CISCO START
Simple Secure Smart

# Cisco ASA with Firepower Services

# Easy Setup Guide

You can easily set up your ASA in this step-by-step guide.

1. Connecting PC to ASA
2. Installing ASDM
3. Configuring ASA
4. Using Umbrella DNS

CISCO

# 1 Connecting PC to ASA

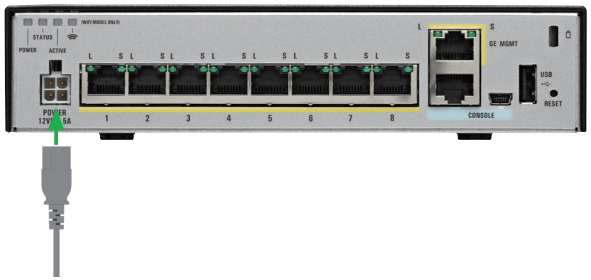
## 1-1 Before You Begin

Before you begin the installation, make sure that you have the following equipment:

- ASA Chassis
- AC Power Cable (& Supply with ASA 5506-X)
- Ethernet Cable x 3
- PC

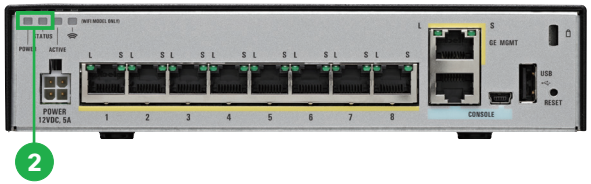
Make sure that nothing is connected to the ASA and your PC settings are configured to use DHCP.

## 1-2 Connecting PC to ASA



**1** Connect the AC power cable to the AC power connector of the ASA and a grounded AC outlet.

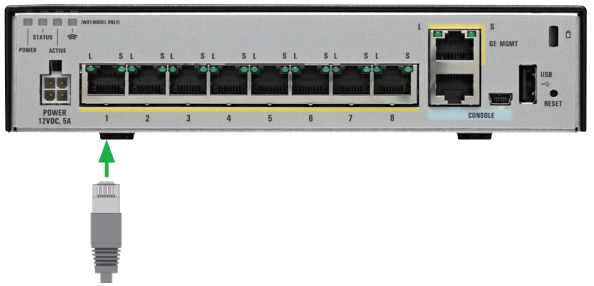
The power turns on automatically when you plug in the power cable. There is no power button.




**2** Confirm that the POWER LED and STATUS LED are solid green.

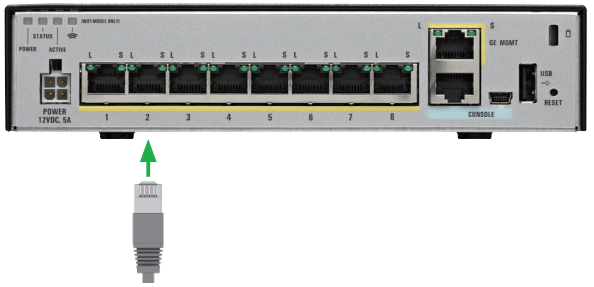
If the POWER LED is solid green, the device is powered on. After the STATUS LED is solid green, the system has passed power-on diagnostics.





**3** Connect the first Ethernet cable to the Ethernet port #1 of the ASA, and the other end of the cable to the Ethernet port of your WAN device.

Wait until the port LEDs on the ASA and your WAN device are green or blinking green. Green LEDs indicate a successful connection.



**4** Connect the second Ethernet cable to the Ethernet port #2 of the ASA, and the other end of the cable to the Ethernet port of your PC.

Wait until the port LEDs on the ASA and your PC are green or blinking green. Green LEDs indicate a successful connection.

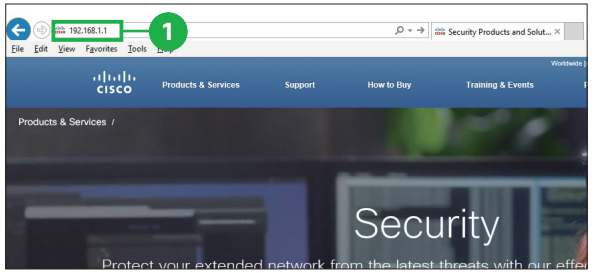
**Caution**

At step ❷, if the STATUS LED does not turn solid green, or turns amber, the ASA failed the power-on diagnostics, reconnect the AC power cable to the ASA AC power connector and a grounded AC outlet. Nevertheless the STATUS LED does not turn solid green, or turns amber, contact your Cisco representative or reseller.

At step ❸ & ❹, the ASA port to connect an Ethernet cable is the RJ-45 Ethernet port, not the RJ-45 management port. The RJ-45 Ethernet ports are numbered.

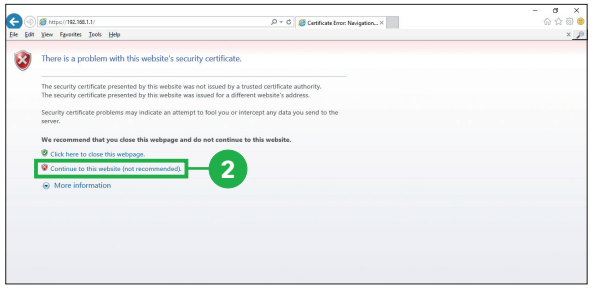
# 2 Installing ASDM

To configure the ASA, use the Cisco Adaptive Security Device Manager (ASDM). Follow these steps to download the Cisco ASDM from the ASA and install it to your PC.




**1** Launch a Web browser PC and enter the IP address "https://192.168.1.1" into the address bar, then press Enter key.

Depending on your environment, the security certificate page appears.



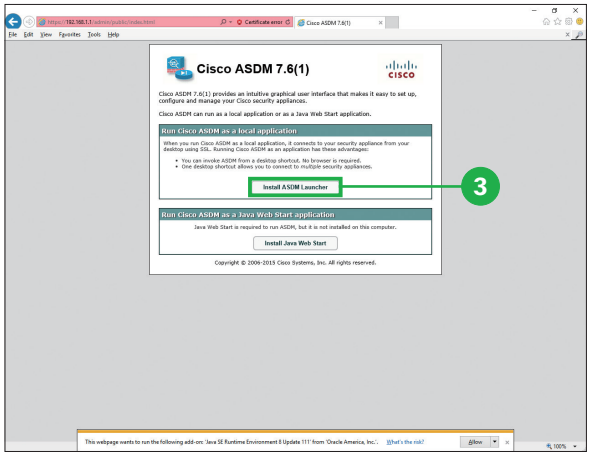

**2** Click [Continue to this website (not recommended)].

The Cisco ASDM web page appears.

**Caution**

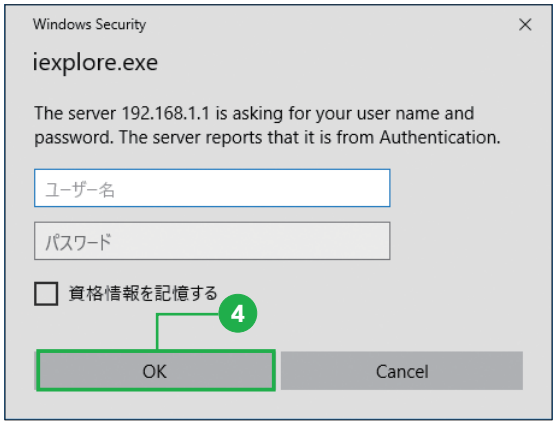
If the Cisco ASDM web page does not appear, make sure that:

- The POWER LED and STATUS LED are solid green.
- You connect a straight-through cable to an Ethernet port on the ASA.
- Any pop-up blockers or proxy settings on your browser are disabled and that any wireless client is disabled on your PC or laptop.
- Your PC settings use DHCP. The ASA acts as a DHCP server. If your PC has a static IP address, temporarily configure your PC settings to use DHCP.



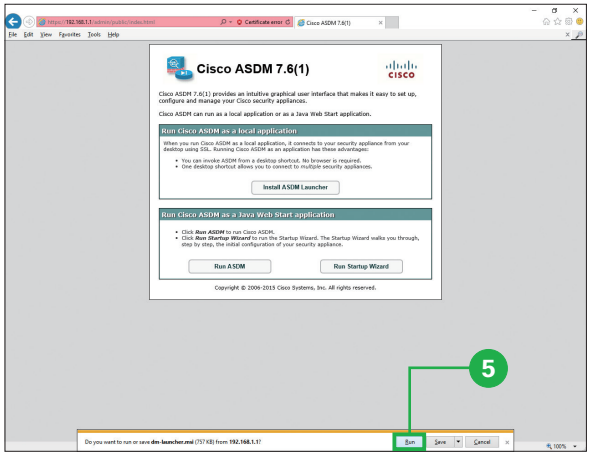

**3** Click [Install ASDM Launcher].

Depending on your environment, the authentication dialog box appears.



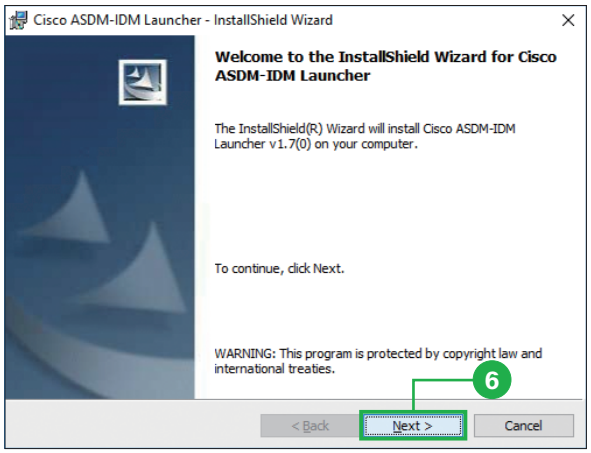

**4** Click [OK].

Leave the username and password fields empty.

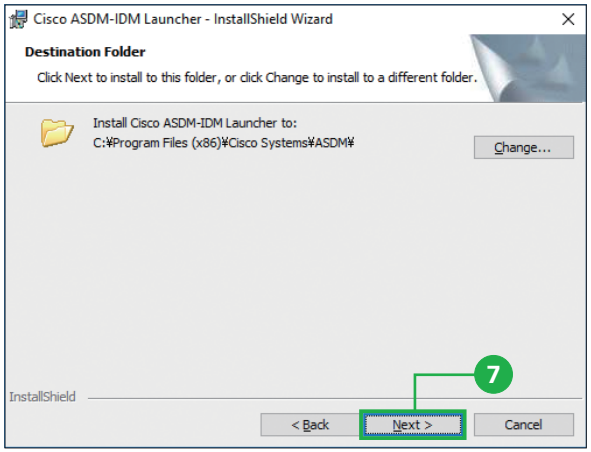



**5** Click [Run].

The InstallShield Wizard for Cisco ASDM Launcher appears.

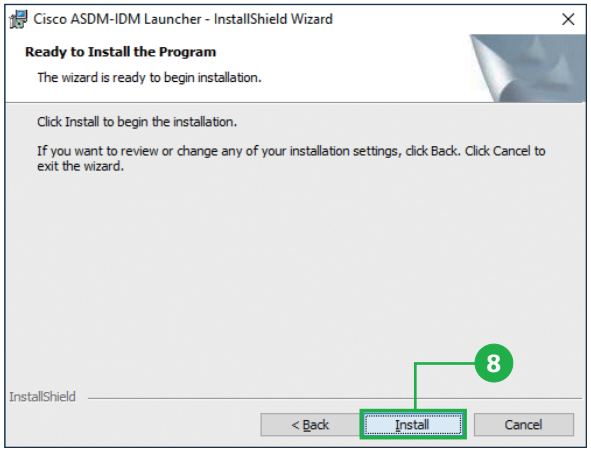



**6** Click [Next].

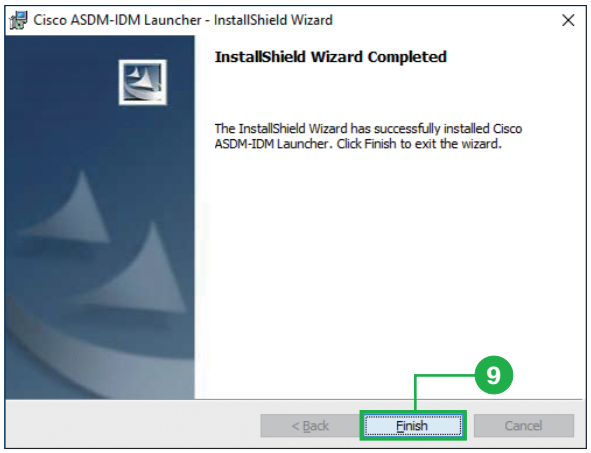



**7** Click [Next].

If you want to change the default installation folder, click [Change] and enter or choose the desired installation folder.




**8** Click [Install].




**9** Click [Finish].

The Cisco ASDM Launcher appears.

**⚠ Caution**

Your PC must meet the following requirements to run Cisco ASDM.

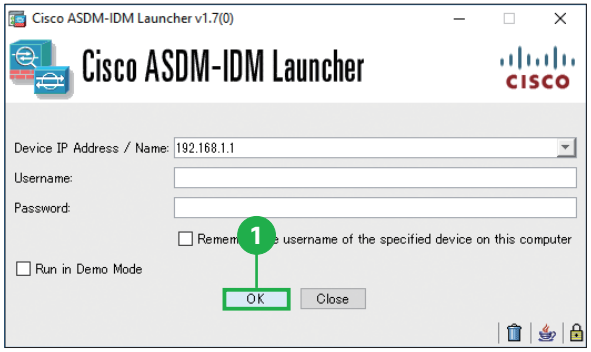
- Microsoft Windows 7, 8:
  - Microsoft Internet Explorer
  - Mozilla Firefox
  - Google Chrome
  - Java SE Plug-in 7.0 or later
- Apple OS X 10.4 and later
  - Mozilla Firefox
  - Apple Safari
  - Google Chrome (64-bit version only)
  - Java SE Plug-in 7.0 or later

You can also use Microsoft Windows 8.1, 10 (but they are not officially supported).

# 3 Configuring ASA

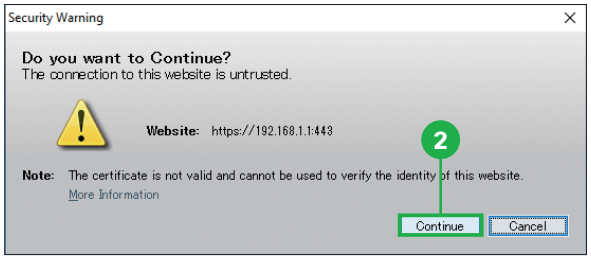
## 3-1 Launching ASDM

Now you can launch the Cisco ASDM with the Cisco ASDM Launcher.

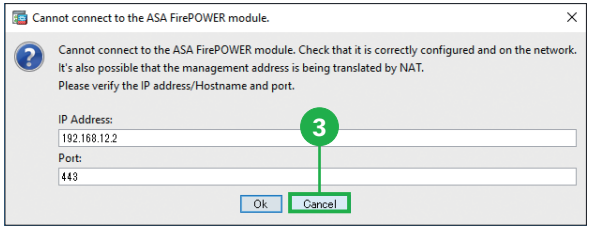



**1** Click [OK.]

Leave the username and password fields empty. The Security warning appears.




**2** Click [Continue].




**3** Click [Cancel].

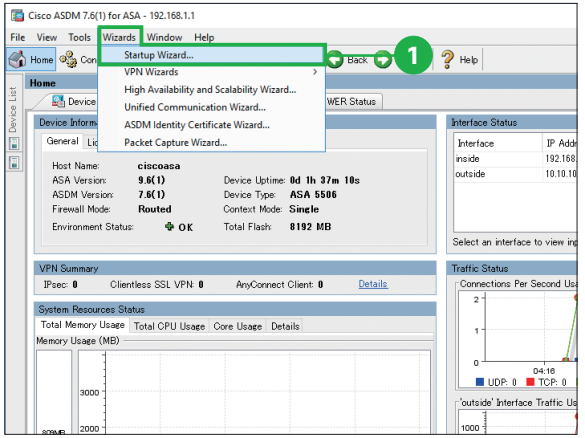
The main ASDM window appears.

**MEMO**

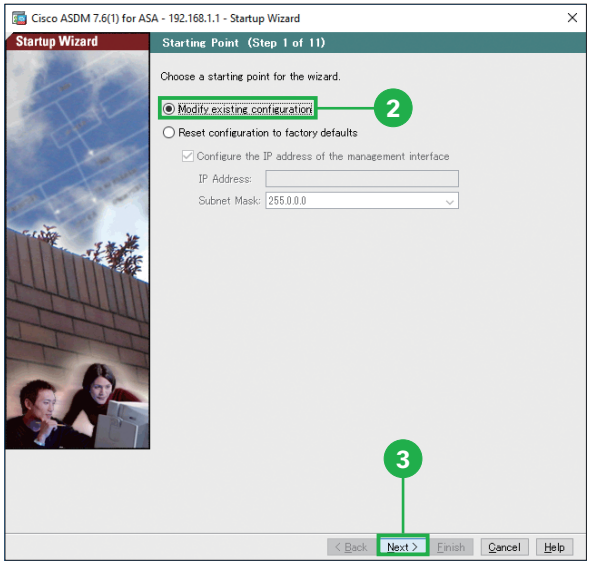
At step **3**, you are prompted to provide the IP address of the ASA Firepower module. You can later set the module IP address to the correct IP address using the Startup Wizard.

## 3-2 Launching Startup Wizard

After launching ASDM, use the Startup Wizard to perform initial configuration.

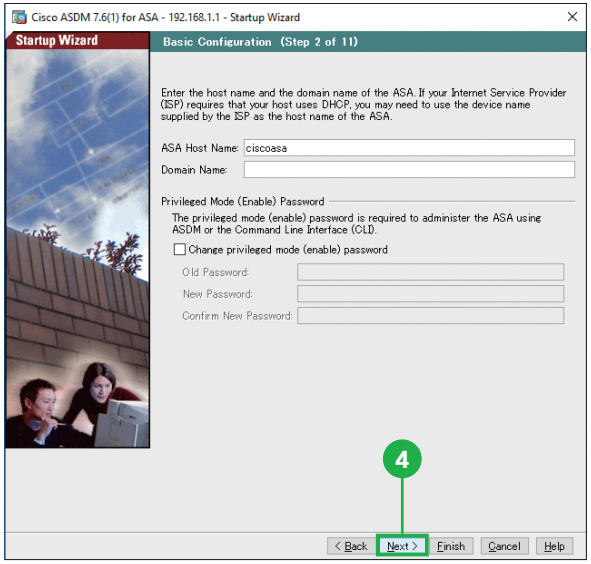



**1** Click [Startup Wizard] from the [Wizards] menu bar.



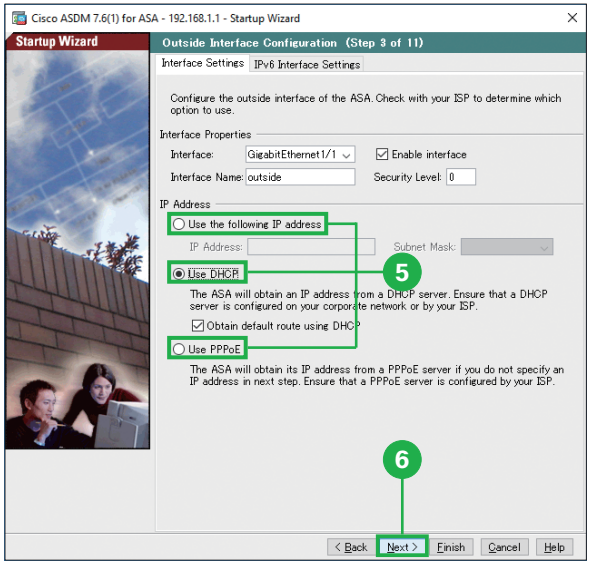

**2** Click [Modify existing configuration].

**3** Click [Next].




## 4 Click [Next].

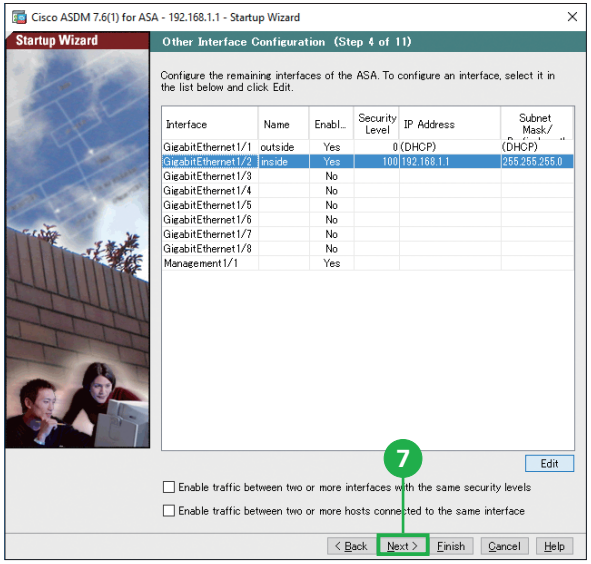
You can enter the host name and the domain name of the ASA.




## 5 Select the appropriate option.

Configure the outside interface of the ASA. If you use the ASA "behind" the existing router, select [Use DHCP] in most cases. If you use the ASA "instead of" the existing router, follow the configuration of the router.

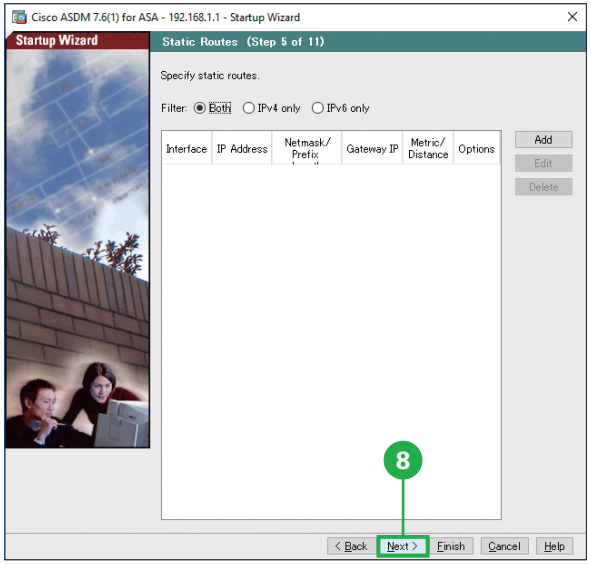
## 6 Click [Next].




## 7 Click [Next].

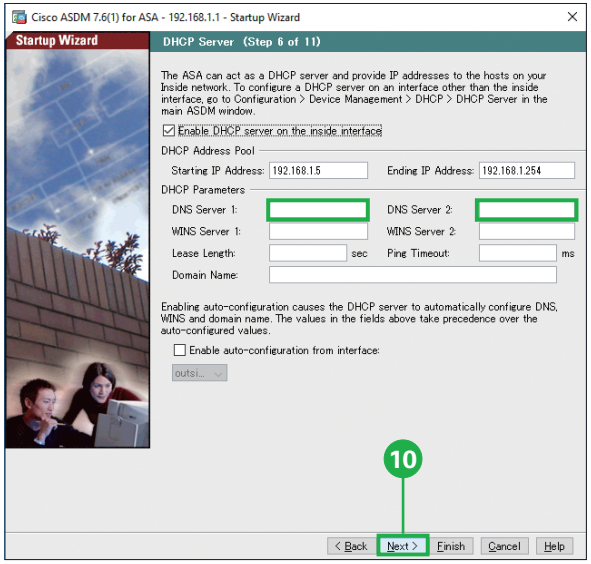
**Caution**

To the inside interfaces, you must assign the range of IP addresses different from the range assigned to the outside interface. For example, if the outside range is 192.168.1.x, the inside range should be 192.168.10.x, and so on. You can change the range by selecting an interface and clicking [Edit].




## 8 Click [Next].

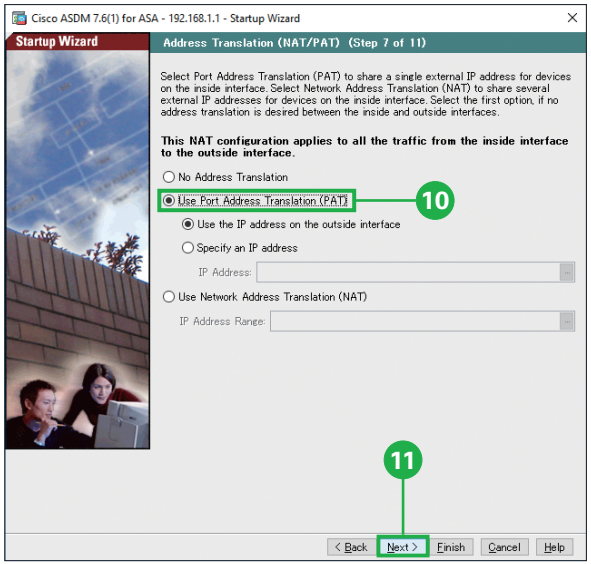
You can specify static routes if your network has multiple routers.




**9** Click [Next].

The ASA can act as a DHCP server and provide IP addresses to the hosts on your inside network.

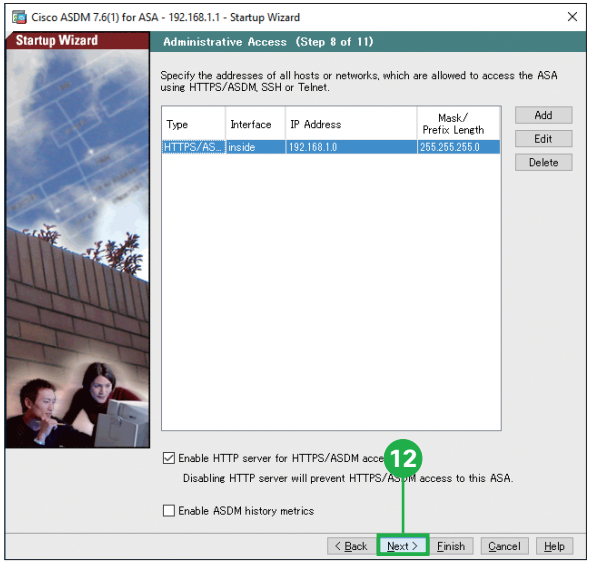
> **MEMO**
> To connect to the free and fast Cisco Umbrella global network DNS service, enter the "208.67.222.222" in the [DNS Server 1] field and the "208.67.220.220" in the [DNS Server 2] field.




**10** Click [Use Port Address Translation (PAT)].

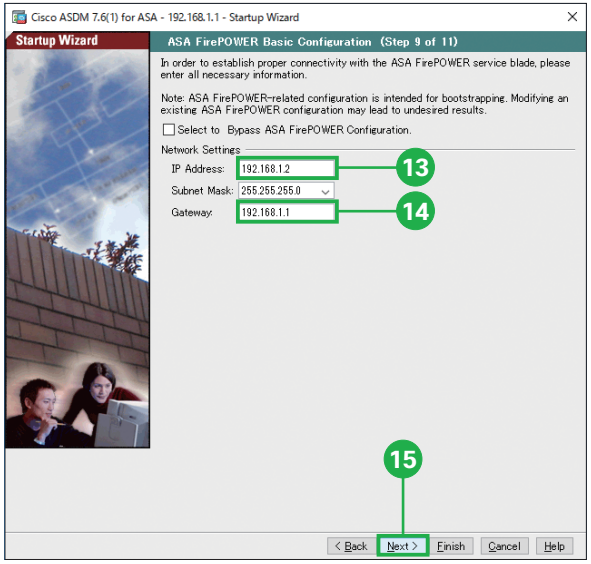
Select [Use Port Address Translation (PAT)] to share a single external IP address for devices on the inside interface. Select [Use Network Address Translation (NAT)] to share several external IP address for devices on the inside interface.

**11** Click [Next].




**12** Click [Next].

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



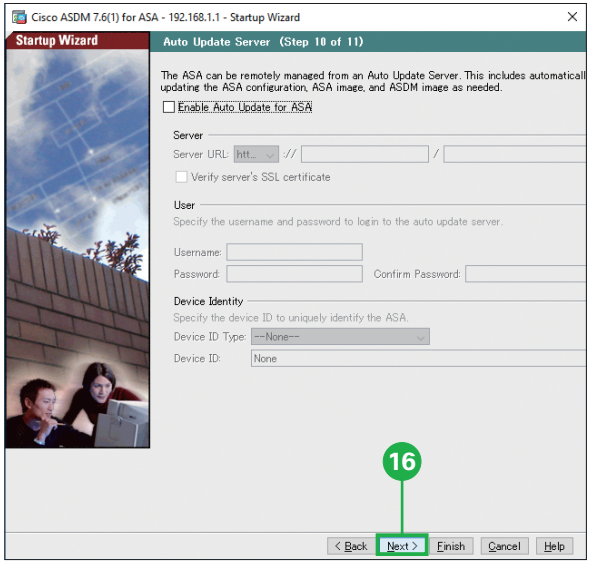

**13** Enter the IP address for the ASA Firepower module.

For example, the "192.168.1.2" works with the default configuration.

**14** Enter the IP address of the Default Gateway.

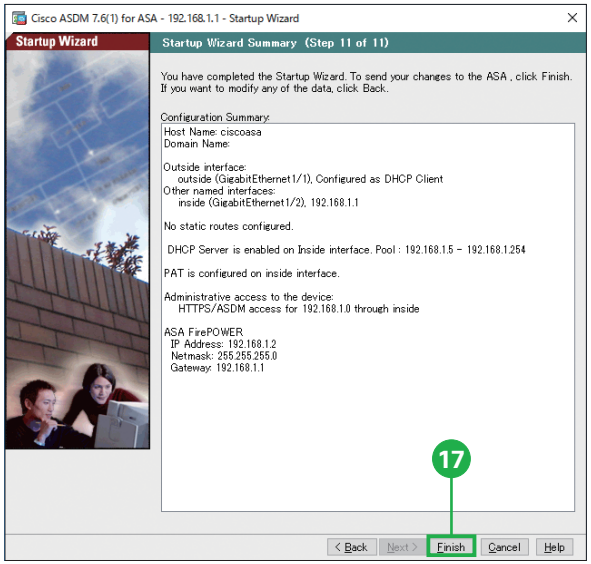
For example, the "192.168.1.1" works with the default configuration.

**15** Click [Next].




**16** Click [Next].

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

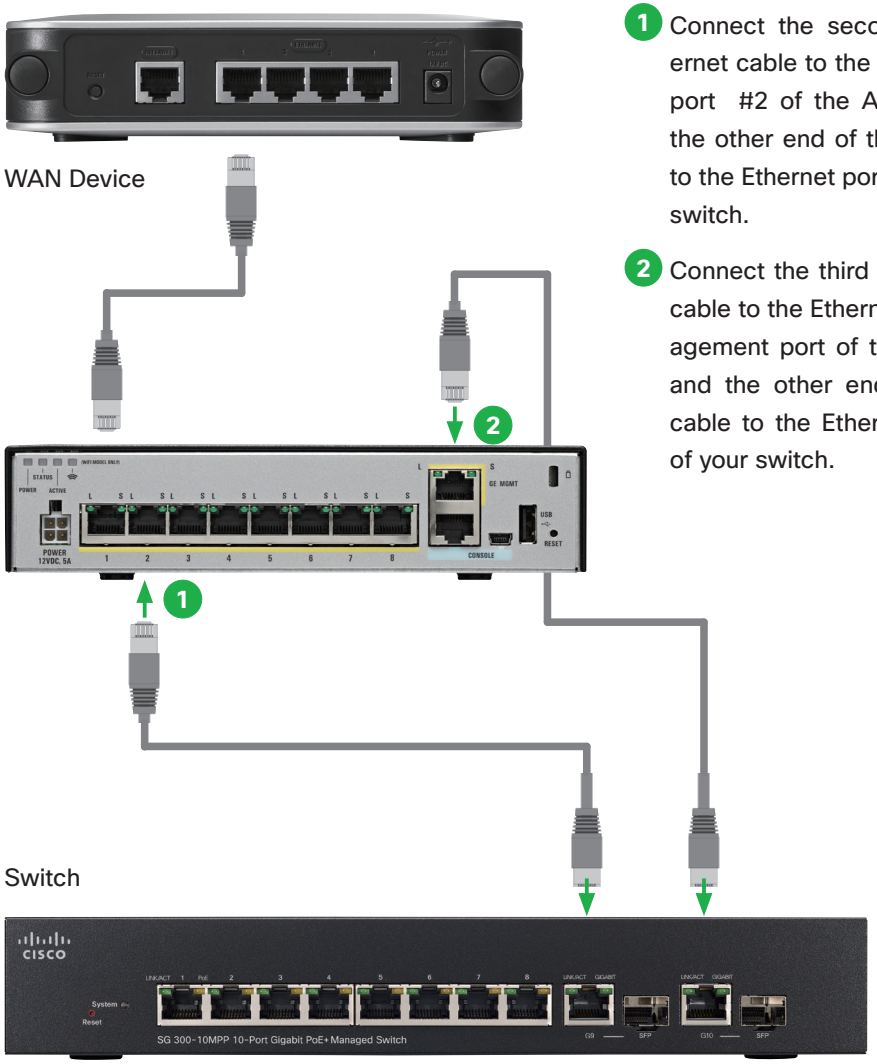



**17** Click [Finish].

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].

# 3-3 Connecting Switch to ASA

After completing the Startup Wizard, exit the ASDM and disconnect the Ethernet cable from your PC. Then, follow these steps to connect your switch to the ASA. Make sure that nothing is connected to the switch, its settings are configured to use DHCP, and the first Ethernet cable is still connected between the ASA and your WAN device.

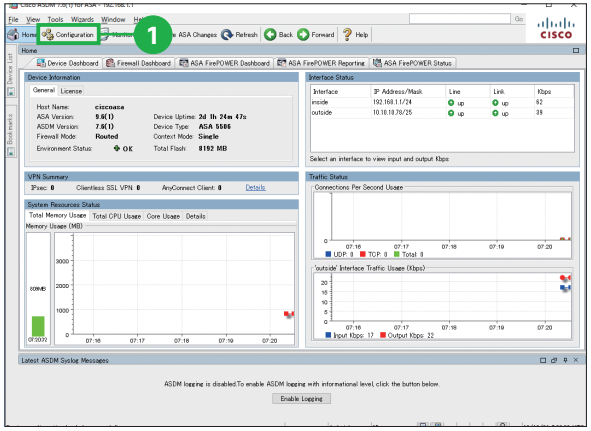



**1** Connect the second Ethernet cable to the Ethernet port #2 of the ASA, and the other end of the cable to the Ethernet port of your switch.

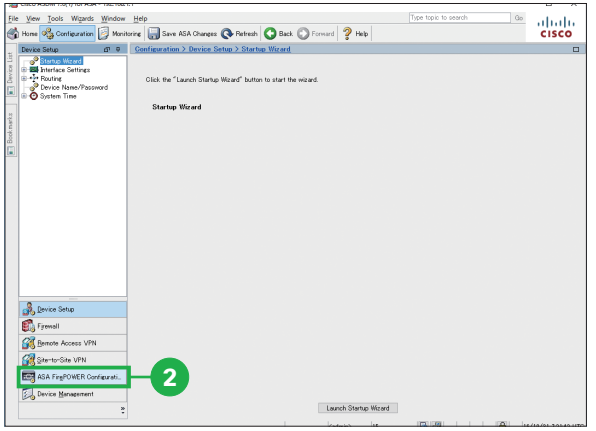
**2** Connect the third Ethernet cable to the Ethernet management port of the ASA, and the other end of the cable to the Ethernet port of your switch.

# 3-4 Install Licenses

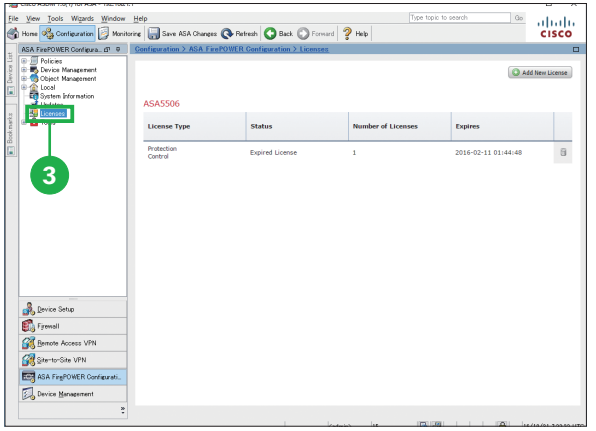
Now you can access to the ASA Firepower module with the Cisco ASDM. Relaunch the Cisco ASDM and install the licenses. The Control and Protection licenses are provided by default and the Product Authorization Key (PAK) is included on a print-out in your box. If you ordered additional licenses, you should have PAKs for those licenses in your email.



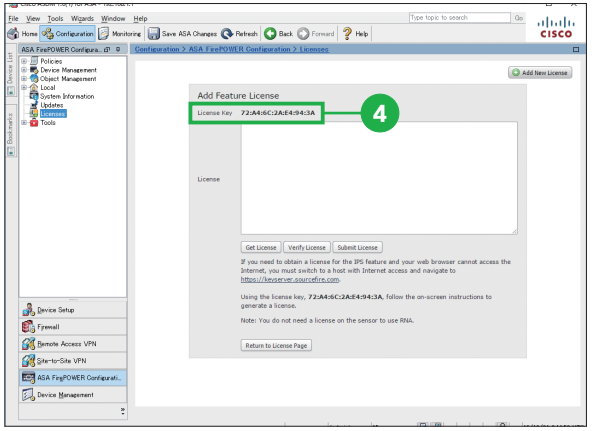

1 Launch ASDM and Click [Configuration].




2 Click [ASA FirePOWER Configuration].




3 Click [Licenses].



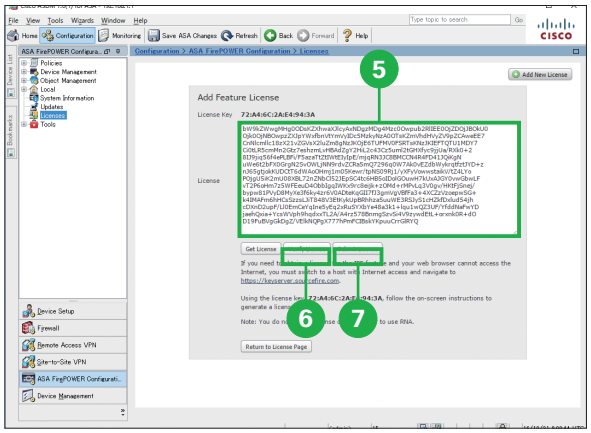

4 Copy [License Key] text and get the license from the licensing portal (see the MEMO in the next page).

The example of the License Key is 72:78:DA:6E:D9:93:35.

**MEMO**

The Cisco ASA with Firepower Services ship with a base license for **Application Visibility and Control (AVC)**. Optional subscriptions for **Next-Generation IPS (NGIPS)**, **Cisco Advanced Malware Protection (AMP)**, and **URL Filtering (URL)** can be added to the base configuration for advanced functionality.

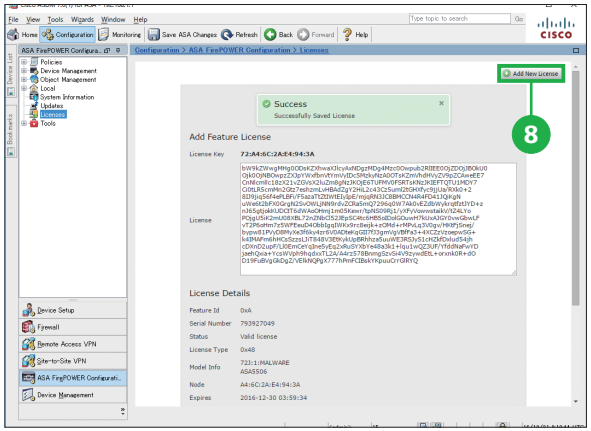
- **AVC**: Supports more than 3,000 application-layer and risk-based controls that can launch tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.
- **NGIPS**: Provides highly effective threat prevention and full contextual awareness of users, infrastructure, applications, and content to detect multivector threats and automate defense response.
- **AMP**: Delivers inline network protection against sophisticated malware and Cisco Threat Grid sandboxing.
- **URL**: Adds the capability to filter more than 280 million top-level domains by risk level and more than 82 categories.




5 Paste the license activation key into [License] box.

6 Click [Verify License].

7 Click [Submit License].




8 If you have additional licenses, click [Add New License] and repeat the steps 5 to 7.

**MEMO**

You can get the license (license activation key) from the **licensing portal**.

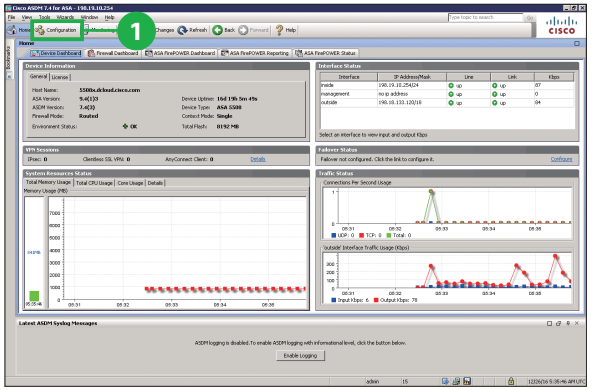
1. Go to **http://www.cisco.com/go/license**.
2. Enter the PAKs separated by commas in the **Get New Licenses** field, and click **Fulfill**.
3. You will be asked for the **License Key** and email address among other fields.
4. Copy the resulting **license activation key** from either the website display or from the zip file attached to the licensing email that the system automatically delivers.

# 4 Using Umbrella DNS

As the administrator of Cisco ASA, you are able to connect to the free and fast Cisco Umbrella global network DNS service which offers you visibility into all Internet traffic originating from your ASA, and result in a faster Internet experience for your users. If you then want to add an additional layer of DNS security to your ASA, the easy-to-establish connection to Umbrella enables you to access our free trial—which you can setup (by yourself) in less than five minutes.

## 4-1 Setting Up Umbrella

Launch the Cisco ASDM and configure internal DNS servers to use Umbrella as their DNS forwarders.

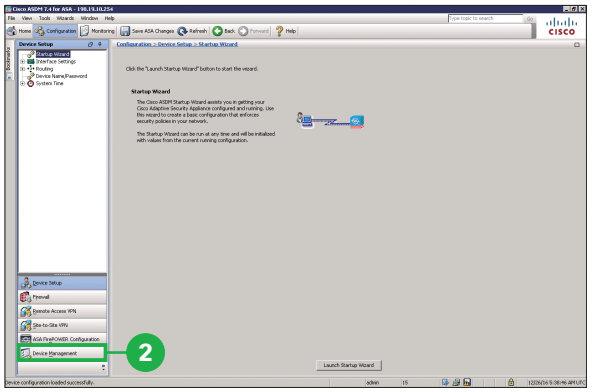



1 Launch ASDM and Click [Configuration].

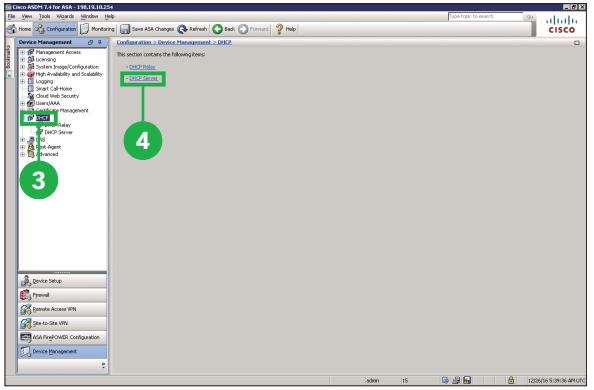
**MEMO**

If you are using a DNS forwarder as the primary DNS server for your network, update the server to use the Umbrella IP addresses of 208.67.222.222 and 208.67.220.220.

If you' re not certain whether you have a DNS forwarder on your ASA or DNS server, the best way to determine what needs to be changed is to see what device is being used as the DNS server for client workstations that are receiving DHCP from the network. This information is typically in the DNS section of the network adapter settings on the client workstation.

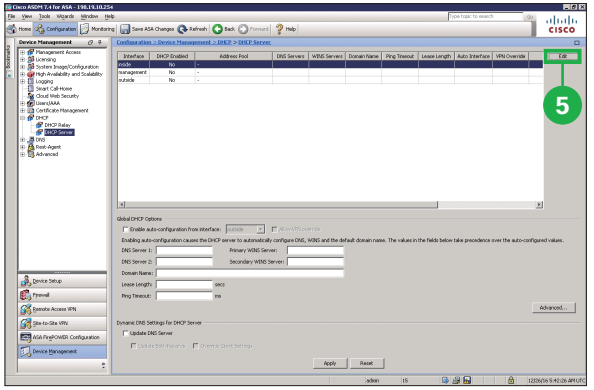



2 Click [Device Management].

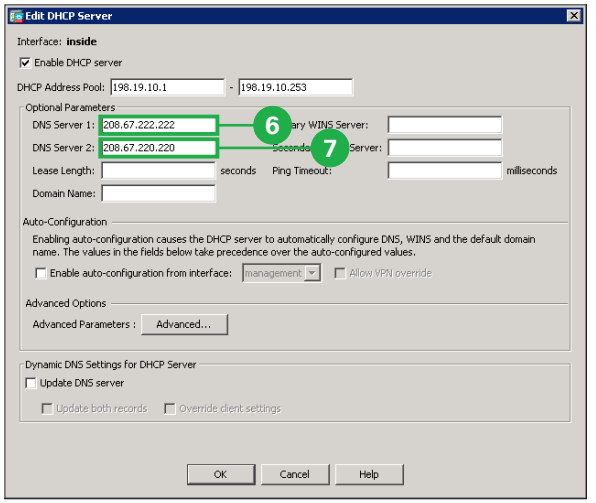



3 Click [DHCP] .

4 Click [DHCP Server] .

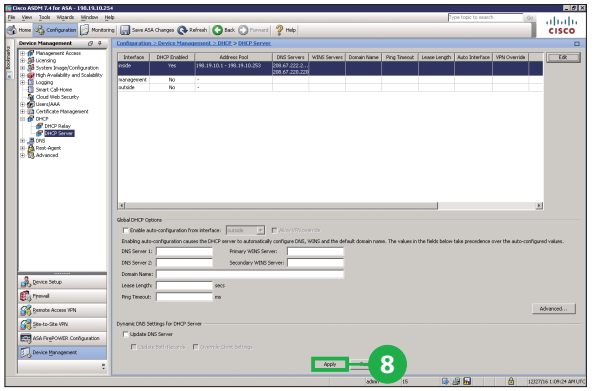



5 Click [Edit].




6 Enter “208.67.222.222” in the [DNS Server 1] field.

7 Enter “208.67.220.220” in the [DNS Server 2] field.




8 Click [Apply].

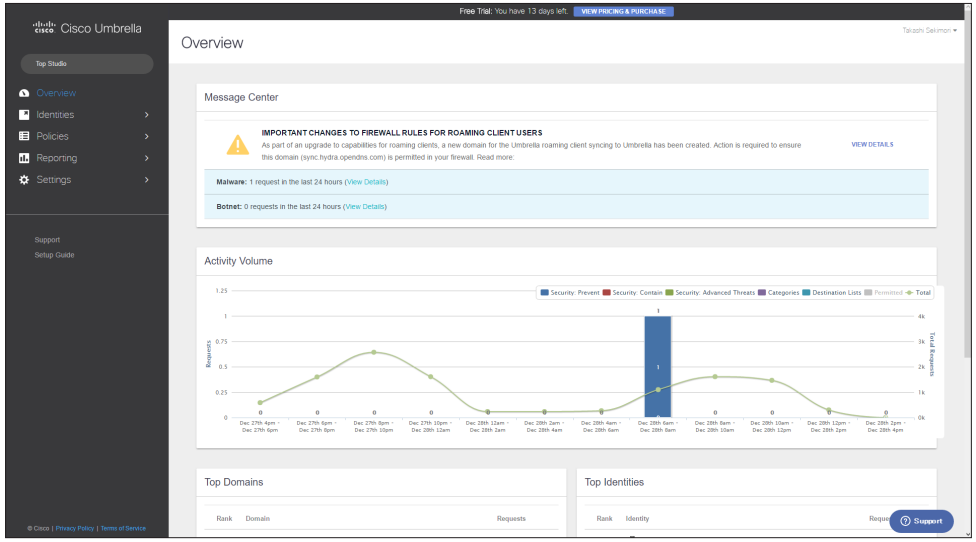
# 4-2 Signing Up for Umbrella

Once you' ve configured your Cisco ASA to point to Cisco Umbrella, you can sign up for either a free premium DNS account or a free 14-day trial of Umbrella.

- **Free Premium DNS** (https://signup.opendns.com/premiumdns):
  We offer a free, fast recursive DNS service which gives you visibility into all of your Internet traffic originating from your ASA device.

- **Free Umbrella 14-Day Trial** (https://signup.opendns.com/freetrial):
  If you want to add an additional layer of DNS security to your ASA, try our free trial—you can set it up yourself in less than five minutes, no credit card or phone call required. The trial includes:

  - Threat protection like no other — block malware, C2 callbacks, and phishing.
  - Predictive Intelligence — automates threat protection to detect attacks before they are launched.
  - Worldwide Coverage, Fast — no hardware to install or software to maintain.
  - Weekly security report — get a personalized summary of malware requests & more, directly to your inbox.



# Appendix Transition Guide

Most Next-Generation Firewalls (NGFWs) reduce risk by providing access control over applications and users. But they don' t eliminate threats because attackers can still exploit open web connections and approved applications. For superior protection, an NGFW must be able to provide deep visibility into and across the network, apply intelligent automation to identify threats, adapt protections to a dynamic network environment, and quickly scope and recover from attacks to minimize damage. Cisco ASA with Firepower Services delivers all of those capabilities, so upgrade to Cisco' s newest NGFW today and protect your high-value digital assets.

| Feature | Typical NGFW | Cisco ASA withFirepower Services |
|---|---|---|
| NSS Breach Detection and NGIPS Leadership Position Reports | Partial or Not Available | **Superior** |
| Reputation-Based Proactive Protection | Not Available | **Superior** |
| Intelligent Security Automation | Not Available | **Superior** |
| File Reputation, File Trajectory, Retrospective Analysis | Not Available | **Superior** |
| Application Visibility and Control (AVC) | Available | **Superior** |
| AMP and NGIPS in a Single Device | Limited | **Superior** |
| Threat Feeds Updated Daily from Security Intelligence to Provide Timely Threat Detection Capability | Limited | **Superior** |

| Legacy Models | FW + AVC | FW + AVC + IPS | Current Models | 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 |

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)