CHAPTER 5

適応型セキュリティ アプライアンスの設定

この章では、適応型セキュリティ アプライアンスの初期設定について説明します。設定手順を実行するには、ブラウザベースの Cisco Adaptive Security Device Manager（ASDM）またはコマンドライン インターフェイス（CLI）のいずれかを使用します。この章の手順では、ASDM を使用して適応型セキュリティ アプライアンスを設定する方法を説明します。

この章には、次の項があります。

工場出荷時のデフォルト設定について

Cisco 適応型セキュリティ アプライアンスは、すぐに使用を開始できるように工場でデフォルト設定されて出荷されます。ASA 5505 は、次のように事前設定されています。

- 2 つの VLAN：VLAN 1 と VLAN2。
- VLAN 1 のプロパティは次のとおりです。
  - 名前：「inside」
  - 割り当てられているスイッチ ポート：Ethernet 0/1 から Ethernet 0/7
  - セキュリティ レベル 100
  - 割り当てられているスイッチ ポート：Ethernet 0/1 から 0/7
  - IP アドレス：192.168.1.1 255.255.255.0
- VLAN2 のプロパティは次のとおりです。
  - 名前：「outside」
  - 割り当てられているスイッチ ポート：Ethernet 0/0
  - セキュリティ レベル：0
  - DHCP を使用して IP アドレスを取得するように設定されている
- デバイスに接続し、ASDM　を使用して設定を入力するための内部インターフェイス。

デフォルトでは、適応型セキュリティ アプライアンスの内部インターフェイスには、デフォルト DHCP アドレス プールが組み込まれています。この設定により、内部ネットワークのクライアントは、適応型セキュリティ アプライアンスに接続するためにアプライアンスから DHCP アドレスを取得できます。このため、管理者は ASDM を使用して適応型セキュリティ アプライアンスを設定および管理できます。

CLI を使用した設定

適応型セキュリティ アプライアンスは、ASDM Web コンフィギュレーション ツールだけでなく、コマンドライン インターフェイスを使用しても設定できます。

vpnsetup ipsec-remote-access steps および **vpnsetup site-to-site steps** コマンドを使用すると、CLI 自体で、基本的なリモート アクセスと LAN ツー LAN 接続を設定する方法を示した、ステップごとの例を見ることができます。これらのコマンドの詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

適応型セキュリティ アプライアンスのすべての機能領域に関するステップごとの設定手順については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

Adaptive Security Device Manager を使用した設定

Adaptive Security Device Manager（ASDM）は、適応型セキュリティ アプライアンスを管理および監視できる、豊富な機能を持つグラフィカル インターフェイスです。Web ベースの設計によってセキュアなアクセスが実現されるため、Web ブラウザを使用して、どこからでも適応型セキュリティ アプライアンスに接続し、管理することができます。

設定と管理の機能がそろっているだけでなく、ASDM には適応型セキュリティ アプライアンスの導入を簡素化および促進するインテリジェント ウィザードが搭載されています。

この項は、次の内容で構成されています。

ASDM の使用準備

ASDM を使用できるようにするには、次の手順に従います。

ステップ 1　まだ行っていない場合は、イーサネット ケーブルを使用して、MGMT インターフェイスをスイッチまたはハブに接続します。同じスイッチに、適応型セキュリティ アプライアンス設定用の PC を接続します。

ステップ 2　DHCP を使用するように PC を設定します（適応型セキュリティ アプライアンスから自動的に IP アドレスを受信するため）。この設定により、PC が ASA 5505 およびインターネットと通信できるようになるだけでなく、ASDM を実行して設定および管理のタスクを行えます。

または、192.168.1.0 サブネットの中からアドレスを選択して、スタティック IP アドレスを使用中の PC に割り当てることもできます（有効なアドレスは 192.168.1.2 ～ 192.168.1.254、マスクは 255.255.255.0、デフォルトのルートは 192.168.1.1 です）。

他のデバイスを任意の内部ポートに接続する場合は、同じ IP アドレスが使用されていないことを確認します。

（注）　デフォルトでは、適応型セキュリティ アプライアンスの MGMT インターフェイスが 192.168.1.1 に割り当てられているため、このアドレスは使用できません。

ステップ 3　MGMT インターフェイスの LINK LED を確認します。

接続が確立されると、適応型セキュリティ アプライアンスの LINK LED インターフェイスと、スイッチまたはハブの対応する LINK LED が緑色に点灯します。

初期セットアップ用の設定情報の収集

次の情報を収集します。

- ネットワーク上の適応型セキュリティ　アプライアンスを識別する一意のホスト名。
- ドメイン名。
- 設定する外部インターフェイス、内部インターフェイス、およびその他のインターフェイスの IP アドレス。
- ASDM の HTTPS、SSH、または Telnet を使用して、このデバイスに管理アクセスできるホストの IP アドレス。
- 管理アクセス用の特権モードのパスワード。
- NAT または PAT アドレス変換に使用する IP アドレス（存在する場合）。
- DHCP サーバの IP アドレス範囲。
- WINS サーバの IP アドレス。
- 設定するスタティック ルート。
- DMZ を作成する場合、3 つ目の VLAN を作成して、その VLAN にポートを割り当てる必要があります（デフォルトでは、2 つの VLAN が設定されています）。
- インターフェイスの設定情報。つまり、同じセキュリティ レベルのインターフェイス間でトラフィックを許可するかどうか、同じインターフェイスのホスト間でトラフィックを許可するかどうか。
- Easy VPN ハードウェア クライアントを設定する場合は、プライマリおよびセカンダリの Easy VPN サーバの IP アドレス、クライアントをクライアント モードまたはネットワーク拡張モードで実行するかどうか、プライマリおよびセカンダリの Easy VPN サーバに設定されたユーザおよびグループ ログイン認定証に一致するそれぞれの認定証。

ASDM Launcher のインストール

ASDM は、ASDM Launcher ソフトウェアをダウンロードして ASDM を PC 上でローカルに実行する方法、または Web ブラウザで Java と JavaScript を有効にして PC から ASDM にリモート アクセスする方法のいずれかで起動できます。この手順は、ASDM をローカルで実行するようにシステムをセットアップする方法を示しています。

ASDM Launcher をインストールするには、次の手順に従います。

ステップ 1　スイッチまたはハブに接続された PC で、インターネット ブラウザを起動します。

a. ブラウザのアドレス フィールドに、**https://192.168.1.1/** という URL を入力します。

（注） 適応型セキュリティ アプライアンスは、192.168.1.1 のデフォルト IP アドレスが設定されて出荷されます。「**https**」の「**s**」を付け忘れると、接続は失敗します。HTTP over SSL（HTTPS）を使用すると、ブラウザと適応型セキュリティ アプライアンスとの間の安全な接続が可能になります。

Cisco ASDM のスプラッシュ画面が表示されます。

b. **Install ASDM Launcher and Run ASDM** をクリックします。

c. ユーザ名とパスワードの入力を求めるダイアログボックスでは、どちらのフィールドも空のままにします。**OK** をクリックします。

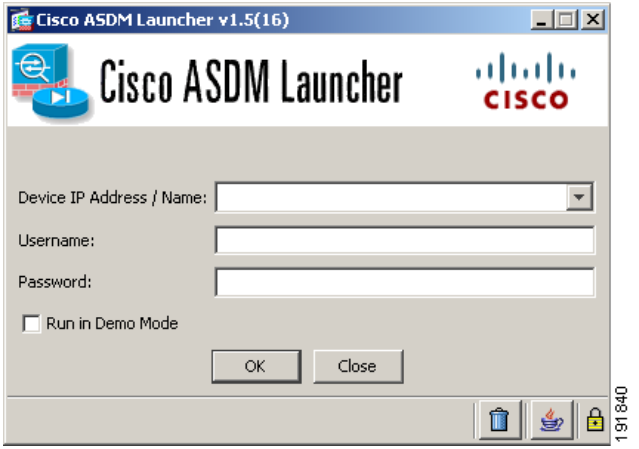
d. **Yes** をクリックして、証明書を受け入れます。後続の認証および証明書に関するすべてのダイアログボックスで、**Yes** をクリックします。

e. File Download ダイアログボックスが表示されたら、**Open** をクリックして、インストール プログラムを直接実行します。インストール ソフトウェアをハード ドライブに保存する必要はありません。

f. InstallShield Wizard が表示されたら、手順に従って ASDM Launcher ソフトウェアをインストールします。

ステップ 2　デスクトップから、Cisco ASDM Launcher ソフトウェアを起動します。

ダイアログボックスが表示されます。



ステップ 3　適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力します。

ステップ 4　Username と Password のフィールドは空白のままにしておきます。

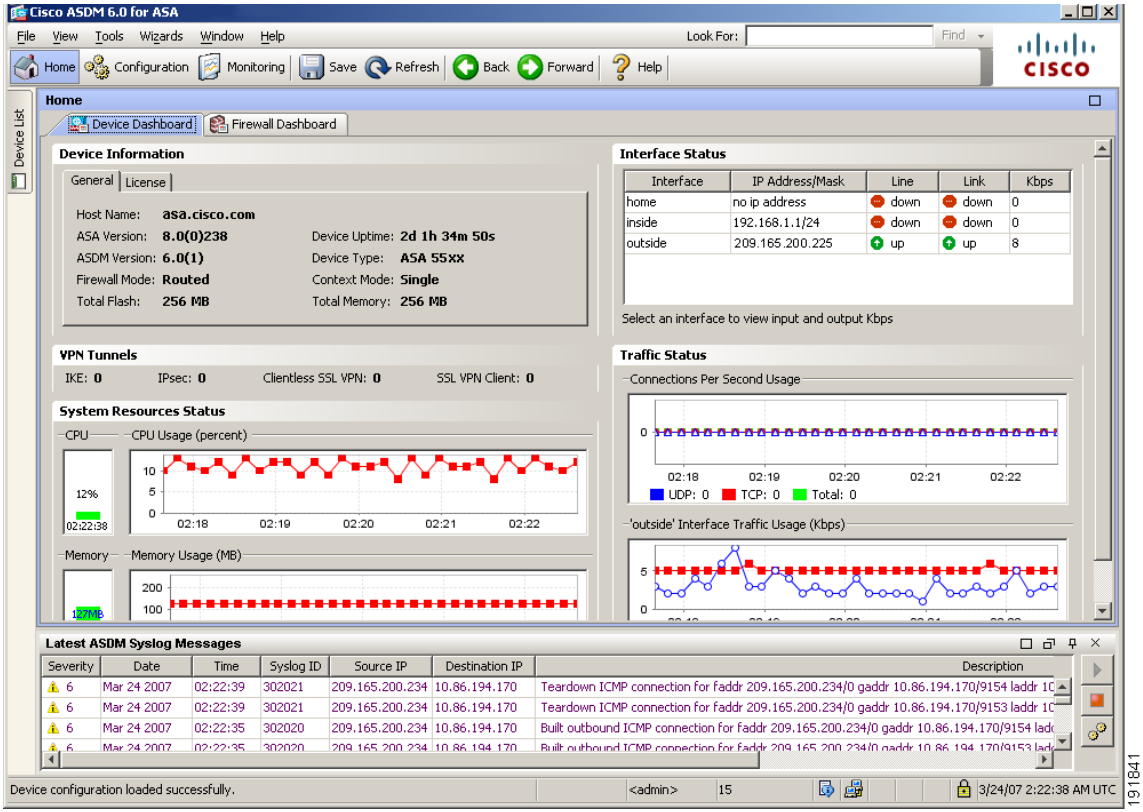
（注）　デフォルトでは、Cisco ASDM Launcher に Username と Password は設定されていません。

ステップ 5　OK をクリックします。

ステップ 6　証明書の受け入れ要求を含むセキュリティ警告が表示された場合は、**Yes** をクリックします。

ASA が、アップデートされたソフトウェアがあるかどうか確認し、ある場合は自動的にダウンロードします。

メイン ASDM ウィンドウが表示されます。



ASDM が起動され、メイン ウィンドウが表示されます。

Web ブラウザを使用した ASDM の起動

Web ブラウザで ASDM を実行するには、アドレス フィールドに工場出荷時のデフォルト IP アドレス **https://192.168.1.1/admin/** を入力します。

（注） 「**https**」の「**s**」を付け忘れると、接続は失敗します。HTTP over SSL（HTTPS）を使用すると、ブラウザと適応型セキュリティ アプライアンスとの間の安全な接続が可能になります。

メイン ASDM ウィンドウが表示されます。

ASDM Startup Wizard の実行

ASDM には、適応型セキュリティ アプライアンスの初期設定を簡素化する Startup Wizard が用意されています。Startup Wizard を使用すると、わずかな手順で、内部ネットワークと外部ネットワーク間でパケットが安全に流れるように適応型セキュリティ アプライアンスを設定できます。

Startup Wizard を使用して適応型セキュリティ アプライアンスの基本設定をセットアップするには、次の手順に従います。

ステップ 1　ASDM ウィンドウ上部の Wizards メニューから、Startup Wizard を選択します。

ステップ 2　Startup Wizard の手順に従って適応型セキュリティ アプライアンスを設定します。

Startup Wizard のフィールドの詳細を確認するには、ウィンドウ下部にある **Help** ボタンをクリックします。

（注）　DES ライセンスまたは 3DES/AES ライセンスを要求するエラーが表示された場合は、付録 A「3DES/AES ライセンスの取得」を参照してください。

（注）　また、ネットワークのセキュリティ ポリシーに基づいて、外部インターフェイス、または必要なその他すべてのインターフェイスを経由する ICMP トラフィックをすべて拒否するように適応型セキュリティ アプライアンスを設定することを検討する必要もあります。このアクセス コントロール ポリシーは、ASDM を使用して設定できます。ASDM メイン ページで、**Configuration > Properties > ICMP Rules** をクリックします。外部インターフェイス用のエントリを追加します。IP アドレスを 0.0.0.0 に、ネットマスクを 0.0.0.0 に、Action を拒否にそれぞれ設定します。

次の作業

次の 1 つ以上の章を使用して、それぞれの構成に応じた適応型セキュリティ アプライアンスを設定します。

実行内容	参照先
DMZ Web サーバ を保護するための適応型セキュリティ アプライアンスの設定	第 6 章「シナリオ：DMZ 設定」
リモートアクセス VPN 用の適応型セキュリティ アプライアンスの設定	第 7 章「シナリオ：IPsec リモートアクセス VPN 設定」
ソフトウェア クライアントを使用した SSL VPN 接続用の適応型セキュリティ アプライアンスの設定	第 8 章「シナリオ：Cisco AnyConnect VPN クライアント用の接続の設定」
Web ブラウザを使用した SSL VPN 接続用の適応型セキュリティ アプライアンスの設定	第 9 章「シナリオ：SSL VPN クライアントレス接続」
サイトツーサイト VPN 用の適応型セキュリティ アプライアンスの設定	第 10 章「シナリオ：サイトツーサイト VPN 設定」
Easy VPN リモート デバイスとしての適応型セキュリティ アプライアンスの設定	第 11 章「シナリオ：Easy VPN ハードウェア クライアント設定」