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。ただし、この章の手順では、ASDM を使用する方法を示します。

（注） ASDM を使用するには、DES ライセンスまたは 3DES-AES ライセンスが必要です。詳細については、付録 A「DES ライセンスまたは 3DES-AES ライセンスの取得」を参照してください。

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。この工場出荷時のデフォルト設定により、インターフェイスが自動的に設定されるため、デバイスに即時接続して、ASDM で設定を完了することができます。

デフォルトでは、適応型セキュリティ アプライアンスの管理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。

Adaptive Security Device Manager について

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。

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。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』および『*Cisco Security Appliance Command Reference*』を参照してください。

Startup Wizard の使用

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。

（注） スロット 0 のポートは内部インターフェイス用、スロット 1 のポートは外部インターフェイス用として使用する必要があります。

この項では、Startup Wizard を使用した基本的な設定パラメータの設定方法について説明します。次のトピックについて取り上げます。

Startup Wizard を起動する前に

Startup Wizard を起動する前に、次の手順を実行します。

ステップ 1　DES ライセンスまたは 3DES-AES ライセンスを取得します。

ASDM を実行するには、DES ライセンスまたは 3DES-AES ライセンスが必要です。適応型セキュリティ アプライアンスの購入時にこれらのライセンスを購入していない場合は、取得方法とアクティブ化の方法について、付録 A「DES ライセンスまたは 3DES-AES ライセンスの取得」を参照してください。

ステップ 2　Web ブラウザで Java と Javascript をイネーブルにします。

ステップ 3　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
- 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

- NAT または PAT の設定に使用する IP アドレス
- DHCP サーバの IP アドレス範囲

Startup Wizard の実行

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　管理ポートに接続していない場合は、接続します。

a. 両端に RJ-45 コネクタの付いたイーサネット ケーブルを見つけます。

b. RJ-45 コネクタ 1 個を管理 0/0 ポートに接続します。

c. イーサネット　ケーブルのもう一方の端を、コンピュータまたは管理ネットワークのイーサネット ポートに接続します。

d. 管理ネットワークに接続している場合は、適応型セキュリティ　アプライアンスを設定するための PC を管理ネットワークに接続します。

ステップ 2　Startup Wizard を起動します。

a. スイッチ、ハブ、または管理ネットワークに接続された PC で、インターネット ブラウザを起動します。

b. 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。

c. ASDM ソフトウェアの実行方法を選択するウィンドウで、ASDM ランチャをダウンロードする方法と ASDM ソフトウェアを Java アプレットとして実行する方法のいずれかを選択します。

ステップ 3　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。**Enter** キーを押します。

ステップ 4　**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。

ASDM が起動します。

ステップ 5　Wizards メニューから、Startup Wizard を選択します。

ステップ 6　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）　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、**icmp** コマンドで設定できます。**icmp** 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。

ファイバ インターフェイスのメディア タイプ設定

スロット 1 でファイバ接続を使用する場合、メディア タイプ設定をデフォルト設定からファイバ コネクタに変更する必要があります。

（注） デフォルトのメディア タイプ設定は銅線イーサネット ポートなので、使用する銅線イーサネット ポートのメディア タイプ設定は、あらためて設定する必要はありません。

ASDM を使用してファイバ インターフェイスのメディア タイプを設定するには、ASDM のメイン ウィンドウから次の手順を実行します。

ステップ 1　ASDM ウィンドウで、**Configuration** をクリックします。

ステップ 2　Features ペインで、**Interfaces** をクリックします。

ステップ 3　**4GE SSM** インターフェイスをクリックし、**Edit** をクリックします。Edit Interface ダイアログボックスが表示されます。

ステップ 4　**Configure Hardware Properties** をクリックします。Hardware Properties ダイアログボックスが表示されます。

ステップ 5　Media Type ドロップダウン リストで、**Fiber Connector** を選択します。

ステップ 6　**OK** をクリックして Edit Interfaces ダイアログボックスに戻り、**OK** をクリックしてインターフェイス設定ダイアログボックスに戻ります。

ステップ 7　各ファイバ インターフェイスに対して、この手順を繰り返します。

コマンドラインからメディア タイプを設定することもできます。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の「Configuring Ethernet Settings and Subinterfaces」を参照してください。

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 6 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 7 章「シナリオ：リモートアクセス VPN の設定」
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 8 章「シナリオ：サイトツーサイト VPN の設定」