CHAPTER 7

# 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。設定の手順は、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）で実行できます。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について説明します。

この章は、次の項で構成されています。

# 工場出荷時のデフォルト設定について

シスコの適応型セキュリティ アプライアンスは、すぐにスタートアップできるように、工場出荷時のデフォルト設定が設定されて出荷されます。ASA 5500 シリーズ は、次のように事前設定されています。

- 2 つの VLAN：VLAN 1 および VLAN2
- VLAN 1 には次のプロパティがある
  - 名前は「inside」
  - イーサネット 0/1 ～ イーサネット 0/7 のスイッチ ポートが割り当てられている
  - セキュリティ レベルは 100
  - イーサネット 0/1 ～ 0/7 のスイッチ ポートが割り当てられている
  - IP アドレスは 192.168.1.1 255.255.255.0
- VLAN2 には次のプロパティがある
  - 名前は「outside」
  - スイッチ ポート イーサネット 0/0 が割り当てられている
  - セキュリティ レベルは 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
- デバイスに接続するための内部インターフェイスで、ASDM を使用して設定を完了する。

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は、デフォルトの DHCP アドレス プールで設定されます。この設定によって、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 アプライアンスから DHCP アドレスを取得し、装置に接続できます。この後、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

ASDM Web 設定ツールのほかに、コマンドライン インターフェイスでも適応型セキュリティ アプライアンスを設定できます。

**vpnsetup ipsec-remote-access steps** コマンドおよび **vpnsetup site-to-site steps** コマンドを使用して、基本的なリモートアクセスおよび LAN-to-LAN 接続を CLI で設定する方法を示す段階的な例を参照できます。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のステップバイステップ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、機能が豊富なグラフィカル インターフェイスです。Web ベースの設計によって、Web ブラウザを使用して任意の場所から適応型セキュリティ アプライアンスに接続し、管理できるように、セキュアなアクセスが提供されます。


完全な設定機能および管理機能のほかに、ASDM には、適応型セキュリティ アプライアンスの配置を簡素化し、高速化するインテリジェント ウィザードが含まれています。

この項では、次のトピックについて取り上げます。



## ASDM を使用するための準備

ASDM を使用する前に、次の手順を実行します。

**ステップ 1**　まだ実行していない場合は、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 アプライアンスの設定に使用する 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 IP アドレスを自動的に受信するため）。この操作を行うと、PC が適応型セキュリティ アプライアンスやインターネットと通信でき、ASDM で設定および管理タスクを実行できます。

または、192.168.1.0 サブネットでアドレスを選択して、PC に固定 IP アドレスを割り当てることができます（有効なアドレスは 192.168.1.2 ～ 192.168.1.254 で、マスクが 255.255.255.0、デフォルト ルートが 192.168.1.1 です）。

他のデバイスを内部ポートのいずれかに接続する場合、デバイスの IP アドレスが同じでないことを確認します。

**（注）**　デフォルトで、適応型セキュリティ アプライアンスの MGMT インターフェイスに 192.168.1.1 が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。

## 初期セットアップのための情報収集

ASDM Startup Wizard で使用する、次の情報を収集します。

- ネットワークで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
- 外部インターフェイス、内部インターフェイス、および設定するその他のすべてのインターフェイスの IP アドレス
- ASDM 用の HTTPS、SSH、または Telnet を使用してこのデバイスへの管理者アクセス権を持っている必要があるホストの IP アドレス
- 管理者アクセス権用の特権モード パスワード
- NAT または PAT のアドレス変換に使用する IP アドレス
- 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 を作成する場合は、3 つの VLAN を作成し、この VLAN にポートを割り当てる（デフォルトでは、2 つの VLAN が設定されています）
- インターフェイス設定情報：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が許可されているかどうか、また同じインターフェイス上のホスト間でトラフィックが許可されているかどうか
- 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 Easy VPN サーバの IP アドレス、Easy VPN ハードウェア クライアントをクライアント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 Easy VPN サーバ上の設定と一致させるためのユーザおよびグループ ログイン認定証

## ASDM Launcher のインストール

ASDM は、次の 2 つ方法のどちらかを使用して起動できます。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と、Web ブラウザで Java と JavaScript を有効にして PC からリモートで ASDM にアクセスする方法です。ここでは、ASDM をローカルに実行するようにシステムを設定する方法について説明します。

ASDM Launcher をインストールするには、次の手順を実行します。

**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、URL「**https://192.168.1.1/**」を入力します。

**（注）** 適応型セキュリティ アプライアンスの出荷時のデフォルト IP アドレスは 192.168.1.1 です。「**s**」を追加して「**https**」にすることに注意してください。追加しないと、接続が失敗します。HTTPS（HTTP over SSL）は、ブラウザと適応型セキュリティ アプライアンスとの間でセキュアな接続を提供します。

Cisco ASDM 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を要求するダイアログボックスで、両方のフィールドを空のままにします。**OK** をクリックします。

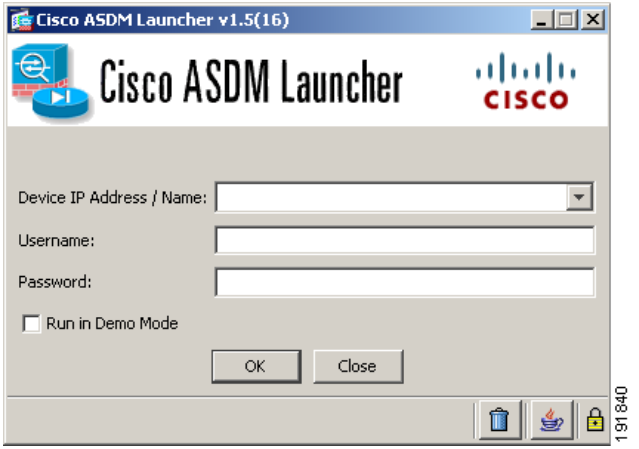
**d.** **Yes** をクリックして、証明書を受け付けます。すべてのユーザ認証および証明書ダイアログボックスで、**Yes** をクリックします。

**e.** File Download ダイアログボックスが開いたら、**Open** をクリックし、直接 ASDM Launcher をインストールします。このインストール プログラムをハードディスクに保存する必要はありません。

**f.** InstallShield Wizard が表示されたら、指示に従って 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 および Password フィールドはブランクのままにします。

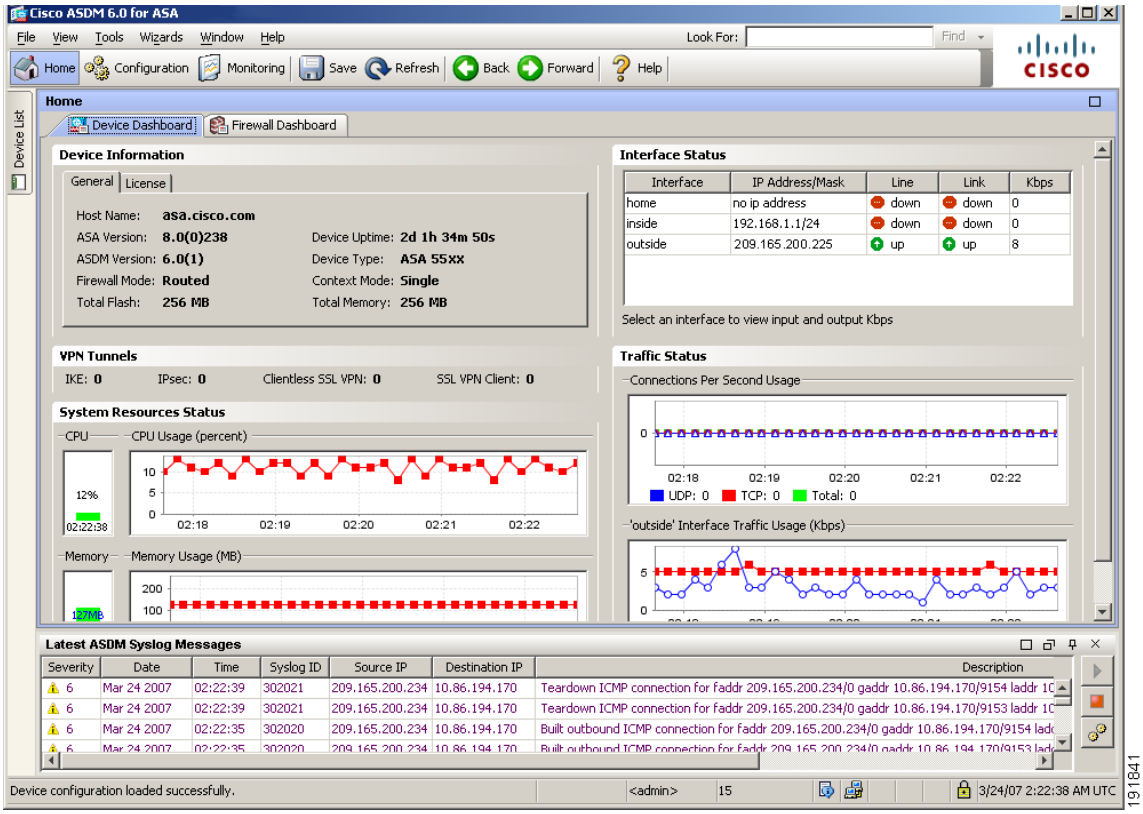
**（注）**　デフォルトで、Cisco ASDM Launcher には Username および Password は設定されていません。

**ステップ 5**　OK をクリックします。

**ステップ 6**　証明書を受け入れるよう要求するセキュリティ警告が表示されたら、**Yes**　をクリックします。

ASA は更新するソフトウェアがあるかどうかを確認し、ある場合は自動的にダウンロードします。

ASDM のメイン ウィンドウが表示されます。




ASDM が起動し、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

ASDM を Web ブラウザで実行するには、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）** 「**s**」を追加して「**https**」にすることに注意してください。追加しないと、接続が失敗します。HTTP over SSL（HTTP）は、ブラウザと適応型セキュリティ アプライアンスとの間でセキュアな接続を提供します。

ASDM のメイン 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 が含まれています。Startup Wizard を使用すると、内部ネットワークと外部ネットワークの間でパケットがセキュアに流れるように、わずかな手順で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、次の手順を実行します。

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

**ステップ 2**　Startup Wizard の指示に従い、適応型セキュリティ アプライアンスをセットアップします。

Startup Wizard のフィールドの詳細については、ウィンドウの下部の **Help** をクリックしてください。

**（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、付録 A「3DES/AES ライセンスの取得」で詳細を確認してください。

**（注）** ネットワーク セキュリティ ポリシーに基づき、外部インターフェイスまたは必要なその他の任意のインターフェイスを経由するすべての ICMP トラフィックを拒否するように、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があります。このようなアクセス コントロール ポリシーは、ASDM を使用して設定できます。ASDM のメイン 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 deny にそれぞれ設定します。

# 次の手順

次の章のいずれか、または複数を使用して、配置用に適応型セキュリティ アプライアンスを設定します。

| 作業内容 | 参照先 |
|---|---|
| DMZ Web サーバ保護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 : DMZ の設定」 |
| 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 9 章「シナリオ : IPSec リモートアクセス VPN の設定」 |
| 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 10 章「シナリオ : Cisco AnyConnect VPN Client 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 11 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 12 章「シナリオ : サイトツーサイト VPN の設定」 |