CHAPTER 4

スタートアップ ウィザードの使用

ASDM Startup Wizard の案内に従って適応型セキュリティ アプライアンスの初期設定を行い、適応型セキュリティ アプライアンスの以下の設定を定義できます。

- ホスト名
- ドメイン名
- ASDM または CLI からの管理アクセスを制限するためのパスワード
- 外部インターフェイスの IP アドレス情報
- 内部インターフェイスや DMZ インターフェイスなどのその他のインターフェイス
- NAT または PAT ルール
- DHCP サーバで使用する場合の内部インターフェイスの DHCP 設定

メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、次のいずれかの方法を選択します。

- **Wizards > Startup Wizard** を選択する。
- **Configuration > Device Setup > Startup Wizard** を選択して、**Launch Startup Wizard** をクリックする。

詳細情報

- P.3-11 の「Web ブラウザによる ASDM の起動」を参照してください。
- 『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

ここでは、次の項目について説明します。

- ASA 5500 シリーズと PIX 500 シリーズ セキュリティ アプライアンスの Startup Wizard 画面（P. 4-2）
- ASA 5505 適応型セキュリティ アプライアンスの Startup Wizard 画面（P. 4-3）

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ASA 5500 シリーズと PIX 500 シリーズ セキュリティ アプライアンスの Startup Wizard 画面

表 4-1 に、ASA 5500 シリーズ適応型セキュリティ アプライアンスおよび PIX シリーズ セキュリティ アプライアンスのみを設定する場合に必要な Startup Wizard の画面を一覧表示します。画面の実際の順序は、設定時の選択によって決まります。示される順序は、ASA 5505 適応型セキュリティ アプライアンスにのみ適用されます。「使用できるモード」列には、各画面が表示されるときのモードおよび追加の設定情報が一覧表示されます。選択した画面の情報を表示するには、名前をクリックしてください。

表 4-1　ASA 5500 シリーズと PIX 500 シリーズ セキュリティ アプライアンスの Startup Wizard 画面

画面名	使用できるモード
Step 1 - Starting Point or Welcome（P. 4-3）	すべてのモード。Step 1 の工場出荷時のデフォルト オプションは PIX セキュリティ アプライアンスでは使用できません。
Step 2 - Basic Configuration（P. 4-4）	
Step 3 - Auto Update Server（P. 4-5）	シングル ルーテッドおよびシングル透過モード。シングル透過モードでイネーブルにすると、Interface Configuration 画面と Step 13 - DHCP Server 画面は表示されません。
Step 4 - Management IP Address Configuration（P. 4-6）	シングル透過モードのみ。
Outside Interface Configuration（P. 4-22）	シングル ルーテッド モードのみ。
Outside Interface Configuration - PPPoE（P. 4-21）	
Interface Configuration（P. 4-21）	シングル透過モードのみ。
Other Interfaces Configuration（P. 4-19）	すべてのモード。
Step 12 - Static Routes（P. 4-13）	
Step 13 - DHCP Server（P. 4-13）	
Step 14 - Address Translation (NAT/PAT)（P. 4-14）	シングル ルーテッド モードのみ。
Step 15 - Administrative Access（P. 4-16）	すべてのモード。
Step 17 - Startup Wizard Summary（P. 4-19）	

ASA 5505 適応型セキュリティ アプライアンスの Startup Wizard 画面

表4-2 に、ASA 5505 適応型セキュリティ アプライアンスのみを設定する場合に必要な Startup Wizard の画面のすべてを一覧表示します。一覧での画面の順序は、シングル ルーテッド モードでの設定を表します。「使用できるモード」列には、各画面が表示されるときのモードおよび追加の設定情報が一覧表示されます。選択した画面の情報を表示するには、名前をクリックしてください。

表 4-2　ASA 5505 適応型セキュリティ アプライアンスの Setup Wizard 画面

画面名および順序	使用できるモード
Step 1 - Starting Point or Welcome（P. 4-3）	すべてのモード。Step 2 の Teleworker オプションは ASA-5505 でのみ選択できます。
Step 2 - Basic Configuration（P. 4-4）	
Step 3 - Auto Update Server（P. 4-5）	シングル ルーテッドおよびシングル透過モード。Teleworker を使用する設定の場合にのみイネーブルにされます。
Step 4 - Management IP Address Configuration（P. 4-6）	シングル透過モードのみ。
Step 5 - Interface Selection（P. 4-6）	シングル ルーテッド モードのみ。
Step 6 - Switch Port Allocation（P. 4-7）	
Step 7 - Interface IP Address Configuration（P. 4-8）	
Step 8 - Internet Interface Configuration - PPPoE（P. 4-9）	
Step 9 - Business Interface Configuration - PPPoE（P. 4-10）	
Step 10 - Home Interface Configuration - PPPoE（P. 4-11）	
Step 11 - General Interface Configuration（P. 4-12）	
Step 12 - Static Routes（P. 4-13）	すべてのモード。Teleworker を使用する設定の場合にのみイネーブルにされます。
Step 13 - DHCP Server（P. 4-13）	すべてのモード。
Step 14 - Address Translation (NAT/PAT)（P. 4-14）	シングル ルーテッド モードのみ。
Step 15 - Administrative Access（P. 4-16）	すべてのモード。
Step 16 - Easy VPN Remote Configuration（P. 4-17）	シングル ルーテッド モード。Teleworker を使用する場合にのみイネーブルにされます。
Step 17 - Startup Wizard Summary（P. 4-19）	すべてのモード。

Step 1 - Starting Point or Welcome

ASDM アプリケーション ウィンドウからこの機能にアクセスする（マルチモードの場合を除く）には、**File > Reset Device to the Factory Default Configuration** を選択します。

フィールド

- Modify existing configuration：既存の設定を変更するには、このオプションを選択します。
- Reset configuration to factory defaults：設定を内部インターフェイスの工場出荷時デフォルト値に戻すには、このオプションを選択します。
- Configure the IP address of the management interface：管理インターフェイスの IP アドレスとサブネット マスクを設定するには、このチェックボックスをオンにします。
- IP Address：管理インターフェイスの IP アドレスを指定します。
- Subnet Mask：ドロップダウン リストから管理インターフェイスのサブネット マスクを選択します。

（注）　設定を工場出荷時のデフォルト値にリセットすると、**Cancel** をクリックしたり、この画面を閉じたりしても、変更を元に戻せません。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Step 2 - Basic Configuration

メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、次のいずれかの方法を選択します。

- **Configuration > Properties > Device Administration > Device**
- **Configuration > Properties > Device Administration > Password**

フィールド

- Configure the device for Teleworker usage：リモート ワーカーを対象とした一群の設定値を指定するには、このチェックボックスをオンにします。詳細については、P.4-17 の「Step 16 - Easy VPN Remote Configuration」を参照してください。
- Host Name：適応型セキュリティ アプライアンスのホスト名を指定します。ホスト名は、大文字と小文字を含む最大 63 文字の英数字で指定できます。使用するセキュリティ アプライアンスに応じて、デバイス タイプが「ASA」または「PIX」と表示されます。
- Domain Name：適応型セキュリティ アプライアンスの IPSec ドメイン名を指定します。このドメイン名は証明書で使用できます。ドメイン名は、特殊文字やスペースを含まない、最大 63 文字の英数字で指定できます。
- Privileged Mode (Enable) Password section：ASDM または CLI からの適応型セキュリティ アプライアンスへの管理アクセスを制限できます。

（注）　パスワード フィールドを空白にすると、非常に大きなセキュリティ リスクであることを警告する Password Confirmation ダイアログボックスが表示されます。

  - Change privileged mode (enable) password：現在の特権モード（イネーブル）パスワードを変更するには、このチェックボックスをオンにします。
  - Old Password：変更前のイネーブル パスワードがある場合は、そのパスワードを指定します。
  - New Password：新しいイネーブル パスワードを指定します。パスワードは最大 32 文字の英数字で、大文字と小文字を区別します。

— Confirm New Password：新しいイネーブル パスワードを再入力します。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Step 3 - Auto Update Server

この画面により、適応型セキュリティ アプライアンスを Auto Update サーバからリモートで管理できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、**Configuration > Interfaces** を選択します。

フィールド

- Enable Auto Update：セキュリティ アプライアンスと Auto Update サーバ間の通信をイネーブルにするには、このチェックボックスをオンにします。
- Server URL：ドロップダウン リストから、HTTPS または HTTP を選択して、Auto Update サーバの URL の先頭を定義します。
- Verify Server SSL certificate : Auto Update サーバで SSL 認証がイネーブルになっていることを確認するには、このチェックボックスをオンにします。
- Username：Auto Update サーバにログインするユーザ名を指定します。
- Password：Auto Update サーバにログインするためのパスワードを指定します。
- Confirm Password：確認のためパスワードを再入力します。
- Device ID Type：ドロップダウン リストをクリックし、適応型セキュリティ アプライアンスを一意に識別する ID タイプを選択します。**User-defined name** を選択し、一意の ID を指定するための Device ID フィールドをイネーブルにします。
- Device ID:適応型セキュリティ アプライアンス ID として使用する一意の文字列を指定します。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Step 4 - Management IP Address Configuration

この画面では、このコンテキストでのホストの管理 IP アドレスを設定できます。ASDM アプリケーション ウィンドウからこの機能にアクセスするには、**Configuration > Properties > Management IP** を選択します。

フィールド

- Management IP Address : ASDM またはセッション プロトコルを使用し、管理目的でこのコンテキストにアクセスできるホストの IP アドレスを指定します。
- Subnet Mask：管理 IP アドレスのサブネット マスクを指定します。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	—	—	—

Step 5 - Interface Selection

この画面では、ASA 5505 の 8 つのファースト イーサネット スイッチ ポートを 3 つの VLAN にグループ化できます。これらの VLAN は、別のレイヤ 3 ネットワークとして機能します。グループ化後、外部（Internet）、内部（Business）、または DMZ（Home）で構成されるインターフェイスごとに、ネットワークを定義する VLAN を 1 つずつ選択または作成できます。DMZ は、ニュートラル ゾーンにある別のネットワークで、プライベート（内部）ネットワークとパブリック（外部）ネットワークの間にあります。

フィールド

Outside VLAN または Internet VLAN セクション

- Choose a VLAN：ドロップダウン リストから事前定義済みの外部 VLAN を番号で選択します。
- Create a VLAN：新しい外部 VLAN を作成するには、このチェックボックスをオンにします。
- Enable VLAN：外部 VLAN をイネーブルにするには、このチェックボックスをオンにします。

Inside VLAN または Business VLAN セクション

- Choose a VLAN：ドロップダウン リストから事前定義済みの内部 VLAN を番号で選択します。
- Create a VLAN：新しい内部 VLAN を作成するには、このチェックボックスをオンにします。
- Enable VLAN：内部 VLAN をイネーブルにするには、このチェックボックスをオンにします。

DMZ VLAN または Home VLAN (Optional) セクション

- Choose a VLAN：ドロップダウン リストから事前定義済み VLAN を番号で選択します。
- Create a VLAN：新しい VLAN を作成するには、このチェックボックスをオンにします。
- Do not configure：この VLAN の設定をディセーブルにするには、このチェックボックスをオンにします。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 6 - Switch Port Allocation

この画面では、外部（Internet）、内部（Business）、または DMZ（Home）インターフェイスにスイッチ ポートを割り当てることができます。DMZ インターフェイスは透過モードでは使用できません。関連付けられた VLAN にポートを追加する必要があります。デフォルトでは、スイッチ ポートはすべて VLAN1 で始まります。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、**Configuration > Interfaces** を選択します。

フィールド

Switch Ports for Outside VLAN (vlan*id*) または Switch Ports for Internet VLAN (vlan*id*) セクション

- Available Ports：使用できるポートのリストから、追加または削除するポートを選択します。
- Allocated Ports：割り当てられたポートのリストから、追加または削除するポートを選択します。
- Add：使用できるポートのリスト、または割り当てられたポートのリストにポートを追加します。
- Remove：使用できるポートのリスト、または割り当てられたポートのリストからポートを削除します。

Switch Ports for Inside VLAN (vlan*id*) または Switch Ports for Business VLAN (vlan*id)* セクション

- Available Ports：使用できるポートのリストから、追加または削除するポートを選択します。
- Allocated Ports：割り当てられたポートのリストから、追加または削除するポートを選択します。
- Add：使用できるポートのリスト、または割り当てられたポートのリストにポートを追加します。
- Remove：使用できるポートのリスト、または割り当てられたポートのリストからポートを削除します。

Switch Ports for DMZ VLAN (vlan*id*) または Switch Ports for Home VLAN (vlan*id*) セクション

- Available Ports：使用できるポートのリストから、追加または削除するポートを選択します。
- Allocated Ports：割り当てられたポートのリストから、追加または削除するポートを選択します。
- Add：使用できるポートのリスト、または割り当てられたポートのリストにポートを追加します。
- Remove：使用できるポートのリスト、または割り当てられたポートのリストからポートを削除します。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 7 - Interface IP Address Configuration

この画面では、PPPoE サーバまたは DHCP サーバから IP アドレスを取得するか、または IP アドレスとサブネット マスクを指定することによって、インターフェイスを設定できます。

フィールド

Outside IP Address または Internet IP Address セクション

- Use the following IP address：外部 IP アドレスを指定するには、このオプションを選択します。
- IP Address/ Mask：特定の IP アドレスを入力し、ドロップダウン リストからサブネット マスクを選択します。
- Use DHCP：DHCP サーバから外部 IP アドレスを取得するには、このオプションを選択します。
- Obtain default rote using DHCP：DHCP サーバから外部 IP アドレスのデフォルト ルートを取得するには、このチェックボックスをオンにします。
- Use PPPoE：PPPoE サーバから外部 IP アドレスを取得するには、このオプションを選択します。

Inside IP Address または Business IP Address セッション

- Use the following IP address：内部 IP アドレスを指定するには、このオプションを選択します。
- IP Address/ Mask：特定の内部 IP アドレスを入力し、ドロップダウン リストからサブネット マスクを選択します。
- Use DHCP：DHCP サーバから内部 IP アドレスを取得するには、このオプションを選択します。
- Use PPPoE：PPPoE サーバから内部 IP アドレスを取得するには、このオプションを選択します。

DMZ IP Address または Home IP Address セクション

- Use the following IP address：DMZ IP アドレスを指定するには、このオプションを選択します。
- IP Address/ Mask：特定の DMZ IP アドレスを入力し、ドロップダウン リストからサブネットマスクを選択します。
- Use DHCP：DHCP サーバから DMZ IP アドレスを入手するには、このオプションを選択します。
- Use PPPoE：PPPoE サーバから DMZ IP アドレスを取得するには、このオプションを選択します。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 8 - Internet Interface Configuration - PPPoE

この画面では、PPPoE サーバから IP アドレスを取得することによって、指定された外部インターフェイスを設定できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、**Configuration > Interfaces** を選択します。

（注） ASA 5505 以外のすべての ASA 5500 シリーズ モデルの場合、フル ライセンスの適応型セキュリティ アプライアンスは、最大で 3 つの外部インターフェイスを含む 5 つのインターフェイスをサポートします。制限モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 3 つ、透過モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 2 つサポートします。最大数のインターフェイスを作成した後、または最大数のインターフェイスに名前を付けた後は、VLAN を新規作成することはできなくなり、既存の VLAN を選択することが必要になります。

フィールド

- Group Name：PPPoE サーバにあるグループの名前を指定します。次に進むには、グループ名を指定する必要があります。

User Authentication セクション

- PPPoE Username：PPPoE サーバでのユーザ名を指定します。
- PPPoE Password：PPPoE サーバでのパスワードを指定します。
- Confirm PPPoE Password：最初に入力した PPPoE パスワードを指定します。

Authentication Method セクション

- PAP：PAP 認証を使用します。
- CHAP：CHAP 認証を使用します。
- MSCHAP：MSCHAP 認証を使用します。

IP Address セクション

- Obtain an IP address using PPPoE：PPPoE サーバからインターフェイスの IP アドレスを取得するには、このオプションを選択します。このフィールドは透過モードの場合には表示されません。
- Specify an IP Address：インターネット インターフェイスの IP アドレスを指定します。このフィールドは透過モードの場合には表示されません。
  - IP Address：インターネット インターフェイスで使用する IP アドレスを指定します。
  - Subnet Mask：ドロップダウン リストからインターネット インターフェイスのサブネット マスクを選択します。
- Obtain default route using PPPoE：PPPoE サーバを使用してデフォルトのルーティングを設定するには、このチェックボックスをオンにします。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 9 - Business Interface Configuration - PPPoE

この画面では、PPPoE サーバから IP アドレスを取得することによって内部インターフェイスを設定できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、**Configuration > Interfaces** を選択します。

（注） ASA 5505 以外のすべての ASA 5500 シリーズ モデルの場合、フル ライセンスの適応型セキュリティ アプライアンスは、最大で 3 つの外部インターフェイスを含む 5 つのインターフェイスをサポートします。制限モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 3 つ、透過モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 2 つサポートします。最大数のインターフェイスを作成した後、または最大数のインターフェイスに名前を付けた後は、VLAN を新規作成することはできなくなり、既存の VLAN を選択することが必要になります。

フィールド

- Group Name：PPPoE サーバにあるグループの名前を指定します。次に進むには、グループ名を指定する必要があります。

User Authentication セクション

- PPPoE Username：PPPoE サーバでのユーザ名を指定します。
- PPPoE Password：PPPoE サーバでのパスワードを指定します。
- Confirm PPPoE Password：最初に入力した PPPoE パスワードを指定します。

Authentication Method セクション

- PAP：PAP 認証を使用します。
- CHAP：CHAP 認証を使用します。
- MSCHAP：MSCHAP 認証を使用します。

IP Address セクション

- Obtain an IP address using PPPoE：PPPoE サーバからインターフェイスの IP アドレスを取得するには、このオプションを選択します。このフィールドは透過モードの場合には表示されません。
- Specify an IP Address：内部インターフェイスの IP アドレスを指定します。このフィールドは透過モードの場合には表示されません。
  - IP Address：内部インターフェイスで使用する IP アドレスを指定します。

— Subnet Mask：ドロップダウン リストからインターネット インターフェイスのサブネット マスクを選択します。

- Obtain default route using PPPoE：PPPoE サーバを使用してデフォルトのルーティングを設定するには、このチェックボックスをオンにします。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 10 - Home Interface Configuration - PPPoE

この画面では、PPPoE サーバから IP アドレスを取得することによって DMZ インターフェイスを設定できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、**Configuration > Interfaces** を選択します。

（注） ASA 5505 以外のすべての ASA 5500 シリーズ モデルの場合、フル ライセンスの適応型セキュリティ アプライアンスは、最大で 3 つの外部インターフェイスを含む 5 つのインターフェイスをサポートします。制限モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 3 つ、透過モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 2 つサポートします。最大数のインターフェイスを作成した後、または最大数のインターフェイスに名前を付けた後は、VLAN を新規作成することはできなくなり、既存の VLAN を選択することが必要になります。

フィールド

- Group Name：PPPoE サーバにあるグループの名前を指定します。次に進むには、グループ名を指定する必要があります。

User Authentication セクション

- PPPoE Username：PPPoE サーバでのユーザ名を指定します。
- PPPoE Password：PPPoE サーバでのパスワードを指定します。
- Confirm PPPoE Password：最初に入力した PPPoE パスワードを指定します。

Authentication Method セクション

- PAP：PAP 認証を使用します。
- CHAP：CHAP 認証を使用します。
- MSCHAP：MSCHAP 認証を使用します。

IP Address セクション

- Obtain an IP address using PPPoE：PPPoE サーバからインターフェイスの IP アドレスを取得するには、このオプションを選択します。このフィールドは透過モードの場合には表示されません。

- Specify an IP Address：DMZ インターフェイスの IP アドレスを指定します。このフィールドは透過モードの場合には表示されません。
  - IP Address：DMZ インターフェイスで使用する IP アドレスを指定します。
  - Subnet Mask：ドロップダウン リストからインターネット インターフェイスのサブネット マスクを選択します。
- Obtain default route using PPPoE：PPPoE サーバを使用してデフォルトのルーティングを設定するには、このチェックボックスをオンにします。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 11 - General Interface Configuration

この画面では、インターフェイス間のトラフィック、および同じインターフェイスに接続されたホスト間のトラフィックを、イネーブルにしたり制限したりできます。

トラフィック制限は、オプションの設定ではありません。制限付きのライセンスしか持っていない場合は、1 つのインターフェイスから他のすべてのインターフェイスへのトラフィックを制限する必要があります。フル ライセンスまたはデバイスが透過モードの場合、Restrict Traffic エリアのフィールドは表示されません。

フィールド

- Enable traffic between two or more interfaces with the same security level：同じセキュリティ レベルにある複数のインターフェイス間のトラフィックをイネーブルにするには、このチェックボックスをオンにします。
- Enable traffic between two or more hosts connected to the same interface：同じインターフェイスに接続された複数のホスト間のトラフィックをイネーブルにするには、このチェックボックスをオンにします。

Restrict traffic エリア

- From interface：ドロップダウン リストからインターフェイスを選択することによって、そのインターフェイスからのトラフィックを制限できます。
- To interface：ドロップダウン メニューからインターフェイスを選択することによって、そのインターフェイスへのトラフィックを制限できます。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 12 - Static Routes

この画面では、任意のインターフェイスのルータに接続されたネットワークにアクセスするスタティック ルートを、作成、編集、および削除できます。

詳細情報

- Static Routes（P. 16-41）
- Add/Edit Static Routes（P. 4-13）
- 『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Static Routes

このダイアログボックスでは、スタティック ルートを追加または編集できます。詳細については、P.16-45 の「Add/Edit Static Route」を参照してください。

Step 13 - DHCP Server

この画面では、内部インターフェイスでホストする DHCP サーバとして適応型セキュリティ アプライアンスを設定できます。メイン ASDM アプリケーション ウィンドウから他のインターフェイスの DHCP サーバを設定するには、**Configuration > Properties > DHCP Services > DHCP Server** を選択します。詳細については、P.11-5 の「DHCP Server」を参照してください。

フィールド

- Enable DHCP server on the inside interface：内部インターフェイスから DHCP サーバへの接続を許可するには、このチェックボックスをオンにします。

DHCP Address Pool セクション

- Starting IP Address：DHCP サーバ プールの開始範囲を、IP アドレス ブロックとして最下位から最上位の順に指定します。

（注）　適応型セキュリティ アプライアンスは、最大で 256 の IP アドレスをサポートします。

- Ending IP Address：DHCP サーバ プールの終了範囲を、IP アドレス ブロックで最下位から最上位の順に指定します。

DHCP Parameters セクション

- Enable auto-configuration：DNS サーバ、WINS サーバ、リース期間、および ping タイムアウトの設定の自動コンフィギュレーションを許可するには、このチェックボックスをオンにします。
- DNS Server 1：DNS サーバの IP アドレスを指定します。
- WINS Server 1：WINS サーバの IP アドレスを指定します。
- DNS Server 2：代替 DNS サーバの IP アドレスを指定します。
- WINS Server 2：代替 WINS サーバの IP アドレスを指定します。
- Lease Length (secs)：リース期間が終了するまでに、割り当てられた IP アドレスをクライアントが使用できる時間（秒単位）を指定します。デフォルト値は、3600 秒（1 時間）です。
- Ping Timeout：ping のタイムアウト値のパラメータをミリ秒単位で指定します。
- Domain Name：DNS を使用する DNS サーバのドメイン名を指定します。
- Enable auto-configuration from interface：DHCP 自動コンフィギュレーションをイネーブルにし、メニューからインターフェイスを選択するには、このチェックボックスをオンにします。画面の前のセクションで指定する値は、自動コンフィギュレーションによる設定値よりも優先されます。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Step 14 - Address Translation (NAT/PAT)

この画面では、使用するセキュリティ アプライアンスでの NAT および PAT を設定できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、**Configuration > NAT** を選択します。

PAT により、設定した IP アドレスの 1 つだけがグローバル アドレスとして使用されます。また、複数の発信セッションが 1 つの IP アドレスから開始されたかのように見せることができます。PAT では、最大 65,535 のホストが 1 つの外部 IP アドレスで接続を開始できます。

NAT を使用する場合は、内部インターフェイスのすべてのアドレスを外部インターフェイスのアドレスに変換するときに使用するアドレス範囲を入力します。プールのグローバル アドレスは、各発信接続で使用される IP アドレスと、発信接続が着信接続になった場合の IP アドレスに使用されます。

PAT を使用する場合は、以下の点に注意してください。

- PAT は、キャッシング ネーム サーバでは動作しません。
- マルチメディア アプリケーション プロトコルがセキュリティ アプライアンスを通過するには、該当する検査エンジンをイネーブルにする必要があります。
- PAT は、**established** コマンドでは動作しません。
- パッシブ FTP を使用する場合は、**inspect protocol ftp strict** コマンドを **access-list** コマンドと一緒に使用して、発信 FTP トラフィックを許可します。
- 上位レベルのセキュリティ インターフェイス上の DNS サーバでは、PAT を使用できません。

フィールド

- Use Network Address Translation (NAT) : NAT および変換に使用される IP アドレス範囲をイネーブルにする場合に選択します。
- Starting Global IP Address：変換に使用される IP アドレス範囲の最初の IP アドレスを指定します。
- Ending Global IP Address：変換に使用される IP アドレス範囲の最後の IP アドレスを指定します。
- Subnet Mask (optional)：変換に使用される IP アドレス範囲のサブネット マスクを指定します。
- Use Port Address Translation (PAT)：PAT をイネーブルにする場合に選択します。このオプションを選択する場合は、次の中から 1 つ選択してください。

（注） IPSec に PAT を使用すると正しく動作しない場合があります。これは、外部のトンネル エンドポイント デバイスが、同じ IP アドレスの複数のトンネルを処理できないためです。

  - Use the IP address on the outside interface：PAT で外部インターフェイスの IP アドレスを使用する場合に選択します。
  - Specify an IP address：PAT で使用する IP アドレスを入力します。

    IP Address：PAT の対象になる外部インターフェイスの IP アドレスを指定します。

    Subnet Mask (optional)：ドロップダウン リストからサブネット マスクを選択します。
- Enable traffic through the firewall without translation：トラフィックを変換しないでファイアウォールを通過させる場合に選択します。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 15 - Administrative Access

この画面では、セキュリティ アプライアンスでの管理アクセスを設定できます。

フィールド

- Type：ホストまたはネットワークがセキュリティ アプライアンスにアクセスするときに、ASDM の HTTP over SSL、SSH、または Telnet のどれを使用するかを指定します。
- Interface：ホスト名またはネットワーク名を表示します。
- IP Address：ホストまたはネットワークの IP アドレスを表示します。
- Mask：ホストまたはネットワークのサブネット マスクを表示します。
- Enable HTTP server for HTTPS/ASDM access：ASDM にアクセスするための HTTP サーバへのセキュアな接続をイネーブルにするには、このチェックボックスをオンにします。
- Add：アクセス タイプとインターフェイスを追加し、次に管理目的でのみそのインターフェイスに接続するホスト ネットワークの IP アドレスとネットマスクを指定します。詳細については、「Add/Edit Administrative Access Entry」を参照してください。
- Edit：インターフェイスを変更します。詳細については、「Add/Edit Administrative Access Entry」を参照してください。
- Delete：インターフェイスを削除します。
- Enable ASDM history metrics：ASDM で統計を収集および表示できるようにするには、このチェックボックスをオンにします。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Administrative Access Entry

このダイアログボックスでは、ホストを設定できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、次のいずれかの方法を選択します。

- **Configuration > Properties > Device Access > HTTPS/ASDM**
- **Configuration > Properties > Device Access > Telnet**
- **Configuration > Properties > Device Access > SSH**
- **Configuration > Properties > History Metrics**

フィールド

- Access Type：ドロップダウン リストで、次に示す CLI コンソール セッションの事前設定された接続タイプの 1 つを選択します。
  - ASDM/HTTPS
  - SSH
  - Telnet

（注）　ASDM は、セキュリティ アプライアンスとのすべての通信で HTTP over SSL を使用します。

- Interface Name：事前設定されたインターフェイスのリストから選択します。
- IP Address：インターフェイスの IP アドレスを指定します。
- Subnet Mask：サブネット マスクの IP アドレスの選択肢から、インターフェイスのサブネット マスクを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Step 16 - Easy VPN Remote Configuration

この画面では、適応型セキュリティ アプライアンスと、リモート Cisco VPN 3000 コンセントレータ、Cisco ルータ、または Easy VPN サーバとして動作している適応型セキュリティ アプライアンスの間に、セキュアな VPN トンネルを設定できます。適応型セキュリティ アプライアンスは Easy VPN リモート デバイスとして動作するため、離れた場所に VPN を展開できます。

（注）　この画面にアクセスするには、Step 2 - Basic Configuration で **Configure the device for Teleworker usage** チェックボックスをオンにし、Interface Configuration の **Enable Auto Update** チェックボックスをオフにする必要があります。

次の 2 つの動作モードを使用できます。

- Client Mode（クライアント モード）
- Network Extension Mode（ネットワーク拡張モード）

クライアントモードでは、適応型セキュリティ アプライアンスは内部ネットワークのクライアントの IP アドレスを公開しません。代わりに、適応型セキュリティ アプライアンスは、NAT を使用してプライベート ネットワークの IP アドレスを特定の IP アドレスに変換します。このモードでは、プライベート ネットワークの外部からデバイスに ping を実行したり、デバイスにアクセスしたりできません。

拡張モードでは、適応型セキュリティ アプライアンスが、割り当てられた IP アドレスを置き換えることによってローカル ホストの IP アドレスを保護することはありません。したがって、VPN 接続の相手側ホストは、ローカル ネットワークのホストと直接通信できます。

適応型セキュリティ アプライアンスをこれらの 2 つのモードのいずれかに設定するには、次のガイドラインに従ってください。

次の場合はクライアント モードを使用します。

- VPN 接続をクライアント トラフィックで開始する場合

- ローカル ホストの IP アドレスをリモート ネットワークで非表示にする場合
- ASA 5505 の DHCP からローカル ホストに IP アドレスを渡す場合

次の場合はネットワーク拡張モードを使用します。

- トラフィック転送の必要がなくても VPN 接続を開いておく場合
- リモート ホストをローカル ネットワークから直接通信を可能にする場合
- ローカル ネットワークのホストがスタティック IP アドレスの場合

フィールド

- Enable Easy VPN remote：適応型セキュリティ アプライアンスが Easy VPN リモート デバイスとして動作できるようにするには、このチェックボックスをオンにします。この機能をイネーブルにしない場合、VPN トンネルからインターフェイス外部の適応型セキュリティ アプライアンスにアクセスできるホストは、その適応型セキュリティ アプライアンスをリモート管理できます。

Mode セクション

- Client Mode : DHCP サーバで、内部ネットワーク上のホストのダイナミック IP アドレスを生成します。
- Network extension：内部ネットワークのホストにスタティック IP アドレスがある場合、クリックします。

Group Settings セクション

- Use X.509 Certificate：X.509 証明書を使用して IPSec Main モードをイネーブルにします。ドロップダウン リストからトラストポイントを選択するか、または入力します。
- Use group password：ユーザ グループのパスワードを入力します。
  - Group Name：ユーザ グループの名前を入力します。
  - Password：ユーザ グループのパスワードを入力します。
  - Confirm password：パスワードの確認を要求します。

User Settings セクション

- Username：設定のユーザ名を入力します。
- Password：設定のパスワードを入力します。
- Confirm Password：設定のパスワードの確認を要求します。

Easy VPN Server セクション

- Primary server：プライマリ Easy VPN サーバの IP アドレスを入力できます。
- Secondary server：セカンダリ Easy VPN サーバの IP アドレスを入力できます。

（注） 適応型セキュリティ アプライアンスは、1 台のプライマリ サーバと 10 台までのセカンダリ サーバで構成される、最大で 11 台の Easy VPN サーバをサポートします。ASA の Easy VPN リモート デバイスを Easy VPN サーバに接続できるようにするには、ISP を利用して両方のデバイス間のネットワーク接続を確立しておく必要があります。ASA 5500 シリーズ適応型セキュリティ アプライアンスを DSL またはケーブル モデムに接続した後は、ISP の指示に従ってネットワーク接続設定を完了してください。IP アドレスは、PPPoE サーバ、DHCP サーバ、またはスタティック コンフィギュレーションから取得できます。

詳細情報

『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Step 17 - Startup Wizard Summary

この画面には、セキュリティ アプライアンスに対して行ったすべての設定の概要が表示されます。

- 前の画面での設定を変更するには、**Back** をクリックします。
- Startup Wizard をブラウザから直接起動した場合は、**Finish** をクリックすると、ウィザードで作成されたコンフィギュレーションが適応型セキュリティ アプライアンスに自動的に送信され、フラッシュ メモリに保存されます。
- ASDM 内で Startup Wizard を実行した場合は、そのコンフィギュレーションを明示的にフラッシュ メモリに保存する必要があります。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および『*Cisco ASA 5505 Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Other Interfaces Configuration

この画面では、残りのインターフェイスを設定できます。

フィールド

- Interface：元のホストまたはネットワークに接続されているネットワーク インターフェイスを表示します。
- Name：設定するインターフェイスの名前を表示します。
- Security Level：インターフェイスのセキュリティ レベル範囲が 0 ～ 100 で表示されます。100 は内部インターフェイス、0 は外部インターフェイスに設定されています。境界インターフェイスには、1 ～ 99 の範囲の番号が使用されます。0 ～ 100 のセキュリティ レベルは、デフォルトでは設定されません。
- Enable traffic between two or more interfaces with same security levels：同じセキュリティ レベルを複数のインターフェイスに設定し、それらのインターフェイス間のトラフィックをイネーブルにするには、このチェックボックスをオンにします。

- Enable traffic between two or more hosts connected to the same interface：複数のホストにあるインターフェイスでトラフィックをイネーブルにするには、このチェックボックスをオンにします。
- Edit：Edit Interface ダイアログボックスでインターフェイスのコンフィギュレーションを変更します。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Edit Interface

メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、**Configuration > Interfaces** を選択します。

フィールド

- Interface：編集対象として選択したインターフェイスの名前を表示します。
- Interface Name：選択したインターフェイスの名前を表示します。このインターフェイスの名前は変更できます。
- Security Level：選択したインターフェイスのセキュリティ レベルを表示します。インターフェイスのセキュリティ レベルは選択できます。インターフェイスのセキュリティ レベルを下げると、警告メッセージが表示されます。
- Use PPPoE：外部インターフェイスに IP アドレスを割り当てる場合に PPPoE を認証方式として使用するには、このチェックボックスをオンにします。

（注）　PPPoE は複数のインターフェイスで使用できるので、PPPoE クライアントの各インスタンスでは、別のユーザ名とパスワードを持つ異なる認証レベルを必要とする場合があります。

- Use DHCP：適応型セキュリティ アプライアンスを DHCP サーバとして使用するには、このチェックボックスをオンにします。
- Uses the following IP address：インターフェイスの特定の IP アドレスを入力するには、このチェックボックスをオンにします。
- IP Address：インターフェイスの IP アドレスを編集します。
- Subnet Mask：ドロップダウン リストから既存のサブネット マスクを選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Interface Configuration

この画面では、残りのインターフェイスを設定し、複数のインターフェイス間のトラフィックをイネーブルにすることができます。

フィールド

- Edit：Edit Interface ダイアログボックスでインターフェイスのコンフィギュレーションを変更します。
- Enable traffic between two or more interfaces with the same security level：同じセキュリティ レベルにある複数のインターフェイス間のトラフィックをイネーブルにするには、このチェックボックスをオンにします。

（注）　IP 関連のフィールドは、透過モードでは表示されません。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

Outside Interface Configuration - PPPoE

この画面では、PPPoE サーバから IP アドレスを取得することによって、外部インターフェイスを設定できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、**Configuration > Interfaces** を選択します。

フィールド

- Group Name：インターフェイスの名前を指定できます。次に進むには、グループ名を指定する必要があります。
- User Authentication エリア
  - PPPoE Username：認証に必要な PPPoE ユーザ名を指定します。
  - PPPoE Password：認証に必要な PPPoE パスワードを指定します。

- Confirm PPPoE Password：PPPoE パスワードを確認します。

- Authentication Method エリア

  PPPoE のデフォルト認証方式は PAP です。CHAP または MS-CHAP を手動で設定するオプションも選択できます。

  - PAP：PAP を認証方式として選択するには、このチェックボックスをオンにします。この方式では、ユーザ名とパスワードは暗号化されません。
  - CHAP：CHAP 認証を選択するには、このチェックボックスをオンにします。CHAP はリモート エンドを識別するのみで、不正アクセスを防止するわけではありません。その後、アクセス サーバはユーザにアクセス権限があるかどうかを判断します。
  - MSCHAP：Windows オペレーティング システムを使用するコンピュータとアクセス サーバの間の PPP 接続用に MS-CHAP 認証を選択するには、このチェックボックスをオンにします。

- IP Address エリア

  PPPoE のデフォルト認証方式は PAP です。CHAP または MS-CHAP を手動で設定するオプションも選択できます。

  - Obtain IP Address using PPPoE：IP アドレスを PPPoE サーバから取得します。
  - Specify an IP address：インターフェイスの IP アドレスを指定します。

    IP Address：インターフェイスの IP アドレスを入力できます。

    Subnet Mask：ドロップダウン リストからインターフェイスのサブネット マスクを入力または選択できます。
  - Obtain default route using PPPoE：PPPoE サーバと PPPoE クライアント間のデフォルト ルートを取得します。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Outside Interface Configuration

この画面では、IP アドレスを指定するか、PPPoE サーバまたは DHCP サーバから IP アドレスを取得することによって､外部インターフェイスを設定できます。メイン ASDM アプリケーション ウィンドウからこの機能にアクセスするには、**Configuration > Interfaces** を選択します。

（注）　ASA 5505 以外のすべての ASA 5500 シリーズ モデルの場合、フル ライセンスの適応型セキュリティ アプライアンスは、最大で 3 つの外部インターフェイスを含む 5 つのインターフェイスをサポートします。制限モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 3 つ、透過モードの適応型セキュリティ アプライアンスはインターフェイスを最大で 2 つサポートします。最大数のインターフェイスを作成した後、または最大数のインターフェイスに名前を付けた後は、VLAN を新規作成することはできなくなり、既存の VLAN を選択することが必要になります。

フィールド

- Interface：ドロップダウン リストからインターフェイスを選択します。
- Interface Name：新しいインターフェイスに名前を追加するか、または既存のインターフェイスに関連付けられた名前を表示します。
- Enable interface：インターフェイスを特権モードでアクティブにするには、このチェックボックスをオンにします。
- Security Level：インターフェイスのセキュリティ レベル範囲が 0 ～ 100 で表示されます。100 は内部インターフェイス、0 は外部インターフェイスに割り当てられます。境界インターフェイスには、1 ～ 99 の範囲の番号が使用されます。0 ～ 100 のセキュリティ レベルは、デフォルトでは設定されません。
- Use PPPoE：PPPoE サーバから IP アドレスを取得します。
- Use DHCP：DHCP サーバから IP アドレスを取得します。
- Obtain default route using DHCP：DHCP を使用してデフォルト ゲートウェイの IP アドレスを取得するには、このチェックボックスをオンにします。
- Use the following IP address：インターフェイスの IP アドレスを手動で指定するには、このオプションを選択します。このフィールドは透過モードの場合には表示されません。
- IP Address：外部インターフェイスの IP アドレスを指定します。このフィールドは透過モードの場合には表示されません。
- Subnet Mask：ドロップダウン リストから外部インターフェイスのサブネット マスクを選択します。

詳細情報

『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—