースが、Cisco Secure クライアントの AnyConnect VPN モジュールに対してセキュア モビリティ ソリューションライセンシングをサポートしている必要があります。また、セキュアクライアント のリリースが、「セキュア モビリティ ソリューション」の機能をサポートしている必要もあります。詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

ステップ 9 [セキュアクライアント カスタム属性（AnyConnect Client Custom Attributes）] タブを選択し、定義済みのカスタム属性を表示して、このポリシーに関連付けます。また、カスタム属性を定義してから、それらをこのポリシーに関連付けることもできます。

カスタム属性はセキュアクライアントに送信され、アップグレードの延期などの機能を設定するために使用されます。カスタム属性にはタイプと名前付きの値があります。まず属性のタイプを定義した後、このタイプの名前付きの値を 1 つ以上定義できます。機能に対して設定する固有のカスタム属性の詳細については、使用しているセキュアクライアントリリースの『*Cisco Secure Client Administrator Guide*』を参照してください。

カスタム属性は、[設定（Configuration）] > [リモートアクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [詳細設定（Advanced）] > [セキュアクライアントカスタム属性（Custom Attributes）] および [セキュアクライアントカスタム属性名（Custom Attribute Names）] で事前に定義できます。事前に定義したカスタム属性は、ダイナミック アクセス ポリシーとグループ ポリシーの両方で使用されます。

DAP を使用した SAML 認証の設定

外部サーバー（RADIUS またはLDAP）に依存して認可属性を取得することなく、DAP を使用して SAML 認可およびグループポリシーの選択を設定できます。

SAML ID プロバイダーは、認証アサーションに加えて認可属性を送信するように設定できます。ASA の SAML サービス プロバイダー コンポーネントは、SAML アサーションを解釈し、受信したアサーションに基づいて認可またはグループポリシーの選択を行います。アサーション属性は、ASDM で設定された DAP ルールを使用して処理されます。

グループポリシー属性は、属性名 **cisco_group_policy** を使用する必要があります。この属性は、設定されている DAP に依存しません。ただし、DAP が設定されている場合は、DAP ポリシーの一部として使用できます。

グループポリシーの選択

cisco_group_policy という名前の属性が受信されると、対応する値を使用して接続 group-policy が選択されます。

接続が確立されると、複数のソースからグループポリシー情報が取得され、それらが組み合わされて、接続に適用される有効な group-policy が作成されます。

受信したグループポリシー情報を組み合わせると、次のシナリオが考えられます。

SAML 認証で受信したグループポリシー、承認が設定されていません

このシナリオでは、有効なグループポリシーは、優先順位の降順で次のように決定されます。

1. SAML 属性で指定されたグループポリシー。
2. トンネルグループで指定されたグループポリシー。
3. デフォルトのグループポリシー。

SAML 認証で受信したグループポリシー、承認が設定されています

このシナリオでは、有効なグループポリシーは、優先順位の降順で次のように決定されます。

1. 許可属性で指定されたグループポリシー。
2. ユーザーグループポリシー：存在する場合、許可サーバーから返された値を使用します。
3. ユーザーグループポリシー：SAML 属性で返された値を使用します。
4. トンネルグループで指定されたグループポリシー。
5. デフォルトのグループポリシー。

手順

ステップ 1 ASDM では、**[設定（Configuration）] > [リモートアクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [ダイナミックアクセスポリシー（Dynamic Access Policies）] > [ダイナミックポリシーの追加/編集（Add/Edit Dynamic Access Policy）]**を選択します。

ステップ 2 AAA 属性の選択領域で、[追加（Add）] をクリックします。

a) [AAA属性タイプ（AAA Attribute Type）] ドロップダウンから、[SAML] を選択します。

b) 属性 *ID*として **memberOf** を指定します。

c) *memberOf* 属性の**値**を入力するか、AD サーバーグループが設定されている場合は [ADグループの取得（Get AD Group）] をクリックします。

追加の AD サーバーグループを設定するには、**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [AAA/ローカルユーザー（AAA/Local Users）] > [AAA サーバーグループ（AAA Server Groups）]**に移動します。

グループポリシー選択属性を構成するには、必要に応じて、同じ DAP ポリシーまたは別の DAP ポリシーで次の設定を選択します。

- [AAA属性タイプ（AAA Attribute Type）] : SAML
- [属性 ID（Attribute ID）] : cisco_group_policy
- [値（Value）] : グループポリシー名

ステップ 3 [OK] をクリックします。

ステップ 4 [OK] をクリックして、DAP ポリシーを保存します。

DAP トレースの実行

DAP トレースを実行すると、すべての接続済みデバイスの DAP エンドポイント属性が表示されます。

手順

ステップ 1 SSH ターミナルから ASA にログオンして特権 EXEC モードを開始します。

ASA の特権 EXEC モードでは、表示されるプロンプトは `hostname#` となります。

ステップ 2 DAP デバッグをイネーブルにします。セッションのすべての DAP 属性がターミナル ウィンドウに表示されます。

```
hostname# debug dap trace
endpoint.anyconnect.clientversion="0.16.0021";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.platformversion="4.1";
endpoint.anyconnect.devicetype="iPhone1,2";
endpoint.anyconnect.deviceuniqueid="dd13ce3547f2fa1b2c3d4e5f6g7h8i9j0fa03f75";
```

ステップ 3 （任意） DAP トレースの出力を検索するには、コマンドの出力をシステム ログに送ります。ASA でのロギングの詳細については、『*Cisco ASA Series General Operations ASDM Configuration Guide*』の「*Configure Logging*」を参照してください。

DAP の例

DAP を使用したネットワーク リソースの定義

この例は、ユーザーまたはグループのネットワーク リソースを定義する方法として、ダイナミック アクセス ポリシーを設定する方法を示しています。Trusted_VPN_Access という名前の DAP ポリシーは、 Cisco Secure Client のクライアントレス VPN アクセスと AnyConnect VPN モジュールアクセスを許可します。Untrusted_VPN_Access という名前のポリシーは、クライアントレス VPN アクセスだけを許可します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Dynamic Access Policies]** > **[Add/Edit Dynamic Access Policy]** > **[Endpoint]** に移動します。

ステップ 2 各ポリシーの次の属性を設定します。

属性	Trusted_VPN_Access	Untrusted_VPN_Access
Endpoint Attribute Type Policy	Trusted	Untrusted
Endpoint Attribute Process	ieexplore.exe	—
Advanced Endpoint Assessment	AntiVirus= McAfee Attribute	
CSD Location	Trusted	Untrusted
LDAP memberOf	Engineering、Managers	ベンダー

属性	Trusted_VPN_Access	Untrusted_VPN_Access
ACL		Web-Type ACL
アクセス	セキュアクライアントおよび Web ポータル	Web Portal

DAP を使用した WebVPN ACL の適用

DAP では、Network ACLs（IPsec およびセキュアクライアント の場合）、URL リスト、および Functions を含め、アクセスポリシー属性のサブセットを直接適用できます。グループ ポリシーが適用されるバナーまたはスプリット トンネル リストなどには、直接適用できません。[Add/Edit Dynamic Access Policy] ペインの [Access Policy Attributes] タブには、DAP が直接適用される属性の完全なメニューが表示されます。

Active Directory/LDAP は、ユーザー グループ ポリシー メンバーシップをユーザー エントリの「memberOf」属性として保存します。AD グループ内のユーザー（memberOf）= ASA が設定済み Web タイプ ACL を適用する Engineering となるように、DAP を定義します。

手順

ステップ 1 ASDM で、[Add AAA Attributes] ペインに移動します（**[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Dynamic Access Policies]** > **[Add/Edit Dynamic Access Policy]** > **[AAA Attributes section]** > **[Add AAA Attribute]**）。

ステップ 2 AAA 属性タイプとしては、ドロップダウン リストを使用して [LDAP] を選択します。

ステップ 3 [Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 4 [Value] フィールドで、ドロップダウン リストを使用して [=] を選択し、隣のフィールドに「Engineering」と入力します。

ステップ 5 ペインの [Access Policy Attributes] 領域で、[Web-Type ACL Filters] タブをクリックします。

ステップ 6 [Web-Type ACL] ドロップダウン リストを使用して、AD グループ（memberOf）= Engineering のユーザーに適用する ACL を選択します。

DAP による CSD チェックの強制とポリシーの適用

この例では、ユーザーが 2 つの特定 AD/LDAP グループ（Engineering および Employees）と 1 つの特定 ASA トンネル グループに属することをチェックする DAP を作成します。その後、ACL をユーザーに適用します。

DAP が適用される ACL により、リソースへのアクセスを制御します。それらの ACL は、ASA のグループ ポリシーで定義されるどの ACL よりも優先されます。また ASA は、スプリットトンネリング リスト、バナー、DNS など、DAP で定義または制御されない要素に通常の AAA グループ ポリシー継承ルールと属性を適用します。

手順

ステップ 1 ASDM で、[Add AAA Attributes] ペインに移動します（**[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Dynamic Access Policies]** > **[Add/Edit Dynamic Access Policy]** > **[AAA Attributes section]** > **[Add AAA Attribute]**）。

ステップ 2 AAA 属性タイプとしては、ドロップダウン リストを使用して [LDAP] を選択します。

ステップ 3 [Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 4 [Value] フィールドで、ドロップダウン リストを使用して [=] を選択し、隣のフィールドに「Engineering」と入力します。

ステップ 5 [Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 6 [Value] フィールドで、ドロップダウン リストを使用して [=] を選択し、隣のフィールドに「Employees」と入力します。

ステップ 7 AAA 属性タイプとしては、ドロップダウン リストを使用して [Cisco] を選択します。

ステップ 8 [Tunnel] グループ ボックスをオンにし、ドロップダウン リストを使用して [=] を選択し、隣のドロップダウン リストで適切なトンネル グループ（接続ポリシー）を選択します。

ステップ 9 [Access Policy Attributes] 領域の [Network ACL Filters] タブで、前のステップで定義した DAP 基準を満たすユーザーに適用する ACL を選択します。

DAP を使用してセッショントークンのセキュリティを確認する

ASA がセキュアクライアントからの VPN 接続要求を認証すると、ASA はセッショントークンをクライアントに返します。AnyConnect 4.9（MR1）以降、ASA とセキュアクライアントは、セッショントークンのセキュリティを強化するメカニズムをサポートします。セキュアクライアントがセッショントークンのセキュリティをサポートするように、DAP を設定する必要があります。

DAP をエンドポイント属性設定と一緒に使用し、LUA スクリプトを使用して、トークンセキュリティをサポートしていないセキュアクライアントバージョンからの接続試行を拒否します。

手順

ステップ 1 ASDM では、**[設定（Configuration）]** > **[リモートアクセス VPN（Remote Access VPN）]** > **[ネットワーク（クライアント）アクセス（Network (Client) Access）]** > **[ダイナミックアクセ**

スポリシー（**Dynamic Access Policies**）]>[ダイナミックポリシーの追加/編集（**Add/Edit Dynamic Access Policy**）]を選択します。

ステップ 2 エンドポイント属性の選択領域で、[追加（Add）] をクリックします。

a) [エンドポイント属性タイプ（Endpoint Attribute Type）] ドロップダウンで、[アプリケーション（Application）] を選択します。
b) [クライアントタイプ（Client Type）] で、等号 (=) 演算子を選択し、ドロップダウンからセキュアクライアントを選択します。
c) [OK] をクリックします。

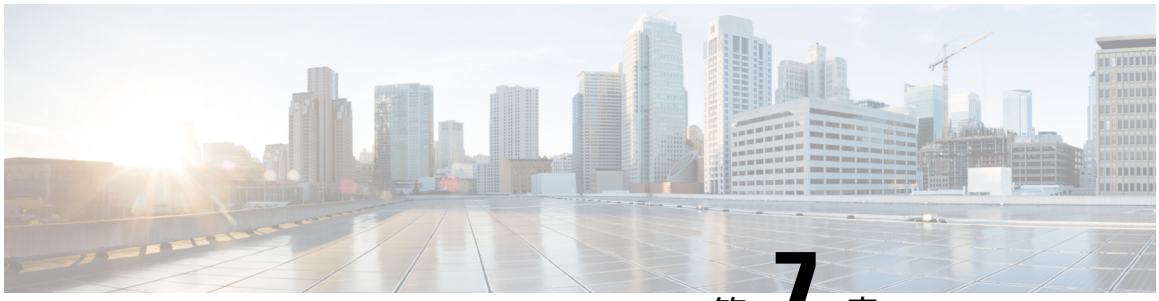
ステップ 3 [Advanced（詳細設定）] の選択基準を設定します。

a) [AND] 演算子を選択します。
b) **論理式**の追加

```
(type(endpoint.anyconnect.session_token_security)~="string" or
EVAL(endpoint.anyconnect.session_token_security,"NE","true","string"))
```

ステップ 4 [アクション（Action）] 領域で、[終了（Terminate）] を選択します。

ステップ 5 オプションのユーザーメッセージを追加し、[OK] をクリックします。



第 7 章

電子メール プロキシ

電子メール プロキシを設定すると、リモート電子メール機能をクライアントレス SSL VPN のユーザーに拡張できます。ユーザーが電子メール プロキシ経由で電子メール セッションを試行すると、電子メール クライアントが SSL プロトコルを使用してトンネルを確立します。

電子メール プロキシ プロトコルは次のとおりです。

POP3S

POP3S は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 995 をリッスンし、ポート 995 または設定されたポートとの接続が自動的に許可されます。POP3 プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に POP3 プロトコルが開始され、認証が行われます。POP3S は、電子メール受信用のプロトコルです。

IMAP4S

IMAP4S は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 993 をリッスンし、ポート 993 または設定されたポートとの接続が自動的に許可されます。IMAP4S プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に IMAP4S プロトコルが開始され、認証が行われます。IMAP4S は、電子メール受信用のプロトコルです。

SMTPS

SMTPS は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 988 をリッスンし、ポート 988 または設定されたポートとの接続が自動的に許可されます。SMTPS プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に SMTPS プロトコルが開始され、認証が行われます。SMTPS は、電子メール送信用のプロトコルです。

• デリミタの設定 （249 ページ）

電子メール プロキシの設定

電子メール プロキシの要件

- 電子メールプロキシを経由してローカルとリモートの両方から電子メールにアクセスするユーザーは、電子メールプログラムで、ローカルアクセス用とリモートアクセス用に別々の電子メール アカウントが必要です。
- 電子メール プロキシ セッションでユーザーが認証される必要があります。

AAA サーバー グループの設定

手順

ステップ 1 **[Configuration]** > **[Features]** > **[VPN]** > **[E-mail Proxy]** > **[AAA]** を参照します。

ステップ 2 適切なタブ（[POP3S]、[IMAP4S]、または [SMTPS]）を選択して AAA サーバー グループを関連付け、これらのセッションに適用するデフォルトのグループ ポリシーを設定します。

- [AAA server groups]：[AAA Server Groups] パネル（[Configuration] > [Features] > [Properties] > [AAA Setup] > [AAA Server Groups]）に移動する場合にクリックします。ここでは、AAA サーバー グループを追加または編集できます。
- [group policies]：[Group Policy] パネル（[Configuration] > [Features] > [VPN] > [General] > [Group Policy]）に移動する場合にクリックします。ここでは、グループ ポリシーを追加または編集できます。
- [Authentication Server Group]：ユーザー認証用の認証サーバー グループを選択します。デフォルトでは、認証サーバーが設定されていません。AAA を認証方式として設定した場合には（[Configuration] > [Features AAA] > [VPN] > [E-Mail Proxy] > [Authentication] パネル）、AAA サーバーを設定してここで選択しないと、常に認証に失敗します。
- [Authorization Server Group]：ユーザー認可用の認可サーバー グループを選択します。デフォルトでは、認可サーバーが設定されていません。
- [Accounting Server Group]：ユーザー アカウンティング用のアカウンティング サーバー グループを選択します。デフォルトでは、アカウンティング サーバーが設定されていません。
- [Default Group Policy]：AAA が CLASSID 属性を返さない場合にユーザーに適用するグループ ポリシーを選択します。長さは、4 ～ 15 文字の英数字です。デフォルトのグループ ポ

リシーが指定されていない場合や、CLASSID が存在しない場合、ASA はセッションを確立できません。

- [Authorization Settings]：ASA が認可のために識別するユーザー名の値を設定します。この名前は、デジタル証明書を使用して認証し、LDAP または RADIUS 認可を必要とするユーザーに適用されます。
  - [Use the entire DN as the username]：認可用の認定者名を使用する場合に選択します。
  - [Specify individual DN fields as the username]：ユーザー認可用に特定の DN フィールドを指定する場合に選択します。

    [DN] フィールドは、プライマリとセカンダリの 2 つを選択できます。たとえば、EA を選択した場合には、ユーザーは電子メール アドレスによって認証されます。John Doe という一般名（CN）と johndoe@cisco.com という電子メールアドレスを持つユーザーは、John Doe または johndoe として認証されません。彼は johndoe@cisco.com として認証される必要があります。EA および O を選択した場合、John Doe は johndoe@cisco.com および Cisco Systems, Inc. として認証される必要があります。
  - [Primary DN Field]：認可用に設定するプライマリ DN フィールドを選択します。デフォルトは [CN] です。オプションには、次のものが含まれます。

DN フィールド	定義
Country（C）	2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
Common Name（CN）	ユーザー、システム、その他のエンティティの名前。これは、ID 階の最下位（最も固有性の高い）レベルです。
DN Qualifier（DNQ）	特定の DN 属性。
E-mail Address（EA）	証明書を所有するユーザー、システム、またはエンティティの電子メル アドレス。
Generational Qualifier（GENQ）	Jr.、Sr.、または III などの世代修飾子。
Given Name（GN）	証明書所有者の名前（名）。
Initials（I）	証明書所有者の姓と名の最初の文字。
Locality（L）	組織が所在する市町村。
Name（N）	証明書所有者の名前。
Organization（O）	会社、団体、機関、協会、その他のエンティティの名前。
Organizational Unit（OU）	組織内のサブグループ。
Serial Number（SER）	証明書のシリアル番号。

DN フィールド	定義
Surname（SN）	証明書所有者の姓。
State/Province（S/P）	組織が所在する州や県。
Title（T）	証明書所有者の役職（Dr. など）。
User ID（UID）	証明書所有者の ID 番号。

- [Secondary DN Field]：（オプション）認可用に設定するセカンダリ DN フィールドを選択します。デフォルトは [OU] です。オプションには、上記の表に記載されているものすべてに加えて、[None] があります。これは、セカンダリ フィールドを指定しない場合に選択します。

電子メール プロキシを使用するインターフェイスの識別

[Email Proxy Access] 画面では、電子メール プロキシを設定するインターフェイスを識別できます。電子メール プロキシは、個々のインターフェイスで設定および編集できます。また、1 つのインターフェイスで電子メール プロキシを設定および編集すれば、その設定をすべてのインターフェイスに適用できます。管理専用のインターフェイスやサブインターフェイスに対して電子メール プロキシは設定できません。

手順

ステップ 1 **[Configuration]** > **[VPN]** > **[E-Mail Proxy]** > **[Access]** を参照して、インターフェイスでイネーブルになっている電子メール プロキシを表示します。

- [Interface]：設定されているすべてのインターフェイスの名前を表示します。
- [POP3S Enabled]：そのインターフェイスで POP3S がイネーブルかどうかを示します。
- [IMAP4s Enabled]：そのインターフェイスで IMAP4S がイネーブルかどうかを示します。
- [SMTPS Enabled]：そのインターフェイスで SMTPS がイネーブルかどうかを示します。

ステップ 2 [Edit] をクリックし、強調表示されているインターフェイスの電子メール プロキシ設定を変更します。

電子メール プロキシの認証の設定

電子メール プロキシのタイプごとに認証方式を設定します。

手順

ステップ 1 **[Configuration]** > **[Features]** > **[VPN]** > **[E-mail Proxy]** > **[Authentication]** を参照します。

ステップ 2 複数の認証方式から選択できます。

- [AAA]：AAA認証を必須にする場合に選択します。このオプションを使用するには、AAAサーバーを設定する必要があります。ユーザーは、ユーザー名、サーバー、およびパスワードを入力します。ユーザーは、VPN ユーザー名と電子メール ユーザー名の両方を入力する必要があります。そのとき、互いのユーザー名が異なる場合にだけ、VPN名デリミタによって区切ります。

- [Certificate]：証明書認証を必須にする場合に選択します。

  （注）
  現在の ASA ソフトウェア リリースでは、証明書認証は電子メール プロキシに対して機能しません。

  証明書認証を使用する場合、ユーザーは、ASA が SSL ネゴシエーション時に検証できる証明書を持っている必要があります。SMTPS プロキシでは、証明書認証を唯一の認証方式として使用できます。その他の電子メールプロキシでは2種類の認証方式が必要です。

  証明書認証には、すべて同じ CA から発行された 3 種類の証明書が必要です。

  - ASA の CA 証明書。

  - クライアント PC の CA 証明書。

  - クライアント PC の Web ブラウザ証明書。個人証明書または Web ブラウザ証明書とも呼ばれます。

- [Piggyback HTTPS]：ピギーバック認証を必須にする場合に選択します。

  この認証スキームは、ユーザーがすでにクライアントレス SSL VPN セッションを確立していることを必須とします。ユーザーは電子メール ユーザー名だけを入力します。パスワードは不要です。ユーザーは、VPN ユーザー名と電子メール ユーザー名の両方を入力する必要があります。そのとき、互いのユーザー名が異なる場合にだけ、VPN名デリミタによって区切ります。

  IMAP は、同時ユーザー数によって制限されない多数のセッションを生成しますが、ユーザー名に対して許可されている同時ログインの数を数えません。IMAP セッションの数がこの最大値を超え、クライアントレス SSL VPN 接続の有効期限が切れた場合には、その後ユーザーが新しい接続を確立できません。以下の解決策があります。

SMTPS電子メールは、最も頻繁にピギーバックを使用します。ほとんどのSMTPサーバーが、ユーザーがログインすることを許可していないためです。

（注）
IMAP は、同時ユーザー数によって制限されない多数のセッションを生成しますが、ユーザー名に対して許可されている同時ログインの数を数えません。IMAP セッションの数がこの最大値を超え、クライアントレス SSL VPN 接続の有効期限が切れた場合には、その後ユーザーが新しい接続を確立できません。以下の解決策があります。

- ユーザーはIMAPアプリケーションを終了してASAとのセッションをクリアしてから、新しいクライアントレス SSL VPN 接続を確立できる。

- 管理者が IMAP ユーザーの同時ログイン数を増やす（[Configuration] > [Features] > [VPN] > [General] > [Group Policy] > [Edit Group Policy] > [General]）。

- 電子メール プロキシの HTTPS/ピギーバック認証をディセーブルにする。

- [Mailhost]：（SMTPS のみ）メールホスト認証を必須にする場合に選択します。POP3S とIMAP4Sは必ずメールホスト認証を実行するため、このオプションは、SMTPSの場合にだけ表示されます。この認証方式では、ユーザーの電子メールユーザー名、サーバー、およびパスワードが必要です。

プロキシ サーバーの識別

この [Default Server] パネルでは、ASA のプロキシ サーバーを識別し、電子メール プロキシに対してデフォルト サーバー、ポート、および非認証セッション制限を設定することができます。

手順

ステップ 1 **[Configuration]** > **[Features]** > **[VPN]** > **[E-mail Proxy]** > **[Default Servers]** を参照します。

ステップ 2 次のフィールドを設定します。

- [Name or IP Address]：デフォルトの電子メール プロキシ サーバーの DNS 名または IP アドレスを入力します。

- [Port]：ASA が電子メール プロキシ トラフィックをリッスンするポート番号を入力します。設定されたポートに対する接続が自動的に許可されます。電子メール プロキシは、SSL接続だけをこのポートで許可します。SSLトンネルが確立された後に電子メールプロキシが開始され、認証が行われます。

  デフォルトの設定は次のとおりです。

  - 995（POP3S の場合）

- 993（IMAP4S の場合）
- 988（SMTPS の場合）

- [Enable non-authenticated session limit]：非認証電子メール プロキシ セッションの数を制限する場合に選択します。認証プロセスでのセッションの制限を設定でき、それによって DOS 攻撃を防ぎます。新しいセッションが、設定された制限を超えると、ASA が最も古い非認証接続を終了します。非認証接続が存在しない場合には、最も古い認証接続が終了します。それによって認証済みのセッションが終了することはありません。

電子メール プロキシ接続には、3 つの状態があります。

- 新規に電子メール接続が確立されると、「認証されていない」状態になります。
- この接続でユーザー名が提示されると、「認証中」状態になります。
- ASA が接続を認証すると、「認証済み」状態になります。

デリミタの設定

このパネルでは、電子メール プロキシ認証で使用するユーザー名/パスワード デリミタとサーバー デリミタを設定します。

手順

ステップ 1 **[Configuration]** > **[Features]** > **[VPN]** > **[E-mail Proxy]** > **[Delimiters]** を参照します。

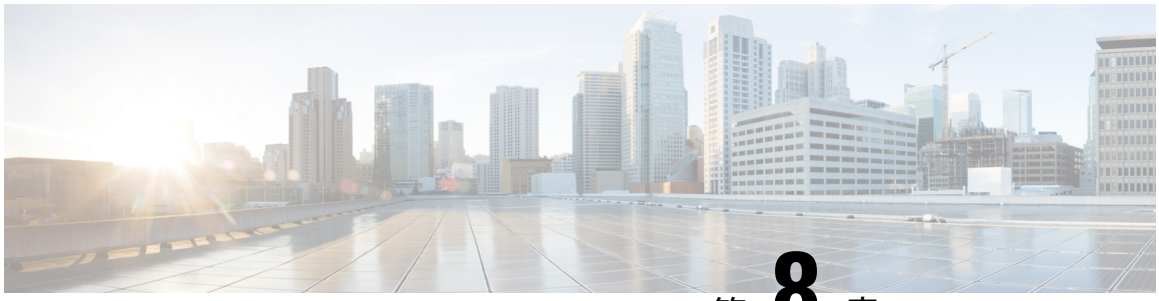
ステップ 2 次のフィールドを設定します。

- [Username/Password Delimiter]：VPN ユーザー名と電子メール ユーザー名を区切るためのデリミタを選択します。電子メール プロキシで AAA 認証を使用する場合、および VPN ユーザー名と電子メールユーザー名が異なる場合に両方のユーザー名を使用します。電子メール プロキシ セッションにログインするときに、ユーザーは両方のユーザー名を入力し、ここで設定したデリミタで区切ります。また、電子メール サーバー名も入力します。

  （注）
  クライアントレス SSL VPN 電子メール プロキシ ユーザーのパスワードに、デリミタとして使用されている文字を含めることはできません。

- [Server Delimiter]：ユーザー名と電子メール サーバー名を区切るためのデリミタを選択します。このデリミタは、VPN 名デリミタとは別にする必要があります。電子メール プロキシセッションにログインする場合には、ユーザー名フィールドにユーザー名とサーバーの両方を入力します。

たとえば、VPN 名デリミタとして : を使用し、サーバー デリミタとして @ を使用する場合には、電子メール プロキシ経由で電子メール プログラムにログインするときに、vpn_username:e-mail_username@server という形式でユーザー名を入力します。



第 8 章

VPN の監視

VPN 接続グラフの監視

ASA の VPN 接続データをグラフ形式または表形式で表示するには、次の画面を参照してください。

[Monitor IPsec Tunnels]

[Monitoring] > [VPN] > [VPN Connection Graphs] > [IPSec Tunnels]

表示や、エクスポートまたは印刷の準備を行う IPsec トンネル タイプのグラフとテーブルを指定します。

[Monitor Sessions]

[Monitoring] > [VPN] > [VPN Connection Graphs] > [Sessions]

表示や、エクスポートまたは印刷の準備を行う VPN セッション タイプのグラフとテーブルを指定します。

VPN 統計の監視

特定のリモートアクセス、または LAN 間セッションの詳細なパラメータおよび統計情報を表示するには、次の画面を参照してください。パラメータと統計情報は、セッションプロトコルによって異なります。また、統計情報テーブルの内容は、選択した接続のタイプによって異なります。各詳細テーブルには、それぞれのセッションの関連パラメータがすべて表示されます。

[Monitor Session] ウィンドウ

[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]

ASA の VPN セッション統計情報を表示します。このペインの 2 番目のテーブルの内容は、[Filter By] リストの選択によって異なります。

（注） 管理者は、非アクティブ状態のユーザー数をトレースし、統計情報を確認できるようになりました。ライセンス数の上限に達することなく、新規ユーザーがログインできるように、最も長時間非アクティブなセッションはアイドル状態であると見なされます（自動的にログオフされます）。これらの統計情報には、**show vpn-sessiondb** CLI コマンドを使用してアクセスすることもできます（『『Cisco ASA Command Reference Guide』の適切なリリース』を参照してください）。

- [All Remote Access]

  このテーブルの値がリモート アクセス（IPsec ソフトウェアおよびハードウェア クライアント）トラフィックに関連することを示します。

- [Username/Connection Profile]：セッションのユーザー名またはログイン名、および接続プロファイル（トンネル グループ）を示します。クライアントが認証にデジタル証明書を使用している場合、フィールドに証明書の Subject CN または Subject OU が表示されます。

- [Group Policy Connection Profile]：セッションのトンネル グループ ポリシー接続プロファイルが表示されます。

- [Assigned IP Address/Public IP Address]：このセッションのリモート クライアントに割り当てられているプライベート（「割り当てられた」）IP アドレスを示します。これは「内部」または「仮想」IP アドレスとも呼ばれ、クライアントはプライベート ネットワーク上のホストとして表示されます。また、このリモート アクセス セッションのクライアントのパブリック IP アドレスも表示します。パブリック IP アドレスは、「外部」IP アドレスとも呼ばれます。通常、これは ISP によってクライアントに割り当てられます。このアドレスにより、クライアントは、パブリック ネットワーク上のホストとして機能することが可能となります。

- [Ping]：ICMP ping（Packet Internet Groper）パケットを送信して、ネットワークの接続をテストします。具体的には、ASA は選択されたホストに ICMP Echo Request メッセージを送信します。ホストが到達可能な場合は、Echo Reply メッセージが返され、ASA はテストしたホストの名前と共に Success メッセージを表示し、さらに要求を送信してから応答を受信するまでの経過時間も表示します。何らかの理由でシステムに到達できない場合（ホストがダウンしている、ホストで ICMP が実行されていない、ルートが設定されていない、中間ルータがダウンしている、ネットワークがダウンまたは輻輳しているなど）、ASA では、テストしたホストの名前が記された [Error] 画面が表示されます。

- [Logout By]：ログアウトするセッションのフィルタリングに使う基準を選択します。--All Sessions-- 以外を選択した場合、[Logout By] リストの右側のボックスがアクティブになります。値に Protocol for Logout By を選択した場合、ボックスがリストに変わり、ログアウト フィルタとして使用するプロトコル タイプを選択できます。このリストのデフォルト値は IPsec です。Protocol 以外の値を選択した場合は、このボックスに適切な値を入力する必要があります。

[アクティブ VPN セッションのモニタリング（Monitor Active VPN AnyConnect Sessions）]

[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]

ユーザー名、IPアドレス、アドレスタイプ、またはパブリックアドレスでソートされたセキュアクライアント セッションを表示します。

[Monitor VPN Session Details]

[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] > [Details]

選択したセッションのコンフィギュレーション設定、統計情報、およびステート情報を表示します。

- [NAC Result and Posture Token]

ASDM では、ASA にネットワーク アドミッション コントロールが設定されている場合にのみ、このカラムに値が表示されます。

- [Accepted]：ACS は正常にリモート ホストのポスチャを検証しました。
- [Rejected]：ACS はリモート ホストのポスチャの検証に失敗しました。
- [Exempted]：ASA に設定されたポスチャ検証免除リストに従って、リモート ホストはポスチャ検証を免除されています。
- [Non-Responsive]：リモート ホストは EAPoUDP Hello メッセージに応答しませんでした。
- [Hold-off]：ポスチャ検証に成功した後、ASA とリモート ホストの EAPoUDP 通信が途絶えました。
- [N/A]：VPN NAC グループ ポリシーに従い、リモート ホストの NAC はディセーブルにされています。
- [Unknown]：ポスチャ検証が進行中です。

ポスチャ トークンは、Access Control Server で設定可能な情報文字列です。ACS は情報提供のために ASA にポスチャ トークンをダウンロードし、システム モニタリング、レポート、デバッグ、およびロギングを支援します。NAC Result に続く一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected または Unknown です。

[Session Details] ペインの [Details] タブには、次のカラムが表示されます。

- [ID]：セッションにダイナミックに割り当てられた一意の ID。ID は、セッションへの ASA のインデックスとして機能します。このインデックスを使用して、セッションに関する情報を維持および表示します。
- [Type]：セッションのタイプ。IKE、IPsec または NAC。
- [Local Addr., Subnet Mask, Protocol, Port, Remote Addr., Subnet Mask, Protocol, and Port]：実際の（ローカル）ピアの両方に割り当てられているアドレスとポートと外部ルーティングのためにそのピアに割り当てられているアドレスとポート。

- [Encryption]：このセッションで使用しているデータ暗号化アルゴリズム（使用している場合）。
- [Assigned IP Address and Public IP Address]：このセッションのリモート ピアに割り当てられているプライベート IP アドレスを示します。内部または仮想 IP アドレスとも呼ばれ、割り当てられている IP アドレスによって、リモート ピアはプライベート ネットワーク上にあるように見えます。2 番目のフィールドには、このセッションのリモート コンピュータのパブリック IP アドレスが表示されます。外部 IP アドレスとも呼ばれ、通常、パブリック IP アドレスは ISP によってリモート コンピュータに割り当てられます。これによって、リモート コンピュータはパブリック ネットワークのホストとして機能できます。
- [Other]：セッションに関連付けられているその他の属性。

次の属性は、IKE セッション、IPsec セッション、および NAC セッションに適用されます。

- [Revalidation Time Interval]：成功した各ポスチャ検証間に必要とされる間隔（秒数）。
- [Time Until Next Revalidation]：最後のポスチャ検証試行が成功しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
- [Status Query Time Interval]：成功したポスチャ検証またはステータス クエリーの応答と次のステータス クエリーの応答との間に許容される時間（秒数）。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、ASA がリモート ホストに発行する要求です。
- [EAPoUDP Session Age]：最後に成功したポスチャ検証から経過した秒数。
- [Hold-Off Time Remaining]：最後のポスチャ検証が成功した場合は 0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。
- [Posture Token]：Access Control Server で設定可能な情報文字列。ACS は情報提供のために ASA にポスチャ トークンをダウンロードし、システム モニタリング、レポート、デバッグ、およびロギングを支援します。一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。
- [Redirect URL]：ポスチャ検証またはクライアントレス認証が終わると、ACS はセッション用のアクセス ポリシーを ASA にダウンロードします。Redirect URL は、アクセス ポリシー ペイロードのオプションの一部です。ASA は、リモート ホストのすべての HTTP（ポート 80）要求と HTTPS（ポート 443）要求を Redirect URL（存在する場合）にリダイレクトします。アクセス ポリシーに Redirect URL が含まれていない場合、ASA はリモート ホストからの HTTP 要求や HTTPS 要求をリダイレクトしません。

  Redirect URL は、IPsec セッションが終了するか、ポスチャ再検証が実行されるまで有効です。ACS は、異なる Redirect URL が含まれるか、Redirect URL が含まれない新しいアクセス ポリシーをダウンロードします。

  [More]：このボタンを押して、セッションやトンネル グループを再検証または初期化します。

ACL タブには、セッションに一致した ACE が含まれる ACL が表示されます。

[Monitor Cluster Loads]

[Monitoring] > [VPN] > [VPN Statistics] > [Cluster Loads]

VPN ロードバランシング クラスタ内のサーバー間における現在のトラフィックの負荷分散を表示します。サーバーがクラスタの一部でない場合、このサーバーが VPN ロードバランシング クラスタに参加していない旨を伝える情報メッセージが表示されます。

[Monitor Crypto Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Crypto Statistics]

ASA で現在アクティブなユーザーと管理者セッションの暗号統計情報を表示します。テーブルの各行は、1 つの暗号統計情報を表します。

[Monitor Compression Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Compression Statistics]

ASA で現在アクティブなユーザーと管理者セッションの圧縮統計情報を表示します。テーブルの各行は、1 つの圧縮統計情報を表します。

[Monitor Encryption Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Encryption Statistics]

ASA で現在アクティブなユーザーと管理者セッションが使用しているデータ暗号化アルゴリズムを表示します。テーブルの各行は、1 つの暗号化アルゴリズム タイプを表します。

[Monitor Global IKE/IPsec Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Global IKE/IPSec Statistics]

ASA で現在アクティブなユーザーと管理者セッションのグローバル IKE/IPsec 統計情報を表示します。テーブルの各行は、1 つのグローバル統計情報を表します。

[Monitor NAC Session Summary]

アクティブな累積ネットワーク アドミッション コントロール セッションを表示します。

- [Active NAC Sessions]：ポスチャ検証の対象のリモート ピアに関する一般的な統計情報。
- [Cumulative NAC Sessions]：現在ポスチャ検証の対象か、または以前から対象だったリモート ピアに関する一般的な統計情報。
- [Accepted]：ポスチャ検証に成功し、Access Control Server によってアクセス ポリシーが与えられたピアの数。
- [Rejected]：ポスチャ検証に失敗し、Access Control Server によってアクセス ポリシーが与えられなかったピアの数。
- [Exempted]：ASA で設定された [Posture Validation Exception] リストのエントリと一致しているため、ポスチャ検証の対象になっていないピアの数。

- [Non-responsive]：Extensible Authentication Protocol（EAP）over UDP のポスチャ検証要求に応答しないピアの数。CTA が実行されていないピアは、この要求に応答しません。ASA のコンフィギュレーションがクライアントレス ホストをサポートしている場合、Access Control Server は、クライアントレス ホストに関連付けられているアクセス ポリシーをこれらのピアの ASA にダウンロードします。クライアントレス ホストをサポートしていない場合、ASA は NAC デフォルト ポリシーを割り当てます。
- [Hold-off]：ポスチャ検証が成功した後に、ASA が EAPoUDP 通信を失ったピアの数。NAC Hold Timer 属性（[Configuration] > [VPN] > [NAC]）は、このタイプのイベントと次のポスチャ検証試行との間の遅延時間を判定します。
- [N/A]：VPN NAC グループ ポリシーに従って NAC が無効になっているピアの数。
- [Revalidate All]：ピアのポスチャまたは割り当てられているアクセス ポリシー（ダウンロードされた ACL）が変更された場合にクリックします。このボタンをクリックすると、ASA によって管理されるすべての NAC セッションの新しい無条件ポスチャ検証が開始されます。このボタンをクリックするまで各セッションに対して有効だったポスチャ検証と割り当てられているアクセス ポリシーは、新しいポスチャ検証が成功または失敗するまで有効のままとなります。ポスチャ検証から免除されているセッションには、このボタンをクリックしても影響はありません。
- [Initialize All]：ピアのポスチャまたは割り当てられているアクセス ポリシー（ダウンロードされた ACL）が変更され、セッションに割り当てられているリソースをクリアする場合にクリックします。このボタンをクリックすると、ASA によって管理されるすべての NAC セッションのポスチャ検証で使用される、EAPoUDP アソシエーションと割り当てられたアクセス ポリシーがパージされ、新しい無条件のポスチャ検証が開始されます。再検証中には NAC のデフォルトの ACL が有効となるため、セッションを初期化するとユーザー トラフィックに影響する場合があります。ポスチャ検証から免除されているセッションには、このボタンをクリックしても影響はありません。

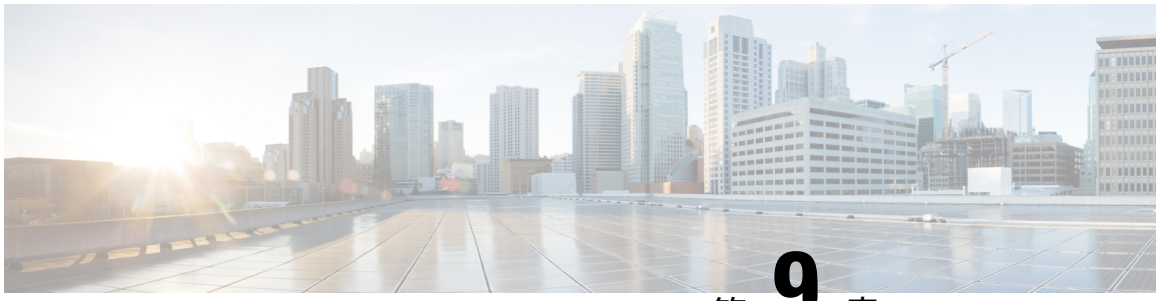
[Monitor Protocol Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Protocol Statistics]

ASA で現在アクティブなユーザーと管理者セッションが使用しているプロトコルを表示します。テーブルの各行は、1 つのプロトコル タイプを表します。

[Monitor VLAN Mapping Sessions]

使用中の各グループ ポリシーの Restrict Access to VLAN パラメータの値で判別された、出力 VLAN に割り当てられているセッション数を表示します。ASA はすべてのトラフィックを指定された VLAN に転送します。



第 9 章

SSL 設定

SSL 設定

次の場所のいずれかで SSL 設定を構成します。

- **[Configuration] > [Device Management] > [Advanced] > [SSL Settings]**
- **[Configuration] > [Remote Access VPN] > [Advanced] > [SSL Settings]**

ASA は、Secure Sockets Layer（SSL）プロトコルと Transport Layer Security（TLS）を使用して、ASDM、クライアントレス SSL VPN、VPN、およびブラウザベースの各セッションのセキュアなメッセージ伝送を実現します。また、DTLS は Secure Clientの接続に使用されます。[SSL Settings] ペインでは、クライアントとサーバーの SSL バージョンおよび暗号化アルゴリズムを設定できます。また、以前に設定したトラストポイントを特定のインターフェイスに適用したり、関連付けられたトラストポイントのないインターフェイスのフォールバック トラストポイントを設定したりすることもできます。

（注） リリース 9.3（2）では、SSLv3 は廃止されています。現在のデフォルトは [any] ではなく [tlsv1] です。[any] キーワードは廃止されました。[any]、[sslv3] または [sslv3-only] を選択した場合、設定は受け入れられますが警告が表示されます。[OK] をクリックして作業を続行します。ASA の次のメジャー リリースでは、これらのキーワードは ASA から削除されます。

バージョン 9.4（1）では、SSLv3 キーワードはすべて ASA 設定から削除されており、SSLv3 のサポートが ASA から削除されました。SSLv3 がイネーブルになっている場合は、SSLv3 オプションを指定したコマンドからブート時エラーが表示されます。ASA はデフォルトの TLSv1 に戻ります。

Citrix モバイル レシーバは TLS 1.1/1.2 プロトコルをサポートしていない可能性があります。互換性については、https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf を参照してください。

フィールド

- [Server SSL Version]：ASA がサーバーとして動作するときに使用する、最小の SSL/TLS プロトコル バージョンをドロップダウン リストから指定します。

いずれか（Any）	SSLv2 クライアントの hello を受け入れ、共通の最新バージョンをネゴシエートします。
SSL V3	SSLv2 クライアントの hello を受け入れ、SSLv3（以降）をネゴシエートします。
TLS V1	SSLv2 クライアントの hello を受け入れ、TLSv1（以降）をネゴシエートします。
TLSV1.1	SSLv2 クライアントの hello を受け入れ、TLSv1.1（以降）をネゴシエートします。
TLSV1.2	SSLv2 クライアントの hello を受け入れ、TLSv1.2（以降）をネゴシエートします。
TLSV1.3	SSLv2 クライアントの hello を受け入れ、TLSv1.3（以降）をネゴシエートします。
DTLSv1	DTLSv1 クライアントの hello を受け入れ、DTLSv1（以降）をネゴシエートします。
DTLS1.2	DTLSv1.2 クライアントの hello を受け入れ、DTLSv1.2（以降）をネゴシエートします。

（注） DTLS の設定と使用は、Cisco Secure Client 接続の AnyConnect VPN モジュールにのみ適用されます。

DTLS と同等以上の TLS バージョンを使用して、TLS セッションを DTLS セッションと同等以上にセキュアにする必要があります。DTLSV1.2 は、TLSV1.2 および TLSV1.3 をサポートします。すべての TLS バージョンは DTLS 1 以上であるため、DTLS1 で使用できます。ただし、TLSV1.2 以前で server-max-version を構成すると、ASDM 接続が終了します。

TLSV1.3 には、Cisco Secure Client バージョン 5.0 以降が必要です。

- [Client SSL Version]：ASA がクライアントとして動作するときに使用する、最小の SSL/TLS プロトコル バージョンをドロップダウン リストから指定します。（SSL クライアント ロールに対して DTLS は使用不可）

いずれか（Any）	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。

SSL 設定

SSL V3	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。
TLS V1	TLSv1 クライアントの hello を送信し、TLSv1（以降）をネゴシエートします。
TLSV1.1	TLSv1.1 クライアントの hello を送信し、TLSv1.1（以降）をネゴシエートします。
TLSV1.2	TLSv1.2 クライアントの hello を送信し、TLSv1.2（以降）をネゴシエートします。
TLSV1.3	TLSv1.3 クライアントの hello を送信し、TLSv1.3（以降）をネゴシエートします。

- [Diffie-Hellmann group to be used with SSL]：ドロップダウン リストからグループを選択します。使用可能なオプションは、[Group1]（768 ビット絶対値）、[Group2]（1024 ビット絶対値）、[Group5]（1536 ビット絶対値）、[Group14]（2048 ビット絶対値、224 ビット素数位数）、および [Group24]（2048 ビット絶対値、256 ビット素数位数）です。デフォルト値は [Group2] です。
- [ECDH group to be used with SSL]：ドロップダウン リストからグループを選択します。使用可能なオプションは、[Group19]（256 ビット EC）、[Group20]（384 ビット EC）、および [Group21]（521 ビット EC）です。デフォルト値は [Group19] です。

（注） 優先度が最も高いのは ECDSA 暗号および DHE 暗号です。

- [Encryption]：サポートするバージョン、セキュリティ レベル、および SSL 暗号化アルゴリズムを指定します。[Configure Cipher Algorithms/Custom String] ダイアログボックスを使用してテーブル エントリを定義または変更するには、[Edit] をクリックします。SSL 暗号のセキュリティ レベルを選択し、[OK] をクリックします。
  - [Cipher Version]：ASA でサポートされ、SSL 接続に使用される暗号バージョンを一覧表示します。
  - [Cipher Security Level]：ASA でサポートされ、SSL 接続に使用される暗号セキュリティ レベルを一覧表示します。次のいずれかのオプションを選択します。

    [All]：NULL-SHA を含むすべての暗号。

    [Low]：NULL-SHA を除くすべての暗号。

    [Medium]：NULL-SHA、DES-CBC-SHA、RC4-MD5（これがデフォルトです）、RC4-SHA、および DES-CBC3-SHA を除くすべての暗号。

    [高（High）]：SHA-2 暗号を使用する AES-256 のみを含み、TLS バージョン 1.2 および TLS バージョン 1.3 でサポートされている暗号にのみ適用されます。

[Custom]：[Cipher algorithms/custom string] ボックスで指定する 1 つ以上の暗号。このオプションでは、OpenSSL 暗号定義文字列を使用して暗号スイートを詳細に管理できます。

- [Cipher Algorithms/Custom String]：ASA でサポートされ、SSL 接続に使用される暗号アルゴリズムを一覧表示します。OpenSSL を使用する暗号の詳細については、https://www.openssl.org/docs/manmaster/man1/ciphers.htmlを参照してください。

  ASA は、サポートされている暗号方式の優先順位を、TLSv1.3/TLSv1.2 のみでサポートされている暗号方式、TLSv1.1、TLSv1.2、または TLSv1.2 でサポートされていない暗号方式の順に指定します。

次の暗号方式がサポートされています。

- [Server Name Indication (SNI)]：ドメイン名とそのドメインに関連付けることを指定します。[Add/Edit Server Name Indication (SNI)] ダイアログボックスを使用して各インターフェイスのドメインやトラストポイントを定義または変更するには、[Add] または [Edit] をクリックします。

暗号化方式	TLSv1.1 / DTLS V1	TLSV1.2 / DTLSV 1.2	TLSv1.3
TLS_AES_128_GCM_SHA256	×	×	○
TLS_CHACHA20_POLY1305_SHA256	×	×	○
TLS_AES_256_GCM_SHA384	×	×	○
AES128-GCM-SHA256	×	○	×
AES128-SHA	○	○	×
AES128-SHA256	×	○	×
AES256-GCM-SHA384	×	○	×
AES256-SHA	○	○	×
AES256-SHA256	×	○	×
DERS-CBC-SHA	×	×	×
DES-CBC-SHA	○	○	×
DHE-RSA-AES128-GCM-SHA256	×	○	×
DHE-RSA-AES128-SHA	○	○	×
DHE-RSA-AES128-SHA256	×	○	×
DHE-RSA-AES256-GCM-SHA384	no	l	×
DHE-RSA-AES256-SHA	○	○	×

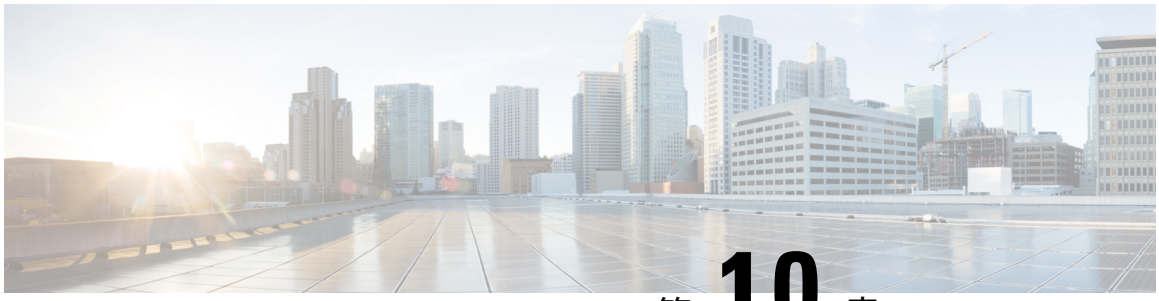
暗号化方式	TLSv1.1 / DTLS V1	TLSV1.2 / DTLSV 1.2	TLSv1.3
ECDHE-ECDSA-AES128-GCM-SHA256	×	○	×
ECDHE-ECDSA-AES128-SHA256	×	○	×
ECDHE-ECDSA-AES256-GCM-SHA384	×	○	×
ECDHE-ECDSA-AES256-SHA384	×	○	×
ECDHE-RSA-AES128-GCM-SHA256	○	○	×
ECDHE-RSA-AES128-SHA256	×	○	×
ECDHE-RSA-AES256-GCM-SHA384	×	○	×
ECDHE-RSA-AES256-SHA384	×	○	×
NULL-SHA	×	×	×
RC4-MD5	×	×	×
RC4-SHA	×	×	×

（注） DTLS1.2 トンネルは TLSv1.3 で動作しますが、DTLS1.2 は TLSv1.3 暗号をサポートしていません。DTLS1.2 トンネルには、サポートされている最も優先度の高い暗号が選択されます。

- [Specify domain]：ドメイン名を入力します。
- [Select trustpoint to associate with domain]：ドロップダウン リストからトラストポイントを選択します。

- [Certificates]：各インターフェイスの SSL 認証に使用する証明書を割り当てます。[Select SSL Certificate] ダイアログボックスを使用して各インターフェイスのトラストポイントを定義または変更するには、[Edit] をクリックします。
  - [Primary Enrolled Certificate]：このインターフェイスの証明書に使用するトラストポイントを選択します。
  - [Load Balancing Enrolled Certificate]：VPN ロードバランシングが設定されている場合、証明書で使用するトラストポイントを選択します。
- [Fallback Certificate]：証明書が関連付けられていないインターフェイスで使用する証明書を選択します。[None] を選択すると、ASA はデフォルトの RSA キー ペアと証明書を使用します。
- [Forced Certification Authentication Timeout]：証明書認証がタイムアウトするまでの分数を設定します。

- [Apply]：変更内容を保存します。
- [Reset]：変更内容を取り消し、SSL パラメータを以前に定義した値にリセットします。



第 10 章

仮想トンネル インターフェイス

この章では、VTI トンネルの設定方法について説明します。

仮想トンネル インターフェイスについて

ASA は、仮想トンネルインターフェイス（VTI）と呼ばれる論理インターフェイスをサポートします。ポリシーベースの VPN の代わりに、VTI を使用してピア間に VPN トンネルを作成できます。VTI は、各トンネルの終端に IPsec プロファイルが付加されたルートベースの VPN をサポートします。動的ルートまたは静的ルートを使用できます。VTIからの出力トラフィックは暗号化されてピアに送信され、VTI への入力トラフィックは関連付けされた SA によって復号化されます。

VTI を使用することにより、静的暗号マップのアクセス リストを設定してインターフェイスにマッピングすることが不要になります。すべてのリモート サブネットを追跡し、暗号マップのアクセスリストに含める必要がなくなります。展開が簡単になるほか、ダイナミック ルーティング プロトコルのルート ベースの VPN をサポートするステティック VTI があると、仮想プライベートクラウドの多くの要件を満たすこともできます。

スタティック VTI

2 つのサイト間でトンネルが常にオンになっているサイト間接続用に、スタティック VTI 設定を使用できます。スタティック VTI インターフェイスの場合、物理インターフェイスをトンネルソースとして定義する必要があります。デバイスごとに最大 1024 の VTI を関連づけることができます。スタティック VTI インターフェイスを作成するには、VTI インターフェイスの追加 （271 ページ）を参照してください。

Dynamic VTI

ダイナミック VTI は、サイト間 VPN に高度に安全でスケーラブルな接続を提供します。ダイナミック VTI は、大規模な企業向けハブアンドスポーク展開でのピアの構成を容易にします。

ハブの複数のスタティック VTI 構成を単一の ダイナミック VTI に置き換えることができます。ハブの構成を変更せずに、新しいスポークをハブに追加できます。ダイナミック VTI テクノロジーは、ダイナミック クリプト マップとトンネルを確立するためのダイナミック ハブアンドスポーク方式にとって代わるものです。管理センターでは、ダイナミック VTI はハブアンドスポークトポロジのみをサポートします。

ダイナミック VTI では、IPsec インターフェイスの動的なインスタンス化および管理のために、仮想テンプレートが使用されます。仮想テンプレートは、VPN セッションごとに固有の仮想アクセスインターフェイスを動的に生成します。ダイナミック VTI は、複数の IPsec セキュリティアソシエーションをサポートし、スポークによって提案された複数の IPsec セレクターを受け入れます。ダイナミック VTI はダイナミック（DHCP）スポークもサポートします。ダイナミック VTI インターフェイスを作成するには、ダイナミック VTI インターフェイスの追加（274 ページ）を参照してください。

ASA で VPN セッションのダイナミック VTI トンネルを作成する方法

1. ASA で仮想テンプレートを作成します（[設定（Configuration）]>[デバイスの設定（Device Setup）] > [インターフェイス設定（Interface Settings）] > [インターフェイス（Interfaces）] > [追加（Add）] > [DVTIインターフェイス（DVTI Interface）] を選択）。

   このテンプレートは、複数の VPN セッションに使用できます。

2. このテンプレートをトンネルグループに適用します。1 つの仮想テンプレートを複数のトンネルグループに適用することができます。

3. スポークは、ハブとのトンネル要求を開始します。

4. ハブはスポークを認証します。

5. ASA は、仮想テンプレートを使用して、スポークとの VPN セッション用にハブ上に仮想アクセスインターフェイスを動的に作成します。

6. ハブは、仮想アクセスインターフェイスを使用して、スポークとのダイナミック VTI トンネルを確立します。

7. IKEv2 交換で VTI インターフェイス IP をアドバタイズするように、IKEv2 route set interface オプションを設定します。このオプションにより、トンネルを介して機能する BGP またはパスモニタリングの VTI インターフェイス間のユニキャスト到達可能性が有効になります。

8. VPN セッションが終了すると、トンネルは切断され、ハブは対応する仮想アクセスインターフェイスを削除します。

仮想トンネル インターフェイスの注意事項

コンテキストモードとクラスタリング

- シングル モードでだけサポートされています。

- クラスタリングはサポートされません。

ファイアウォール モード

ルーテッド モードのみでサポートされます。

BGP IPv4 および IPv6 のサポート

VTI を介した IPv4 および IPv6 BGP ルーティングをサポートします。

EIGRP サポート

VTI を介した IPv4 および IPv6 EIGRP ルーティングをサポートします。

OSPF IPv4 および IPv6 のサポート

VTI を介した IPv4 および IPv6 OSPF ルーティングをサポートします。

IPv6 のサポート

- IPv6 アドレスが指定された VTI を設定できます。
- VTI のトンネル送信元とトンネル接続先の両方に IPv6 アドレスを設定できます。
- パブリック IP バージョンを介した VTI IP（または内部ネットワーク IP バージョン）の次の組み合わせがサポートされています。
  - IPv6 over IPv6
  - IPv4 over IPv6
  - IPv4 over IPv4
  - IPv6 over IPv4
- トンネルの送信元および接続先としてサポートされるのは、静的IPv6アドレスだけです。
- トンネル送信元インターフェイスには IPv6 アドレスを設定できます。トンネルエンドポイントとして使用するアドレスを指定できます。指定しない場合、デフォルトでは、リスト内の最初の IPv6 グローバルアドレスがトンネルエンドポイントとして使用されます。
- トンネルモードを IPv6 として指定できます。指定した場合、VTIを介して IPv6 トラフィックをトンネリングできます。ただし、単一 VTI のトンネルモードは IPv4 または IPv6 のいずれかになります。

一般的な設定時の注意事項

- LAN-to-LAN VPN でダイナミッククリプトマップとダイナミック VTI を使用する場合は、ダイナミック VTI トンネルのみが起動します。この動作は、クリプトマップとダイナミック VTI の両方がデフォルトのトンネルグループを使用しようとするために発生します。

  次のいずれかを実行することを推奨します。

- LAN-to-LAN VPN をダイナミック VTI に移行します。
- 独自のトンネルグループを持つ静的クリプトマップを使用します。

- VTI は IPsec モードのみで設定可能です。ASA で GRE トンネルを終了することはサポートされていません。
- トンネルインターフェイスを使用するトラフィックには、静的、BGP、OSPF、または EIGRP IPv4 ルートを使用できます。
- スタティックおよびダイナミック VTI の場合は、借用 IP インターフェイスを VTI インターフェイスのトンネルソース IP アドレスとして使用しないでください。
- VTI の MTU は、基盤となる物理インターフェイスに応じて自動的に設定されます。ただし、VTI を有効にした後で物理インターフェイス MTU を変更した場合は、新しい MTU 設定を使用するために VTI を無効にしてから再度有効にする必要があります。
- ダイナミック VTI の場合、仮想アクセスインターフェイスは、設定されたトンネル送信元インターフェイスから MTU を継承します。トンネル送信元インターフェイスを指定しない場合、仮想アクセスインターフェイスは、ASA が VPN セッション要求を受け入れる送信元インターフェイスから MTU を継承します。
- スタティック VTI の場合、デバイスには最大 1024 の VTI を設定できます。VTI 数を計算する際は、次の点を考慮してください。
  - nameif サブインターフェイスを含めて、デバイスに設定できる VTI の総数を導き出します。
  - ポートチャネルのメンバーインターフェイスに nameif を設定することはできません。したがって、トンネル数は実際のメイン ポートチャネル インターフェイスの数だけ減少し、そのメンバーインターフェイスの数は減少しません。
  - プラットフォームが 1024 個を超えるインターフェイスをサポートしている場合でも、VTI の数はそのプラットフォームで設定可能な VLAN の数に制限されます。たとえば、500 の VLAN をサポートしているモデルの場合、トンネル数は 500 から設定された物理インターフェイスの数を引いた数になります。
- ダイナミック VTI の場合、ダイナミックに作成された仮想アクセス インターフェイスの最大数は、1024 またはプラットフォームの合計インターフェイス制限のいずれか少ない方です。
- VTI は IKE のバージョン v1 および v2 をサポートしており、トンネルの送信元と宛先の間でのデータ送受信に IPsec を使用します。
- NAT を適用する必要がある場合、IKE および ESP パケットは、UDP ヘッダーにカプセル化されます。
- IKE および IPsec のセキュリティ アソシエーションには、トンネル内のデータ トラフィックに関係なく、継続的にキーの再生成が行われます。これにより、VTI トンネルは常にアップした状態になります。

- トンネルグループ名は、ピアが自身の IKEv1 または IKEv2 識別情報として送信するものと一致する必要があります。
- サイト間トンネルグループの IKEv1 では、トンネルの認証方式がデジタル証明書である場合、かつ/またはピアがアグレッシブモードを使用するように設定されている場合、IP アドレス以外の名前を使用できます。
- 暗号マップに設定されるピア アドレスと VTI のトンネル宛先が異なる場合、VTI 設定と暗号マップの設定を同じ物理インターフェイスに共存させることができます。
- VTI 経由のトラフィックを制御するため、VTI インターフェイスにアクセスルールを適用することができます。
- ICMP ping は、VTI インターフェイス間でサポートされます。
- IKEv2 サイト間 VPN トンネルのピアデバイスが IKEv2 設定要求ペイロードを送信した場合、ASA はデバイスとの IKEv2 トンネルを確立できません。ASA がピアデバイスとの VPN トンネルを確立するには、ピアデバイスで config-exchange 要求を無効にする必要があります。
- ダイナミック VTI は HA および IKEv2 をサポートします。

デフォルト設定

- デフォルトでは、VTI 経由のトラフィックは、すべて暗号化されます。
- VTI インターフェイスのデフォルトのセキュリティレベルは 0 です。セキュリティレベルを設定することはできません。

VTI の制限事項

ASA は、VTI 復号化の後にセキュリティ グループ タグ（SGT）フレームとパケットをドロップします。

ダイナミック VTI は以下をサポートしていません。

- ECMP と VRF
- クラスタリング
- IKEv1
- QoS

ダイナミック VTI では、トンネル送信元が指定されていないと、管理専用インターフェイスとフェールオーバーインターフェイスを除くデバイスのすべてのインターフェイスで、IKEv2 が有効になります。

VTI トンネルの作成

VTI トンネルを設定するには、IPsecプロポーザル（トランスフォームセット）を作成します。IPsec プロポーザルを参照する IPsec プロファイルを作成した後で、IPsec プロファイルを持つ VTI インターフェイスを作成します。リモートピアには、同じ IPsec プロポーザルおよび IPsec プロファイルパラメータを設定します。SA ネゴシエーションは、すべてのトンネルパラメータが設定されると開始します。

（注） VPN および VTI ドメインの両方に属し、物理インターフェイス上で BGP 隣接関係を持つ ASA では、次の動作が発生します。

インターフェイスヘルスチェックによって状態の変更がトリガーされると、物理インターフェイスでのルートは、新しいアクティブなピアとの BGP 隣接関係が再確立されるまで削除されます。この動作は、論理 VTI インターフェイスには該当しません。

VTI 経由のトラフィックを制御するため、VTI インターフェイスにアクセス制御リストを適用することができます。IPsec トンネルから送信されるすべてのパケットに対して、ACL で発信元インターフェイスと宛先インターフェイスをチェックせずに許可するには、グローバル コンフィギュレーション モードで sysopt connection permit-vpn コマンドを入力します。

ACL をチェックせずに ASA を通過する IPsec トラフィックをイネーブルにするための次のコマンドを使用できます。

hostname(config)# sysopt connection permit-vpn

外部インターフェイスと VTI インターフェイスのセキュリティレベルが 0 の場合、VTI インターフェイスに ACL が適用されていても、same-security-traffic が設定されていなければヒットしません。

この機能を設定するには、グローバルコンフィギュレーションモードで **intra-interface** 引数を指定して **same-security-traffic** コマンドを実行します。

手順

ステップ 1 IPsec プロポーザル（トランスフォーム セット）を追加します。

ステップ 2 IPsec プロファイルを追加します。

ステップ 3 VTI トンネルを追加します。

IPsec プロポーザル（トランスフォーム セット）の追加

トランスフォームセットは、VTI トンネル内のトラフィックを保護するために必要です。これは、VPN 内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムのセットであり、IPsec プロファイルの一部として使用されます。

始める前に

- VTI に関連付けられた IKE セッションを認証するには、事前共有キーまたは証明書のいずれかを使用できます。IKEv2 では、非対称認証方式とキーが使用できます。IKEv1 と IKEv2 のどちらも、VTI に使用するトンネル グループの下に事前共有キーを設定する必要があります。
- IKEv1 を使用した証明書ベースの認証には、イニシエータで使用されるトラストポイントを指定する必要があります。レスポンダについては、tunnel-group コマンドでトラストポイントを設定する必要があります。IKEv2 では、イニシエータとレスポンダの両方について、認証に使用するトラストポイントを tunnel-group コマンドで設定する必要があります。

手順

ステップ 1 **[Configuration]** > **[Site-to-Site VPN]** > **[Advanced]** > **[IPsec Proposals (Transform Sets)]** を選択します。

ステップ 2 セキュリティ アソシエーションを確立するための IKEv1 または IKEv2 を設定します。

- IKEv1 を設定します。

a) [IKEv1 IPsec Proposals (Transform Sets)] パネルで [Add] をクリックします。
b) [Set Name] を入力します。
c) [Tunnel] チェックボックスは、デフォルトの選択のままにします。
d) [ESP Encryption] および [ESP Authentication] を選択します。
e) [OK] をクリックします。

- IKEv2 を設定します。

a) [IKEv2 IPsec Proposals] パネルで [Add] をクリックします。
b) [Name] と [Encryption] を入力します。
c) [Integrity Hash] を選択します。
d) **[OK]** をクリックします。

IPsec プロファイルの追加

IPsec プロファイルには、その参照先の IPsec プロポーザルまたはトランスフォーム セット内にある必要なセキュリティ プロトコルおよびアルゴリズムが含まれています。これにより、2つのサイト間 VTI VPN ピアの間でセキュアな論理通信パスが確保されます。

手順

ステップ 1 **[Configuration]** > **[Site-to-Site VPN]** > **[Advanced]** > **[IPsec Proposals (Transform Sets)]** を選択します。

ステップ 2 [IPsec Profile] パネルで [Add] をクリックします。

ステップ 3 [Name] に IPsec プロファイル名を入力します。

ステップ 4 [IKE v1 IPsec Proposal] または [IKE v2 IPsec Proposal] に、IPsec プロファイルのために作成する IKE v1 IPsec プロポーザルまたは IKE v2 IPsec プロポーザルを入力します。IKEv1 トランスフォーム セットまたは IKEv2 IPsec プロポーザルのいずれかを選択できます。

ステップ 5 VTI トンネルの一端をレスポンダとしてのみ動作させる必要がある場合は、[Responder only] チェックボックスをオンにします。

- VTI トンネルの一端をレスポンダとしてのみ動作するように設定できます。レスポンダのみの端は、トンネルまたはキー再生成を開始しません。
- IKEv2 を使用する場合、セキュリティ アソシエーションのライフタイム期間は、イニシエータ側の IPsec プロファイルのライフタイム値より大きく設定します。こうすることで、イニシエータ側での正常なキー再生成が促進され、トンネルのアップ状態が保たれます。
- イニシエータ側のキー再生成の設定が不明の場合、レスポンダのみのモードを解除して SA の確立を双方向にするか、レスポンダのみの端の IPsec ライフタイム値を無期限にして期限切れを防ぎます。

ステップ 6 （任意）[Enable security association lifetime] チェックボックスをオンにして、セキュリティ アソシエーションの期間の値を**キロバイト**および**秒**で入力します。

ステップ 7 （任意）[PFS Settings] チェックボックスをオンにして、必要な Diffie-Hellman グループを選択します。

Perfect Forward Secrecy（PFS）は、暗号化された各交換に対し、一意のセッション キーを生成します。この一意のセッション キーにより、交換は、後続の復号化から保護されます。PFS を設定するには、PFS セッション キーを生成する際に使用する Diffie-Hellman キー導出アルゴリズムを選択する必要があります。キー導出アルゴリズムは、IPsec セキュリティ アソシエーション（SA）キーを生成します。各グループでは、異なるサイズの係数が使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。Diffie-Hellman グループは、両方のピアで一致させる必要があります。

これにより、暗号キー決定アルゴリズムの強度が確立されます。ASA はこのアルゴリズムを使用して、暗号キーとハッシュ キーを導出します。

ステップ 8 （任意）[Enable sending certificate] チェックボックスをオンにして、VTI トンネル接続の開始時に使用する証明書を定義する**トラストポイント**を選択します。必要に応じて、[Chain] チェックボックスをオンにします。

ステップ 9 この IPsec プロファイルのリバース ルート インジェクション（RRI）を有効にするには、[リバースルートインジェクションを有効にする（Enable Reverse Route Injection）] チェックボックスをオンにします。

RRI は、ASA を実行している場合は OSPF、EIGRP などのダイナミック ルーティング プロトコルを実行する内部ルータのルーティングテーブルを入力します。それ以外の場合は、リモート VPN クライアントまたは LAN-to-LAN セッションの RIP を実行する内部ルータのルーティングテーブルを入力します。RRIは設定で行われ、静的とみなされます。設定が変更または削除されるまでそのままになります。ASAは、ルーティングテーブルにスタティックルートを自動的に追加し、OSPF を使用してそれらのルートをプライベートネットワークまたは境界ルータに通知します。送信元/宛先（0.0.0.0/0.0.0.0）を保護ネットワークとして指定する場合は、RRIをイネーブルにしないでください。デフォルトルートを使用するトラフィックに影響します。

ステップ 10 [ダイナミック（Dynamic）] チェックボックスをオンにして、リバースルートをダイナミックルートとして設定します。

ステップ 11 [OK] をクリックします。

ステップ 12 [IPsec Proposals (Transform Sets)] メイン パネルで [Apply] をクリックします。

ステップ 13 [Preview CLI Commands] ダイアログボックスで、[Send] をクリックします。

VTI インターフェイスの追加

新しい VTI インターフェイスを作成して VTI トンネルを確立するには、次の手順を実行します。

（注） アクティブなトンネル内のルータが使用できないときにトンネルをアップした状態に保つため、IP SLA を実装します。http://www.cisco.com/go/asa-config の『ASA General Operations Configuration Guide』の「Configure Static Route Tracking」を参照してください。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 **[Add]** > **[VTI Interface]** の順に選択します。[Add VTI Interface] ウィンドウが表示されます。

ステップ 3 [General] タブで次の手順を実行します。

a) **VTI ID** を入力します。範囲は 0 ～ 10413 です。最大 10413 の VTI インターフェイスがサポートされます。

b) [Interface Name] を入力します。

c) [インターフェイスの有効化（Enable Interface）] チェックボックスがオンになっていることを確認します。
d) [パスモニタリング（Path Monitoring）] ドロップダウンリストから [IPv4] または [IPv6] を選択し、ピアの IP アドレスを入力します。
e) [コスト（Cost）] を入力します。指定できる範囲は 1 ～ 65535 です。

コストは、複数の VTI 間でトラフィックを負荷分散するための優先順位を決定します。最も小さい番号が最も高い優先順位になります。

f) IP アドレスの設定：

[アドレス（Address）] オプションボタンをクリックして、IP アドレスとサブネットマスクを設定します。

または

[アンナンバード（Unnumbered）] オプションボタンをクリックし、[IPアンナンバード（IP Unnumbered）] ドロップダウンリストからインターフェイスを選択して、その IP アドレスを借用します。リストからループバックインターフェイスまたは物理インターフェイスを選択することができます。

ステップ 4 [詳細（Advanced）] タブで次の操作を実行します。

a) [Destination IP] に入力します。
b) [送信元インターフェイス（Source Interface）] ドロップダウンリストから、トンネル送信元インターフェイスを選択します。

ループバック インターフェイスまたは物理インターフェイスを選択することもできます。

c) [IPsecポリシーによるトンネル保護（Tunnel Protection with IPsec Policy）] フィールドで、IPsec ポリシーを選択します。
d) [Tunnel Protection with IPsec Profile] フィールドで、IPsec プロファイルを選択します。
e) [Ensure the Enable Tunnel Mode IPv4 IPsec] チェックボックスをオンにします。

ステップ 5 [OK] をクリックします。

ステップ 6 [Interfaces] パネルで [Apply] をクリックします。

ステップ 7 [Preview CLI Commands] ダイアログボックスで、[Send] をクリックします。

更新された設定が読み込まれると、新しい VTI がインターフェイスのリストに表示されます。この新しい VTI は、IPsec サイト間 VPN の作成に使用できます。

例

ASA と IOS デバイスの間の VTI トンネル（IKEv2 を使用）の設定例

```
ASA□

crypto ikev2 policy 1
```

```
 encryption aes-gcm-256
 integrity null
 group 21
 prf sha512
 lifetime seconds 86400
!
crypto ipsec ikev2 ipsec-proposal gcm256
 protocol esp encryption aes-gcm-256
 protocol esp integrity null
!
crypto ipsec profile asa-vti
 set ikev2 ipsec-proposal gcm256
!
interface Tunnel 100
 nameif vti
 ip address 10.10.10.1 255.255.255.254
 tunnel source interface [asa-source-nameif]
 tunnel destination [router-ip-address]
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile asa-vti
!
tunnel-group [router-ip-address] ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
crypto ikev2 enable [asa-interface-name]


IOS □

!
crypto ikev2 proposal asa-vti
 encryption aes-gcm-256
 prf sha512
 group 21
!
crypto ikev2 policy asa-vti
 match address local [router-ip-address]
 proposal asa-vti
!
crypto ikev2 profile asa-vti
 match identity remote address [asa-ip-address] 255.255.255.255
 authentication local pre-share key cisco
 authentication remote pre-share key cisco
 no config-exchange request
!
crypto ipsec transform-set gcm256 esp-gcm 256
!
crypto ipsec profile asa-vti
 set ikev2-profile asa-vti
 set transform-set gcm256
!
interface tunnel 100
 ip address 10.10.10.0 255.255.255.254
 tunnel mode ipsec ipv4
 tunnel source [router-interface]
```

```
tunnel destination [asa-ip-address]
tunnel protection ipsec profile asa-vti
!
```

ダイナミック VTI インターフェイスの追加

ダイナミック VTI の仮想テンプレートを作成するには、次の手順を行います。

（注） アクティブなトンネル内のルータが使用できないときにトンネルをアップした状態に保つため、IP SLA を実装します。http://www.cisco.com/go/asa-config の『ASA General Operations Configuration Guide』の「Configure Static Route Tracking」を参照してください。

始める前に

IPsec プロファイルと IP アンナンバード インターフェイスが設定されていることを確認します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 **[追加（Add）]** > **[DVTIインターフェイス（DVTI Interface）]** の順に選択します。[DVTIインターフェイスの追加（Add DVTI Interface）] ウィンドウが表示されます。

ステップ 3 [General] タブで次の手順を実行します。

a) **DVTI ID** を入力します。この ID には 1 ー 10413 の任意の値を指定できます。デバイスごとに 最大 1024 の VTI インターフェイスがサポートされます。

b) [Interface Name] を入力します。

c) [アラートの有効化（Enable Alert）] チェックボックスがオンになっていることを確認します。

d) [IPアンナンバード（IP Unnumbered）] ドロップダウンリストからインターフェイスを選択します。

仮想テンプレートは、選択したインターフェイスの IP アドレスを継承します。トンネル送信元 IP アドレスとは異なる IP アドレスを使用していることを確認してください。任意の物理インターフェイスまたはデバイスに設定されているループバックアドレスを選択できます。

e) [説明（Description）] フィールドにダイナミック VTI の説明を入力します。

ステップ 4 [Advanced] タブで、次の手順を実行します。

a) [送信元インターフェイス（Source Interface）] ドロップダウンリストから、トンネル送信元インターフェイスを選択します。インターフェイスの IP アドレスは、スポークの宛先

IPアドレスになります。リストから選択できるのは、物理インターフェイスとループバック インターフェイスだけです。

b) トンネル送信元 IP アドレスが設定されたインターフェイスのみから VPN セッション要求を受け入れるには、[IPv6送信元アドレスの有効化（Enable IPv6 Source Address）] チェックボックスをオンにします。このオプションを有効にしない場合、ASA はすべてのインターフェイスからの VPN セッション要求を受け入れます。

また、仮想アクセスインターフェイスは、設定されたトンネル送信元インターフェイスからMTUを継承します。上記のオプションを有効にしない場合、仮想アクセスインターフェイスは、ASA が VPN セッション要求を受け入れる送信元インターフェイスから MTU を継承します。

c) [IPsecプロファイルによるトンネル保護（Tunnel Protection with IPsec Profile）] ドロップダウンリストから、IPsec プロファイルを選択します。

d) [IPSecのトンネルモードIPオーバーレイの有効化（Enable Tunnel Mode IP Overlay for IPSec）] チェックボックスをオンにし、[IPv4] または [IPv6] オプションボタンを選択して、IPSec トンネルモードを有効にします。

ステップ 5 [IPv6] タブで次の操作を実行します。

a) [IPv6アドレスアンナンバード（IPv6 Address Unnumbered）] 参照ボタンをクリックし、リストから IPv6 アドレスを選択します。

仮想テンプレートから複製されたすべての仮想アクセスインターフェイスは、同じIPアドレスを持つことになります。

b) [OK] をクリックします。

ステップ 6 [CLIコマンドのプレビュー（Preview CLI Commands）] ダイアログボックスで、仮想テンプレートコマンドを表示できます。

ステップ 7 [送信（Send）] をクリックします。

次のタスク

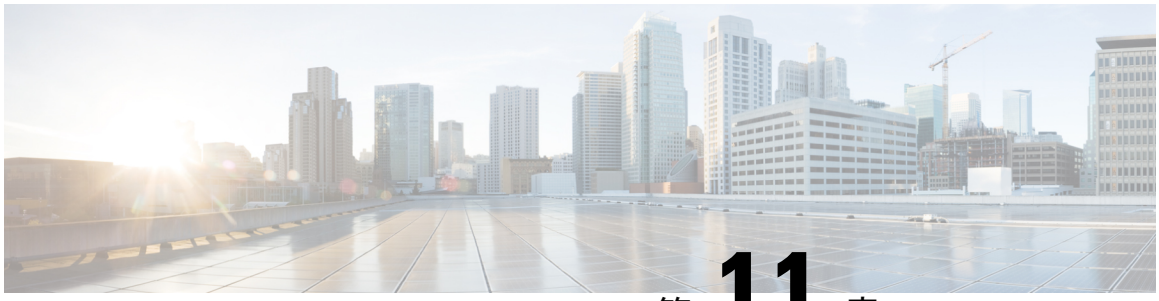
このテンプレートをトンネルグループに適用します。詳細については、「Site-to-Site トンネル グループ （154 ページ）」を参照してください。

仮想トンネルインターフェイスの機能履歴

機能名	リリース	機能情報
ダイナミック仮想トンネルインターフェイスのサポート	9.19(1)	ダイナミック VTI を作成し、それを使用して、ハブアンドスポークトポロジでルートベースのサイト間 VPN を設定できます。ダイナミック VTI は、大規模な企業向けハブアンドスポーク展開でのピアの構成を容易にします。ハブの複数のスタティック VTI 構成を単一の ダイナミック VTI に置き換えることができます。ハブの構成を変更せずに、新しいスポークをハブに追加できます。 新規/変更された画面：**[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [追加（Add）] > [DVTIインターフェイス（DVTI Interface）] > [詳細（Advanced）]**
OSPF IPv4 および IPv6 のサポート	9.19(1)	VTI 経由の OSPF IPv4 および IPv6 ルーティングプロトコルをサポートします。
EIGRP のサポート	9.19(1)	VTI 経由の EIGRP IPv4 および IPv6 ルーティングプロトコルをサポートします。
スタティックおよびダイナミック VTI のループバックインターフェイスのサポート	9.19(1)	ループバック インターフェイスを VTI の送信元インターフェイスとして設定できるようになりました。静的に設定された IP アドレスの代わりに、ループバック インターフェイスから IP アドレスを継承するサポートも追加されました。ループバック インターフェイスは、パス障害の克服に役立ちます。インターフェイスがダウンした場合、ループバック インターフェイスに割り当てられた IP アドレスを使用してすべてのインターフェイスにアクセスできます。 新規/変更された画面：**[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [VTIインターフェイスの追加（Add VTI Interface）] > [詳細（Advanced）]**
ローカルトンネル ID のサポート	9.17(1)	ASA は、ASA が NAT の背後に複数の IPsec トンネルを持ち、Cisco Umbrella Secure Internet Gateway（SIG）に接続できるようにする、一意のローカルトンネル ID をサポートしています。ローカル ID は、すべてのトンネルのグローバル ID ではなく、IKEv2 トンネルごとに一意の ID を設定するために使用されます。

機能名	リリース	機能情報
スタティック VTI での IPv6 のサポート	9.16(1)	ASA は、仮想トンネルインターフェイス（VTI）の設定で IPv6 アドレスをサポートしています。 VTI トンネル送信元インターフェイスには、トンネルエンドポイントとして使用するように設定できる IPv6 アドレスを設定できます。トンネル送信元インターフェイスに複数の IPv6 アドレスがある場合は、使用するアドレスを指定できます。指定しない場合は、リストの最初の IPv6 グローバルアドレスがデフォルトで使用されます。 トンネルモードは、IPv4 または IPv6 のいずれかです。ただし、トンネルをアクティブにするには、VTI で設定されている IP アドレスタイプと同じである必要があります。IPv6 アドレスは、VTI のトンネル送信元インターフェイスまたはトンネル宛先インターフェイスに割り当てることができます。
デバイスあたり 1024 個の VTI インターフェイスのサポート	9.16(1)	デバイスに設定できる VTI の最大数が、100 個から 1024 個に増加しました。 プラットフォームが 1024 個を超えるインターフェイスをサポートしている場合でも、VTI の数はそのプラットフォームで設定可能な VLAN の数に制限されます。たとえば、ASA 5510 は 100 個の VLAN をサポートしているため、トンネル数は 100 から設定された物理インターフェイスの数を引いた数になります。 新規/変更された画面：なし
VTI での DHCP リレーサーバーのサポート	9.14(1)	ASA は、インターフェイスを接続する DHCP リレーサーバーとして VTI インターフェイスを設定することを可能にします。 DHCP リレーに VTI インターフェイスを指定できるように次の画面が変更されました。 **[Configuration] > [Device Management] > [DHCP] > [DHCP Relay] > [DHCP Relay Interface Servers]**
VTI での IKEv2、証明書ベース認証、および ACL のサポート	9.8(1)	仮想トンネル インターフェイス（VTI）は、BGP（静的 VTI）をサポートするようになりました。スタンドアロン モードとハイ アベイラビリティ モードで、IKEv2 を使用できます。IPsec プロファイルにトラストポイントを設定することにより、証明書ベースの認証を使用できます。また、入力トラフィックをフィルタリングする access-group コマンドを使用して、VTI 上でアクセス リストを適用することもできます。 次の画面で、証明書ベース認証のトラストポイントを選択するオプションが導入されました。 **[設定（Configuration）] > [サイト間VPN（Site-to-Site VPN）] > [詳細（Advanced）] > [IPsecプロポーザル（トランスフォームセット）（IPsec Proposals (Transform Sets)）] > [IPsecプロファイル（IPsec Profile）] > [追加（Add）]**

機能名	リリース	機能情報
仮想トンネルインターフェイス（VTI）のサポート	9.7.(1)	ASA が、仮想トンネルインターフェイス（VTI）と呼ばれる新しい論理インターフェイスによって強化されました。VTI はピアへの VPN トンネルを表すために使用されます。これは、トンネルの各終端に接続されている IPsec プロファイルを利用したルート ベースの VPN をサポートします。VTI を使用することにより、静的暗号マップのアクセス リストを設定してインターフェイスにマッピングすることが不要になります。 次の画面が導入されました。 **[設定（Configuration）] > [サイト間VPN（Site-to-Site VPN）] > [詳細（Advanced）] > [IPsecプロポーザル（トランスフォームセット）（IPsec Proposals (Transform Sets)）] > [IPsecプロファイル（IPsec Profile）]** **[設定（Configuration）] > [サイト間VPN（Site-to-Site VPN）] > [詳細（Advanced）] > [IPsecプロポーザル（トランスフォームセット）（IPsec Proposals (Transform Sets)）] > [IPsecプロファイル（IPsec Profile）] > [追加（Add）] > [IPsecプロファイルの追加（Add IPsec Profile）]** **[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [追加（Add）] > [VTIインターフェイス（VTI Interface）]** **[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [追加（Add）] > [VTIインターフェイス（VTI Interface）] > [全般（General）]** **[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [追加（Add）] > [VTIインターフェイス（VTI Interface）] > [詳細（Advanced）]**



第 11 章

VPN の外部 AAA サーバーの設定

外部 AAA サーバーについて

この ASA は、外部の LDAP、RADIUS、TACACS+ サーバーを使用して、ASA の認証、認可、アカウンティング（AAA）をサポートするように設定できます。外部 AAA サーバーは、設定されたアクセス許可と属性を適用します。外部サーバーを使用するように ASA を設定する前に、適切な ASA 許可属性を指定して外部 AAA サーバーを設定し、それらの属性のサブセットから特定のアクセス許可を個々のユーザーに割り当てる必要があります。

許可属性のポリシー適用の概要

ASA は、ユーザー認可属性（ユーザー権利またはユーザー権限とも呼ばれる）を VPN 接続に適用するためのいくつかの方法をサポートしています。ASA を設定して、次のいずれかの組み合わせからユーザー属性を取得できます。

- ASA のダイナミック アクセス ポリシー（DAP）
- 外部 RADIUS または LDAP 認証および許可サーバー（およびその両方）
- ASA のグループ ポリシー

ASA がすべてのソースから属性を受信すると、それらの属性は評価されて集約され、ユーザー ポリシーに適用されます。属性の間で衝突がある場合、DAP 属性が優先されます。

ASA は次の順序で属性を適用します。

1. ASA 上の DAP 属性：バージョン 8.0(2) で導入されたこの属性は、他のどの属性よりも優先されます。DAP 内でブックマークまたは URL リストを設定した場合は、グループ ポリシーで設定されているブックマークや URL リストよりも優先されます。

2. AAA サーバー上のユーザー属性：ユーザー認証や認可が成功すると、サーバーからこの属性が返されます。これらの属性を、ASA のローカル AAA データベースで個々のユーザーに設定されている属性（ASDM のユーザー アカウント）と混同しないようにしてください。

3. ASA で設定されているグループ ポリシー：RADIUS サーバーからユーザーに対して RADIUS CLASS 属性 IETF-Class-25 （OU=*group-policy*）の値が返された場合、ASA はそのユーザーを同じ名前のグループ ポリシーに配置し、そのグループ ポリシーの属性のうち、サーバーから返されないものを適用します。

   LDAP サーバーでは、任意の属性名を使用してセッションのグループ ポリシーを設定できます。ASA 上に設定された LDAP 属性マップによって、LDAP 属性が Cisco 属性 IETF-Radius-Class にマッピングされます。

4. 接続プロファイル（CLI では「トンネル グループ」と呼ばれます）によって割り当てられたグループ ポリシー：接続プロファイルには、接続の事前設定が含まれているほか、認証前にユーザーに適用されるデフォルトのグループ ポリシーが含まれています。ASA に接続しているすべてのユーザーは、最初にこのグループに所属します。このグループで、DAP、サーバーから返されるユーザー属性、ユーザーに割り当てられているグループ ポリシーにはない属性が提供されます。

5. ASA で割り当てられたデフォルトのグループ ポリシー（DfltGrpPolicy）：システムのデフォルト属性は、DAP、ユーザー属性、グループ ポリシー、接続プロファイルで不足している値を提供します。

外部 AAA サーバーを使用する際のガイドライン

ASA は、数値の ID ではなく属性名に基づいて LDAP 属性を適用します。RADIUS 属性は、名前ではなく数値 ID によって適用されます。

ASDM バージョン 7.0 の LDAP 属性には、cVPN3000 プレフィックスが含まれています。ASDM バージョン 7.1 以降では、このプレフィックスは削除されています。

LDAP 属性は、RADIUS の章に記載されている RADIUS 属性のサブセットです。

複数証明書認証の設定

セキュアクライアント SSL クライアントプロトコルと IKEv2 クライアントプロトコルを使用して、セッションごとに複数の認証を検証できるようになりました。たとえば、マシン証明書の発行元が特定の CA と一致することでデバイスが企業から支給されたデバイスであることを確認できます。

複数証明書オプションを使用すると、証明書を通じたマシンとユーザー両方の証明書認証が可能になります。このオプションがなければ、両方ではなく一方のみの証明書認証しか行うことができません。

（注） 複数の証明書認証にはマシン証明書とユーザー証明書（または2つのユーザー証明書）が必要であるため、この機能では セキュアクライアント Start Before Logon（SBL）を使用できません。

ユーザー名の事前入力フィールドでは、2 つ目の（ユーザー）証明書のフィールドを解析し、AAA および証明書認証済みの接続で以降の AAA 認証に使用することができます。プライマリとセカンダリの両方の事前入力のユーザー名は、常にクライアントから受信した2つ目の（ユーザー）証明書から取得されます。

9.14(1) 以降、ASA では、複数証明書認証を設定し、認証または許可にユーザー名の事前入力オプションを使用する場合に、プライマリユーザー名およびセカンダリユーザー名を取得する証明書を指定できます。詳細については、セキュアクライアント接続プロファイル、認証属性（126 ページ）を参照してください。

複数証明書認証では、2つの証明書が認証されます。クライアントから受信した2つ目の（ユーザー）証明書は、事前入力および証明書由来のユーザー名のプライマリおよびセカンダリ ユーザー名による解析対象です。

SAML による複数証明書認証も設定できます。

複数証明書認証では、その接続試行を認証するために使用された証明書のフィールドに基づいてポリシー決定を行うことができます。複数証明書認証中にクライアントから受信したユーザーおよびマシンの証明書は DAP にロードされ、証明書のフィールドに基づいてポリシーを設定することができます。接続試行を許可または拒否するルールを設定できるようにダイナミック アクセス ポリシー（DAP）を使用して複数証明書認証を追加するには、『ASA VPN ASDM Configuration Guide』の適切なリリースの「*Add Multiple Certificate Authentication to DAP*」を参照してください。

Active Directory/LDAP VPN リモート アクセス許可の例

この項では、Microsoft Active Directory サーバーを使用している ASA で認証および認可を設定するための手順の例を示します。説明する項目は次のとおりです。

- ユーザー ベースの属性のポリシー適用 （282 ページ）
- セキュアクライアント トンネルのスタティック IP アドレス割り当ての適用 （284 ページ）
- ダイヤルイン許可または拒否アクセスの適用 （286 ページ）
- ログオン時間と Time-of-Day ルールの適用 （289 ページ）

その他の設定例については、Cisco.com にある次のテクニカル ノートを参照してください。

- 『ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example』
- 『PIX/ASA 8.0: Use LDAP Authentication to Assign a Group Policy at Login』

ユーザー ベースの属性のポリシー適用

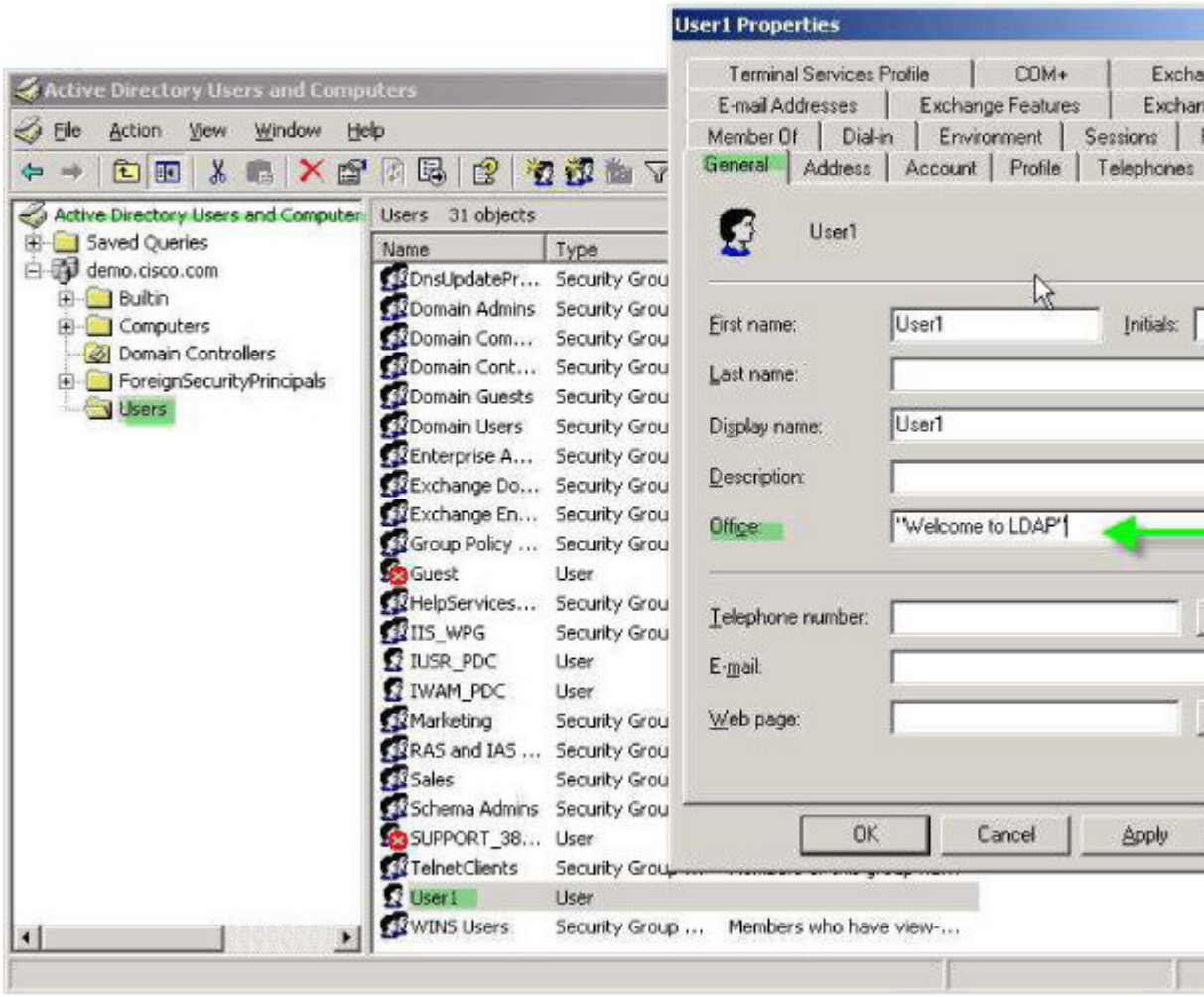
この例では、ユーザー向けの簡易バナーを表示して、標準の LDAP 属性を既知のベンダー固有属性（VSA）にマッピングする方法と 1 つ以上の LDAP 属性を 1 つ以上の Cisco LDAP 属性にマッピングする方法を示します。IPsec VPN クライアントやセキュアクライアントなど、どの接続タイプにも適用されます。

AD LDAP サーバー上で設定されたユーザーに簡易バナーを適用するには、[General] タブの [Office] フィールドを使用してバナー テキストを入力します。このフィールドでは、physicalDeliveryOfficeName という名前の属性を使用します。ASA で、physicalDeliveryOfficeName を Cisco 属性 Banner1 にマッピングする属性マップを作成します。

認証時、ASA はサーバーから physicalDeliveryOfficeName の値を取得し、その値を Cisco 属性 Banner1 にマッピングしてユーザーにバナーを表示します。

手順

ステップ 1 ユーザー名を右クリックして、[Properties] ダイアログボックスの [General] タブを開き、AD/LDAP 属性 physicalDeliveryOfficeName を使用する [Office] フィールドにバナー テキストを入力します。



ステップ 2 ASA で LDAP 属性マップを作成します。

Banner というマップを作成し、AD/LDAP 属性 physicalDeliveryOfficeName を Cisco 属性 Banner1 にマッピングします。

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

ステップ 3 LDAP 属性マップを AAA サーバーに関連付けます。

AAA サーバー グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバー ホスト コンフィギュレーション モードを開始し、以前作成した属性マップ Banner を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

ステップ 4 バナーの適用をテストします。

セキュアクライアント トンネルのスタティック IP アドレス割り当ての適用

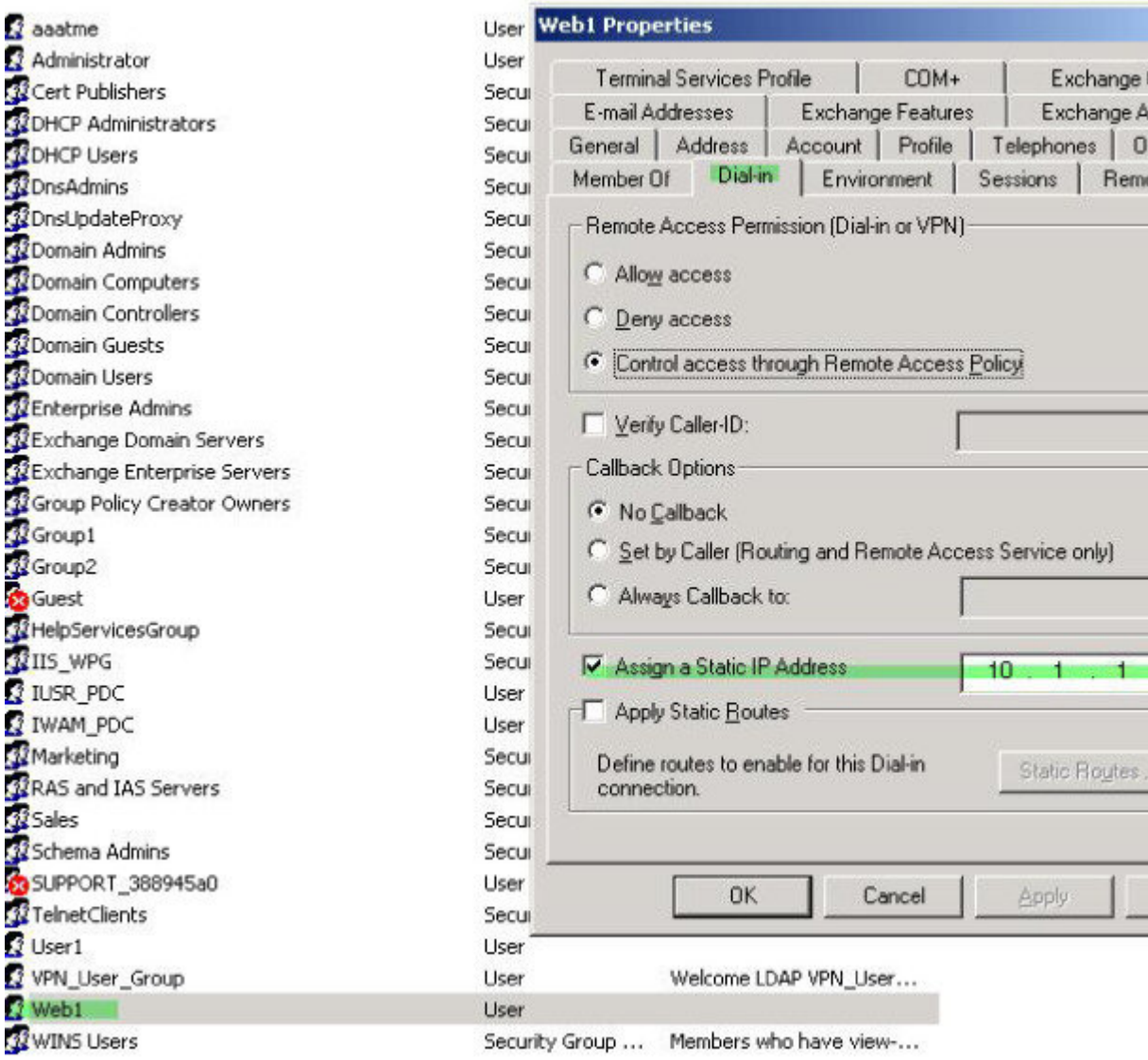
この例は、IPsec クライアントや SSL VPN クライアントなどのフルトンネル クライアントに適用されます。

スタティック セキュアクライアント スタティック IP 割り当てを適用するには、セキュアクライアントユーザー Web1 をスタティック IP アドレスを受信するように設定して、そのアドレスを AD LDAP サーバーの [ダイヤルイン（Dialin）] タブの [スタティックIPアドレスの割り当て（Assign Static IP Address）] フィールド（このフィールドで msRADIUSFramedIPAddress 属性が使用される）に入力し、この属性を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングする属性マップを作成します。

認証時に、ASA はサーバーから msRADIUSFramedIPAddress の値を取得し、その値を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングして、User1 にスタティック アドレスを渡します。

手順

ステップ 1 ユーザー名を右クリックして、[Properties] ダイアログボックスの [Dial-in] タブを開き、[Assign Static IP Address] チェックボックスをオンにして、10.1.1.2 という IP アドレスを入力します。



ステップ 2 図に示す LDAP コンフィギュレーションの属性マップを作成します。

[Static Address] フィールドで使用される AD 属性 msRADIUSFramedIPAddress を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングします。

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

ステップ 3 LDAP 属性マップを AAA サーバーに関連付けます。

AAA サーバー グループ MS_LDAP のホスト 10.1.1.2 に対して AAA サーバー ホスト コンフィギュレーション モードを開始し、作成した属性マップ static_address を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

ステップ 4 **vpn-address-assignment** コマンドが AAA を指定するように設定されているかどうかを確認するために、コンフィギュレーションのこの部分を表示します。

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa   << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

ステップ 5 ASA とセキュアクライアントとの接続を確立します。サーバーで設定され、ASA にマッピングされた IP アドレスをユーザーが受信することを確認します。

ステップ 6 **show vpn-sessiondb svc** コマンドを使用してセッションの詳細を表示し、割り当てられたアドレスを確認します。

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

ダイヤルイン許可または拒否アクセスの適用

この例では、ユーザーによって許可されるトンネリングプロトコルを指定する LDAP 属性マップを作成します。[Dialin] タブの許可アクセスと拒否アクセスの設定を Cisco 属性 Tunneling-Protocol にマッピングします。この属性は次のビットマップ値をサポートします。

値	トンネリング プロトコル
1	PPTP
2	L2TP
4	IPsec（IKEv1）
8	L2TP/IPsec
16	クライアントレス SSL

値	トンネリング プロトコル
32	SSL クライアント：セキュアクライアントまたはSSL VPN クライアント
64	IPsec（IKEv2）

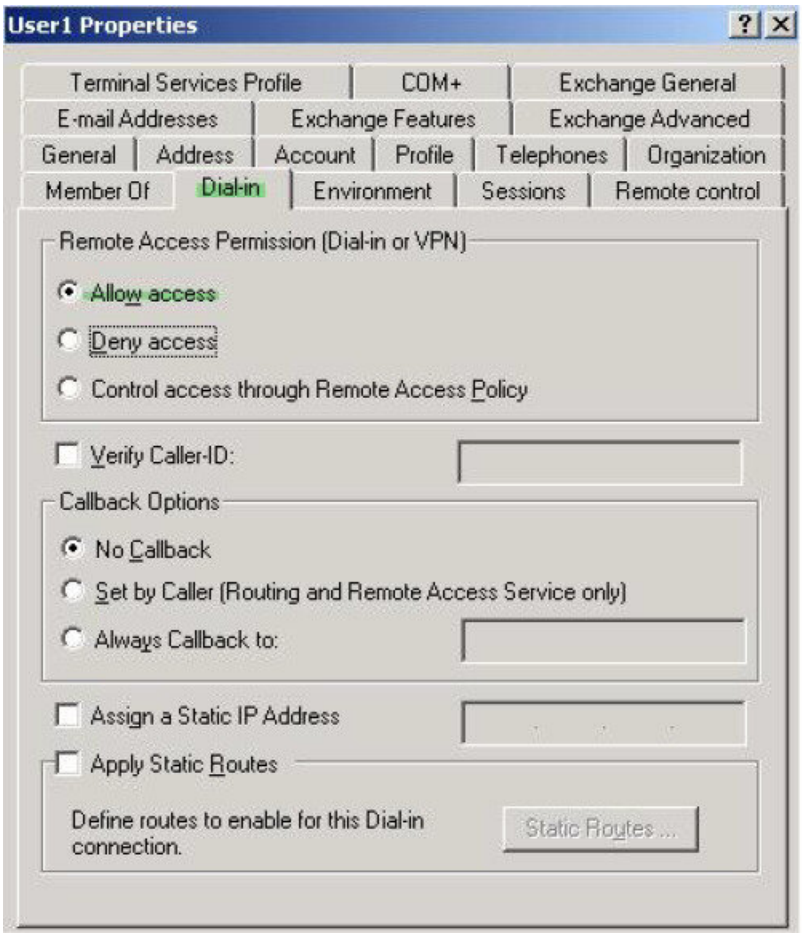
1 （1）IPsec と L2TP over IPsec は同時にはサポートされません。そのため、値 4 と 8 は相互排他値となります。
2 （2）注 1 を参照。

この属性を使用して、プロトコルの [Allow Access]（TRUE）または [Deny Access]（FALSE）の条件を作成し、ユーザーがアクセスを許可される方法を適用します。

ダイヤルイン許可アクセスまたは拒否アクセスの適用に関するその他の例については、テクニカル ノート『ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example』を参照してください。

手順

ステップ 1 ユーザー名を右クリックして、[Properties] ダイアログボックスの [Dial-in] タブを開き、[Allow Access] オプション ボタンをクリックします。



（注）
[Control access through the Remote Access Policy] オプションを選択した場合は、サーバーから値が返されず、適用される権限は ASA の内部グループ ポリシー設定に基づいて決定されます。

ステップ 2 IPsec と セキュアクライアント の両方の接続を許可する一方で、クライアントレス SSL 接続を拒否する属性マップを作成します。

a) マップ tunneling_protocols を作成します。

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) [Allow Access] 設定で使用される AD 属性 msNPAllowDialin を Cisco 属性 Tunneling-Protocols にマッピングします。

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) マップ値を追加します。

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

ステップ 3 LDAP 属性マップを AAA サーバーに関連付けます。

a) AAA サーバー グループ MS_LDAP でホスト 10.1.1.2 の AAA サーバー ホスト コンフィギュレーション モードを開始します。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) 作成した属性マップ tunneling_protocols を関連付けます。

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

ステップ 4 属性マップが設定したとおりに機能することを確認します。

クライアントレス SSL を使用して接続を試みます。ユーザーには、許可されていない接続メカニズムが接続の失敗の原因であることが通知されます。IPsec クライアントの接続は成功します。これは、属性マップに従って IPsec にトンネリング プロトコルが許可されるためです。

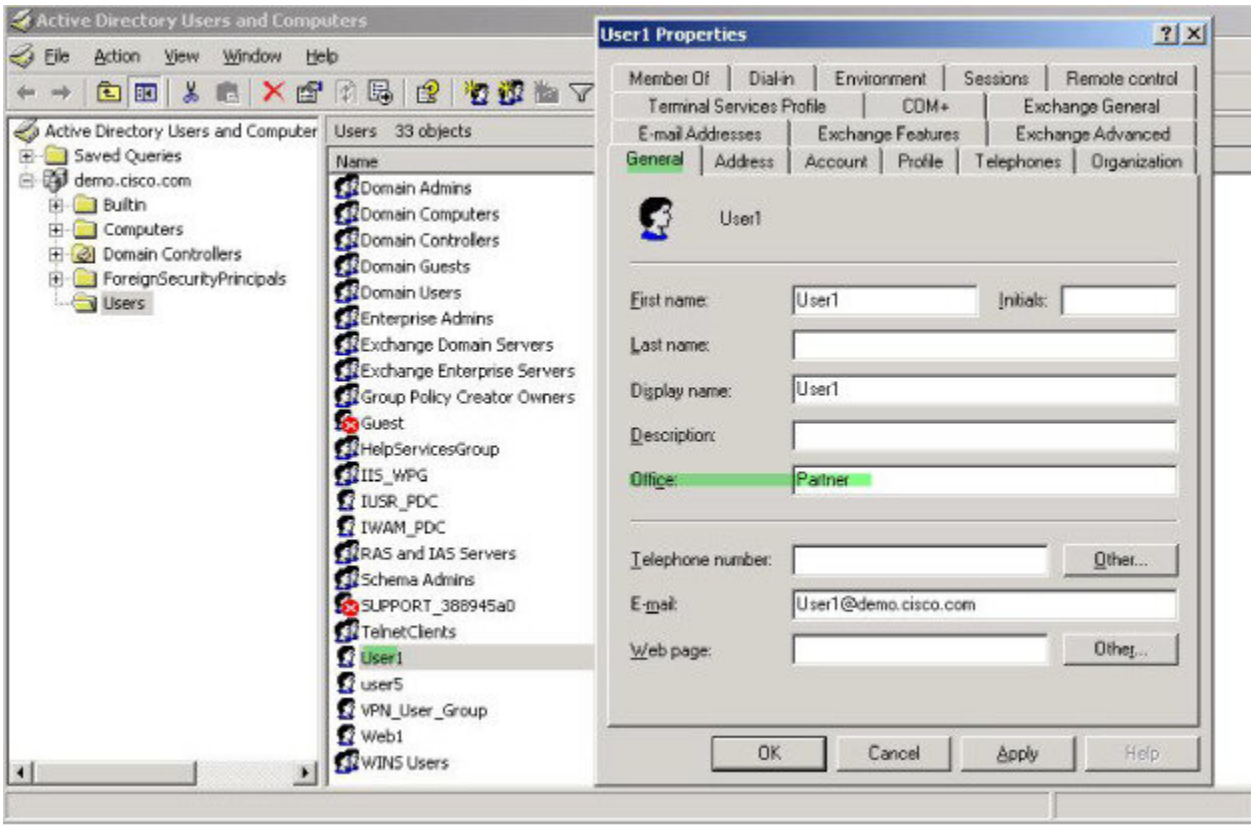
ログオン時間と Time-of-Day ルールの適用

次の例では、クライアントレス SSL ユーザー（たとえばビジネス パートナー）にネットワークへのアクセスを許可する時間帯を設定して適用する方法を示します。

AD サーバー上で、[Office] フィールドを使用してパートナーの名前を入力します。このフィールドでは、physicalDeliveryOfficeName 属性が使用されます。次に、ASA で属性マップを作成し、その属性を Cisco 属性 Access-Hours にマッピングします。認証時に、ASA は physicalDeliveryOfficeName の値を取得して Access-Hours にマッピングします。

手順

ステップ 1 ユーザーを選択して、[Properties] を右クリックし、[General] タブを開きます。



ステップ 2 属性マップを作成します。

属性マップ access_hours を作成し、[Office] フィールドで使用される AD 属性 physicalDeliveryOfficeName を Cisco 属性 Access-Hours にマッピングします。

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

ステップ 3 LDAP 属性マップを AAA サーバーに関連付けます。

AAA サーバー グループ MS_LDAP のホスト 10.1.1.2 に対して AAA サーバー ホスト コンフィギュレーション モードを開始し、作成した属性マップ access_hours を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

ステップ 4 各値にサーバーで許可された時間範囲を設定します。

パートナー アクセス時間を月曜日から金曜日の午前 9 時から午後 5 時に設定します。

```
hostname(config)# time-range Partner
```

```
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

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