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、P.A-1 の「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。

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。この設定は、ほとんどの小規模および中規模のビジネス ネットワーキング環境に適合します。

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。

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。

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 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。また、Web ブラウザで Java および JavaScript をイネーブルにする必要があります。

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 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（GigabitEthernet0/1）と外部ネットワーク（GigabitEthernet0/0）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　次の手順のいずれかを実行していない場合、実行します。

- ASA 5520 または 5540 の場合、イーサネット ケーブルで内部 GigabitEthernet0/1 インターフェイスをスイッチまたはハブに接続する。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 を接続する。
- ASA 5510 の場合、イーサネット ケーブルで内部 Ethernet 1 インターフェイスをスイッチまたはハブに接続する。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 を接続する。

ステップ 2　DHCP を使用するように（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ように）、PC を設定します。または、192.168.1.0 ネットワークの外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 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)。

（注）　デフォルトで、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 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　次の手順のいずれかを実行します。

- ASA 5520 または 5540 の場合、GigabitEthernet0/1 インターフェイスの LINK LED を確認する。
- ASA 5510 の場合、Ethernet 1 インターフェイスの LINK LED を確認する。

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。

ステップ 4　Startup Wizard を起動します。

a.　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。

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。

ステップ 5　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 6　**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 7　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 8　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。

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」
侵入防御用の AIP SSM の設定	第 9 章「AIP SSM の設定」
コンテント セキュリティ用の CSC SSM の設定	第 10 章「CSC SSM の設定」

次の手順