Cisco Firepower Threat Defense for the ASA クイック スタート ガイド

初版:2016 年 3 月 21 日
最終更新日:2016 年 8 月 8 日

1. Firepower Threat Defense デバイスについて

Firepower Threat Defense デバイスは、ステートフル ファイアウォール、ルーティング、Next-Generation Intrusion Prevention System(NGIPS)、Application Visibility and Control(AVC)、URL フィルタリング、および高度なマルウェア防御(AMP)などの次世代ファイアウォール サービスを提供します。シングル コンテキスト モードとルーテッドまたはトランスペアレント モードで Firepower Threat Defense デバイスを使用できます。

このマニュアルでは、Firepower Threat Defense をインストールして、ASA 5500-X シリーズ上で実行するように設定する方法を説明します。

Firepower Threat Defense ソフトウェアをサポートする ASA プラットフォーム

Firepower Threat Defense ソフトウェアまたは ASA ソフトウェアのいずれかをサポートするモデルは、次のとおりです。

- ASA 5506-X
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X

(注) Firepower Threat Defense ソフトウェアを実行するには、アプライアンスに Solid State Drive(SSD)がインストールされている必要があります。

(注) ASA 5506W-X には、ASA に統合されている Cisco Aironet 702i ワイヤレス アクセス ポイントが含まれています。

2. Firepower Threat Defense の前提条件

プロセスの再イメージ化を容易にするには、次の前提条件チェックを行う必要があります。次の点を確認してください。

- シスコ スマート アカウント。Cisco Software Central（https://software.cisco.com/）で作成できます。
- Firepower システムのリリース ノートの十分な理解。
- スマート アカウントに追加された Firepower Threat Defense 基本ライセンス（L-ASA5516T-BASE= など）。
- Firepower Management Center（仮想または物理）へのアクセス。
- Firepower Threat Defense がインストールされる 5500-X アプライアンスのコンソール ポートへのアクセス。Firepower Threat Defense のインストールに使用されるコンピュータから直接アクセスするか、またはターミナル サーバを介してアクセスします。推奨される配線およびトポロジについては、6. ネットワークへの Firepower Threat Defense の推奨される導入（11 ページ）を参照してください。
- 既存の設定のバックアップ。

  （注）5500-X アプライアンスで Firepower Threat Defense を再イメージ化およびインストールすると、ASA に保存された以前のファイルおよび設定はすべて失われます。
- フラッシュ（disk0）で使用可能な必要最低限の空き領域（3GB + ブート ソフトウェアのサイズ）。
- アプライアンスにインストールされた SSD。
- Firepower Threat Defense OS イメージをホストするための TFTP サーバへのアクセス。
  - ASA 5506-X シリーズ、ASA 5508-X、および ASA 5516-X アプライアンスの Firepower Threat Defense OS には、*.lfbff ファイルが必要です。
  - ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X アプライアンスの Firepower Threat Defense OS には、*.cdisk ファイルが必要です。
- Firepower Threat Defense システム パッケージをホストするための HTTP または FTP サーバへのアクセス。
  - Firepower Threat Defense システム自体には、システム パッケージの *.pkg ビルド ファイルが必要です。

3. Firepower Threat Defense の再イメージ化およびインストール

始める前に：

- デバイスへのコンソール接続および Firepower Management Center とデバイスの間のネットワーク接続を確認します。推奨される配線およびトポロジについては、6. ネットワークへの Firepower Threat Defense の推奨される導入（11 ページ）を参照してください。
- 配線および接続が完了したら、リストされている順序で次の手順を実行します。

1. コンソール ポートへのアクセス（3 ページ）
2. ROMMON イメージのアップグレード（3 ページ）（ファームウェアの最低バージョン 1.1.8）。
3. Firepower Threat Defense OS イメージのインストール（4 ページ）
4. Firepower Threat Defense システム パッケージのインストール（6 ページ）
5. Firepower Management 用のデバイス設定（7 ページ）
6. デバイスの Firepower Management Center への登録およびスマート ライセンスの割り当て（9 ページ）
7. ワイヤレス アクセス ポイントの有効化（ASA 5506W-X のみ）（9 ページ）

コンソール ポートへのアクセス

再イメージ化を実行するには、PC をコンソール ポートに接続する必要があります。

ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X では、サードパーティ製のシリアル USB 変換ケーブルを使用して接続する必要がある場合があります。他のモデルには、ミニ USB タイプ B コンソール ポートが搭載されているため、ミニ USB ケーブルを使用できます。Windows では、software.cisco.com から USB シリアル ドライバをインストールする必要がある場合があります。コンソール ポート オプションおよびドライバ要件の詳細については、ハードウェア ガイドを参照してください。http://www.cisco.com/go/asa5500x-install

9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナル エミュレータを使用します。

ROMMON イメージのアップグレード

ASA 5506-X シリーズ、ASA 5508-X、および ASA 5516-X モデルの場合にのみ、システム上の ROMMON バージョンを 1.1.8 以降にして、Firepower Threat Defense ソフトウェアに再イメージ化する必要があります。次の手順に従って、ROMMON バージョンを確認し、必要に応じて ROMMON イメージをアップグレードします。新バージョンへのアップグレードのみ可能です。ダウングレードはできません。

始める前に:

現在のバージョンを確認するには、**show module** コマンドを入力して、MAC アドレス範囲テーブルの Mod 1 の出力で Fw バージョンを調べます。

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.2        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

手順

1. Cisco.com から新しい ROMMON イメージを取得して、サーバ上に置いて ASA にコピーします。ASA は多数のタイプのサーバをサポートします。詳細については、**copy** コマンドを参照してください。
   http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1/c4.html#pgfId-2171368

   次の URL からイメージをダウンロードします。

   https://software.cisco.com/download/type.html?mdfid=286283326&flowid=77251

2. ROMMON イメージを ASA フラッシュ メモリにコピーします。この手順では FTP コピーを示します。

   copy ftp://*user*:*password*@*server_ip*/**asa5500-firmware**-*xxxx*.**SPA disk0:asa5500-firmware**-*xxxx*.**SPA**

   例:

   ```
   ciscoasa# copy ftp://admin:test@10.86.118.21/asa5500-firmware-1108.SPA
   disk0:asa5500-firmware-1108.SPA
   ```

3. ROMMON イメージをアップグレードします。

   upgrade rommon disk0:asa5500-firmware-*xxxx*.**SPA**

   例:

   ```
   ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
   Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

   Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                         eefe8f182491652ee4c05e6e751f7a4f
   ```

```
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash    SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

4. プロンプトが表示されたら、確認して ASA をリロードします。

   ASA が ROMMON イメージをアップグレードして、その後 ASA をリロードします。

次の作業

次の項の説明に従って、Firepower Threat Defense OS イメージをインストールします。

Firepower Threat Defense OS イメージのインストール

ASA を Firepower Threat Defense ソフトウェアに再イメージ化するには、ROMMON プロンプトにアクセスする必要があります。ROMMON では、管理インターフェイスで TFTP を使用して Firepower Threat Defense ブート イメージをダウンロードする必要があります。サポートされるのは、TFTP のみです。その後、ブート イメージは、HTTP または FTP を使用して Firepower Threat Defense システム ソフトウェアのインストール パッケージをダウンロードできます。TFTP のダウンロードには時間がかかることがあります。パケットの損失を防ぐために、ASA と TFTP サーバの間の接続が安定していることを確認してください。

手順

1. 管理インターフェイスの ASA からアクセス可能な TFTP サーバに Firepower Threat Defense ブート イメージをダウンロードします。

   ASA 5506-X、5508-X、および 5516-X では、管理 1/1 ポートを使用してイメージをダウンロードする必要があります。他のモデルでは、任意のインターフェイスを使用できます。

2. 管理インターフェイスの ASA からアクセス可能な HTTP または FTP サーバに Firepower Threat Defense システム ソフトウェアのインストール パッケージをダウンロードします。

3. コンソール ポートから、ASA をリロードします。

   ```
   ciscoasa# reload
   ```

4. ブートアップ中に ROMMON プロンプトを表示するよう要求されたら、Esc を押します。

   モニタを注視します。

例:

```
[...]
Booting from ROMMON

Cisco Systems ROMMON Version (2.1(9)8) #1: Wed Oct 26 17:14:40 PDT 2011

Platform ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in   7 seconds.
```

この時点で、Esc を押します。

次のメッセージが表示された場合は、時間がかかりすぎです。ブートの終了後、再度 ASA をリロードする必要があります。

```
Launching BootLoader...
Boot configuration file contains 2 entries.
[...]
```

5. ROMMON プロンプトで、**set** を入力して次のパラメータを設定し、TFTP サーバへの一時的な接続を確立します。
   - (ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X のみ)管理インターフェイス ID。他のモデルは常に管理 1/1 インターフェイスを使用します。
   - 管理インターフェイスの IP アドレス
   - TFTP サーバの IP アドレス
   - ゲートウェイ IP アドレス。同一ネットワーク上にある場合、このアドレスをサーバ IP アドレスと同じに設定します。
   - TFTP ファイル パスと名前。

   その後、ブート イメージをロードします。

   例:

```
rommon #0> interface gigabitethernet0/0
rommon #1> address 10.86.118.4
rommon #2> server 10.86.118.21
rommon #3> gateway 10.86.118.21
rommon #4> file ftd-boot-latest.cdisk
rommon #5> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=ftd-boot-latest.cdisk
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon #5> sync

Updating NVRAM Parameters...

rommon #6: tftpdnld
```

   Firepower Threat Defense ブート イメージがダウンロードされ、ブート CLI にブートアップされます。

6. (オプション)**sync** を入力して、設定を保存します。

7. （オプション）**ping** コマンドを発行して、ROMMON から TFTP サーバへの接続を確認します。

   TFTP サーバへの ping が成功することを確認します。

8. **tftpdnld** コマンドを発行して、ダウンロードおよび起動プロセスを開始します。

   OS イメージは、TFTP 経由でダウンロードを開始する必要があります。OS のダウンロードが完了すると、システムはダウンロードしたばかりのイメージを使用して自動的に起動し、ブート CLI プロンプトで停止します。

次の作業

- 次の項の説明に従って、ブート CLI を使用して Firepower Threat Defense パッケージのインストールと設定を続行します。

Firepower Threat Defense システム パッケージのインストール

OS イメージのインストール後、ブート CLI は自動的にロードします。次の手順では、設定コマンドを使用して基本のネットワーク接続を確立し、Firepower Threat Defense システム パッケージをダウンロードして、その後パッケージをインストールする方法を説明します。パッケージがロードされたら、システムは再起動して、最初のブート スクリプトと初期化を実行します。

手順

1. ブート CLI から **setup** と入力して、管理インターフェイスのネットワーク設定を行い、システム ソフトウェア パッケージをダウンロードしてインストールできるように HTTP または FTP サーバーへの一時的な接続を確立します。次に例を示します。
   - ホスト名：**ftd1**
   - IPv4 アドレス：**10.86.118.4**
   - ネットマスク：**255.255.252.0**
   - ゲートウェイ：**10.86.116.1**
   - DNS サーバ：**10.86.116.5**
   - NTP サーバ：**ntp.example.com**
2. Firepower Threat Defense システム ソフトウェアのインストール パッケージをダウンロードします。この手順では、HTTP のインストールを示します。

   system install [**noconfirm**] *url*

   例：

   ```
   > system install noconfirm http://10.86.118.21/ftd-6.0.1-949.pkg
   ```

   確認メッセージに応答しない場合は、**noconfirm** オプションを指定します。

3. インストールが完了して、デバイスの再起動オプションが表示されたら [はい（Yes）] を選択します。

   再起動には約 30 分かかりますが、より長時間かかる可能性があります。再起動時に、Firepower Threat Defense CLI が表示されます。

   この時点で、OS およびパッケージのインストールは完了です。

次の作業

- 次の項の説明に従って、Firepower Threat Defense デバイスをネットワーク接続および Firepower Management 用に設定します。

Firepower Management 用のデバイス設定

最初に CLI にアクセスするときに、セットアップ ウィザードによって、Firepower Threat Defense デバイスの設定に必要な基本のネットワーク設定パラメータのプロンプトが表示され、Firepower Management Center への登録が要求されます。管理 IP アドレスと関連するゲートウェイ ルートは、インターフェイス リストの Firepower Management Center Web インターフェイスまたはデバイスのスタティック ルートに含まれて**いません**。これらは、セットアップ スクリプトおよび CLI によってのみ設定できます。

手順

1. たとえば、コンソール ポートから、または SSH を使用して、デバイスに接続します。
   - モニタとキーボードが取り付けられたデバイスの場合は、コンソールからログインします。
   - デバイスの管理インターフェイスへのアクセスでは、管理インターフェイスのデフォルト IPv4 アドレス（192.168.45.45）に SSH を実行します。
2. デフォルトのユーザ名：**admin**、パスワード：**Admin123** を使用してログインします。
3. EULA を受け入れて、パスワードを変更し、プロンプトに従って管理用のネットワーク設定を再入力します。

   IPv4 と IPv6 の両方の管理アドレスを設定できます。

   次に例を示します。

```
System initialization in progress.Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <new password>
Confirm new password: <repeat password>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.133.128.47
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.248.0
Enter the IPv4 default gateway for the management interface []: 10.133.128.1
Enter a fully qualified hostname for this system [firepower]: laurel.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.33.16.6
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

4. 新しいログイン クレデンシャルを使用して、アプライアンスに再接続します。
5. ファイアウォール モードを設定します。次に例を示します。

```
Configure firewall mode? (routed/transparent) [routed]
```

   （注） 初期設定でファイアウォール モードを設定することをお勧めします。デフォルト モードは*ルーテッド*です。初期設定後にファイアウォール モードを変更すると、実行コンフィギュレーションが消去されます。詳細については、『*Firepower Management Center 構成ガイド*』の「トランスペアレントまたはルーテッド ファイアウォール モード」の章を参照してください。

6. デフォルトのシステム設定が処理されるのを待ちます。数分かかることがあります。

```
Update policy deployment information
    - add device configuration

You can register the sensor to a Management Center and use the Management Center
to manage it.Note that registering the sensor to a Management Center disables
on-sensor FirePOWER Services management capabilities.
```

```
When registering the sensor to a Management Center, a unique alphanumeric
registration key is always required.In most cases, to register a sensor
to a Management Center, you must provide the hostname or the IP address along
with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Management Center are separated by a NAT device,
you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Management Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Management Center.
```

7. Firepower Threat Defense デバイスを Firepower Management Center に登録します。

   > **configure manager add** {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

   引数の説明

   - {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} は、Firepower Management Center の完全修飾ホスト名または IP アドレスのいずれかを指定します。Firepower Management Center を直接アドレス指定できない場合は、DONTRESOLVE を使用します。
   - *reg_key* は、Firepower Threat Defense モジュールを Firepower Management Center へ登録するのに必要な一意の英数字による登録キーです。

   （注） 登録キーは、ユーザ生成の 1 回しか使用できないキーです。37 文字以下にする必要があります。有効な文字には、英数字（A-Z、a-z、0-9）、およびハイフン（-）などがあります。デバイスを Firepower Management Center に追加するときに、この登録キーを思い出す必要があります。

   - *nat_id* は、Firepower Management Center と Firepower Threat Defense モジュール間の登録プロセス中に使用されるオプションの英数字文字列です。hostname が DONTRESOLVE に設定されている場合に必要です。

8. **configure manager add** コマンドを使用して、このデバイスを管理する Firepower Management Center アプライアンスを指定します。

   登録キーは、ユーザ生成の 1 回しか使用できないキーです。Firepower Threat Defense デバイスを Firepower Management Center のインベントリに追加する必要があります。次に、簡単な例を示します。

   ```
   > configure manager add MC.example.com 123456
   Manager successfully configured.
   ```

   デバイスと Firepower Management Center が NAT デバイスによって分けられている場合は、登録キーと一緒に一意の NAT ID を入力し、ホスト名の代わりに DONTRESOLVE を指定します。たとえば次のようにします。

   ```
   >configure manager add DONTRESOLVE my_reg_key my_nat_id
   Manager successfully configured.
   ```

9. CLI を閉じます。

   ```
   > exit
   ```

次の作業

- 次の項の説明に従って、デバイスを Firepower Management Center に登録します。

デバイスの Firepower Management Center への登録およびスマート ライセンスの割り当て

はじめる前に

- Firepower Management Center でスマート ライセンスを設定します。

手順

1. ブラウザで HTTPS 接続を使用して、上記で入力したホスト名またはアドレスを使用して Firepower Management Center にログインします。たとえば、https://MC.example.com などです。
2. デバイスを追加するには、[デバイス管理(Device Management)] ページ([デバイス(Devices)] > [デバイス管理(Device Management)])を使用します。詳細については、オンライン ヘルプまたは『*Firepower Management Center 構成ガイド*』の「デバイスの管理」の章を参照してください。
3. CLI 設定時に、デバイスに設定済みの管理 IP アドレスを入力します。
4. CLI 設定時にデバイスで指定されたのと同じ登録キーを使用します。
5. [スマート ライセンス割り当て(Smart Licensing)] オプション([脅威(Threat)]、[URL]、[高度なマルウェア(Advanced Malware)])を選択します。

   これらのライセンスは、スマート アカウントにすでに存在している必要があります。スマート アカウントにアプライアンスの基本ライセンスを持っている必要があります。2. Firepower Threat Defense の前提条件(2 ページ)を参照してください。
6. [登録(Register)] をクリックして、デバイス登録の成功を確認します。

次の作業

- 組み込みワイヤレス アクセス ポイントを備えた ASA 5506W-X がある場合は、次の項の説明に従ってアクセス ポイントを有効化します。
- デバイスのポリシーとデバイス設定を構成します。

ワイヤレス アクセス ポイントの有効化(ASA 5506W-X のみ)

ASA 5506W-X ワイヤレス アクセス ポイントは、デフォルトで無効化されています。ワイヤレス無線を有効化し、SSID およびセキュリティの設定を行うには、アクセス ポイント GUI に接続してください。

はじめる前に

- ASA 5506W-X デバイスを管理している Firepower Management Center にログインします。この手順は、インターフェイス設定のごく一部にすぎません。この時点では、他のパラメータを設定しないようにします。
- アクセス ポイントは、GigabitEthernet 1/9 インターフェイス上で内部的に ASA に接続します。すべての WiFi クライアントは GigabitEthernet 1/9 ネットワークに属します。セキュリティ ポリシーにより、WiFi ネットワークが他のインターフェイス上の任意のネットワークにアクセスする方法が規定されます。アクセス ポイントには、外部インターフェイスやスイッチ ポートは含まれません。

手順

1. [デバイス(Devices)] > [デバイス管理(Device Management)] を選択して、Firepower Threat Defense デバイスの編集アイコン( )をクリックします。

   [インターフェイス(Interfaces)] タブがデフォルトで選択されています。
2. 編集するインターフェイス(今回は、GigabitEthernet1/9)の横にある編集アイコン( )をクリックします。
   a. [モード(Mode)] ドロップダウン リストで、[なし(None)] を選択します。

b. オプションで、[名前(Name)] を追加します。たとえば、AP-FTD などです。

c. [有効化(Enabled)] チェック ボックスをオンにして、インターフェイスを有効化します。

d. 内部インターフェイスと同じゾーンに GigabitEthernet1/9 を追加します。

e. オプションで、[説明(Description)] を追加します。

f. IP アドレスを設定します。たとえば、192.168.10.2-254 などです。

これは、アクセス ポイント自体の IP アドレスとアクセス ポイント上のクライアントの IP アドレスを指定します。

g. [OK] をクリックします。

3. [保存(Save)] をクリックします。
4. [DHCP] をクリックします。
   a. [サーバを追加(Add Server)] ダイアログ ボックスで [GigabitEthernet1/9] を選択します。
   b. このインターフェイスに以前指定したのと同じ IP アドレス プールを追加します。たとえば、192.168.10.2-254 などです。
   c. [DHCP サーバを有効化(Enable DHCP Server)] チェック ボックスをオンにして、DHCP サーバを有効化します。
   d. [OK] をクリックします。
5. [保存(Save)] をクリックします。
6. ASA の内部ネットワークに接続されているコンピュータで、Web ブラウザを起動します。
7. [アドレス(Address)] フィールドで、GigabitEthernet1/9 インターフェイスの設定にマップする IP アドレスを入力します。

   たとえば、アドレス範囲として 192.168.10.2-254 を入力した場合、アクセス ポイントの IP アドレスはその範囲の最初のアドレス(192.168.10.2)になります。

   ユーザ名とパスワードの入力を求められます。
8. ユーザ名 **Cisco** とパスワード **Cisco** を入力します。アクセス ポイント GUI が表示されます。
9. 左側の [簡易設定(Easy Setup)] > [ネットワーク構成(Network Configuration)] をクリックします。
10. [無線構成(Radio Configuration)] 領域で、[無線 2.4 GHz(Radio 2.4GHz)] セクションおよび [無線 5 GHz(Radio 5GHz)] セクションのそれぞれに対して、次のパラメータを設定し、セクションごとに [適用(Apply)] をクリックします。
    - **SSID**
    - **Broadcast SSID in Beacon**
    - **Universal Admin Mode**:**Disable**
    - **Security**(お客様が選択)
11. 左側の [サマリー(Summary)] をクリックし、メイン ページの [ネットワーク インターフェイス(Network Interfaces)] で、2.4 GHz 無線に対応するホットリンクをクリックします。
12. [設定(Settings)] タブをクリックします。
13. [無線を有効化(Enable Radio)] の設定では、[有効化(Enable)] ラジオ ボタンをクリックし、ページ下部の [適用(Apply)] をクリックします。
14. 手順を繰り返して 5 GHz 無線を設定します。
15. 詳細については、次のマニュアルを参照してください。
    - ワイヤレス LAN コントローラの使用の詳細については、Cisco Wireless LAN Controller ソフトウェアのマニュアルを参照してください。
    - ワイヤレス アクセス ポイントのハードウェアおよびソフトウェアの詳細については、Cisco Aironet 700 シリーズのマニュアルを参照してください。

4. デバイスの初期設定

Firepower Threat Defense システム ソフトウェアをインストールして、デバイスを Management Center に追加すると、Firepower Management Center ユーザ インターフェイスを使用してデバイス管理設定を構成したり、アクセス コントロール ポリシーや Firepower Threat Defense システムを使用してトラフィックを管理するためのその他の関連ポリシーを設定および適用することができます。

5. Firepower Threat Defense CLI へのアクセス

初期設定またはトラブルシューティングでは、Firepower Threat Defense CLI にアクセスします。

手順

1. Firepower Threat Defense のインストールに使用した管理コンピュータから直接、またはターミナル サーバを介して、Firepower Threat Defense がインストールされている 5500-X アプライアンスのコンソール ポートにアクセスします。
2. ログインするには、セットアップ プロセスで作成した管理者ユーザ アカウント（および対応するパスワード）を使用します。

   （注） デフォルトのログイン クレデンシャルは、ユーザ名：**admin**、パスワード：**Admin123** です。
3. 使用可能なコマンドのリストを表示するには、疑問符（?）を入力します。

   例：

   ```
   > ?
   ```
4. システム診断にアクセスするには、**system support diagnostic-cli** を入力します。

   例：

   ```
   > system support diagnostic-cli
   ```
5. Firepower Threat Defense 接続を終了するには、**exit** を入力します。

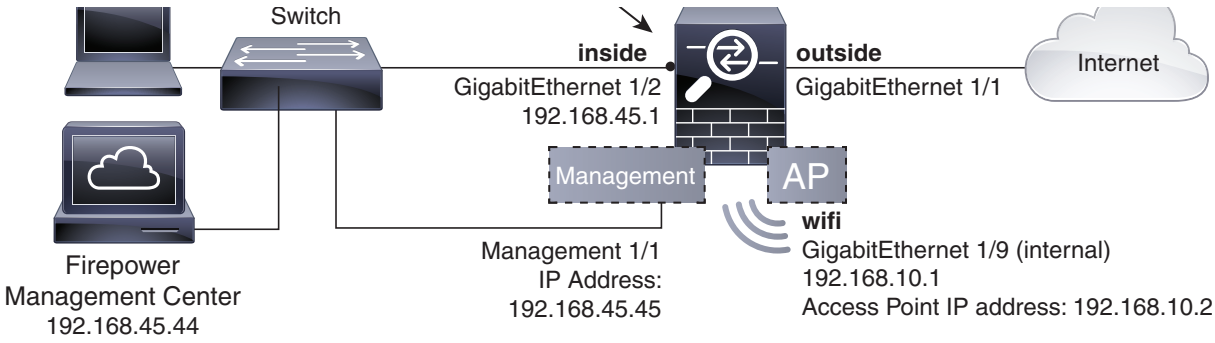
   例：

   ```
   > exit
   >
   ```

6. ネットワークへの Firepower Threat Defense の推奨される導入

次の図に、ASA 5500-X シリーズ アプライアンスで推奨される Firepower Threat Defense のネットワーク導入を示します。

（注） ポートの番号付け、つまりインターフェイスの番号付けは、いくつかの ASA デバイス モデルとは異なります。ASA ポートの番号付けは、ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X では 0 から始まります。一方で、ASA 5506-X シリーズ、ASA 5508-X、および ASA 5516-X では 1 から始まります。



（注） 導入には、別々の内部スイッチを使用する必要があります。.

設定例では、次の動作によって上記のネットワーク導入を有効化します。

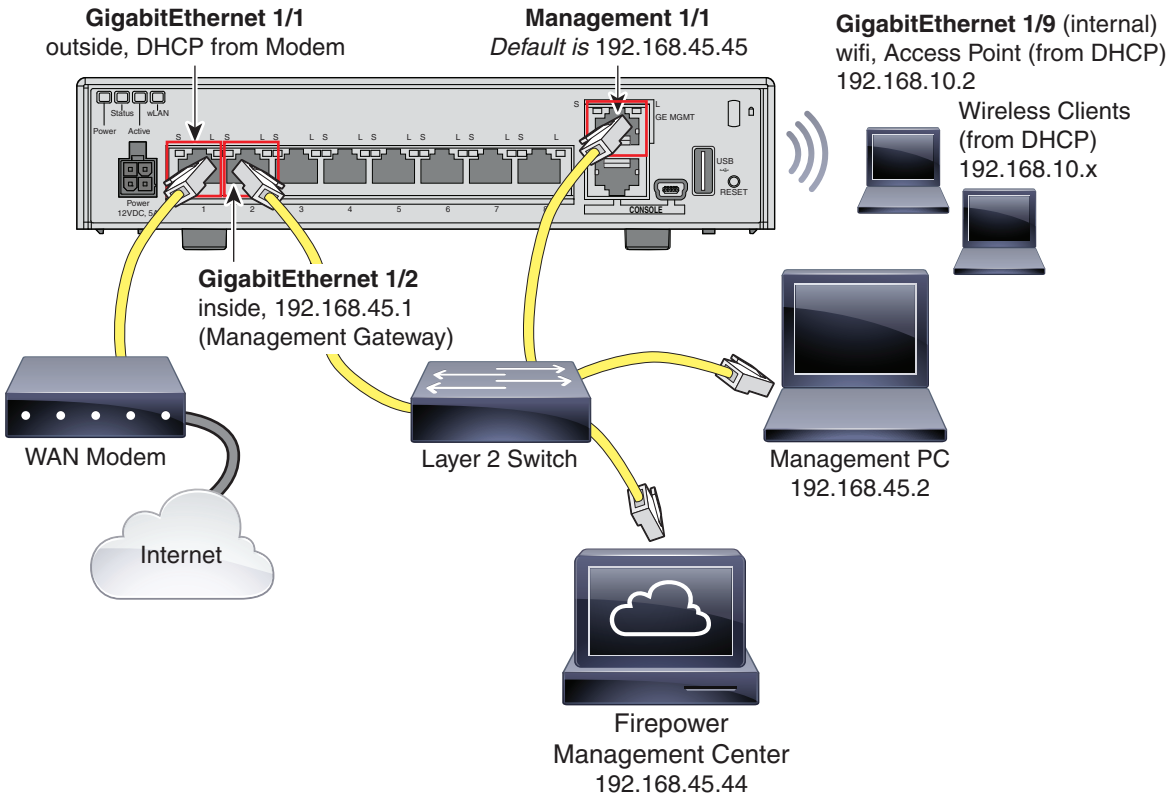
- **内部 --> 外部**へのトラフィック フロー
- **DHCP** からの**外部 IP** アドレス
- （ASA 5506W-X）**WiFi <--> 内部**、**WiFi --> 外部**へのトラフィック フロー
- **内部**および **WiFi** 上のクライアントに対する **DHCP**アクセス ポイントおよびそのすべてのクライアントが ASA を DHCP サーバとして使用します。
- **管理 0/0 または 管理 1/1** は、Firepower Threat Defense デバイスを Firepower Management Center に設定および登録するために使用されます。

  管理インターフェイスは、更新にインターネット アクセスが必要です。内部インターフェイスと同じネットワーク上に管理を配置すると、Firepower Threat Defense デバイスを内部のスイッチのみで導入して、内部インターフェイスをゲートウェイとして示すことができます。

  （注） 物理的な管理インターフェイスは、管理論理インターフェイスと診断論理インターフェイスの間で共有できます。Firepower Threat Defense デバイスの管理アクセス（13 ページ）を参照してください。
- **内部** インターフェイスおよび **WiFi** インターフェイス上の **Firepower Management Center アクセス**

  （注） 内部ネットワーク上に別のルータを導入すると、管理と内部の間でルーティングできます。別の導入設定例については、『*Firepower Management Center 構成ガイド*』の「Firepower Threat Defense インターフェイス」の章を参照してください。

ASA 5506-X シリーズ、ASA 5508-X、または ASA 5516-X で上記のシナリオをケーブル接続するには、次を参照してください。



Firepower Threat Defense デバイスの管理アクセス

Firepower Threat Defense デバイスは、セットアップ IP アドレスを使用して、Firepower Management Center による管理用にルートをゲートウェイに関連付けます。管理 IP アドレスとルートは、インターフェイス リストの Firepower Management Center Web インターフェイスまたはデバイスのスタティック ルートに含まれて**いません**。セットアップ スクリプトおよび CLI によってのみ設定できます。初期設定を実行した後、Firepower Management Center を使用してセキュリティおよびアクセス ポリシー、デバイス設定、およびインターフェイスを設定します。

物理管理ポートを介した syslog または SNMP レポートを選択する場合、Firepower Management Center Web インターフェイスを使用して診断 0/0 または診断 1/1 インターフェイス用に別々の IP アドレスとルート、および外部認証を設定する必要があります。ただし、導入を簡素化するために、レポート用にデータ ポートを使用することをお勧めします。

7. 次の作業

- Firepower Management Center による Firepower Threat Defense の管理の詳細については、Firepower Management Center の構成ガイドまたはFirepower Management Center のオンライン ヘルプを参照してください。
- すべての Firepower System のマニュアルのリンクについては、Cisco Firepower System マニュアルのナビゲーションを参照してください。
- ASA のすべてのマニュアルのリンクについては、Cisco ASA シリーズ マニュアルのナビゲーションを参照してください。