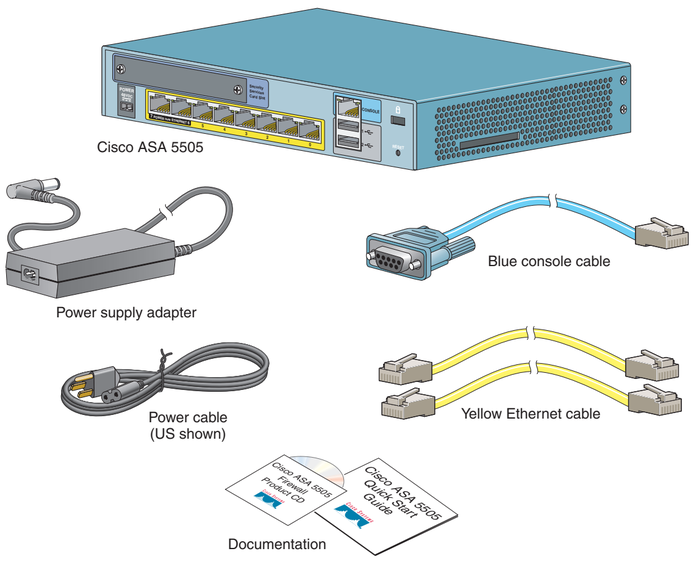
Before you install the Cisco ASA 5505 Adaptive Security Appliance, please read the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series Adaptive Security Appliance* document on Cisco.com or in the product CD that ships with the chassis.

1. Verifying the Package Contents



2. Installing the Chassis

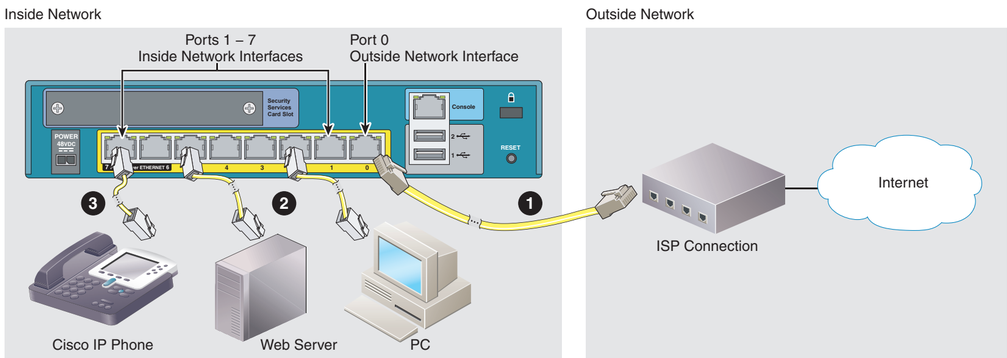
The adaptive security appliance ships with a default configuration that includes two preconfigured networks (the Inside network and the Outside network) and an Inside interface configured with dynamic addressing. Clients on the Inside network obtain a dynamic IP address from the adaptive security appliance so that they can communicate with each other as well as with devices on the Internet.

Step 1 Connect one end of a yellow straight-through Ethernet cable to port 0 on the adaptive security appliance. (By default, switch port 0 is the Outside interface.) Connect the other end to a cable/DSL/ISDN modem (the Outside network).

Step 2 Connect your devices (such as PCs, printers, and servers) with straight-through Ethernet cables to ports 1 through 7.

Note Connect a PC to the adaptive security appliance so that you can run Adaptive Security Device Manager (ASDM). See "4. Initial Configuration Considerations."

Step 3 Connect PoE devices (such as Cisco IP Phones or network cameras) with straight-through Ethernet cables to switch ports 6 or 7 (the only ports providing power to PoE devices).



If you connect a server (such as a web server) to the adaptive security appliance, you can use ASDM to make services on that server accessible by internal and external users. See "7. (Optional) Making Internal Services Accessible from the Internet."

3. Powering on and Verifying Interface Connectivity

Step 1 Connect the power supply adaptor to the power cable.

Step 2 Connect the rectangular connector of the power supply adaptor to the power connector on the rear panel of the adaptive security appliance.

Step 3 Connect the AC power connector of the power cable to an electrical outlet. (The adaptive security appliance does not have a power switch. Completing this step powers on the device.)

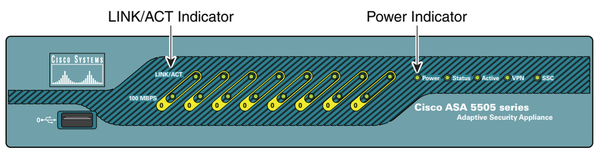
Step 4 Check the Power LED on the front of the adaptive security appliance; if it is solid green, the device is powered on.

Step 5 If you connected a PC to the adaptive security appliance to run ASDM, restart the PC. (The PC obtains a dynamic IP address from the adaptive security appliance and must be restarted.)

Step 6 Check the LINK/ACT indicators to verify interface connectivity.

Interface Connectivity

Each Ethernet interface has an LED to indicate a physical link is established. When the LED is solid green, a link is established. When the LED is flashing green, there is network activity.



If a LINK/ACT LED is not lit, the link could be down due to a duplex mismatch. If auto-negotiation is disabled, verify you are using a straight-through Ethernet cable.

For a description of all chassis components, see the *Cisco ASA 5500 Series Hardware Installation Guide* on the product CD or Cisco.com.

4. Initial Configuration Considerations

The adaptive security appliance ships with a default configuration that, in most cases, is sufficient for your basic deployment. You configure the adaptive security appliance by using Adaptive Security Device Manager (ASDM). ASDM is a graphical interface that allows you to manage the adaptive security appliance from any location by using a web browser.

However, changing certain settings is recommended or required. For example, you should change the following settings from their defaults:

- The privileged mode (enable) password that is required to administer the adaptive security appliance through ASDM and the CLI
- When using the adaptive security appliance as a VPN endpoint (using the SSL VPN features):
  - The hostname, domain name, and DNS server names
  - Setting a static Outside interface IP address
  - Creating an identity certificate
  - Configuring WINS names when access to Windows file shares is required

Use the Start up Wizard in ASDM to make these changes. See "6. Running the Startup Wizard in ASDM."

Requirements for Running ASDM

The PC connected to the adaptive security appliance must meet the following requirements to run ASDM.

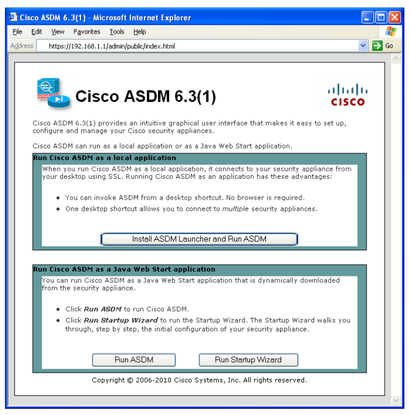
Operating System and Version	Browser
Microsoft Windows Vista	Internet Explorer 6.0 or higher with Sun Java (JRE)[1] 5.0 (1.5) or 6.0
Microsoft Windows XP	Firefox 1.5 or higher with Sun Java (JRE) 5.0 (1.5) or 6.0
Microsoft Windows 2003 Server (English or Japanese)	
Microsoft Windows 2000 (Service Pack 4 or higher)	
Apple Macintosh® OS X	Firefox 1.5 or 2.0 or Safari 2.0 with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0[2]
Red Hat Linux Desktop	Firefox 1.5 or higher with Sun Java (JRE) 5.0 (1.5) or 6.0
Red Hat Enterprise Linux WS version 4 running GNOME or KDE	

1. Obtain Sun Java from java.sun.com.
2. With Apple Macintosh, only 32-bit Java SE will be supported. Currently, this also excludes Java 6. The 32-bit Java can run on a 64-bit Mac OS.

5. Launching ASDM (Adaptive Security Device Manager)

Step 1 On the PC connected to the adaptive security appliance, launch a web browser. (Verify that Java and JavaScript are enabled in your web browser. See "Requirements for Running ASDM" for information.)

Step 2 In the Address field, enter the following URL: **https://192.168.1.1/admin**. The Cisco ASDM web page appears.



Step 3 Click **Run Startup Wizard**.

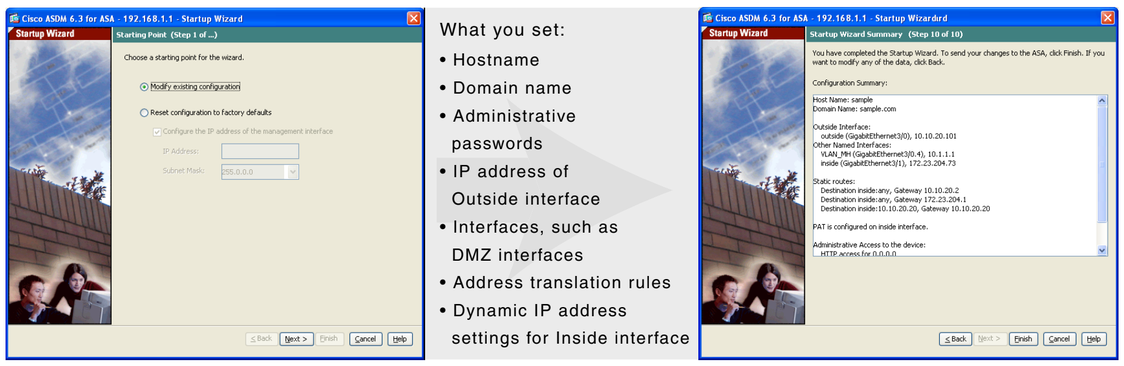
Step 4 Click **Yes** in each dialog box to accept the certificates. The Cisco ASDM-IDM Launcher appears.

Step 5 Leave the username and password fields empty and click **OK**.

The main ASDM window appears and the Startup Wizard opens. See "6. Running the Startup Wizard in ASDM."

6. Running the Startup Wizard in ASDM

Run the **Startup Wizard** to modify the default configuration so that you can customize the security policy to suit your deployment.



To run the Startup Wizard:

Step 1 In the main ASDM window, choose **Wizards > Startup Wizard**.

Step 2 Follow the instructions in the Startup Wizard to configure your adaptive security appliance.

If you get an error when launching the wizard requesting a DES license or a 3DES-AES license or you want to review your license information, choose **Configuration > Device Management > Licensing**.

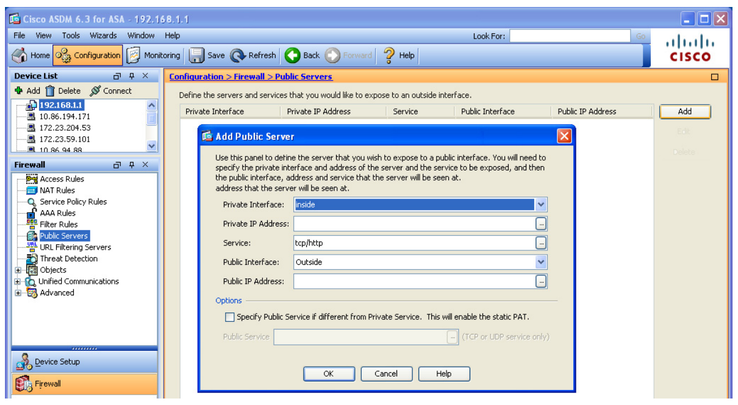
Step 3 While running the wizard, you can accept the default settings or change them as required. (For information about any wizard field, click **Help** in the window.)

After running the Startup Wizard, you can run other wizards to configure remote access with the adaptive security appliance. See "8. (Optional) Running the IPsec VPN Wizard in ASDM" and "9. (Optional) Running the SSL VPN Wizard in ASDM."

7. (Optional) Making Internal Services Accessible from the Internet

As a business owner, you might have internal network services, such as a web or FTP server, that need to be available to an outside user. You can place these services on a separate network behind the adaptive security appliance, called a demilitarized zone (DMZ). The adaptive security appliance allows limited access to the DMZ and only includes public servers. An attack there does not affect the Inside network.

The Public Servers pane displays a list of public servers, internal and external addresses, the interfaces that the internal or external addresses apply to, and the service that is exposed.



To set up public server access:

Step 1 In the main ASDM window, choose **Configuration > Firewall > Public Servers**. The Public Server pane appears.

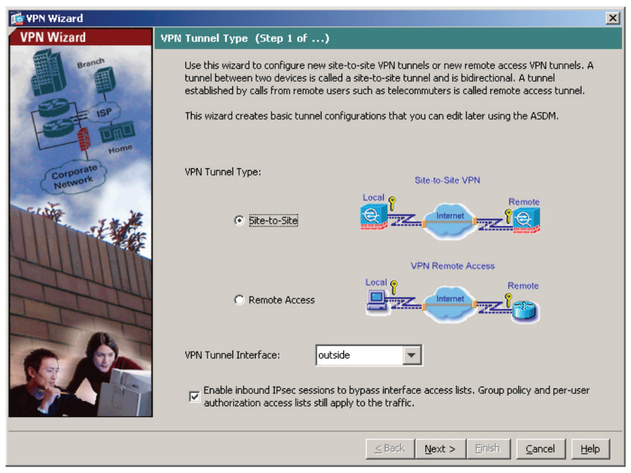
Step 2 Click **Add**, then enter the public server settings in the dialog box. (For information about any field, click **Help** in the dialog box.)

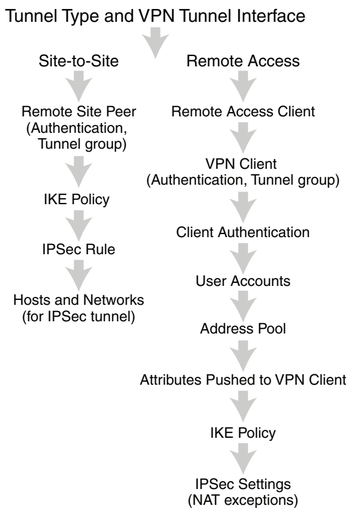
Step 3 Click **OK**. The server appears in the list.

Step 4 Click **Apply** to submit the configuration to the adaptive security appliance.

8. (Optional) Running the IPsec VPN Wizard in ASDM

The IPSec VPN Wizard helps you to configure basic site-to-site (or LAN-to-LAN) and remote access VPN connections.





To run the IPSec VPN Wizard:

Step 1 In the main ASDM window, choose **Wizards > IPSec VPN Wizard**.

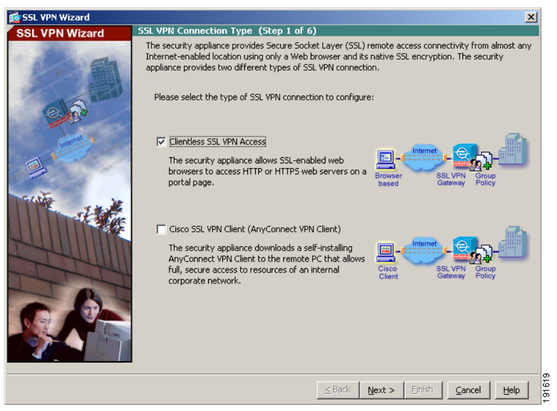
Step 2 Click a tunnel type, Site-to-Site or Remote Access, then follow the wizard instructions. (For information about any wizard field, click **Help** in the window.)

9. (Optional) Running the SSL VPN Wizard in ASDM

The SSL VPN Wizard enables you to configure an SSL VPN policy on your adaptive security appliance.

Clientless, browser-based SSL VPN lets users establish a secure, remote-access VPN tunnel to the security appliance using a web browser. After authentication, users access a portal page and can access specific, supported internal resources. The network administrator provides access to resources by users on a group basis. Users have no direct access to resources on the Inside network.

The Cisco AnyConnect VPN client provides secure SSL connections to the adaptive security appliance for remote users with full VPN tunneling to corporate resources. The adaptive security appliance downloads the AnyConnect Client to remote users.



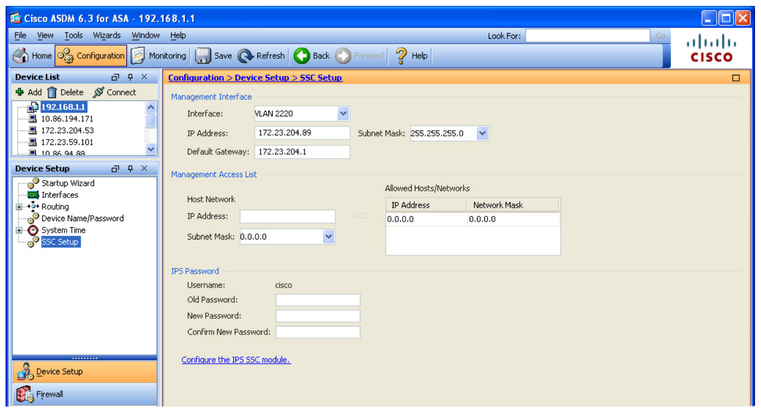
To run the IPSec VPN Wizard:

Step 1 In the main ASDM window, choose **Wizards > SSL VPN Wizard**.

Step 2 Select the SSL VPN connection type (Clientless, Cisco SSL, or both), and then follow the wizard instructions. (For information about any wizard field, click **Help** in the window.)

10. (Optional) Configuring the SSC in ASDM

If your adaptive security appliance came installed with a Security Services Card (SSC), you can use ASDM to set up the SSC and configure the Intrusion Prevention System (IPS) application to run on the SSC. An SSC does not have any external interfaces.



To set up the SSC and IPS:

Step 1 In the main ASDM window, choose **Configuration > Device Setup > SSC Setup**. The SSC pane appears.

Step 2 Complete the SSC setup fields and click **Apply**. (For information about any field, click **Help** in the dialog box.)

Step 3 To configure the IPS module on the SSC, click the Configure the IPS SSC module link. The Startup Wizard appears. Click **Launch Startup Wizard**. (Alternatively, you can choose **Configure > IPS > Sensor Setup > Startup Wizard** to access the wizard.)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.

Printed in the USA on recycled paper containing 10% postconsumer waste.

78-19188-01

QUICK START GUIDE

Cisco ASA 5505 Adaptive Security Appliance, Version 8.3