



# Cisco ASA with Firepower Services

## かんたんセットアップ ガイド



本ガイドの手順で ASA を  
かんたんにセットアップできます

- 1 機器と PC の接続
- 2 ASDM のインストール
- 3 初期セットアップ
- 4 Umbrella DNS の設定



# 1

## 機器と PC の接続

### 1-1

#### 必要な機器を準備する

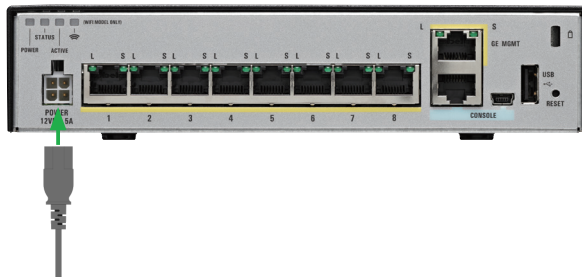
次のものを準備し、Cisco ASA を、セットアップを実行するコンピュータ(PC)に接続します。

- ASA 本体
- AC 電源コード(または電源アダプタ)
- イーサネット ケーブル x 3
- PC

ASA には何も接続しない状態で始めます。また、PC が DHCP を使用して IP アドレスを自動的に取得する設定になっているかどうか、確認してください。

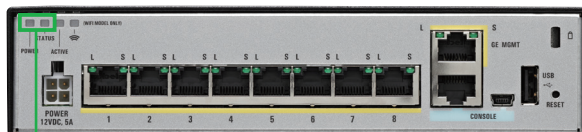
### 1-2

#### ASA を PC に接続する



- 1 AC 電源コードを ASA 背面の AC 電源コネクタと AC 電源コンセントに接続

ASA に電源を投入します。 .



- 2 POWER LED と STATUS LED の点灯を確認

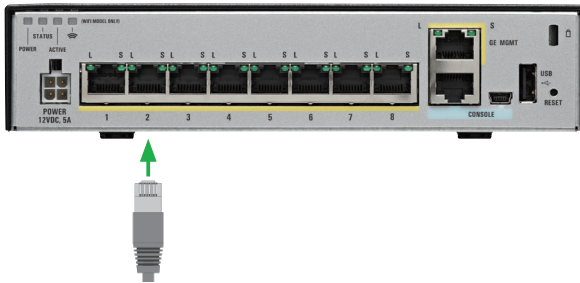
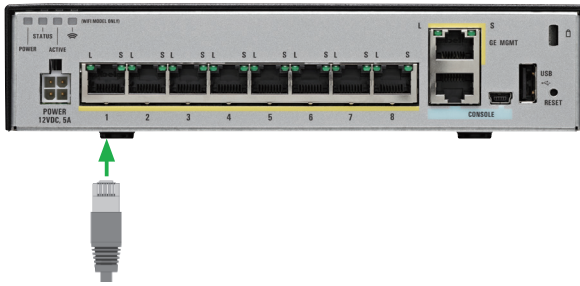
ASA に電源を投入すると POWER LED がグリーンに点灯し、セルフテストが開始されます。STATUS LED もグリーンに点灯したら、セルフテストは完了です。

- 3** 1 本目のイーサネット ケーブルを ASA のイーサネット ポート 1 と WAN デバイスのイーサネット ポートに接続

ASA 側のイーサネット ケーブルを接続したポート LED がグリーンに点灯または点滅したら、1 本目の接続は完了です。

- 4** 2 本目のイーサネット ケーブルを ASA のイーサネット ポート 2 と PC のイーサネット ポートに接続

ASA および PC のイーサネット ケーブルを接続したポート LED がグリーンに点灯または点滅したら、2 本目の接続は完了です。



### ⚠ 注意

- 2**で、STATUS LED がグリーンに点灯しない、またはアンバーに点灯する場合、AC 電源コードを接続し直して、再度、電源を投入してください。それでも STATUS LED がグリーンに点灯しない、またはアンバーに点灯する場合は、ご購入元にお問い合わせください。
- 3**および**4**で、イーサネット ケーブルを接続する ASA 側のポートは、下部にポート番号があるイーサネットポートです。GE MGMT ポートには接続しないでください。

# 2

## ASDM のインストール

Web ベースの管理インターフェイス「Cisco Adaptive Security Device Manager (ASDM)」を利用して、ASA を初期設定します。ASA から ASDM をダウンロードして、インストールしてください。



1 ブラウザを開き、アドレス バーに「https://192.168.1.1」を入力して Enter キーを押す



2 [このサイトの閲覧を続行する (推奨されません。)] をクリック

セキュリティ証明書の警告メッセージが表示される場合がありますが、クリックして続行します。「Cisco ASDM」ページが開きます。

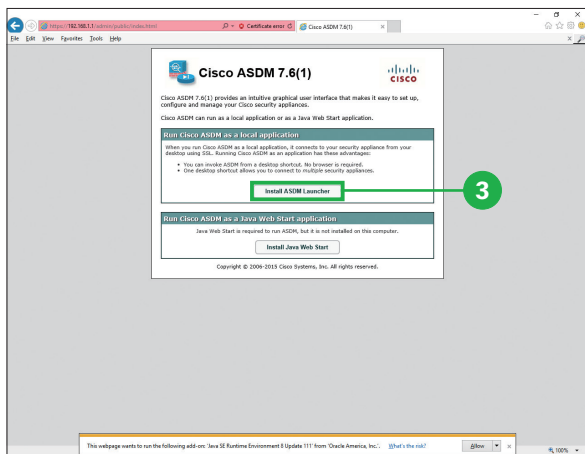
### ⚠ 注意

「Cisco ASDM」ページが開かない場合は、ASA と PC の接続が失敗している可能性があります。

- POWER LED および STATUS LED がグリーンに点灯しているかどうか、確認してください。
  - イーサネット ケーブルにはストレートケーブルを使用しているかどうか、確認してください。
  - ブラウザのポップアップ ブロック設定やプロキシ設定が無効になっているかどうか、および PC の無線 LAN が無効になっているかどうか、確認してください。
  - PC が DHCP を使用して IP アドレスを自動的に取得する設定になっているかどうか、確認してください。
- Windows ではデフォルトで DHCP を使用して IP アドレスを自動的に取得する設定になっていますが、手動設定になっている場合は自動設定に戻して Windows を再起動してください。

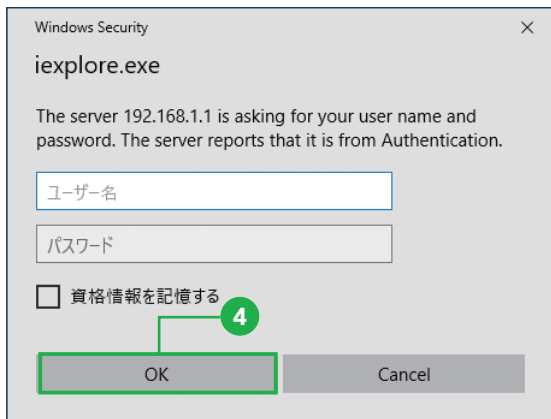
## 2 ASDM のインストール

### 3 [Install ASDM Launcher] をクリック



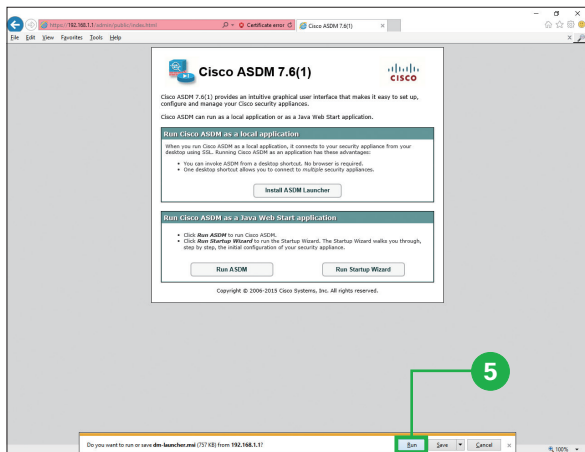
### 4 [OK] をクリック

認証ダイアログ ボックスが表示される場合がありますが、[ユーザー名] および [パスワード] は入力せずに、クリックして続行します。

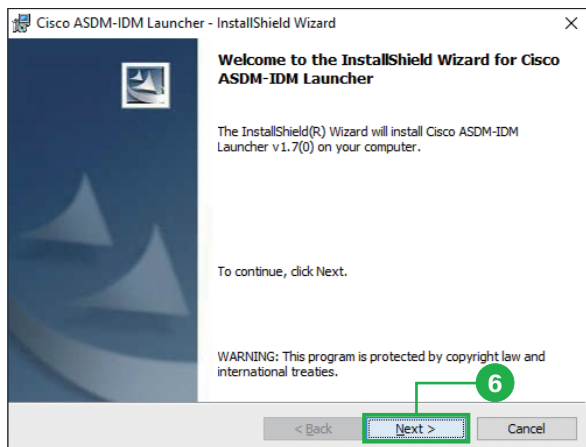


### 5 [実行] をクリック

インストーラが起動します。

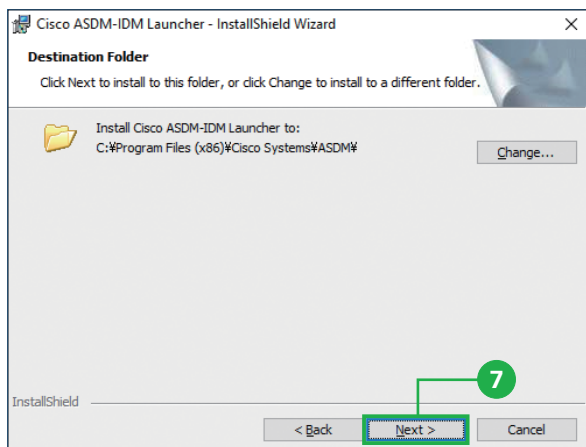


## 6 [Next] をクリック

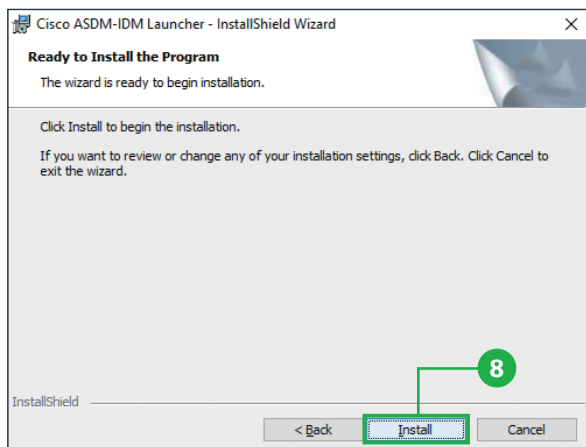


## 7 [Next] をクリック

インストール先のフォルダを変更する場合は [Change] をクリックして、ダイアログ ボックスからインストール先のフォルダを選択してください。

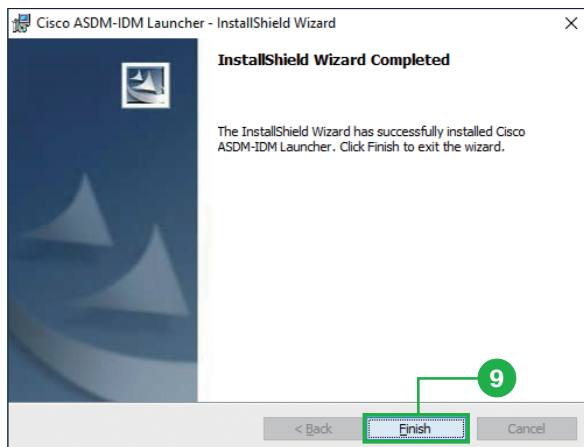


## 8 [Install] をクリック



## 9 [Finish] をクリック

「Cisco ASDM Launcher」が起動します。

**!** 注意

ASDM の利用には、次の要件を満たすコンピュータおよびブラウザが必要です。

- Microsoft Windows 7、8
  - Microsoft Internet Explorer
  - Mozilla Firefox
  - Google Chrome
  - Java SE Plug-in 7.0 以上
- Apple OS X 10.4 以上
  - Mozilla Firefox
  - Apple Safari
  - Google Chrome (64 ビット)
  - Java SE Plug-in 7.0 以上

Windows 8.1 および 10 でも動作は確認されていますが、公式にはサポートしていません。

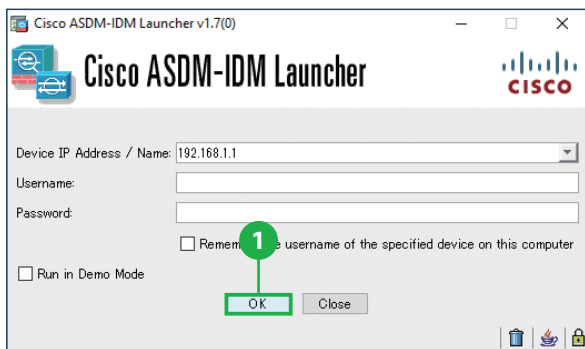
# 3

## 初期セットアップ

### 3-1

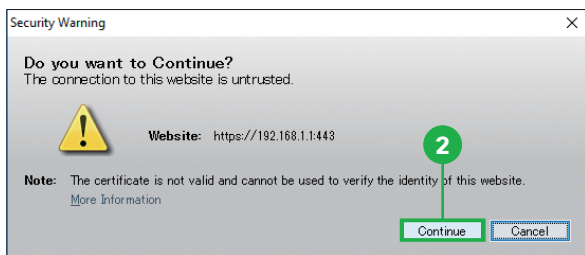
### ASDM を起動する

「Cisco ASDM Launcher」から ASDM を起動します。

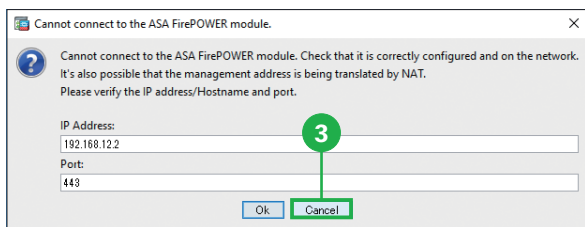


#### 1 [OK] をクリック

[Username] および [Password] は入力せずに、クリックして続行します。セキュリティ警告が表示されます。



#### 2 [続行] をクリック



#### 3 [Cancel] をクリック

ASDM が起動します。



#### MEMO

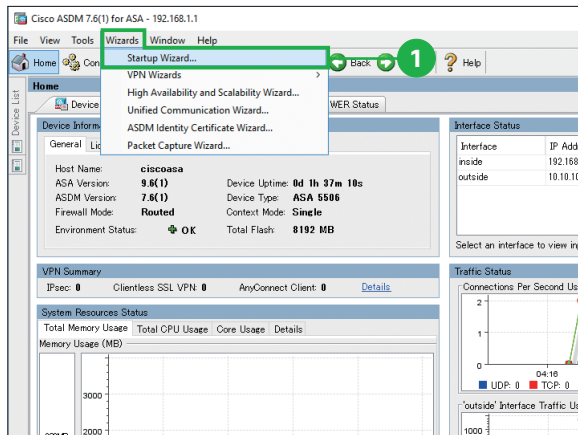
3で、「ASA Firepower module」の IP アドレスを入力するように求められますが、ここではキャンセルして続行します。この IP アドレスは「3-2 スタートアップ ウィザードを起動する」で設定します。



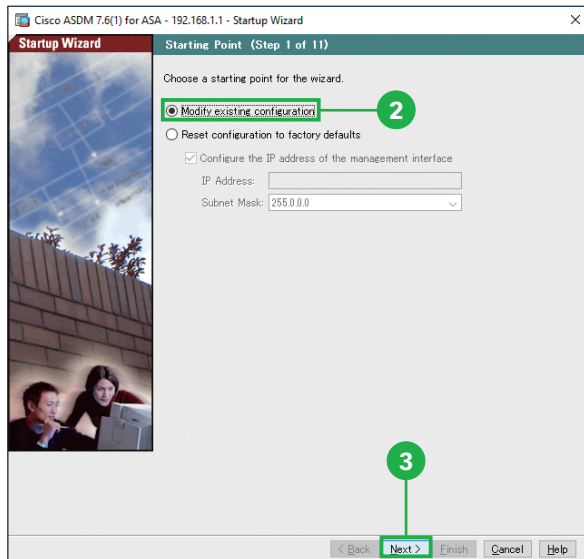
## 3-2

## スタートアップ ウィザードを起動する

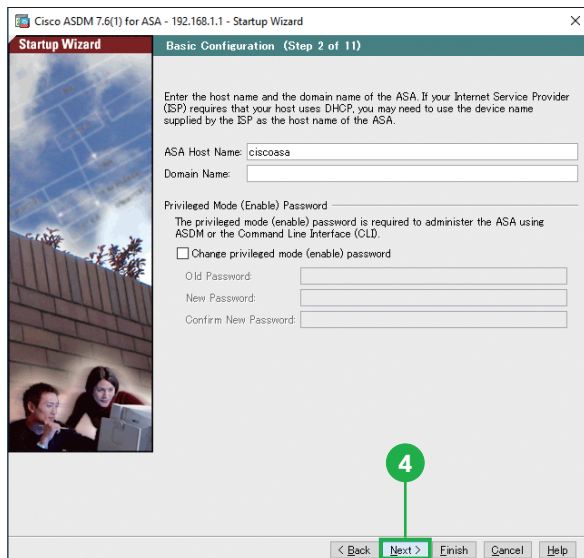
ASDM を起動したら、スタートアップ ウィザードを使用して初期設定します。



- 1 [Wizards] メニュー バーから [Startup Wizard] をクリック

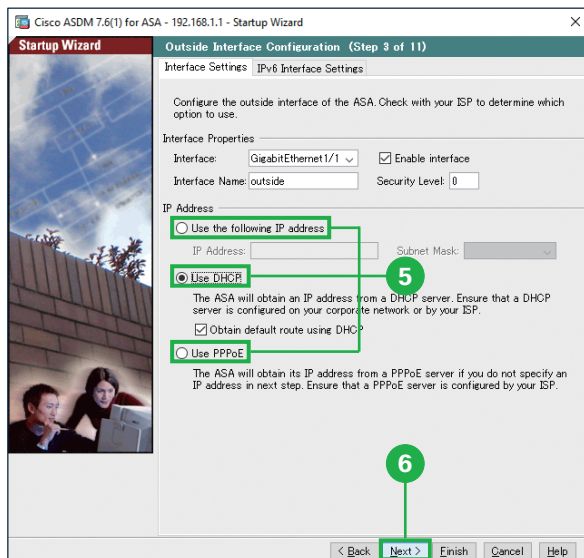


- 2 [Modify existing configuration] をクリック
- 3 [Next] をクリック



#### 4 [Next] をクリック

必要に応じて [ASA Host Name] を変更および [Domain Name] を入力できます。



#### 5 適切な WAN 接続オプションを選択

ASA の WAN 接続オプションとして、外部 (outside) インターフェイスを設定します。既存ルータの「下位で」ASA を使用する場合は、一般的には DHCP を使用します。既存ルータの「代わりに」ASA を使用する場合は、ルータの設定、たとえば PPPoE の設定を引き継ぎます。

#### 6 [Next] をクリック

## 7 [Next] をクリック

## ⚠ 注意

内部 (inside) インターフェイスには外部 (outside) インターフェイスとは異なる範囲の IP アドレスを割り当てる必要があります。たとえば、外部の範囲が「192.168.1.x」の場合は、内部の範囲を「192.168.10.x」のように割り当てます。変更したいインターフェイス (ここでは [inside]) を選択して [Edit] をクリックすれば、IP アドレスの範囲を設定できます。

Cisco ASDM 7.6(1) for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Other Interface Configuration (Step 4 of 11)

Configure the remaining interfaces of the ASA. To configure an interface, select it in the list below and click Edit.

Interface	Name	Enabl...	Security Level	IP Address	Subnet Mask/...
GigabitEthernet1/1	outside	Yes	0 (DHCP)		(DHCP)
GigabitEthernet1/2	inside	Yes	100	192.168.1.1	255.255.255.0
GigabitEthernet1/3		No			
GigabitEthernet1/4		No			
GigabitEthernet1/5		No			
GigabitEthernet1/6		No			
GigabitEthernet1/7		No			
GigabitEthernet1/8		No			
Management1/1		Yes			

Enable traffic between two or more interfaces with the same security levels  
 Enable traffic between two or more hosts connected to the same interface

< Back **Next >** Finish Cancel Help

## 8 [Next] をクリック

必要に応じてスタティック ルートを設定できます。

Cisco ASDM 7.6(1) for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Static Routes (Step 5 of 11)

Specify static routes.

Filter:  IPv4  IPv6 only  IPv4 only

Interface	IP Address	Netmask/ Prefix	Gateway IP	Metric/ Distance	Options
-----------	------------	--------------------	------------	---------------------	---------

Add Edit Delete

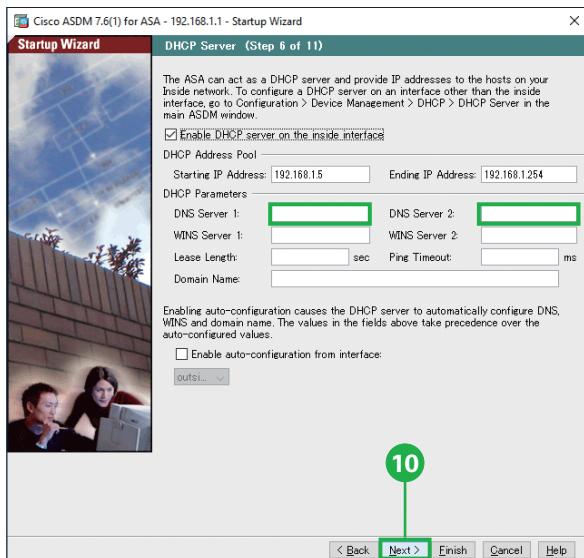
< Back **Next >** Finish Cancel Help

## 9 [Next] をクリック

ASA は DHCP サーバとして機能して、ネットワーク内部のデバイスに IP アドレスを配布します。

### MEMO

Cisco Umbrella の DNS サービスを利用する場合、[DNS Server 1] に「208.67.222.222」、[DNS Server 2] に「208.67.220.220」を入力します。



Cisco ASDM 7.6(1) for ASA - 192.168.1.1 - Startup Wizard

**Startup Wizard** DHCP Server (Step 6 of 11)

The ASA can act as a DHCP server and provide IP addresses to the hosts on your inside network. To configure a DHCP server on an interface other than the inside interface, go to Configuration > Device Management > DHCP > DHCP Server in the main ASDM window.

Enable DHCP server on the inside interface

DHCP Address Pool

Starting IP Address: 192.168.1.5 Ending IP Address: 192.168.1.254

DHCP Parameters

DNS Server 1: [ ] DNS Server 2: [ ]

WINS Server 1: [ ] WINS Server 2: [ ]

Lease Length: [ ] sec Ping Timeout: [ ] ms

Domain Name: [ ]

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and domain name. The values in the fields above take precedence over the auto-configured values.

Enable auto-configuration from interface:

outs...

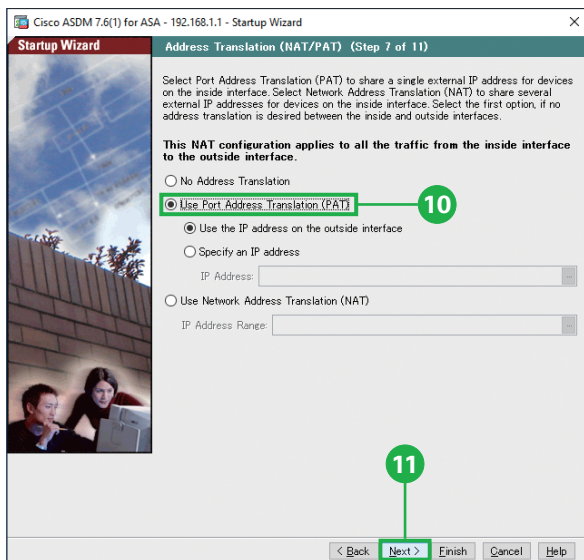
< Back **Next >** Finish Cancel Help

10

## 10 [Use Port Address Translation (PAT)] をクリック

[Use Port Address Translation (PAT)] を選択することで、ネットワーク内部のデバイスと単一の外部 IP アドレスを共有します。[Use Network Address Translation (NAT)] を選択することで、ネットワーク内部のデバイスと複数の外部 IP アドレスを共有します。

## 11 Click [Next] をクリック



Cisco ASDM 7.6(1) for ASA - 192.168.1.1 - Startup Wizard

**Startup Wizard** Address Translation (NAT/PAT) (Step 7 of 11)

Select Port Address Translation (PAT) to share a single external IP address for devices on the inside interface. Select Network Address Translation (NAT) to share several external IP addresses for devices on the inside interface. Select the first option, if no address translation is desired between the inside and outside interfaces.

**This NAT configuration applies to all the traffic from the inside interface to the outside interface.**

No Address Translation

**Use Port Address Translation (PAT)**

Use the IP address on the outside interface

Specify an IP address

IP Address: [ ]

Use Network Address Translation (NAT)

IP Address Range: [ ]

< Back **Next >** Finish Cancel Help

11

## 12 [Next] をクリック

HTTPS/ASDM、SSH、または Telnet を使用して ASA にアクセスできる、デバイスやネットワークのアドレスを設定できます。

Cisco ASDM 7.6(1) for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard Administrative Access (Step 8 of 11)

Specify the addresses of all hosts or networks, which are allowed to access the ASA using HTTPS/ASDM, SSH or Telnet.

Type	Interface	IP Address	Mask/Prefix Length
HTTPS/AS	inside	192.168.1.0	255.255.255.0

Enable HTTP server for HTTPS/ASDM access  
 Disabling HTTP server will prevent HTTPS/ASDM access to this ASA.

Enable ASDM history metrics

## 13 ASA Firepower モジュールの IP アドレスを入力

たとえば、「192.168.1.2」であれば、ASA のデフォルトの内部 IP アドレス「192.168.1.1」と共存できます。

## 14 デフォルト ゲートウェイの IP アドレスを入力

ASA の内部 IP アドレスを入力します。たとえば、デフォルトの内部 IP アドレスは「192.168.1.1」です。

## 15 [Next] をクリック

Cisco ASDM 7.6(1) for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard ASA FirePOWER Basic Configuration (Step 9 of 11)

In order to establish proper connectivity with the ASA FirePOWER service blade, please enter all necessary information.

Note: ASA FirePOWER-related configuration is intended for bootstrapping. Modifying an existing ASA FirePOWER configuration may lead to undesired results.

Select to Bypass ASA FirePOWER Configuration.

Network Settings

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

## 16 [Next] をクリック

必要に応じて、自動アップデート サーバを設定します。

Cisco ASDM 7.6(1) for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Auto Update Server (Step 10 of 11)

The ASA can be remotely managed from an Auto Update Server. This includes automatical updating the ASA configuration, ASA image, and ASDM image as needed.

Enable Auto Update for ASA

Server

Server URL: http:// / /

Verify server's SSL certificate

User

Specify the username and password to login to the auto update server.

Username:

Password:  Confirm Password:

Device Identity

Specify the device ID to uniquely identify the ASA.

Device ID Type: --None--

Device ID: None

< Back Next > Finish Cancel Help

## 17 [Finish] をクリック

スタートアップ ウィザードの完了です。[Finish] をクリックして ASA に設定内容を送信します。設定を変更したい場合は、[Back] をクリックして戻ります。

Cisco ASDM 7.6(1) for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Startup Wizard Summary (Step 11 of 11)

You have completed the Startup Wizard. To send your changes to the ASA, click Finish. If you want to modify any of the data, click Back.

Configuration Summary:

Host Name: ciscoasa

Domain Name:

Outside interface: outside (GigabitEthernet1/1), Configured as DHCP Client

Other named interfaces: inside (GigabitEthernet1/2), 192.168.1.1

No static routes configured.

DHCP Server is enabled on Inside interface. Pool: 192.168.1.5 - 192.168.1.254

PAT is configured on inside interface.

Administrative access to the device: HTTPS/ASDM access for 192.168.1.0 through inside

ASA FirePOWER

IP Address: 192.168.1.2

Netmask: 255.255.255.0

Gateway: 192.168.1.1

< Back Next > Finish Cancel Help

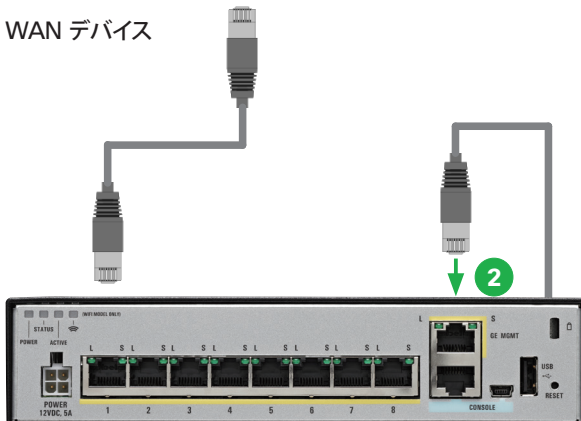
## 3-3

## スイッチを ASA に接続する

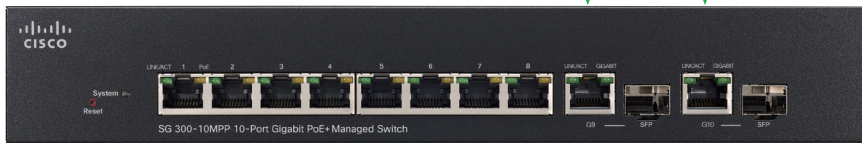
スタートアップ ウィザードが完了したら、ASDM を終了して PC からイーサネット ケーブルを抜きます。それから、次の手順に従ってスイッチを ASA に接続します。スイッチにはイーサネット ケーブルを接続しない状態で始めます。また、スイッチ が DHCP を使用して IP アドレスを自動的に取得する設定になっているかどうか、および ASA と WAN デバイスが 1 本目のイーサネット ケーブルで接続されたままの状態であることも、確認してください。



WAN デバイス



スイッチ



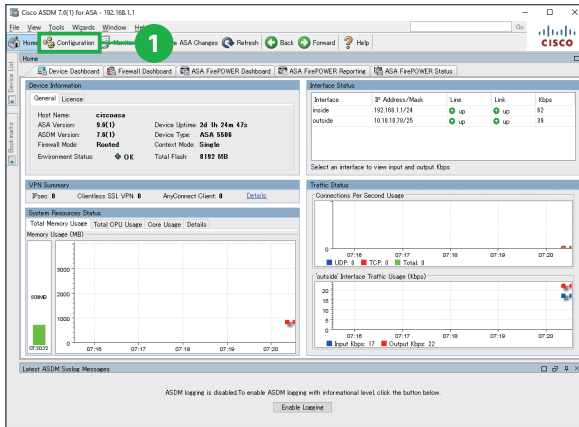
- 1 2 本目のイーサネット ケーブルを ASA のイーサネット ポート 2 とスイッチのイーサネット ポートに接続
- 2 3 本目のイーサネット ケーブルを ASA の GE MGMT ポートとスイッチのイーサネット ポートに接続



## 3-4

# ライセンスをインストールする

ここまでの手順で、Cisco ASDM を使用して ASA Firepower モジュールにアクセスできるようになりました。ASDM を再起動して、ライセンスをインストールします。デフォルトで提供される「Application Visibility and Control (AVC) ライセンス」のアクティベーション キーを取得するための PAK (Product Authorization Key) は、プリントアウトされて製品に同梱されています。その他のライセンスを購入した場合の PAK は電子メールで提供されます。



- 1 ASDM を起動して [Configuration] をクリック

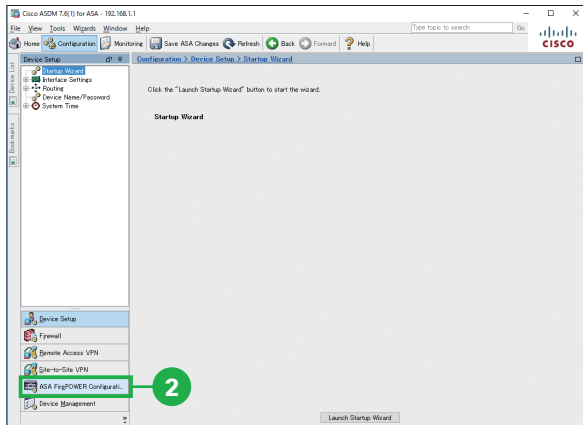
### MEMO

Cisco ASA with Firepower Services には、デフォルトで **Application Visibility and Control (AVC)** ライセンスが付属しています。オプションで **Next-Generation IPS (NGIPS)**、**Cisco Advanced Malware Protection (AMP)**、および **URL フィルタリング (URL)** ライセンスを購入することで、さらに高度な機能を追加できます。

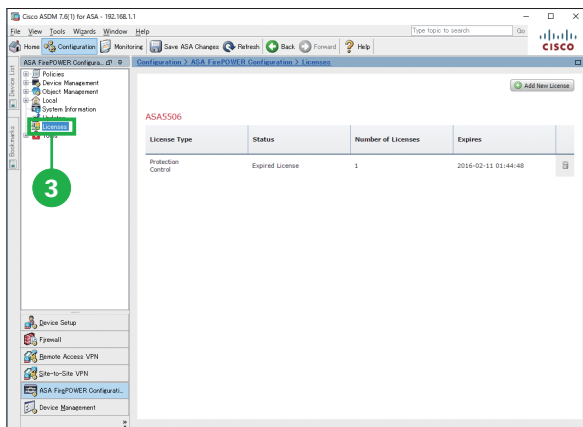
- **AVC** : 3,000 を超えるアプリケーションの識別および制御機能が使用できます。
- **NGIPS** : きわめて効果的な脅威保護と、ユーザ、インフラストラクチャ、アプリケーション、およびコンテンツに対するフル コンテキスト認識機能を備え、マルチベクトルな脅威も検出し、防御対策を自動化します。
- **AMP** : 高度なマルウェアに対してインライン ネットワーク保護および Cisco Threat Grid サンドボックスを提供します。
- **URL** : 2.8 億以上のトップレベルのドメインをリスク レベルごとに 82 以上のカテゴリにフィルタリングできます。



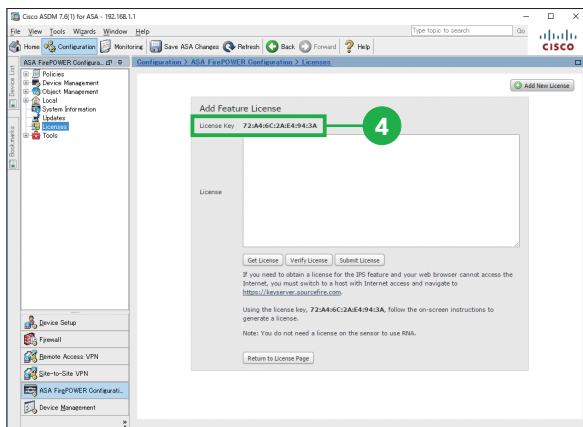
2 [ASA FirePOWER Configuration] をクリック



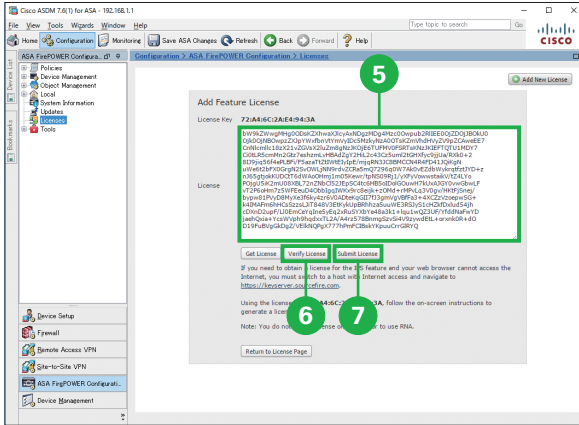
3 [Licenses] をクリック



4 [License Key] の右横に表示されている文字列をコピーして、ライセンシング ポータルからライセンス アクティベーションキーを取得 (次ページ下部のMEMO を参照)



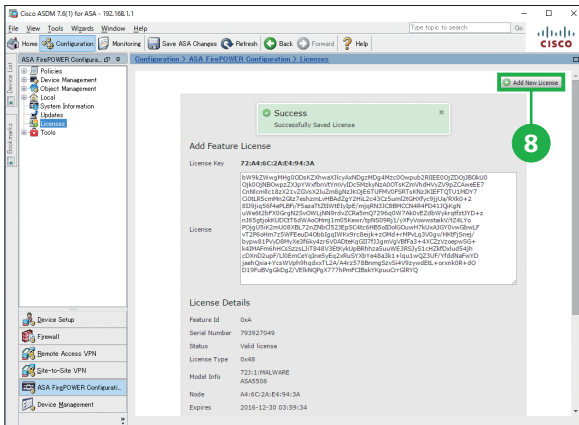
ライセンス キーは、たとえば「72:78:DA:6E:D9:93:35」のようなカンマ区切りの文字列です。



5 ライセンス アクティベーション キーを [License] 欄にペースト

6 [Verify License] をクリック

7 [Submit License] をクリック



8 さらにライセンスを追加する場合は [Add New License] をクリックして5から7の手順をくり返す



## MEMO

ライセンス (ライセンス アクティベーション キー) はライセンスング ポータルで取得します。

1. ブラウザで <http://www.cisco.com/go/license> にアクセス
2. [Get New Licenses] 欄に PAK を入力して [Fulfill] をクリック
3. [License Key] に④でコピーした文字列をペースト、さらにメール アドレスを入力
4. 表示された [license activation key] をコピー (または自動配信されたメールに添付された zip ファイルを解凍、テキスト エディタで開いてコピー)

## 4

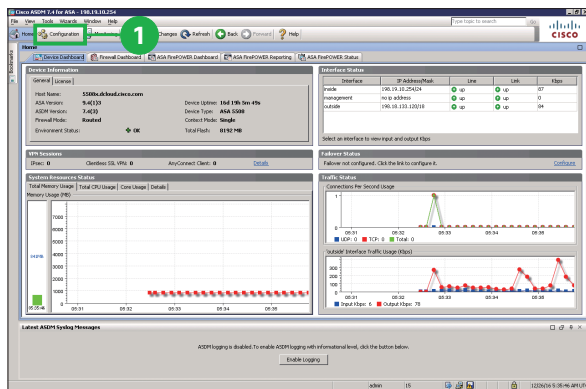
## Umbrella DNS の設定

Cisco ASA ではオプションで、無料かつ高速な「Cisco Umbrella」グローバル ネットワーク DNS サービスに接続して、ASA からインターネットに流れるあらゆるトラフィックを可視化するとともに、快適なインターネット接続をユーザに提供できます。Umbrella への接続は、次の手順に従って簡単に、5 分以内で設定できます。

また、Umbrella ではトラフィックの可視化だけでなく、DNS レイヤのセキュリティ サービスも追加できます。無料のトライアルで、この DNS レイヤ セキュリティを体験できます。

## 4-1 Umbrella を設定する

Cisco ASDM を起動して、Umbrella を DNS フォワーダとして使用するよう ASA 内部の DNS サーバを設定します。



1 ASDM を起動して、[Configuration] をクリック

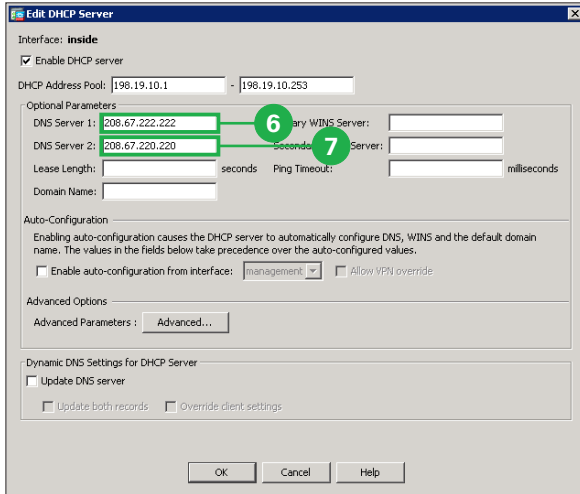
## MEMO

ASA がネットワーク内部の DNS サーバを DNS フォワーダとして使用する必要がある場合、ASA ではなく DNS サーバ上で、Umbrella の IP アドレス「208.67.222.222」および「208.67.220.220」を DNS フォワーダとして使用するよう設定する必要があります。

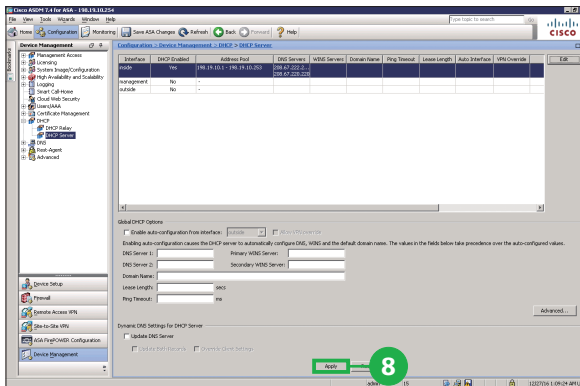


6 [DNS Server 1] 欄に  
「208.67.222.222」を入力

7 [DNS Server 2] 欄に  
「208.67.220.220」を入力

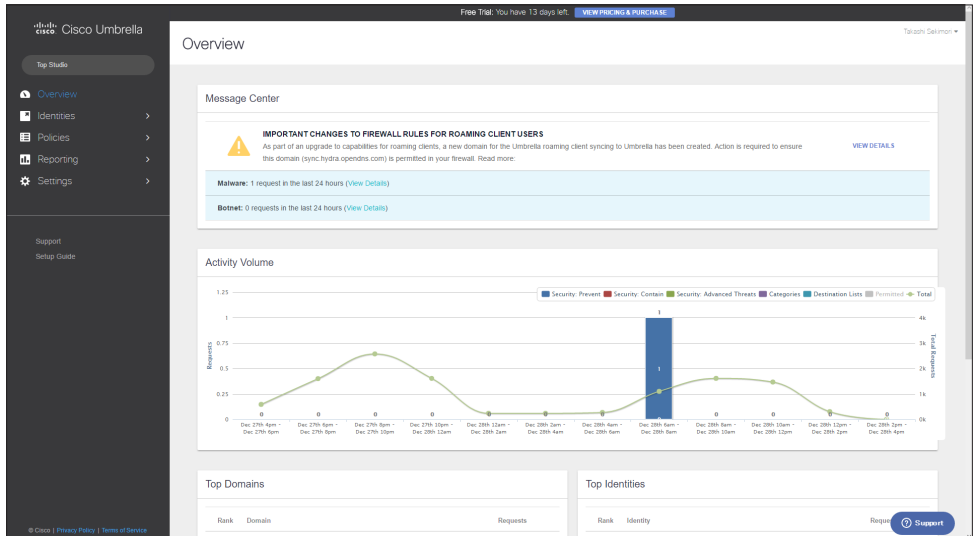


8 [Apply] をクリック



Cisco ASA での設定が完了したら、Umbrella にサインアップして、次のいずれかのサービスの利用を開始します。

- **無料のプレミアム DNS** (<https://signup.opendns.com/premiumdns>):  
無料かつ高速なリカーシブ DNS サービスを提供します。ASA からインターネットに流れるあらゆるトラフィックを可視化します。
- **無料の 14 日間トライアル** (<https://signup.opendns.com/freetrial>):  
トラフィックの可視化に加えて、DNS レイヤのセキュリティ サービスを試用できます。このトライアルへのサインアップにはクレジットカードも電話も必要ありません。次の機能を体験できます。
  - ・比類のない脅威防御：マルウェア、C2 サーバへのコールバック、フィッシングを阻止
  - ・予防に寄与するインテリジェンス：脅威防御を自動化して攻撃が実行される前に検知
  - ・世界中をカバー、迅速な導入：ハードウェアのインストールやソフトウェアのメンテナンスが不要
  - ・セキュリティレポート：マルウェア要求など、セキュリティのサマリーを毎週メール送信



一般的な次世代ファイアウォールは、アプリケーションやユーザに対するアクセスコントロールによってリスクを軽減しますが、脅威を完全に消し去ることはできません。攻撃者はオープンな Web 接続や承認されたアプリケーションを巧妙に利用するからです。より優れた防御手段を得るためには、ネットワーク全体を縦横無尽に洞察して可視化する能力、脅威を特定するためのインテリジェントな自動化機能を適用して動的なネットワーク環境に対応する能力、攻撃を迅速に精査および回復してダメージを最小化する能力が必要です。Cisco ASA with Firepower Services は、これらの能力をすべて備えています。この最新の次世代ファイアウォールにアップグレードして、大切なデジタル資産を保護しましょう。

機能	一般的な次世代ファイアウォール	Cisco ASA with FirePOWER Services
NSS Labs の侵入検知システムおよび次世代 IPS テストで最高スコアを獲得	▲	●
レピュテーションに基づくプロアクティブな防御	-	●
インテリジェントなセキュリティ自動化	-	●
ファイル レピュテーション、ファイルトラジェクトリ、レトロスペクティブ分析	-	●
アプリケーションの可視化と制御 (AVC)	●	●
単一のデバイスによる高度なマルウェア防御 (AMP) と次世代 IPS	▲	●
タイムリーな脅威防御を提供するために、脅威情報を毎日アップデート	▲	●

旧モデル	FW + AVC	FW + AVC + IPS	現行モデル	FW + AVC	FW + AVC + IPS
Cisco ASA 5505	-	-	Cisco ASA 5506-X	250 Mbps	125 Mbps
Cisco ASA 5510	-	-	Cisco ASA 5508-X	450 Mbps	250 Mbps
Cisco ASA 5512	300 Mbps	150 Mbps	Cisco ASA 5516-X	850 Mbps	450 Mbps
Cisco ASA 5515-X	500 Mbps	250 Mbps	Cisco ASA 5516-X	850 Mbps	450 Mbps

# お問い合わせ方法

電話または E メールにてお問い合わせください。

## Cisco Start テクニカル サポート総合受付窓口

電話 **0120-092-255**

「ご希望の番号を選択してください」という自動音声ガイダンスの後、  
電話機のプッシュ番号 **3 番**  
(製品/サービスご購入後の技術的なサポートについてのお問い合わせ) を押します。  
続いて **7 番** (シスコスタート) を押してください。  
最後に **3 番** (ワイヤレス製品) を選択してください。

E メール **start-jp@cisco.com**

受付時間：平日 午前 9 時～午後 18 時 (土日祝日は休み)  
※時間外のお問い合わせは翌営業日の受付となります。

製品サポート期間：購入元にご確認ください。  
ご返答までの目安：受付後、翌営業日までに担当エンジニアよりご連絡いたします。  
※ 5 営業日を目安に復旧策/回避策をご提供いたします。

## お問い合わせに必要な情報

お問い合わせの際には、以下の情報をご用意ください。

E メールでお問い合わせの際には、こちらのテキストと必要事項を記入して送信してください。

### <ご担当者情報>

- ・ご担当者のお名前 (漢字/ふりがな)：
- ・Cisco.com ID：
- ・会社名 (漢字/ふりがな)：
- ・住所 (漢字/ふりがな)：
- ・電話番号：
- ・FAX 番号：
- ・E メール アドレス：

### <製品情報>

- ・シリアル番号：
- ・問題の内容：
- ・製品設置先住所 (漢字/ふりがな)：
- ・サービス契約番号 (お持ちの場合のみ)：

©2017 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書期またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は 2017 年 6 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー  
<http://www.cisco.com/jp>

お問い合わせ先