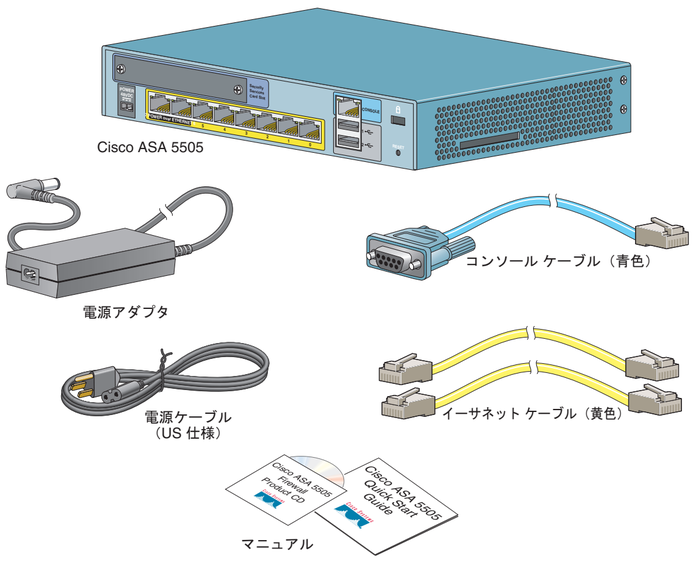
（注） このガイドの手順を実行するときは、『Regulatory Compliance and Safety Information (RCSI)』に記載されている安全上の警告を読み、適切な安全手順に従ってください。RCSI およびその他のマニュアルへのリンクについては、http://www.cisco.com/go/asadocs を参照してください。

1. パッケージ内容の確認



2. シャーシの取り付け

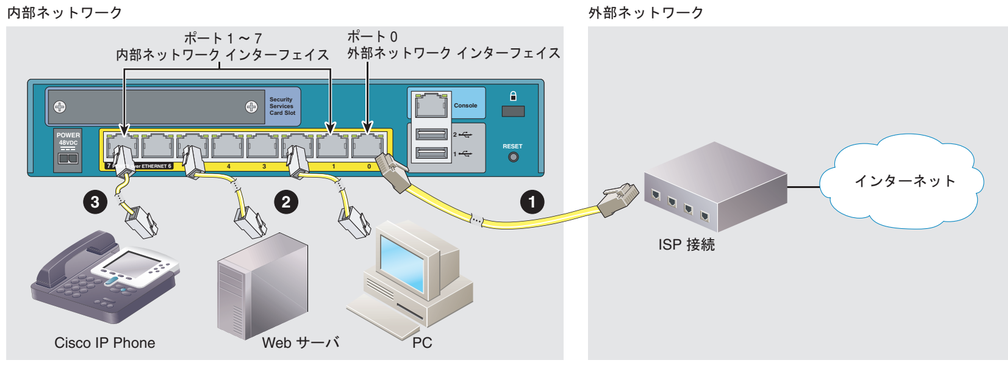
ASA は、デフォルト設定されて出荷されます。この設定には、2 つの事前設定されたネットワーク（内部ネットワークおよび外部ネットワーク）と、DHCP サーバの設定がされた内部インターフェイスが含まれます。内部ネットワークのクライアントは、相互通信できるように、またインターネット上のデバイスと通信できるように ASA からダイナミック IP アドレスを取得します。

ステップ 1 黄色いイーサネット ケーブルの片方の端子を ASA のイーサネット 0 に接続します（デフォルトでは、イーサネット 0 は外部インターフェイスです）。もう一方の端子をケーブル /DSL/ISDN モデム（外部ネットワーク）に接続します。

ステップ 2 イーサネット ケーブルを使用して、デバイス（PC、プリンタ、サーバなど）をイーサネット 1 ～ 7 に接続します。

（注） PC を ASA に接続し、Adaptive Security Device Manager（ASDM）を実行できるようにします。「4. 初期設定に関する考慮事項」を参照してください。

ステップ 3 イーサネット ケーブルを使用して、Power over Ethernet（PoE）デバイス（Cisco IP Phone やネットワーク カメラなど）をスイッチ ポート 6 または 7（PoE デバイスに電源を供給するポートのみ）に接続します。



サーバ（Web サーバなど）を ASA に接続すると、ASDM を使用して、内部および外部のユーザがそのサーバ上でのサービスにアクセス可能となるようにできます。「7.（任意）ASA の背後のパブリック サーバへのアクセスを許可する」を参照してください。

3. 電源投入とインターフェイス接続の確認

ステップ 1 電源アダプタを電源コードに接続します。

ステップ 2 電源アダプタの四角いコネクタを ASA の背面パネルの電源コネクタに接続します。

ステップ 3 電源ケーブルの AC 電源コネクタをコンセントに接続します（ASA には、電源スイッチがありません）。このステップを完了すると、デバイスに電源が入ります）。

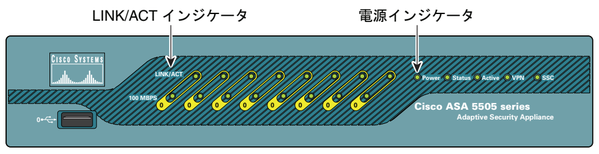
ステップ 4 ASA の前面にある電源 LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。

ステップ 5 管理 PC を確認し、DHCP を使用して 192.168.1.0/24 ネットワークの IP アドレスを受信したことを確認します。

ステップ 6 LINK/ACT インジケータを調べて、インターフェイス接続を確認します。

インターフェイス接続

各イーサネット インターフェイスには、物理リンクの確立状況を示す LED があります。LED が緑色に点灯している場合は、リンクが確立されています。LED が緑色に点滅している場合は、ネットワーク アクティビティが発生しています。



LINK/ACT LED が点灯も点滅もしていない場合は、デュプレックスの不一致が原因となってリンクがダウンしている可能性があります。オートネゴシエーションがディセーブルの場合、ストレート イーサネット ケーブルを使用していることを確認してください。

すべてのシャーシ コンポーネントの説明については、Cisco.com で提供されているハードウェア インストレーション ガイドを参照してください。

4. 初期設定に関する考慮事項

ASA は、デフォルト設定されて出荷されます。ほとんどの場合、このデフォルト設定は、基本構成に十分な内容になっています。ASDM を使用して ASA を設定します。ASDM は、Web ブラウザを使用してどこからでも ASA を管理できるグラフィカル インターフェイスです。

ただし、特定の設定を変更することをお勧めします（必要になることもあります）。たとえば、次の設定については、デフォルトを変更する必要があります。

- ASDM および CLI を使用して ASA を管理するために必要な特権モード（イネーブル）パスワード
- ASA を VPN エンドポイントとして使用する場合（SSL VPN 機能を使用）：
  - ホスト名、ドメイン名、DNS サーバ名
  - 外部インターフェイスの IP アドレスのスタティック アドレスへの変更
  - アイデンティティ証明書
  - WINS 名（Windows ファイル共有へのアクセスが必要な場合）

これらの変更を行うには、ASDM の Start up Wizard を使用します。「6.Startup Wizard の実行」を参照してください。

5.ASDM の起動

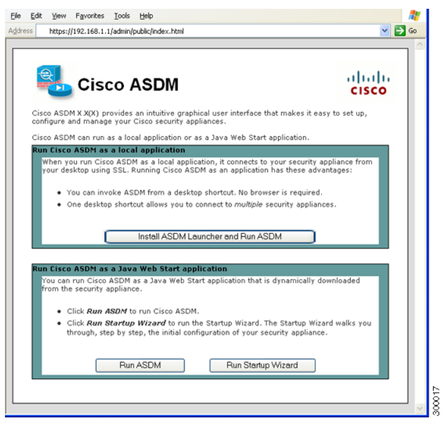
ASDM を実行するための要件については、Cisco.com の ASDM のリリース ノートを参照してください。

ステップ 1 ASA に接続されている PC で、Web ブラウザを起動します

ステップ 2 [Address] フィールドに次の URL を入力します。

https://192.168.1.1/admin

Cisco ASDM Web ページが表示されます。



ステップ 3 [Run Startup Wizard] をクリックします。

ステップ 4 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。

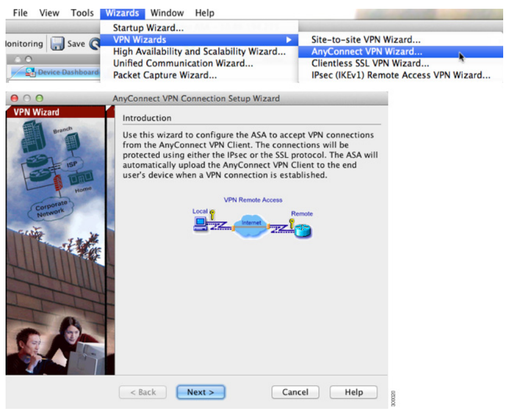
ステップ 5 ユーザ名とパスワードのフィールドは空のまま残し、[OK] をクリックします。

メインの ASDM ウィンドウが表示され、Startup Wizard が開きます。「6.Startup Wizard の実行」を参照してください。

6.Startup Wizard の実行

構成に応じてセキュリティ ポリシーをカスタマイズできるようにデフォルトの設定を変更するには、Startup Wizard を実行します。Startup Wizard を使用して、次の項目を設定できます。

- 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
- ネットワーク アドレス変換規則
- その他



ステップ 1 ウィザードがまだ動作していない場合は、メイン ASDM ウィンドウで [Wizards]> [Startup Wizard] を選択します。

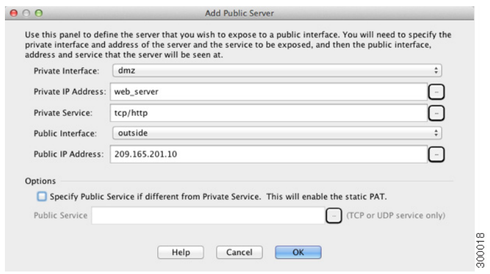
ステップ 2 Startup Wizard の指示に従い、ASA を設定します。

ステップ 3 ウィザードの実行中、デフォルト値をそのまま使用するか、必要に応じて変更することができます（ウィザードのフィールドの詳細については、[Help] をクリックしてください）。

7.（任意）ASA の背後のパブリック サーバへのアクセスを許可する

ASA 8.2 以降

[Public Servers] ペインでは、インターネットから内部のサーバにアクセスできるようにセキュリティ ポリシーを自動的に設定します。ビジネス オーナーとして、外部ユーザがアクセスできるようにすることが必要な内部ネットワーク サービス（Web サーバや FTP サーバなど）を備えることが考えられます。これらのサービスは、ASA の背後にある、非武装地帯（DMZ）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 サーバを配置すると、パブリック サーバに対する攻撃は内部ネットワークには影響しません。



ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Firewall] > [Public Servers] を選択します。[Public Servers] ペインが表示されます。

ステップ 2 [Add] をクリックし、[Add Public Server] ダイアログボックスにパブリック サーバの設定を入力します（フィールドの詳細については、[Help] をクリックしてください）。

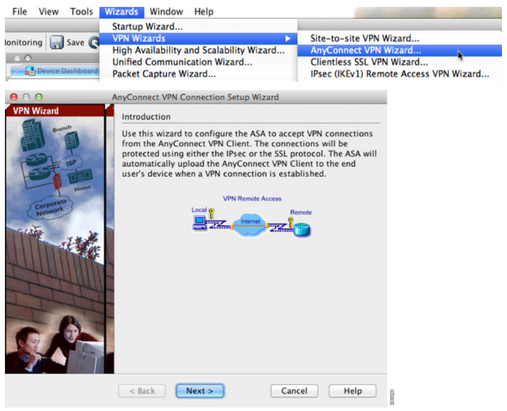
ステップ 3 [OK] をクリックします。リストにサーバが一覧表示されます。

ステップ 4 [Apply] をクリックし、ASA に設定を適用します。

8.（任意）VPN ウィザードの実行

次のウィザードを使用して VPN を設定できます。

- Site-to-Site VPN Wizard : 2 台の ASA 間で、IPsec サイト間トンネルを作成します。
- （ASA 8.0 以降）AnyConnect VPN Wizard : Cisco AnyConnect VPN クライアント用の SSL VPN リモート アクセスを設定します。AnyConnect は ASA へのセキュアな SSL 接続を提供し、これにより、リモート ユーザによる企業リソースへのフル VPN トンネリングが可能となります。ASA ポリシーは、リモート ユーザがブラウザを使用して最初に接続するときに、AnyConnect クライアントをダウンロードするように設定できます。AnyConnect 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。
- （ASA 8.0 以降）Clientless SSL VPN Wizard : ブラウザ用のクライアントレス 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、ユーザは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) 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。



ステップ 1 メイン ASDM ウィンドウで、[Wizards] > [VPN Wizards] を選択し、次のいずれかを選択します。

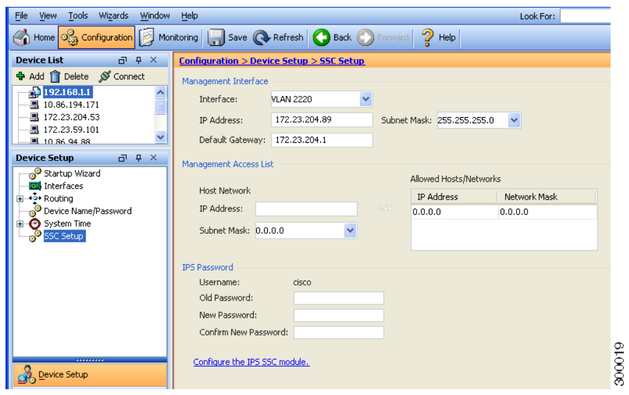
- **Site-to-Site VPN Wizard**
- **AnyConnect VPN Wizard**
- **Clientless VPN Wizard**
- **IPsec (IKEv1) Remote Access VPN Wizard**

ステップ 2 ウィザードの指示に従います（ウィザードのフィールドの詳細については、[Help] をクリックしてください）。

10.（任意）IPS モジュールの設定

ASA 8.2 以降

お使いの ASA にセキュリティ サービス カード（SSC）が備えられている場合は、ASDM を使用して SSC を設定し、SSC を実行するように侵入防御システム（IPS）アプリケーションを設定できます。SSC に外部インターフェイスはありません。



ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [SSC Setup] を選択します。[SSC] ペインが表示されます。

ステップ 2 SSC の設定フィールドに入力し、[Apply] をクリックします（フィールドの詳細については、ダイアログボックスの [Help] をクリックしてください）。

ステップ 3 SSC の IPS モジュールを設定するには、[Configure the IPS SSC module] リンクをクリックします。Startup Wizard が表示されます。[Launch Startup Wizard] をクリックします（または、[Configure] > [IPS] > [Sensor Setup] > [Startup Wizard] を選択してウィザードにアクセスすることもできます）。

IPS モジュールの設定の詳細については、Cisco.com で IPS モジュールのクイック スタート ガイドを参照してください。

お問い合わせは、購入された各代理店へご連絡ください。

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/

78-19752-02-J

クイック スタート ガイド

Cisco ASA 5505 適応型セキュリティ アプライアンス

【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。