



ASA 仮想 の設定

ASA 仮想 の導入では、ASDM アクセスを事前設定します。導入時に指定したクライアント IP アドレスから、Web ブラウザで ASA 仮想 管理 IP アドレスに接続できます。この章では、他のクライアントが ASDM にアクセスできるようにする方法と CLI アクセスを許可する方法（SSH または Telnet）についても説明します。この章で取り上げるその他の必須の設定作業には、ASDM でウィザードが提供するライセンスのインストールおよび一般的な設定作業が含まれます。

- [ASDM の起動（1 ページ）](#)
- [ASDM を使用した初期設定の実行（2 ページ）](#)
- [詳細設定（4 ページ）](#)

ASDM の起動

手順

ステップ 1 ASDM クライアントとして指定した PC で次の URL を入力します。

`https://asa_ip_address/admin`

次のボタンを持つ ASDM 起動ウィンドウが表示されます。

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

ステップ 2 ランチャをダウンロードするには、次の手順を実行します。

- a) [Install ASDM Launcher and Run ASDM] をクリックします。
- b) ユーザー名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証が設定されていない場合は、ユーザー名および **イネーブル** パスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。HTTPS 認証を有効にした場合、ユーザー名と関連付けられたパスワードを入力します。

- c) インストーラをPCに保存して、インストーラを起動します。インストールが完了すると、ASDM-IDM ランチャが自動的に開きます。
- d) 管理 IP アドレスを入力し、ユーザー名とパスワードを空白のままにし（新規インストールの場合）、[OK]をクリックします。HTTPS 認証を有効にした場合、ユーザー名と関連付けられたパスワードを入力します。

ステップ 3 Java Web Start を使用するには：

- a) [Run ASDM] または [Run Startup Wizard] をクリックします。
- b) プロンプトが表示されたら、ショートカットをコンピュータに保存します。オプションで、アプリケーションを保存せずに開くこともできます。
- c) ショートカットから Java Web Start を起動します。
- d) 表示されたダイアログボックスに従って、任意の証明書を受け入れます。Cisco ASDM-IDM Launcher が表示されます。
- e) ユーザー名とパスワードを空白のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証を有効にした場合、ユーザー名と関連付けられたパスワードを入力します。

ASDM を使用した初期設定の実行

次の ASDM ウィザードおよび手順を使用して初期設定を行うことができます。

- Startup Wizard の実行
- （任意）ASA 仮想 の内側にあるパブリックサーバーへのアクセス許可
- （オプション）VPN ウィザードの実行
- （オプション）ASDM の他のウィザードの実行

CLI の設定については、[Cisco Secure Firewall ASA シリーズ CLI コンフィギュレーション ガイド \[英語\]](#) を参照してください。

Startup Wizard の実行

セキュリティ ポリシーをカスタマイズして導入方法に最適化するには、[Startup Wizard] を実行します。

手順

ステップ 1 [Wizards] > [Startup Wizard] を選択します。

ステップ 2 セキュリティ ポリシーをカスタマイズして、導入方法に最適化します。次を設定できます。

- ホスト名

- ドメイン名
- 管理パスワード
- インターフェイス
- IP アドレス
- スタティック ルート
- DHCP サーバー
- ネットワーク アドレス変換規則
- その他の項目

(任意) ASA仮想の内側にあるパブリックサーバーへのアクセス許可

[設定 (Configuration)] > [ファイアウォール (Firewall)] > [パブリックサーバー (Public Servers)] ペインで、セキュリティポリシーが自動的に設定され、インターネットから内部サーバーにアクセスできるようになります。ビジネスオーナーとして、内部ネットワークサービス (Web サーバーや FTP サーバーなど) に外部ユーザーがアクセスできるようにする必要があります。これらのサービスは、ASA 仮想の背後にある、Demilitarized Zone (DMZ; 非武装地帯) と呼ばれる別のネットワーク上に配置できます。DMZ にパブリックサーバーを配置すると、パブリックサーバーに対する攻撃は内部ネットワークには影響しません。

(オプション) VPN ウィザードの実行

次のウィザード ([Wizards] > [VPN Wizards]) を使用して、VPN を設定できます。

- サイト間 VPN ウィザード : ASA 仮想 と別の VPN 対応デバイス間で IPsec サイト間トンネルを作成します。
- AnyConnect VPN ウィザード : Cisco AnyConnect VPN Client の SSL VPN リモートアクセスを設定します。セキュアクライアントでは ASA へのセキュアな SSL 接続が提供されるため、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。ASA ポリシーを設定すると、リモートユーザーが最初にブラウザを使用して接続するときに、セキュアクライアントをダウンロードできます。セキュアクライアント 3.0 以降を使用する場合、クライアントは、SSL または IPsec IKEv2 VPN プロトコルを実行できます。
- Clientless SSL VPN Wizard : ブラウザにクライアントレス SSL VPN リモートアクセスを設定します。クライアントレスブラウザベース SSL VPN によって、ユーザーは 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 VPN トンネルを確立できます。認証されると、ユーザーにはポータルページが表示され、サポートされる特定の内部リソースにアクセスできるようになります。ネットワーク管理者は、グループ単位でユーザーにリソースへのアクセス権限を付与します。ACL は、特定の企業リソースへのアクセスを制限したり、許可するために適用できます。

- IPsec (IKEv1 or IKEv2) Remote Access VPN Wizard : Cisco IPsec クライアント用の IPsec VPN リモート アクセスを設定します。

Azure への ASA 仮想 IPsec 仮想トンネルインターフェイス (VTI) 接続の構成方法については、『[Azure への ASA IPsec VTI 接続の構成](#)』を参照してください。

(オプション) ASDM の他のウィザードの実行

高可用性を備えたフェールオーバー、VPN クラスタ ロード バランシング、およびパケット キャプチャを設定するには、ASDM でその他のウィザードを実行します。

- High Availability and Scalability Wizard : フェールオーバーまたは VPN ロード バランシング を設定します。
- Packet Capture Wizard : パケット キャプチャを設定し、実行します。このウィザードは、入出力インターフェイスのそれぞれでパケット キャプチャを1回実行します。パケットをキャプチャすると、PC にパケット キャプチャを保存し、パケット アナライザでチェック およびリプレイできます。

詳細設定

ASA 仮想 の設定を続行するには、『[Navigating the Cisco Secure Firewall ASA Series Documentation](#)』を参照してください。

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。