CHAPTER 4

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を示します。

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

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 5580 適応型セキュリティ アプライアンスの工場出荷時のデフォルト設定は、次のとおりです。

- 管理インターフェイスの管理 0/0。**configure factory-default** コマンドで IP アドレスを設定しなかった場合、IP アドレスとマスクは 192.168.1.1 と 255.255.255.0 になります。
- DHCP サーバは適応型セキュリティ アプライアンスでイネーブルになっているため、インターフェイスに接続している PC は 192.168.1.2 ～ 192.168.1.254 のアドレスを受信します。
- HTTP サーバは ASDM に対してイネーブルになっており、192.168.1.0 ネットワーク上でユーザにアクセスできます。

この設定は、次のコマンドで構成されています。

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

CLI による設定

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。

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詳細な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 による設定

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。

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（P.4-4）
- 初期セットアップ用の設定情報の収集（P.4-5）
- ASDM Launcher のインストール（P.4-5）
- Web ブラウザでの ASDM の起動（P.4-8）

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　イーサネット ケーブルを使用して管理 0/0 インターフェイスをスイッチまたはハブに接続します（まだ接続していない場合）。適応型セキュリティ アプライアンスを設定するには、このスイッチに 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 アドレスを受信できます）。この設定により、PC は適応型セキュリティ アプライアンスおよびインターネットとの通信が可能になり、設定や管理の作業のために ASDM を実行できます。

あるいは、192.168.1.0 サブネット内のアドレスを選択して、固定 IP アドレスを PC に割り当てます（有効なアドレスは、255.255.255.0 のマスクと 192.168.1.1 のデフォルト ルートを持つ 192.168.1.2 ～ 192.168.1.254 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は、同一の IP アドレスを設定しないようにしてください。

（注）　適応型セキュリティ アプライアンスの管理 0/0 インターフェイスは、デフォルトで 192.168.1.1 に割り当てられます。したがって、このアドレスは使用できません。

ステップ 3　管理 0/0 インターフェイスの LINK LED を確認します。

接続が確立されている場合は、適応型セキュリティ アプライアンスの LINK LED インターフェイスおよび対応するスイッチまたはハブの 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

ASDM Startup Wizard で使用される、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、およびその他のすべてのこれから設定する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 を作成する場合は、3 つ目の VLAN を作成し、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）。
- インターフェイス設定情報（同一セキュリティ　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るかどうか、および同一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 アドレスが必要です。また、クライアントを実行するモード（クライアント モードまたはネットワーク拡張モード）、プライマリおよびセカンダリ Easy VPN サーバに設定されたユーザとグループのログイン クレデンシャルも必要です。

ASDM Launcher のインストール

ASDM を起動するには、2 つの方法があります。ASDM Launcher ソフトウェアをダウンロードして、PC 上で ASDM をローカルで実行する方法、および Web ブラウザで Java と JavaScript をイネーブルにして 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 をローカルで実行するようにシステムをセットアップ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、次の URL を入力します。
https://192.168.1.1/admin

（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 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入れます。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、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 フィールドと Password フィールドを空のままにします。

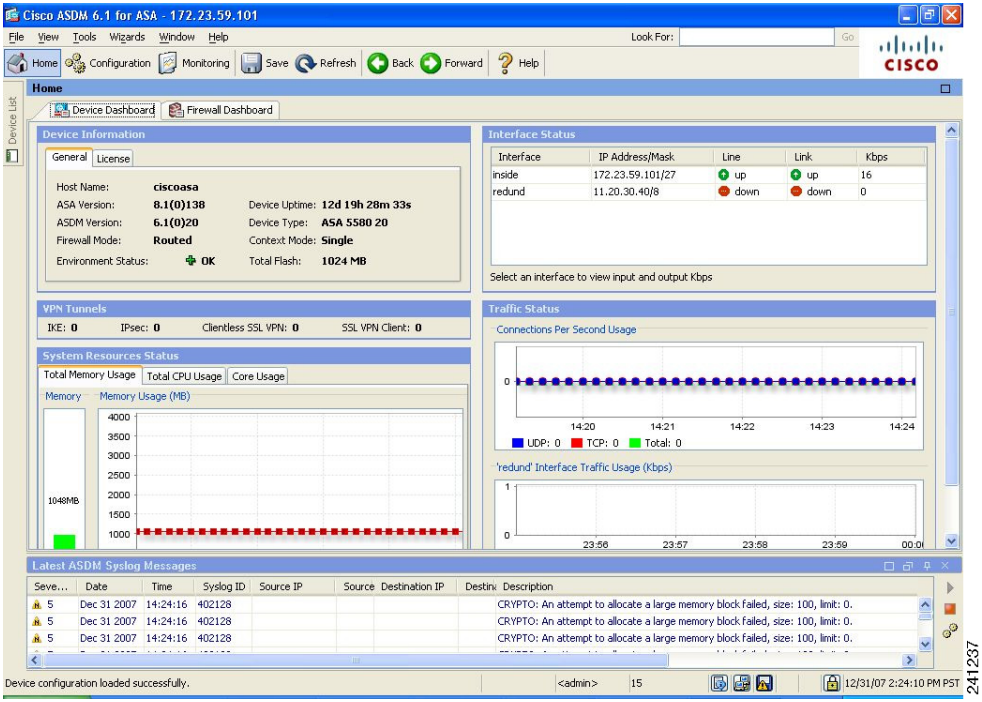
（注）　デフォルトでは、Cisco ASDM Launcher に Username と Password は設定されていません。

ステップ 5　OK をクリックします。

ステップ 6　証明書の受け入れを求める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。

適応型セキュリティ アプライアンスは最新ソフトウェアが存在するかどうかを調べ、存在す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。



Web ブラウザでの 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の 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。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。

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 ウィンドウの上部にあるウィザードのメニューから、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、ウィンドウの下部にある **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は、付録 A「3DES/AES ライセンスの取得」を参照してください。

（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 のメインページから、**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

次に示す 1 つ以上の章を参照し、適応型セキュリティ アプライアンスを設定して配置します。

作業内容	参照先
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 5 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 6 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 7 章「シナリオ:サイトツーサイト VPN 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 8 章「シナリオ：IPsec リモート アクセス VPN の設定」