



QUICK START GUIDE



Cisco ASA 5510, ASA 5520, ASA 5540, ASA 5550

- 1 Verifying the Package Contents
- 2 Powering On the ASA
- 3 Maximizing Throughput (ASA 5550)
- 4 Connecting Interface Cables and Verifying Connectivity
- 5 Launching ASDM
- 6 Running the Startup Wizard
- 7 (Optional) Allowing Access to Public Servers Behind the ASA
- 8 (Optional) Running VPN Wizards
- 9 (Optional) Running Other Wizards in ASDM
- 10 Advanced Configuration

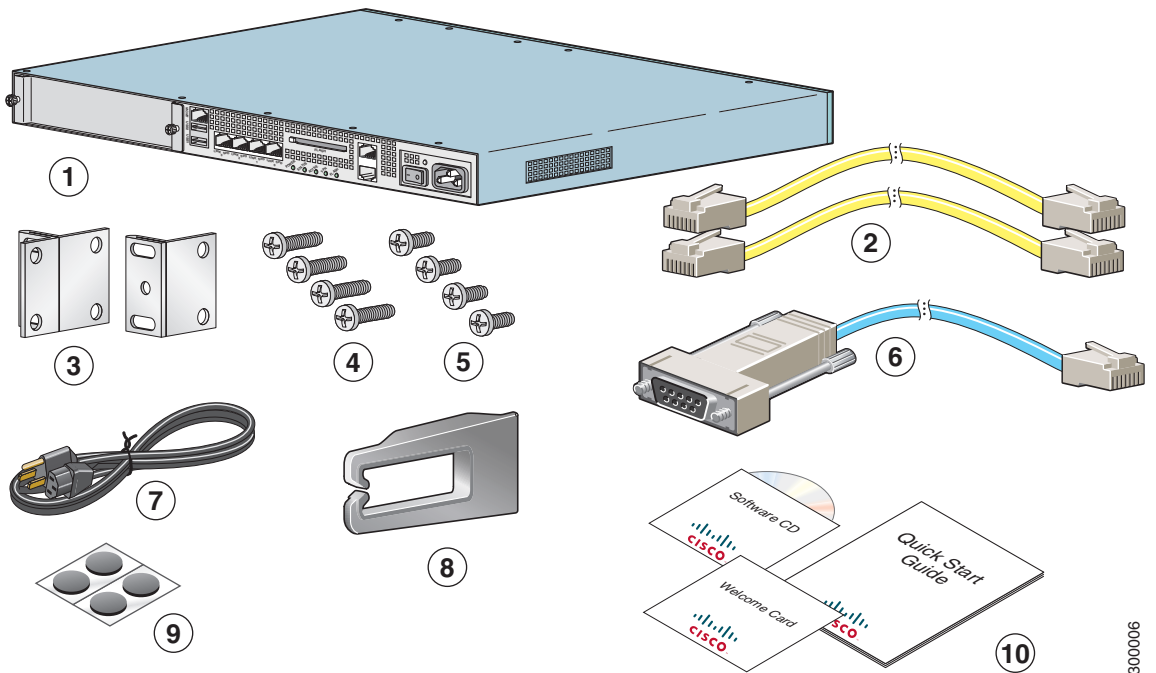
Regulatory Compliance and Safety Information

Read the safety warnings in the Regulatory Compliance and Safety Information (RCSI), and follow proper safety procedures when performing the steps in this guide. See <http://www.cisco.com/go/asadocs> for links to the RCSI and other documents.

1 Verifying the Package Contents

Verify the contents of the packing box to ensure that you have received all items necessary to install your ASA.

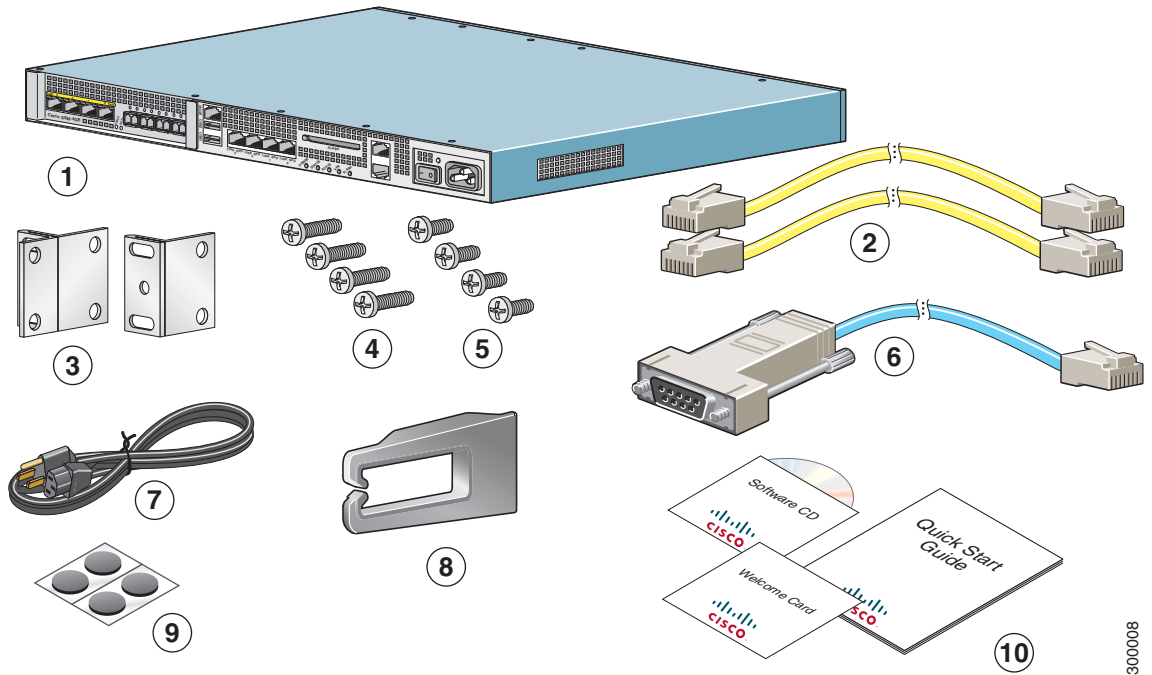
ASA 5510, ASA 5520, or ASA 5540



300006

1	ASA 5510, 20, or 40 Chassis	2	2 Yellow Ethernet Cables
3	Rack-mounting Brackets	4	4 10-32 Phillips Screws
5	4 12-24 Phillips Screws	6	Blue Console Cable PC Terminal Adapter
7	Power Cable (US Shown)	8	Cable Holder
9	4 Rubber Feet	10	Documentation and Software CD

ASA 5550



3000008

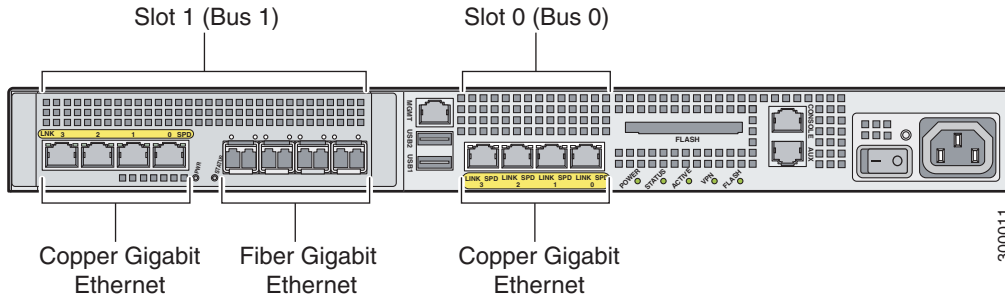
1	ASA 5550 Chassis	2	2 Yellow Ethernet Cables
3	Rack-mounting Brackets	4	4 10-32 Phillips Screws
5	4 12-24 Phillips Screws	6	Blue Console Cable PC Terminal Adapter
7	Power Cable (US Shown)	8	Cable Holder
9	4 Rubber Feet	10	Documentation and Software CD

2 Powering On the ASA

- Step 1** Attach the power cable to the ASA and connect it to an electrical outlet.
 - Step 2** Power on the ASA.
 - Step 3** Check the Power LED on the front of the ASA; if it is solid green, the device is powered on.
 - Step 4** Check the Status LED on the front of the ASA; after it is solid green, the system has passed power-on diagnostics.
-

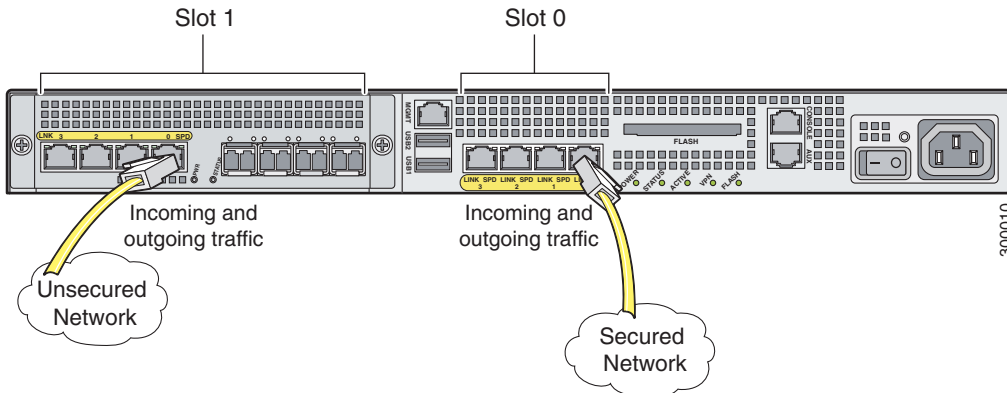
3 Maximizing Throughput (ASA 5550)

The ASA 5550 has two internal buses providing copper Gigabit Ethernet and fiber Gigabit Ethernet connectivity. For Slot 1 (Bus 1), you can use either the copper ports or the fiber ports. The copper ports are enabled by default.



For maximum throughput, configure the ASA so that traffic is distributed equally between the two buses. Lay out the network so that traffic enters through one bus and exits through the other.

For example, the following figure shows the ASA configured so that traffic from the unsecured network and the secure network is evenly distributed between Bus 0 and Bus 1. Traffic from hosts on the secured network flows through interface 0/0 on Bus 0 to hosts on the unsecured network. Traffic from hosts on the unsecured network flows through interface 1/0 on Bus 1 to hosts on the secured network.

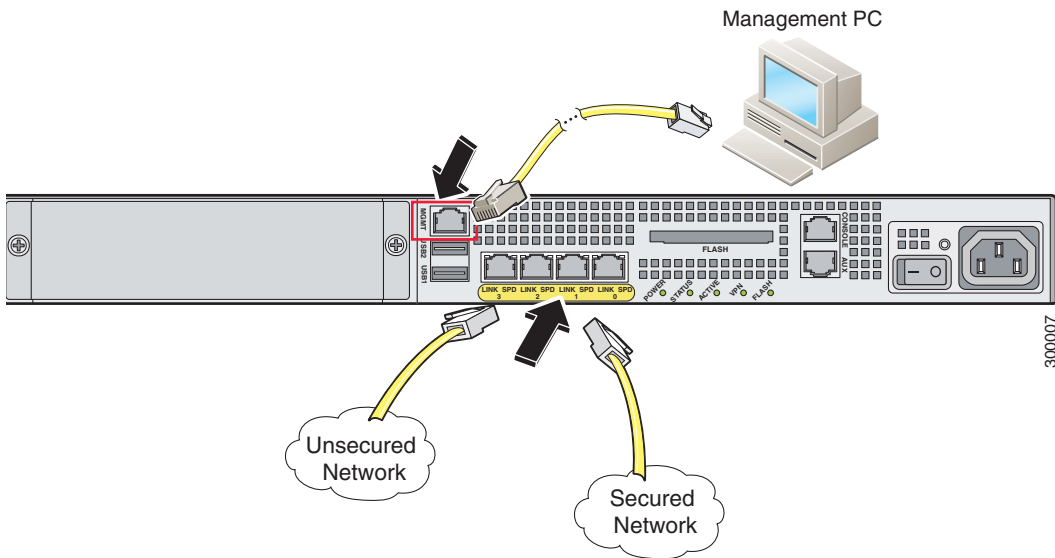


4 Connecting Interface Cables and Verifying Connectivity

Step 1 Connect a management PC to the Management 0/0 interface for use with the Adaptive Security Device Manager (ASDM). You can connect the PC directly with an Ethernet cable, or connect the PC and the ASA to the same management network. Make sure the PC is configured to obtain an IP address using DHCP.

If you want to use the CLI, connect your PC to the console port, and see the CLI configuration guide for more information.

Step 2 Connect your networks to the appropriate ports. For the ASA 5550 or 4GE SSM, if you are using the fiber ports, you need to use SFP modules (not included). See the Hardware Installation Guide for information.



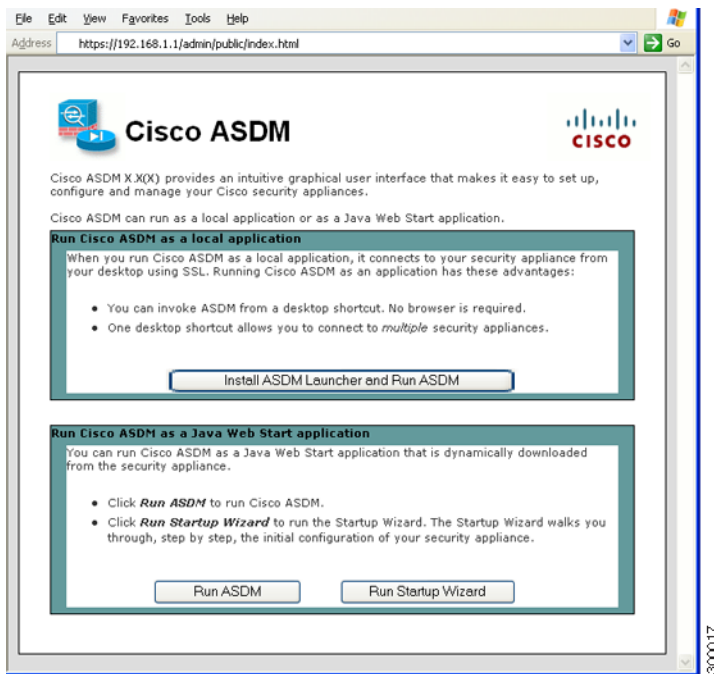
Step 3 Check the LINK/ACT indicators to verify interface connectivity.

5 Launching ASDM

The ASA ships with a default configuration that enables ASDM connectivity to the Management 0/0 interface. Using ASDM, you can use wizards to configure basic and advanced features. ASDM is a graphical user interface that allows you to manage the ASA from any location by using a web browser. See the ASDM release notes on Cisco.com for the requirements to run ASDM.

Step 1 On the PC connected to the ASA, launch a web browser.

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**.

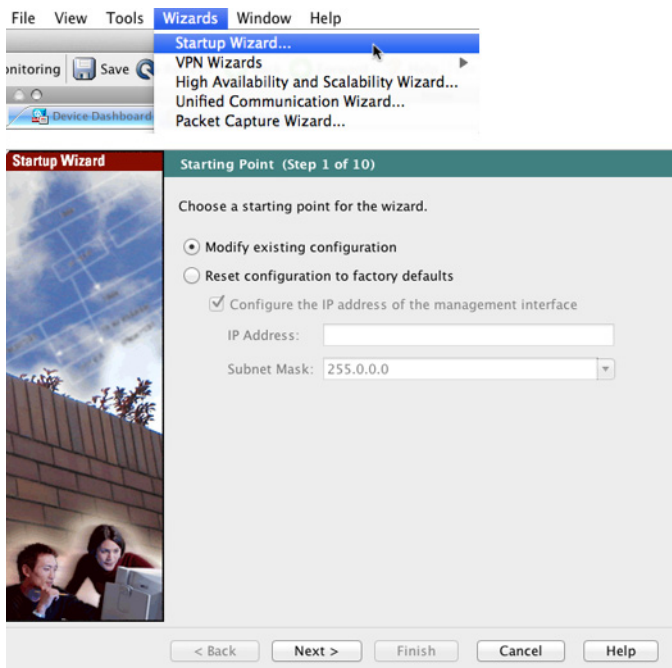
Step 4 Accept any certificates according to the dialog boxes that appear. The Cisco ASDM-IDM Launcher appears.

Step 5 Leave the username and password fields empty, and click **OK**. The main ASDM window appears and the Startup Wizard opens.

6 Running the Startup Wizard

Run the **Startup Wizard** to modify the default configuration so that you can customize the security policy to suit your deployment. Using the startup wizard, you can set the following:

- Hostname
- Domain name
- Administrative passwords
- Interfaces
- IP addresses
- Static routes
- DHCP server
- Network address translation rules
- and more...

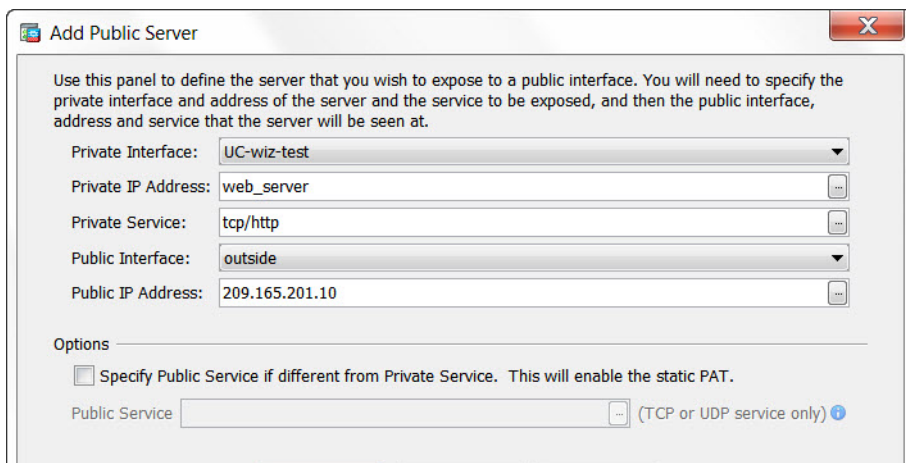


-
- Step 1** If the wizard is not already running, in the main ASDM window, choose **Wizards > Startup Wizard**.
 - Step 2** Follow the instructions in the Startup Wizard to configure your ASA.
 - Step 3** While running the wizard, you can accept the default settings or change them as required. (For information about any wizard field, click **Help**.)
-

7 (Optional) Allowing Access to Public Servers Behind the ASA

ASA 8.2 and Later

The Public Server pane automatically configures the security policy to make an inside server accessible from the Internet. As a business owner, you might have internal network services, such as a web and FTP server, that need to be available to an outside user. You can place these services on a separate network behind the ASA, called a demilitarized zone (DMZ). By placing the public servers on the DMZ, any attacks launched against the public servers do not affect your inside networks.



Use this panel to define the server that you wish to expose to a public interface. You will need to specify the private interface and address of the server and the service to be exposed, and then the public interface, address and service that the server will be seen at.

Private Interface: UC-wiz-test

Private IP Address: web_server

Private Service: tcp/http

Public Interface: outside

Public IP Address: 209.165.201.10

Options

Specify Public Service if different from Private Service. This will enable the static PAT.

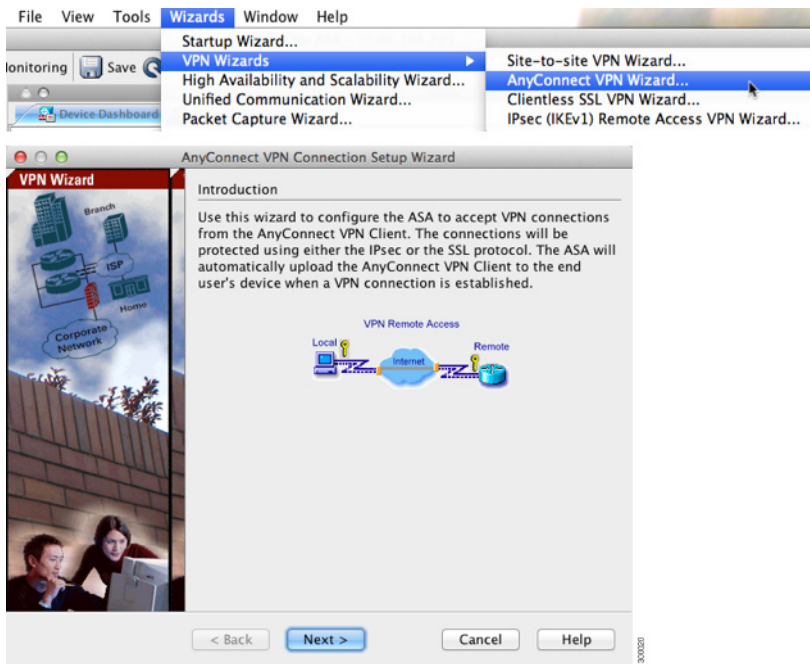
Public Service: (TCP or UDP service only) ?

- 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 Add Public Server dialog box. (For information about any field, click **Help**.)
- Step 3** Click **OK**. The server appears in the list.
- Step 4** Click **Apply** to submit the configuration to the ASA.

8 (Optional) Running VPN Wizards

You can configure VPN using the following wizards:

- **Site-to-Site VPN Wizard**—Creates an IPsec site-to-site tunnel between two ASAs.
- **(ASA 8.0 and later) AnyConnect VPN Wizard**—Configures SSL VPN remote access for the Cisco AnyConnect VPN client. AnyConnect provides secure SSL connections to the ASA for remote users with full VPN tunneling to corporate resources. The ASA policy can be configured to download the AnyConnect client to remote users when they initially connect via a browser. With AnyConnect 3.0 and later, the client can run either the SSL or IPsec IKEv2 VPN protocol.
- **(ASA 8.0 and later) Clientless SSL VPN Wizard**—Configures clientless SSL VPN remote access for a browser. Clientless, browser-based SSL VPN lets users establish a secure, remote-access VPN tunnel to the ASA 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. ACLs can be applied to restrict or allow access to specific corporate resources.
- **IPsec (IKEv1) Remote Access VPN Wizard**—Configures IPsec VPN remote access for the Cisco IPsec client.



Step 1 In the main ASDM window, choose **Wizards > VPN Wizards**, then choose one of the following:

- Site-to-Site VPN Wizard
- AnyConnect VPN Wizard
- Clientless VPN Wizard
- IPsec (IKEv1) Remote Access VPN Wizard

Step 2 Follow the wizard instructions. (For information about any wizard field, click **Help**.)

9 (Optional) Running Other Wizards in ASDM

You can optionally run the following additional wizards in ASDM:

- **High Availability and Scalability Wizard**
Configure active/active or active/standby failover, or VPN cluster load balancing.
- **Unified Communications Wizard**
Configure a proxy on the ASA for remote access or business-to-business communications. (Special licenses may apply. See the CLI configuration guide for information about ASA licensing.)
- **Packet Capture Wizard**
Configure and run packet capture. The wizard will run one packet capture on each of the ingress and egress interfaces. After capturing packets, you can save the packet captures to your PC for examination and replay in the packet analyzer.

10 Advanced Configuration

To continue configuring your ASA, see the documents available for your software version at:

<http://www.cisco.com/go/asadocs>



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.

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)

© 2016 Cisco Systems, Inc. All rights reserved.

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