Cisco ASA 5505
Getting Started Guide
Software Version 7.2

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7817612=
Text Part Number: 78-17612-02
CONTENTS

CHAPTER 1

Before You Begin 1-1

CHAPTER 2

Deployment Planning 2-1
Scenarios for Deployment Planning and Configuration 2-1
Scenario 1: Private Network with External Connectivity 2-3
Scenario 2: Basic Installation with DMZ 2-4
Scenario 3: IPSec Remote-Access VPN 2-5
Scenario 4: Site-to-Site VPN 2-6
Scenario 5: ASA 5505 Deployed as a Hardware VPN Client 2-7
Configuration Procedures for Scenarios 2-8
What to Do Next 2-9

CHAPTER 3

Planning for a VLAN Configuration 3-1
Understanding VLANs on the ASA 5505 3-1
About Physical Ports on the ASA 5505 3-2
About VLANs 3-2
Maximum Number and Types of VLANs 3-3
Deployment Scenarios Using VLANs 3-4
Basic Deployment Using Two VLANs 3-5
DMZ Deployment 3-7
Teleworker Deployment Using Three VLANs 3-8
What to Do Next 3-9
## Contents

### Chapter 4: Installing the ASA 5505

- **Installing the ASA 5505** 4-1
  - Verifying the Package Contents 4-1
  - PoE Ports and Devices 4-3
  - Installing the Chassis 4-3
  - Connecting to Network Interfaces 4-4
  - Powering on the ASA 5505 4-5
  - Setting Up a PC for System Administration 4-6
  - Optional Procedures 4-7
    - Connecting to the Console 4-7
    - Installing a Cable Lock 4-8
  - Ports and LEDs 4-9
    - Front Panel Components 4-9
    - Rear Panel Components 4-12
  - What to Do Next 4-13

### Chapter 5: Configuring the Adaptive Security Appliance

- **Configuring the Adaptive Security Appliance** 5-1
  - About the Factory Default Configuration 5-1
  - About the Adaptive Security Device Manager 5-3
  - Using the Startup Wizard 5-4
    - Before Launching the Startup Wizard 5-4
    - Running the Startup Wizard 5-5
  - What to Do Next 5-7

### Chapter 6: Scenario: DMZ Configuration

- **Scenario: DMZ Configuration** 6-1
  - Example DMZ Network Topology 6-1
  - Configuring the Security Appliance for a DMZ Deployment 6-5
    - Configuration Requirements 6-5
    - Starting ASDM 6-6
Enabling Inside Clients to Communicate with Devices on the Internet  6-7
Enabling Inside Clients to Communicate with the DMZ Web Server  6-7
   Translating Internal Client IP Addresses Between the Inside and DMZ Interfaces  6-8
   Translating the Public Address of the Web Server to its Real Address  6-9
Configuring an External Identity for the DMZ Web Server  6-11
Providing Public HTTP Access to the DMZ Web Server  6-15
What to Do Next  6-18

CHAPTER 7

Scenario: IPSec Remote-Access VPN Configuration  7-1
   Example IPSec Remote-Access VPN Network Topology  7-1
   Implementing the IPSec Remote-Access VPN Scenario  7-2
      Information to Have Available  7-3
      Starting ASDM  7-3
      Configuring the ASA 5505 for an IPSec Remote-Access VPN  7-5
      Selecting VPN Client Types  7-6
      Specifying the VPN Tunnel Group Name and Authentication Method  7-7
      Specifying a User Authentication Method  7-8
      (Optional) Configuring User Accounts  7-10
      Configuring Address Pools  7-11
      Configuring Client Attributes  7-12
      Configuring the IKE Policy  7-13
      Configuring IPSec Encryption and Authentication Parameters  7-15
      Specifying Address Translation Exception and Split Tunneling  7-16
      Verifying the Remote-Access VPN Configuration  7-17
What to Do Next  7-18

CHAPTER 8

Scenario: Site-to-Site VPN Configuration  8-1
   Example Site-to-Site VPN Network Topology  8-1
Implementing the Site-to-Site Scenario  8-2
  Information to Have Available  8-3
  Configuring the Site-to-Site VPN  8-3
  Starting ASDM  8-3
  Configuring the Security Appliance at the Local Site  8-4
  Providing Information About the Remote VPN Peer  8-6
  Configuring the IKE Policy  8-7
  Configuring IPSec Encryption and Authentication Parameters  8-9
  Specifying Hosts and Networks  8-10
  Viewing VPN Attributes and Completing the Wizard  8-11
Configuring the Other Side of the VPN Connection  8-13
What to Do Next  8-13

Scenario: Easy VPN Hardware Client Configuration  9-1
  Using an ASA 5505 as an Easy VPN Hardware Client  9-1
  Client Mode and Network Extension Mode  9-2
  Configuring the Easy VPN Hardware Client  9-5
  Configuring Advanced Easy VPN Attributes  9-8
  What to Do Next  9-9

Obtaining a 3DES/AES License  A-1
Before You Begin

Use the following table to find the installation and configuration steps that are required for your implementation of the adaptive security appliance.

<table>
<thead>
<tr>
<th>To Do This...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn about typical deployments of the ASA 5505</td>
<td>Chapter 2, “Deployment Planning”</td>
</tr>
<tr>
<td>Learn about VLANs and port allocation on the ASA 5505</td>
<td>Chapter 3, “Planning for a VLAN Configuration”</td>
</tr>
<tr>
<td>Install the chassis</td>
<td>Chapter 4, “Installing the ASA 5505”</td>
</tr>
<tr>
<td>Perform initial setup of the adaptive security appliance</td>
<td>Chapter 5, “Configuring the Adaptive Security Appliance”</td>
</tr>
<tr>
<td>Configure the adaptive security appliance for your implementation</td>
<td>Chapter 6, “Scenario: DMZ Configuration”</td>
</tr>
<tr>
<td></td>
<td>Chapter 7, “Scenario: IPSec Remote-Access VPN Configuration”</td>
</tr>
<tr>
<td></td>
<td>Chapter 8, “Scenario: Site-to-Site VPN Configuration”</td>
</tr>
<tr>
<td></td>
<td>Chapter 9, “Scenario: Easy VPN Hardware Client Configuration”</td>
</tr>
</tbody>
</table>
### To Do This... (continued) | See...
---|---
Refine configuration | *Cisco Security Appliance Command Line Configuration Guide*
Configure optional and advanced features | *Cisco Security Appliance Command Reference*
| *Cisco Security Appliance Logging Configuration and System Log Messages*
Deployment Planning

This document is based on several example scenarios that represent typical customer deployments of the ASA 5505. The deployment scenarios in this chapter correspond to subsequent configuration chapters.

This chapter includes the following sections:

- Scenarios for Deployment Planning and Configuration, page 2-1
- Scenario 1: Private Network with External Connectivity, page 2-3
- Scenario 2: Basic Installation with DMZ, page 2-4
- Scenario 4: Site-to-Site VPN, page 2-6
- Scenario 5: ASA 5505 Deployed as a Hardware VPN Client, page 2-7

Scenarios for Deployment Planning and Configuration

An extended adaptive security appliance deployment can include two or more of the different deployment scenarios described in this chapter. You can use the deployment scenarios in this chapter to help you determine how you want to deploy the adaptive security appliance on your network, and then determine which configuration chapters apply to you.

Figure 2-1 illustrates an extended network that includes most of the deployment and configuration scenarios included in this document.
**Figure 2-1** Extended Network Deployment

- **Scenario 1:** Basic Installation
  - Internet
  - Cisco ASA SSC-05
  - Status
  - Security Services
  - Card Slot
  - Console
  - Reset
  - Power 48VDC
  - Power over Ethernet

- **Scenario 2:** Basic Installation with DMZ
  - Personal computers
  - Printer

- **Scenario 3:** IPSec VPN Connection
  - Mobile Client
    - Using VPN software client
  - Internet
  - Remote Site
    - Adaptive Security Appliance

- **Scenario 4:** Site-to-site VPN Connection
  - Adaptive Security Appliance
  - Web Server
  - Email Server
Scenario 1: Private Network with External Connectivity

A basic deployment that is typical for a small private network is shown in Figure 2-2.

*Figure 2-2  Private (Inside) Network with External Connectivity*

In this example, the adaptive security appliance enables all devices on the private network to communicate with each other and enables users on the private network to communicate with devices on the Internet.

**Note**

This deployment is similar to the security deployments using the PIX 501. If you already have a security deployment with PIX 501 security appliances in which devices behind the firewall can communicate internally and externally, you can keep the same deployment and replace the PIX 501 devices with ASA 5505 devices.
For information about how to configure your adaptive security appliance for this deployment, see Chapter 5, “Configuring the Adaptive Security Appliance.”

**Scenario 2: Basic Installation with DMZ**

In this scenario, the adaptive security appliance is used to protect network resources located in a demilitarized zone (DMZ) in addition to the inside network. A DMZ is a separate network located in the neutral zone between a private (inside) network and a public (outside) network.

HTTP clients on the private network can access the web server in the DMZ and can also communicate with devices on the Internet.

*Figure 2-3 Private Network with DMZ*
Scenario 3: IPSec Remote-Access VPN

In this scenario, the adaptive security appliance is configured to accept remote-access IPSec VPN connections. A remote-access VPN allows you to create secure connections, or tunnels, across the Internet, which provides secure access to off-site users.

For information about how to configure an IPSec remote-access VPN deployment, see Chapter 7, “Scenario: IPSec Remote-Access VPN Configuration.”
Scenario 4: Site-to-Site VPN

In this scenario, two adaptive security appliances are configured to create a site-to-site VPN.

Deploying a site-to-site VPN enables businesses to extend their networks across low-cost public Internet connections to business partners and remote offices worldwide while maintaining their network security. A VPN connection enables you to send data from one location to another over a secure connection, or tunnel, first by authenticating both ends of the connection, and then by automatically encrypting all data sent between the two sites.

For information about configuring a site-to-site VPN deployment, see Chapter 8, “Scenario: Site-to-Site VPN Configuration.”
Scenario 5: ASA 5505 Deployed as a Hardware VPN Client

In this scenario, an ASA 5505 is deployed as a hardware client (sometimes called a remote device). Deploying one or more VPN hardware clients in conjunction with a VPN headend device enables companies with multiple sites to establish secure communications among them and share network resources.

Deploying an Easy VPN solution with hardware clients simplifies the deployment and management of a VPN in the following ways:

- Hosts at remote sites no longer have to run VPN client software.
- Security policies reside on a central server and are pushed to the remote hardware clients when a VPN connection is established.
- Few configuration parameters need to be set locally, minimizing the need for on-site administration.

Figure 2-6 illustrates how the different Easy VPN components can be deployed.
For information about how to configure the ASA 5505 as a VPN hardware client, see Chapter 9, “Scenario: Easy VPN Hardware Client Configuration.”

**Configuration Procedures for Scenarios**

Each deployment scenario in this chapter has a corresponding configuration chapter in this document that describes how to configure the ASA 5505 for that type of deployment.
<table>
<thead>
<tr>
<th>To Configure the ASA 5505 For This Scenario</th>
<th>See This Chapter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario 1: Private Network with External Connectivity</td>
<td>Chapter 5, “Configuring the Adaptive Security Appliance”</td>
</tr>
<tr>
<td>Scenario 2: Basic Installation with DMZ</td>
<td>Chapter 6, “Scenario: DMZ Configuration”</td>
</tr>
<tr>
<td>Scenario 4: Site-to-Site VPN</td>
<td>Chapter 8, “Scenario: Site-to-Site VPN Configuration”</td>
</tr>
<tr>
<td>Scenario 5: ASA 5505 Deployed as a Hardware VPN Client</td>
<td>Chapter 9, “Scenario: Easy VPN Hardware Client Configuration”</td>
</tr>
</tbody>
</table>

**What to Do Next**

Continue with Chapter 3, “Planning for a VLAN Configuration.”
Planning for a VLAN Configuration

Grouping ports into logical VLANs on the ASA 5505 enables you to segment large private networks and provide additional protection to critical network segments that may host resources such as servers, corporate computers, and IP phones.

This chapter describes the options of deploying the ASA 5505 in a VLAN configuration and how to determine how many VLANs you need. It also describes allocating ports for each of the VLANs.

This chapter includes the following sections:

- Understanding VLANs on the ASA 5505, page 3-1
- Deployment Scenarios Using VLANs, page 3-4
- What to Do Next, page 3-9

Understanding VLANs on the ASA 5505

After you have made a decision about how to deploy the ASA 5505 in your network, you must decide how many VLANs you need to support that deployment and how many ports to allocate to each VLAN.

This section describes how VLANs work on the ASA 5505 to help you make those decisions.

This section includes the following topics:

- About Physical Ports on the ASA 5505, page 3-2
- About VLANs, page 3-2
About Physical Ports on the ASA 5505

The ASA 5505 has a built-in switch with eight Fast Ethernet ports, called switch ports. Two of the eight physical ports are Power Over Ethernet (PoE) ports. You can connect PoE ports directly to user equipment such as PCs, IP phones, or a DSL modem. You can also connect to another switch. For more information, see Ports and LEDs, page 4-9.

About VLANs

You can divide the eight physical ports into groups, called VLANs, that function as separate networks. This enables you to improve the security of your business because devices in different VLANs can only communicate with each other by passing the traffic through the adaptive security appliance where relevant security policies are applied.

The ASA 5505 comes preconfigured with two VLANs: VLAN1 and VLAN2. By default, Ethernet switch port 0/0 is allocated to VLAN2. All other switch ports are allocated by default to VLAN1.

Physical ports on the same VLAN communicate with each other using hardware switching. VLANs communicate with each other using routes and bridges. For example, when a switch port on VLAN1 is communicating with a switch port on VLAN2, the adaptive security appliance applies configured security policies to the traffic and routes or bridges the traffic between the two VLANs.

To impose strict access control and provide protection of sensitive devices, you can apply security policies to VLANs that restrict communications between VLANs. You can also apply security policies to individual ports. You might want to apply security policies at the port level if, for example, there are two ports on the same VLAN connecting devices that you do not want to be able to communicate with each other.
Before you can enable a switch port on the ASA 5505, it must be assigned to a VLAN. With the Base platform, each switch port can be assigned to only one VLAN at a time. With the Security Plus license, you can use a single port to trunk between three VLANs on an external switch, enabling you to scale your deployment for larger organizations.

You can create VLANs and allocate ports in the following ways:

<table>
<thead>
<tr>
<th>Method of Configuring VLANs</th>
<th>For more information, see...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASDM Startup Wizard</td>
<td>Chapter 5, “Configuring the Adaptive Security Appliance”</td>
</tr>
<tr>
<td>ASDM GUI configuration</td>
<td>ASDM online help</td>
</tr>
<tr>
<td>Command-line interface</td>
<td>Cisco Security Appliance Command Reference</td>
</tr>
</tbody>
</table>

**Maximum Number and Types of VLANs**

Your license determines how many active VLANs that you can have on the ASA 5505.

Although the ASA 5505 comes preconfigured with two VLANs, you can create as many as three VLANs, depending on your license. For example, you could create VLANs for the Inside, Outside, and DMZ network segments. Each access switch port is allocated to a single VLAN. Trunk switch ports may be allocated to multiple VLANs.

With the Base platform, communication between the DMZ VLAN and the Inside VLAN is restricted: the Inside VLAN is permitted to send traffic to the DMZ VLAN, but the DMZ VLAN is not permitted to send traffic to the Inside VLAN.

The Security Plus license removes this limitation, thus enabling a full DMZ configuration.

*Table 3-1* lists the number and types of connections supported by each license.
Chapter 3  Planning for a VLAN Configuration

Deployment Scenarios Using VLANs

Table 3-1  License Restrictions on Active VLANs

<table>
<thead>
<tr>
<th>License Type</th>
<th>Mode</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base Platform</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transparent Mode</td>
<td>Up to two active VLANs.</td>
<td></td>
</tr>
<tr>
<td>Routed Mode</td>
<td>Up to three active VLANs. The DMZ VLAN is restricted from initiating traffic to the inside VLAN.</td>
<td></td>
</tr>
<tr>
<td><strong>Security Plus License</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transparent Mode</td>
<td>Up to three active VLANs, one of which must be used for failover.</td>
<td></td>
</tr>
<tr>
<td>Routed Mode</td>
<td>Up to three active VLANs for normal traffic. One active VLAN for failover. One active VLAN as a backup link to your ISP. The backup interface does not send or receive traffic unless the route through the primary interface fails.</td>
<td></td>
</tr>
</tbody>
</table>

Note: The ASA 5505 adaptive security appliance supports active and standby failover, but not Stateful Failover.

Deployment Scenarios Using VLANs

The number of VLANs you need depends on the complexity of the network into which you are installing the adaptive security appliance. Use the scenarios in this section as a guide to help you determine how many VLANs you need and how many ports to allocate to each.

This section includes the following topics:

- Basic Deployment Using Two VLANs, page 3-5
- DMZ Deployment, page 3-7
- Teleworker Deployment Using Three VLANs, page 3-8
Basic Deployment Using Two VLANs

For most deployments, you only need to create two VLANs: an Inside VLAN and an Outside VLAN, as shown in Figure 3-1.

Figure 3-1  Deployment Using Two VLANs

In this example, the network includes an inside VLAN that permits all devices on the VLAN to communicate with each other and an outside VLAN that permits users to communicate with devices on the Internet.

The Inside VLAN may consist of up to seven physical ports that connect desktop computers, network printers, and other devices. In this scenario, the Outside VLAN consists of a single ISP connection using an external WAN router.

In Figure 3-1, the Inside VLAN uses four switch ports on the ASA 5505 and the Outside VLAN uses only one. Three switch ports are unused.
This deployment is similar to the security deployments using the PIX 501. If you already have a security deployment with PIX 501 security appliances in which devices behind the firewall can communicate internally and externally, you can keep the same deployment and replace the PIX 501 devices with ASA 5505 devices.

If this same customer needed to have two Internet connections, the Outside VLAN could be allocated an additional port, as shown in Figure 3-2. This deployment includes an Inside VLAN and an Outside VLAN with two external connections to provide link redundancy if one fails.

**Figure 3-2  Inside VLAN with Dual ISP Connectivity**

Even very complex networks can be deployed with only two VLANs, one for inside and one for outside.
DMZ Deployment

The only deployment for which you must create three VLANs is when you have a DMZ to protect in addition to your Inside network. If you have a DMZ in your configuration, the DMZ must be on its own VLAN.

*Figure 3-3  Deployment Requiring Three VLANs*

In this example, three physical switch ports are allocated to the Inside VLAN, two switch ports are allocated to the DMZ VLAN, and one switch port is allocated to the Outside VLAN. Two switch ports are left unused.
Teleworker Deployment Using Three VLANs

Although not required, using three VLANs can be useful in other situations, such as when deploying a remote VPN hardware client to support a teleworker.

In Figure 3-4, an ASA 5505 is installed in a home office environment and used as a remote VPN hardware client. The ASA 5505 is configured for three VLANs:

- Inside (Work) VLAN that consists of all devices used to support access to the main corporate network
- DMZ (Home) VLAN that consists of devices that can be used by all members of the family
- Outside (Internet) VLAN that provides Internet connectivity for both the Inside and DMZ VLANs

In this case, the ASA 5505 protects the critical assets on the Inside (Work) VLAN so that these devices cannot be infected by traffic from the DMZ (Home) VLAN. To enable devices in the Inside (Work) VLAN to establish secure connections with corporate headend devices, enable the Easy VPN hardware client functionality so that only traffic from the Inside (Work) VLAN initiates VPN connections. This configuration enables users on the DMZ (Home) VLAN to browse the Internet independently of the Inside (Work) VLAN, and the security of the Inside (Work) VLAN is not compromised.
In this example, the physical ports of the ASA 5505 are used as follows:

- The Inside (Work) VLAN consists of three physical switch ports, one of which is a Power over Ethernet (PoE) switch port that is used for an IP phone.
- The DMZ (Inside) VLAN consists of three physical switch ports.
- The Outside (Internet) VLAN consists of one physical switch port supporting a single ISP connection using an external WAN router or broadband modem.

The printer is shared by both the Inside VLAN and the DMZ VLAN.

For more information about VLANs, see the *Cisco Security Appliance Command Line Configuration Guide*.

**What to Do Next**

Continue with Chapter 4, “Installing the ASA 5505.”
Chapter 3  Planning for a VLAN Configuration

What to Do Next
Installing the ASA 5505

This chapter describes how to install the ASA 5505 adaptive security appliance. This chapter includes the following sections:

- Verifying the Package Contents, page 4-1
- PoE Ports and Devices, page 4-3
- Installing the Chassis, page 4-3
- Connecting to Network Interfaces, page 4-4
- Powering on the ASA 5505, page 4-5
- Setting Up a PC for System Administration, page 4-6
- Optional Procedures, page 4-7
- Ports and LEDs, page 4-9
- What to Do Next, page 4-13

Verifying the Package Contents

Verify the contents of the packing box to ensure that you have received all items necessary to install your Cisco ASA 5505 adaptive security appliance, as shown in Figure 4-1.
Figure 4-1 Contents of ASA 5505 Package

Cisco ASA 5505

- Blue console cable
- Yellow Ethernet cable
- Power supply adapter
- Documentation
- Cable (US shown)
**PoE Ports and Devices**

On the ASA 5505, switch ports Ethernet 0/6 and Ethernet 0/7 support PoE devices that are compliant with the IEEE 802.3af standard, such as IP phones or wireless access points. If you install a non-PoE device or do not connect to these switch ports, the adaptive security appliance does not supply power to the ports and the device must be powered on its own.

These ports are the only ports that can provide power for IP phones or other PoE devices. However, these ports are not restricted to that use. They can also be used as Ethernet switch ports, like the Ethernet switch ports numbered 0 through 5. If a PoE device is not attached, power is not supplied to the port.

When connecting PoE devices, use the following guidelines:

- Use straight-through cable only. Using crossover cable does not enable the ASA 5505 to provide power to the PoE ports.
- Do not disable auto-negotiation (force speed and duplex) on E0/6 and E0/7 when using them to connect PoE devices. If auto-negotiation is disabled, the ASA 5505 does not recognize that a PoE device is attached. In this case, power is not provided to the port.

**Note**

Be careful when connecting a Cisco PoE device to a non-PoE switch port (E0/0 through E0/5). If auto-negotiation is disabled for that switch port, a network loopback might occur with some Cisco Powered Device (PD) models.

- Cisco IP Phone 7970 is always in low-power mode when drawing power from the ASA 5505.

**Installing the Chassis**

To install the ASA 5505, perform the following steps:

**Step 1** Place the chassis on a flat, stable surface. The chassis is not rack mountable.

**Step 2** Connect Port 0 to the public network (that is, the Internet):

a. Use a yellow Ethernet cable to connect the device to a switch or hub.
b. Use one of the yellow Ethernet cables to connect the device to a
cable/DSL/ISDN modem.

Note  By default, switch port 0 is the outside port.

Step 3  Connect your network devices with an Ethernet cable to one of the remaining
seven switched ports (numbered 1 through 7).

If you are connecting any Power over Ethernet (PoE) devices, connect them to one
of the switch ports that support PoE (ports numbered 6 and 7).

Connecting to Network Interfaces

To connect to a network interface, perform the following steps:

Step 1  Locate an RJ-45 to RJ-45 Ethernet cable.

Step 2  Connect one end of the Ethernet cable to an Ethernet port (ports 0 through 7) as
shown in Figure 4-2. (Typically Ethernet port 0 is used to connect to an Internet
router.)
Powering on the ASA 5505

To power on the ASA 5505, perform the following steps:

**Step 1** Connect the power supply with the power cable.
**Step 2** Connect the small, rectangular connector of the power supply cable to the power connector on the rear panel.
**Step 3** Connect the AC power connector of the power supply input cable to an electrical outlet.
Note  The ASA 5505 does not have a power switch. Completing Step 3 powers on the device.

Step 4  Check the power LED; if it is solid green, then the device is powered on.
For more information, see the “Front Panel Components” section on page 4-9.

Setting Up a PC for System Administration

You can perform setup, configuration, and management tasks from a PC using the Adaptive Security Device Manager (ASDM) application, which provides an intuitive graphical user interface (GUI). In addition to configuration and management capability, ASDM also provides configuration wizards for initial configuration, VPN configuration, and high-availability configuration.

For more information about using ASDM for setup and configuration, see Chapter 5, “Configuring the Adaptive Security Appliance.”

To set up a PC from which you can configure and manage the ASA 5505, perform the following steps:

Step 1  Make sure that the speed of the PC interface to be connected to one of the ASA 5505 inside ports is set to autonegotiate. This setting provides the best performance.

By default, the ASA 5505 automatically negotiates the inside interface speed. If autonegotiate is not an option for the PC interface, set the speed to either 10 or 100 Mbps half duplex. Do not set the interface to full duplex; this causes a duplex mismatch that significantly impacts the total throughput capabilities of the interface.

Step 2  Configure the PC to use DHCP (to receive an IP address automatically from the ASA 5505), which enables the PC to communicate with the ASA 5505 and the Internet as well as to run ASDM for configuration and management tasks.

Alternatively, you can assign a static IP address to your PC by selecting an address in the 192.168.1.0 subnet. When you connect other devices to any of the inside ports, make sure that they do not have the same IP address.
Step 3  Use an Ethernet cable to connect the PC to a switched inside port on the rear panel of the ASA 5505 (one of the ports numbered 1 through 7).

Step 4  Check the LINK LED to verify that the PC has basic connectivity to the ASA 5505.

When connectivity is established, the LINK LED on the front panel of the ASA 5505 lights up solid green.

You can now access the ASDM and the ASDM Startup Wizard. See Chapter 5, “Configuring the Adaptive Security Appliance” for information about how to perform initial setup and configuration of the ASA 5505.

Optional Procedures

This section describes how to perform tasks that are not required for the initial setup of the ASA 5505. This section includes the following topics:

- “Connecting to the Console” section on page 4-7
- “Installing a Cable Lock” section on page 4-8

Connecting to the Console

You can access the command line for administration using the console port on the ASA 5505. To do so, you must run a serial terminal emulator on a PC or workstation as shown in Figure 4-3.
To connect a console for local, command-line administrative access, perform the following steps:

**Step 1** Plug one end of the PC terminal adapter into a standard 9-pin PC serial port on your PC.

**Step 2** Plug one end of the blue console cable into the PC terminal adapter.

**Step 3** Plug the other end of the blue console cable into the CONSOLE port.

**Step 4** Configure the PC terminal emulation software or terminal for 9600 baud, 8 data bits, no parity, and 1 stop bit.

### Installing a Cable Lock

The ASA 5505 includes a slot that accepts standard desktop cable locks to provide physical security for small portable equipment, such as a laptop computer. The cable lock is not included.
To install a cable lock, perform the following steps:

**Step 1** Follow the directions from the manufacturer for attaching the other end of the cable for securing the adaptive security appliance.

**Step 2** Attach the cable lock to the lock slot on the back panel of the ASA 5505.

## Ports and LEDs

This section describes the front and rear panels of the ASA 5505. This section includes the following topics:

- Front Panel Components, page 4-9
- Rear Panel Components, page 4-12

### Front Panel Components

The LINK/ACT indicators on the front panel of the ASA 5505 are normally solid green when a link is established and flashing green when there is network activity. Each Ethernet interface (numbered 0 through 7) has two LEDs: one to indicate the operating speed and the other to indicate whether the physical link is established.
Figure 4-4 illustrates the front panel of the ASA 5505.

**Table:**

<table>
<thead>
<tr>
<th>Port / LED</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>—</td>
<td>—</td>
<td>Reserved for future use.</td>
</tr>
<tr>
<td>2</td>
<td>Not lit</td>
<td>—</td>
<td>Network traffic is flowing at 10 Mbps.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>On</td>
<td>Network traffic is flowing at 100 Mbps.</td>
</tr>
<tr>
<td>3</td>
<td>Green</td>
<td>Solid</td>
<td>The physical link established.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>Flashing</td>
<td>There is network activity.</td>
</tr>
<tr>
<td>4</td>
<td>Green</td>
<td>On</td>
<td>The device is powered on.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>—</td>
<td>The device is powered off.</td>
</tr>
<tr>
<td>5</td>
<td>Green</td>
<td>Flashing</td>
<td>The power-up diagnostics are running or the system is booting.</td>
</tr>
<tr>
<td></td>
<td>Solid</td>
<td></td>
<td>The system is operational.</td>
</tr>
<tr>
<td></td>
<td>Amber</td>
<td>Solid</td>
<td>The system has encountered a problem.</td>
</tr>
</tbody>
</table>
### Ports and LEDs

<table>
<thead>
<tr>
<th>Port / LED</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
</table>
| **6**      | Green | Solid | The system is forwarding traffic.  
If the system is part of a high availability setup, a solid green light indicates that the link is forwarding traffic. |
|            | Amber | Solid | The system is on standby.  
If the system is part of a high availability setup, a solid amber light indicates that this is the standby unit. |
| **7**      | Green | Solid | The VPN tunnel is established.  
Flashing: The system is initiating the VPN tunnel. |
|            | Amber | Solid | The tunnel failed to initiate. |
| **8**      | —     | —     | An SSC card is present in the SSC slot. |

* If the LINK/ACT LED does not light up, the link could be down if there is a duplex mismatch. You can fix the problem by changing the settings either on the ASA 5505 or on the other end. If auto-negotiation is disabled (it is enabled by default), you might be using the wrong type of cable. Try replacing the yellow (straight-through) Ethernet cable with the orange (crossover) Ethernet cable.
# Rear Panel Components

Figure 4-5 illustrates the back panel of the ASA 5505.

![ASA 5505 Rear Panel](image)

<table>
<thead>
<tr>
<th>Port or LED</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power connector</td>
</tr>
<tr>
<td>2</td>
<td>Security service card slot</td>
</tr>
<tr>
<td>3</td>
<td>Serial console port</td>
</tr>
<tr>
<td>4</td>
<td>RESET button</td>
</tr>
<tr>
<td>5</td>
<td>2 USB ports v2.0 ports</td>
</tr>
<tr>
<td>6</td>
<td>Ethernet switch ports 0–7</td>
</tr>
<tr>
<td>7</td>
<td>PoE switch ports 6–7</td>
</tr>
</tbody>
</table>
What to Do Next

Continue with Chapter 5, “Configuring the Adaptive Security Appliance.”
CHAPTER 5

Configuring the Adaptive Security Appliance

This chapter describes the initial configuration of the adaptive security appliance. You can perform the configuration steps using either the browser-based Cisco Adaptive Security Device Manager (ASDM) or the command-line interface (CLI). The procedures in this chapter describe how to configure the adaptive security appliance using ASDM.

This chapter includes the following sections:

- About the Factory Default Configuration, page 5-1
- About the Adaptive Security Device Manager, page 5-3
- Using the Startup Wizard, page 5-4
- What to Do Next, page 5-7

About the Factory Default Configuration

Cisco adaptive security appliances are shipped with a factory-default configuration that enables quick startup. The ASA 5505 comes preconfigured with

- Two VLANs: VLAN 1 and VLAN2
- VLAN 1 has the following properties:
  - Named “inside”
  - Allocated switch ports Ethernet 0/1 through Ethernet 0/7
About the Factory Default Configuration

- Security level of 100
- Allocated switch ports Ethernet 0/1 through 0/7
- IP address of 192.168.1.1 255.255.255.0

- VLAN2 has the following properties:
  - Named “outside”
  - Allocated switch port Ethernet 0/0
  - Security level of 0
  - Configured to obtain its IP address using DHCP

- Inside interface to connect to the device and use ASDM to complete your configuration.

By default, the adaptive security appliance Inside interface is configured with a default DHCP address pool. This configuration enables a client on the inside network to obtain a DHCP address from the adaptive security appliance to connect to the appliance. Administrators can then configure and manage the adaptive security appliance using ASDM.

For more information about CLI configuration, see the *Cisco Security Appliance Command Line Configuration Guide*. 
The Adaptive Security Device Manager (ASDM) is a feature-rich graphical interface that allows you to manage and monitor the adaptive security appliance. The web-based design provides secure access so that you can connect to and manage the adaptive security appliance from any location by using a web browser.

In addition to complete configuration and management capability, ASDM features intelligent wizards to simplify and accelerate the deployment of the adaptive security appliance.

In addition to the ASDM web configuration tool, you can configure the adaptive security appliance by using the command-line interface. For more information, see the Cisco Security Appliance Command Line Configuration Guide and the Cisco Security Appliance Command Reference.
Using the Startup Wizard

ASDM includes a Startup Wizard to simplify the initial configuration of your adaptive security appliance. With a few steps, the Startup Wizard allows you to configure the adaptive security appliance so that it allows packets to flow securely between the inside network and the outside network.

This section describes how to use the Startup Wizard to set basic configuration parameters. This section includes the following topics:

- Before Launching the Startup Wizard, page 5-4
- Running the Startup Wizard, page 5-5

Before Launching the Startup Wizard

Before you launch the Startup Wizard, perform the following steps:

Step 1
Enable Java and Javascript in your web browser.

Step 2
Obtain the following information:

- A unique hostname to identify the adaptive security appliance on your network.
- The domain name.
- The IP addresses of your outside interface, inside interface, and any other interfaces to be configured.
- IP addresses for hosts that should have administrative access to this device using HTTPS for ASDM, SSH, or Telnet.
- The privileged mode password for administrative access.
- The IP addresses to use for NAT or PAT address translation, if any.
- The IP address range for the DHCP server.
- The IP address for the WINS server.
- Static routes to be configured.
- If you want to create a DMZ, you must create a third VLAN and assign ports to that VLAN. (By default, there are two VLANS configured.)
Chapter 5      Configuring the Adaptive Security Appliance

Using the Startup Wizard

- Interface configuration information: whether traffic is permitted between interfaces at the same security level, and whether traffic is permitted between hosts on the same interface.
- If you are configuring an Easy VPN hardware client, the IP addresses of primary and secondary Easy VPN servers; whether the client is to run in client or network extension mode; and user and group login credentials to match those configured on the primary and secondary Easy VPN servers.

Running the Startup Wizard

To use the Startup Wizard to set up a basic configuration for the adaptive security appliance, perform the following steps:

Step 1  If you have not already done so, connect a PC to a switch port on the ASA 5505.
  a. Locate an Ethernet cable, which has an RJ-45 connector on each end.
  b. Connect one RJ-45 connector to the switch port.
  c. Connect the other end of the Ethernet cable to the Ethernet port on your computer or to your management network.

Step 2  Start ASDM.
  a. On the PC connected to the ASA 5505, start an Internet browser.
  b. In the address field of the browser, enter this URL: https://192.168.1.1/.

  Note The adaptive security appliance ships with a default IP address of 192.168.1.1. Remember to add the “s” in “https” or the connection fails. HTTP over SSL (HTTPS) provides a secure connection between your browser and the adaptive security appliance.
  c. In the window that requires you to choose the method you want to use to run the ASDM software, choose either to download the ASDM Launcher or to run the ASDM software as a Java applet.

Step 3  In the dialog box that requires a username and password, leave both fields empty. Press Enter.
Using the Startup Wizard

Step 4  Click Yes to accept the certificates. Click Yes for all subsequent authentication and certificate dialog boxes.

The main ASDM window appears.

Step 5  From the Wizards menu, choose Startup Wizard.

Step 6  Follow the instructions in the Startup Wizard to set up your adaptive security appliance.

For information about any field in the Startup Wizard, click Help at the bottom of the window.
Based on your network security policy, you should also consider configuring the adaptive security appliance to deny all ICMP traffic through the outside interface or any other interface that is necessary. You can configure this access control policy using ASDM. From the ASDM main page, click Configuration > Properties > ICMP Rules. Add an entry for the outside interface. Set the IP address to 0.0.0.0, the netmask to 0.0.0.0, and Action to deny.

What to Do Next

Configure the adaptive security appliance for your deployment using one or more of the following chapters:

<table>
<thead>
<tr>
<th>To Do This...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the adaptive security appliance to protect a DMZ web server</td>
<td>Chapter 6, “Scenario: DMZ Configuration”</td>
</tr>
<tr>
<td>Configure the adaptive security appliance for remote-access VPN</td>
<td>Chapter 7, “Scenario: IPSec Remote-Access VPN Configuration”</td>
</tr>
<tr>
<td>Configure the adaptive security appliance for site-to-site VPN</td>
<td>Chapter 8, “Scenario: Site-to-Site VPN Configuration”</td>
</tr>
<tr>
<td>Configure the adaptive security appliance as an Easy VPN remote device</td>
<td>Chapter 9, “Scenario: Easy VPN Hardware Client Configuration”</td>
</tr>
</tbody>
</table>
Scenario: DMZ Configuration

Cisco ASA 5505 DMZ configurations are possible only with the Security Plus license.

This chapter includes the following sections:

- Example DMZ Network Topology, page 6-1
- Configuring the Security Appliance for a DMZ Deployment, page 6-5
- What to Do Next, page 6-18

Example DMZ Network Topology

The example network topology shown in Figure 6-1 is typical of many DMZ implementations of the adaptive security appliance.
This example scenario has the following characteristics:

- The web server is on the DMZ interface of the adaptive security appliance.
- HTTP clients on the private network can access the web server in the DMZ and can also communicate with devices on the Internet.
- Clients on the Internet are permitted HTTP access to the DMZ web server; all other traffic is denied.
- The network has one routable IP address that is publicly available: the outside interface of the adaptive security appliance (209.165.200.225).

Figure 6-2 shows the outgoing traffic flow of HTTP requests from the private network to both the DMZ web server and to the Internet.
In Figure 6-2, the adaptive security appliance permits HTTP traffic originating from inside clients and destined for the DMZ web server. Because the internal network does not include a DNS server, internal client requests for the DMZ web server are handled as follows:

1. A lookup request is sent to the DNS server of the ISP. The public IP address of the DMZ web server is returned to the client.
2. The internal client sends the HTTP request to the adaptive security appliance.
3. The adaptive security appliance translates the public IP address of the DMZ web server to its real address and forwards the request to the web server.
4. The DMZ web server returns the HTTP content to the adaptive security appliance with a destination address of the real IP address of the internal client.
5. The adaptive security appliance forwards the HTTP content to the internal client.
To permit internal clients to request HTTP content from the DMZ web server, the adaptive security appliance configuration must include the following rules:

- A NAT rule between the DMZ and inside interfaces that translates the real IP address of the DMZ web server to the public IP address of the DMZ web server (10.10.10.30 to 209.165.200.225).

- A NAT rule between the inside and DMZ interfaces that translate the real addresses of the internal client network. In this scenario, the real IP address of the internal network is translated to itself when internal clients communicate with the web server in the DMZ (10.10.10.0 to 10.10.10.0).

To permit traffic coming from the Internet to access the DMZ web server, the adaptive security appliance configuration includes the following:

- An address translation rule translating the public IP address of the DMZ web server to the private IP address of the DMZ web server.

- An access control rule permitting incoming HTTP traffic that is destined for the DMZ web server.

Figure 6-3 shows HTTP requests originating from the Internet and destined for the public IP address of the DMZ web server.

![Figure 6-3: Incoming HTTP Traffic Flow From the Internet](image)

The procedures for creating this configuration are detailed in the remainder of this chapter.
Configuring the Security Appliance for a DMZ Deployment

This section describes how to use ASDM to configure the adaptive security appliance for the configuration scenario shown in Figure 6-1. The procedure uses sample parameters based on the scenario.

This configuration procedure assumes that the adaptive security appliance already has interfaces configured for the inside interface, the outside interface, and the DMZ interface. Set up interfaces on the adaptive security appliance by using the Startup Wizard in ASDM. Be sure that the DMZ interface security level is set between 0 and 100. (A common choice is 50.)

For more information about using the Startup Wizard, see Chapter 5, “Configuring the Adaptive Security Appliance.”

The section includes the following topics:
- Configuration Requirements, page 6-5
- Starting ASDM, page 6-6
- Enabling Inside Clients to Communicate with Devices on the Internet, page 6-7
- Enabling Inside Clients to Communicate with the DMZ Web Server, page 6-7
- Configuring an External Identity for the DMZ Web Server, page 6-11
- Providing Public HTTP Access to the DMZ Web Server, page 6-15

The following sections provide detailed instructions for how to perform each step.

Configuration Requirements

Configuring the adaptive security appliance for this DMZ deployment requires the following:
- Internal clients need to be able to communicate with devices on the Internet.
- Internal clients need to be able to communicate with the DMZ web server.
- External clients need to be able to communicate with the DMZ web server.

The remainder of this chapter provides instructions for how to accomplish this configuration.
Starting ASDM

To run ASDM in a web browser, enter the factory default IP address in the address field: \textit{https://192.168.1.1/admin/}.

\textbf{Note}\ Remember to add the “s” in “https” or the connection fails. HTTP over SSL (HTTPS) provides a secure connection between your browser and the adaptive security appliance.

The Main ASDM window appears.
Enabling Inside Clients to Communicate with Devices on the Internet

To permit internal clients to request content from devices on the Internet, the adaptive security appliance translates the real IP addresses of internal clients to the external address of the outside interface (that is, the public IP address of the adaptive security appliance). Outgoing traffic appears to come from this address. The ASA 5505 comes with a default configuration that includes the necessary address translation rule. Unless you want to change the IP address of the inside interface, you do not need to configure any settings to allow inside clients to access the Internet.

Enabling Inside Clients to Communicate with the DMZ Web Server

In this procedure, you configure the adaptive security appliance to allow internal clients to communicate securely with the web server in the DMZ. To accomplish this, you must configure two translation rules:

- A NAT rule between the DMZ and inside interfaces that translates the real IP address of the DMZ web server to its public IP address (10.30.30.30 to 209.165.200.225).
- A NAT rule between the inside and DMZ interfaces that translates the public IP address of the DMZ web server back to its real IP address (209.165.200.225 to 10.30.30.30).

This is necessary because when an internal client sends a DNS lookup request, the DNS server returns the public IP address of the DMZ web server.

Because there is not a DNS server on the inside network, DNS requests must exit the adaptive security appliance to be resolved by a DNS server on the Internet.

This section includes the following topics:

- Translating Internal Client IP Addresses Between the Inside and DMZ Interfaces, page 6-8
Translating Internal Client IP Addresses Between the Inside and DMZ Interfaces

To configure NAT to translate internal client IP addresses between the inside interface and the DMZ interface, perform the following steps:

Step 1
In the main ASDM window, click the Configuration tool.

Step 2
In the Features pane, click NAT.

Step 3
From the Add drop-down list, choose Add Static NAT Rule.

The Add Static NAT Rule dialog field appears.

Step 4
In the Real Address area, specify the IP address to be translated. For this scenario, address translation for inside clients is performed for the entire 10.10.10.0 subnet.

a. From the Interface drop-down list, choose the Inside interface.

b. Enter the IP address of the client or network. In this scenario, the IP address of the network is 10.10.10.0.

c. From the Netmask drop-down list, choose the Netmask. In this scenario, the netmask is 255.255.255.0.

Step 5
In the Static Translation area, do the following:

a. From the Interface drop-down list, choose the DMZ interface.

b. In the IP Address field, enter the IP address of the internal client subnet. In this scenario, the IP address is 10.10.10.0.

c. Click OK to add the Static NAT Rule and return to the Configuration > NAT pane.
Review the configuration pane to verify that the translation rule appears as you expected. The rule should appear similar to the following:

![Configuration Pane](image)

**Step 6** Click **Apply** to complete the adaptive security appliance configuration changes.

Translating the Public Address of the Web Server to its Real Address

To configure NAT rule that translates the public IP address of the web server to its real IP address, perform the following steps:

**Step 1** In the main ASDM window, click the **Configuration** tool.

**Step 2** In the Features pane, click **NAT**.

**Step 3** From the Add drop-down list, choose **Add Static NAT Rule**.

The Add Static NAT Rule dialog box appears.
Step 4  In the Real Address area, do the following:
   a. From the Interface drop-down list, choose DMZ.
   b. Enter or choose from the IP Address drop-down list the public address of the DMZ web server. In this scenario, the IP address is 209.165.200.225.

Step 5  In the Static Translation area, do the following:
   a. From the Interface drop-down list, choose Inside.
   b. Enter or choose from the IP Address drop-down list the real address of the DMZ web server. In this scenario, the IP address is 10.30.30.30.
Step 6 Click OK to return to the Configuration > NAT pane. The configuration should look similar to the following:

![Cisco ASA Configuration Screen]

Configuring an External Identity for the DMZ Web Server

The DMZ web server needs to be accessible by all hosts on the Internet. This configuration requires translating the private IP address of the DMZ web server to a public IP address, which allows outside HTTP clients to access the web server without being aware of the adaptive security appliance. To map the real web server IP address (10.30.30.30) statically to a public IP address (209.165.200.225), perform the following steps:

Step 1 In the ASDM window, click the Configuration tool.
Step 2  In the Features pane, click **NAT**.

Step 3  From the Add drop-down list, choose Add Static NAT Rule. The Add Static NAT Rule dialog box appears.

Step 4  In the Real Address area, specify the real IP address of the web server:
   a. From the Interface drop-down list, choose the DMZ interface.
   b. Enter the real IP address of the DMZ web server. In this scenario, the IP address is 10.30.30.30.
   c. From the Netmask drop-down list, choose the Netmask 255.255.255.255.

Step 5  In the Static Translation area, specify the public IP address to be used for the web server:
   a. From the Interface drop-down list, choose Outside.
   b. From the IP Address drop-down list, choose the (Interface IP) keyword. This is the IP address for the specified interface, in this case, the outside interface.
Step 6 Configure Port Address Translation. Because there is only one public IP address, it is necessary to use Port Address Translation to translate the IP address of the DMZ web server to the public Outside IP address of the adaptive security appliance. To configure Port Address Translation, perform the following steps:

a. Check the **Enable Port Address Translation (PAT)** check box.
b. From the Protocol drop-down list, choose tcp.
c. In the Original Port field, enter 80.
d. In the Translated Port field, enter 80.
e. Click **OK** to add the rule and return to the list of Address Translation Rules.

This rule maps the real web server IP address (10.30.30.30) statically to the public IP address of the web server (209.165.200.225).
**Chapter 6  Scenario: DMZ Configuration**

### Configuring the Security Appliance for a DMZ Deployment

**Step 7** Confirm that the rule was created the way you expected. The displayed configuration should be similar to the following:

![Configuration Screenshot](image)

**Step 8** Click **Apply** to complete the adaptive security appliance configuration changes.
Providing Public HTTP Access to the DMZ Web Server

By default, the adaptive security appliance denies all traffic coming in from the public network. To permit traffic coming from the Internet to access the DMZ web server, you must configure an access control rule permitting incoming HTTP traffic destined for the DMZ web server.

This access control rule specifies the interface of the adaptive security appliance that processes the traffic, that the traffic is incoming, the origin and destination of the traffic, and the type of traffic protocol and service to be permitted.

In this section, you create an access rule that permits incoming HTTP traffic originating from any host or network on the Internet, if the destination of the traffic is the web server on the DMZ network. All other traffic coming in from the public network is denied.

To configure the access control rule, perform the following steps:

---

**Step 1**  
In the ASDM window, do the following:

a. Click the **Configuration** tool.

b. In the Features pane, click **Security Policy**.

c. Click the **Access Rules** tab, then from the Add pull-down list, choose Add Access Rule.

The Add Access Rule dialog box appears.

**Step 2**  
In the Interface and Action area, do the following:

a. From the Interface drop-down list, choose Outside.

b. From the Direction drop-down list, choose Incoming.

c. From the Action drop-down list, choose Permit.

**Step 3**  
In the Source area, choose the keyword Any from the Type drop-down list.

This indicates that traffic originating from any host or network should be allowed.

**Step 4**  
In the Destination area, do the following:

a. Choose the Interface IP keyword from the Type drop-down list.

b. Choose Outside from the Interface drop-down list.
Step 5  In the Protocol and Service area, specify the type of traffic that you want to permit through the adaptive security appliance.

a. From the Protocol drop-down list, choose tcp.

b. In the Source Port area, confirm that the Service radio button is set to “=” (equal to), and then choose any from the next drop-down list.

c. In the Destination Port area, confirm that the Service radio button is set to “=” (equal to), and then choose HTTP/WWW from the next drop-down list.

At this point, the entries in the Add Access Rule dialog box should be similar to the following:

d. Click OK to return to the Security Policy > Access Rules pane.

Step 6  The displayed configuration should be similar to the following. Verify that the information you entered is accurate.
Click **Apply** to save the configuration changes to the configuration that the adaptive security appliance is currently running.

Clients on the public network can now resolve HTTP requests for content from the DMZ web server, while keeping the private network secure.

**Step 7** If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, click **Save**.

Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the old configuration takes effect the next time the device starts.
What to Do Next

If you are deploying the adaptive security appliance solely to protect a web server in a DMZ, you have completed the initial configuration. You may want to consider performing some of the following additional steps:

<table>
<thead>
<tr>
<th>To Do This...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refine configuration and configure optional and advanced features</td>
<td>Cisco Security Appliance Command Line Configuration Guide</td>
</tr>
<tr>
<td>Learn about daily operations</td>
<td>Cisco Security Appliance Command Reference</td>
</tr>
<tr>
<td></td>
<td>Cisco Security Appliance Logging Configuration and System Log Messages</td>
</tr>
</tbody>
</table>

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

<table>
<thead>
<tr>
<th>To Do This...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a remote-access VPN</td>
<td>Chapter 7, “Scenario: IPSec Remote-Access VPN Configuration”</td>
</tr>
<tr>
<td>Configure a site-to-site VPN</td>
<td>Chapter 8, “Scenario: Site-to-Site VPN Configuration”</td>
</tr>
</tbody>
</table>
Scenario: IPSec Remote-Access VPN Configuration

This chapter describes how to use the adaptive security appliance to accept remote-access IPSec VPN connections. A remote-access VPN allows you to create secure connections, or tunnels, across the Internet, which provides secure access to off-site users.

If you are implementing an Easy VPN solution, this chapter describes how to configure the Easy VPN server (sometimes called a headend device).

This chapter includes the following sections:

- Example IPSec Remote-Access VPN Network Topology, page 7-1
- Implementing the IPSec Remote-Access VPN Scenario, page 7-2
- What to Do Next, page 7-18

Example IPSec Remote-Access VPN Network Topology

Figure 7-1 shows an adaptive security appliance configured to accept requests from and establish IPSec connections with VPN clients, such as a Cisco Easy VPN software or hardware clients, over the Internet.
Implementing the IPSec Remote-Access VPN Scenario

This section describes how to configure the adaptive security appliance to accept IPSec VPN connections from remote clients and devices. If you are implementing an Easy VPN solution, this section describes how to configure an Easy VPN server (also known as a headend device).

Values for example configuration settings are taken from the remote-access scenario illustrated in Figure 7-1.

This section includes the following topics:

- Information to Have Available, page 7-3
- Starting ASDM, page 7-3
- Configuring the ASA 5505 for an IPSec Remote-Access VPN, page 7-5
- Selecting VPN Client Types, page 7-6
- Specifying the VPN Tunnel Group Name and Authentication Method, page 7-7
Chapter 7      Scenario: IPSec Remote-Access VPN Configuration

Implementing the IPSec Remote-Access VPN Scenario

• Specifying a User Authentication Method, page 7-8
• (Optional) Configuring User Accounts, page 7-10
• Configuring Address Pools, page 7-11
• Configuring Client Attributes, page 7-12
• Configuring the IKE Policy, page 7-13
• Configuring IPSec Encryption and Authentication Parameters, page 7-15
• Specifying Address Translation Exception and Split Tunneling, page 7-16
• Verifying the Remote-Access VPN Configuration, page 7-17

Information to Have Available

Before you begin configuring the adaptive security appliance to accept remote access IPSec VPN connections, make sure that you have the following information available:

• Range of IP addresses to be used in an IP pool. These addresses are assigned to remote VPN clients as they are successfully connected.
• List of users to be used in creating a local authentication database, unless you are using an AAA server for authentication.
• Networking information to be used by remote clients when connecting to the VPN, including the following:
  – IP addresses for the primary and secondary DNS servers
  – IP addresses for the primary and secondary WINS servers
  – Default domain name
  – List of IP addresses for local hosts, groups, and networks that should be made accessible to authenticated remote clients

Starting ASDM

To run ASDM in a web browser, enter the factory default IP address in the address field: https://192.168.1.1/admin/.
Implementing the IPSec Remote-Access VPN Scenario

Note: Remember to add the “s” in “https” or the connection fails. HTTP over SSL (HTTP) provides a secure connection between your browser and the adaptive security appliance.

The Main ASDM window appears.
Implementing the IPSec Remote-Access VPN Scenario

Chapter 7      Scenario: IPSec Remote-Access VPN Configuration

Configuring the ASA 5505 for an IPSec Remote-Access VPN

To begin the process for configuring a remote-access VPN, perform the following steps:

Step 1
In the main ASDM window, choose **VPN Wizard** from the Wizards drop-down menu. The VPN Wizard Step 1 screen appears.

![VPN Wizard Step 1 Screen](image)

Step 2
In Step 1 of the VPN Wizard, perform the following steps:

a. Click the **Remote Access** radio button.

b. From the drop-down list, choose **Outside** as the enabled interface for the incoming VPN tunnels.

c. Click **Next** to continue.
Selecting VPN Client Types

In Step 2 of the VPN Wizard, perform the following steps:

**Step 1** Specify the type of VPN client that will enable remote users to connect to this adaptive security appliance. For this scenario, click the **Cisco VPN Client** radio button.

You can also use any other Cisco Easy VPN remote product.

**Step 2** Click **Next** to continue.
Specifying the VPN Tunnel Group Name and Authentication Method

In Step 3 of the VPN Wizard, perform the following steps:

**Step 1** Specify the type of authentication that you want to use by performing one of the following steps:

- To use a static preshared key for authentication, click the **Pre-Shared Key** radio button and enter a preshared key (for example, “Cisco”). This key is used for IPSec negotiations between the adaptive security appliances.

- To use digital certificates for authentication, click the **Certificate** radio button, choose the Certificate Signing Algorithm from the drop-down list, and then choose a preconfigured trustpoint name from the drop-down list. If you want to use digital certificates for authentication but have not yet configured a trustpoint name, you can continue with the Wizard by using one of the other two options. You can revise the authentication configuration later using the standard ASDM windows.

- Click the **Challenge/Response Authentication (CRACK)** radio button to use that method of authentication.
Implementing the IPSec Remote-Access VPN Scenario

Step 2
Enter a Tunnel Group Name (such as “Cisco”) for the set of users that use common connection parameters and client attributes to connect to this adaptive security appliance.

Step 3
Click Next to continue.

Specifying a User Authentication Method

Users can be authenticated either by a local authentication database or by using external authentication, authorization, and accounting (AAA) servers (RADIUS, TACACS+, SDI, NT, Kerberos, and LDAP).
In Step 4 of the VPN Wizard, perform the following steps:

**Step 1** If you want to authenticate users by creating a user database on the adaptive security appliance, click the **Authenticate Using the Local User Database** radio button.

**Step 2** If you want to authenticate users with an external AAA server group:
   a. Click the **Authenticate Using an AAA Server Group** radio button.
   b. Choose a preconfigured server group from the Authenticate using an AAA server group drop-down list, or click **New** to add a new AAA server group.

**Step 3** Click **Next** to continue.
(Optional) Configuring User Accounts

If you have chosen to authenticate users with the local user database, you can create new user accounts here. You can also add users later using the ASDM configuration interface.

In Step 5 of the VPN Wizard, perform the following steps:

**Step 1**  To add a new user, enter a username and password, and then click Add.

**Step 2**  When you have finished adding new users, click Next to continue.
Configuring Address Pools

For remote clients to gain access to your network, you must configure a pool of IP addresses that can be assigned to remote VPN clients as they are successfully connected. In this scenario, the pool is configured to use the range of IP addresses 209.165.201.1–209.166.201.20.

In Step 6 of the VPN Wizard, perform the following steps:

**Step 1**  Enter a pool name or choose a preconfigured pool from the Name drop-down list.

Alternatively, click **New** to create a new address pool.

The Add IP Pool dialog box appears.

**Step 2**  In the Add IP Pool dialog box, do the following:

a. Enter the Starting IP address and Ending IP address of the range.

b. (Optional) Enter a subnet mask or choose a subnet mask for the range of IP addresses from the Subnet Mask drop-down list.

c. Click **OK** to return to Step 6 of the VPN Wizard.
Step 3  Click **Next** to continue.

### Configuring Client Attributes

To access your network, each remote access client needs basic network configuration information, such as which DNS and WINS servers to use and the default domain name. Instead of configuring each remote client individually, you can provide the client information to ASDM. The adaptive security appliance pushes this information to the remote client or Easy VPN hardware client when a connection is established.

Make sure that you specify the correct values, or remote clients will not be able to use DNS names for resolution or use Windows networking.
Implementing the IPSec Remote-Access VPN Scenario

In Step 7 of the VPN Wizard, perform the following steps:

**Step 1** Enter the network configuration information to be pushed to remote clients.

![VPN Wizard Attribute Pushed to Client](image)

**Step 2** Click Next to continue.

**Configuring the IKE Policy**

IKE is a negotiation protocol that includes an encryption method to protect data and ensure privacy; it is also an authentication method to ensure the identity of the peers. In most cases, the ASDM default values are sufficient to establish secure VPN tunnels.
To specify the IKE policy in Step 8 of the VPN Wizard, perform the following steps:

**Step 1** Choose the Encryption (DES/3DES/AES), authentication algorithms (MD5/SHA), and the Diffie-Hellman group (1/2/5/7) used by the adaptive security appliance during an IKE security association.

**Step 2** Click **Next** to continue.
Chapter 7   Scenario: IPSec Remote-Access VPN Configuration

Implementing the IPSec Remote-Access VPN Scenario

Configuring IPSec Encryption and Authentication Parameters

In Step 9 of the VPN Wizard, perform the following steps:

**Step 1**   Click the Encryption algorithm (DES/3DES/AES) and authentication algorithm (MD5/SHA).

**Step 2**   Click *Next* to continue.
Specifying Address Translation Exception and Split Tunneling

Split tunneling enables remote-access IPSec clients to send packets conditionally over an IPSec tunnel in encrypted form or to a network interface in text form.

The adaptive security appliance uses Network Address Translation (NAT) to prevent internal IP addresses from being exposed externally. You can make exceptions to this network protection by identifying local hosts and networks that should be made accessible to authenticated remote users.

In Step 10 of the VPN Wizard, perform the following steps:

**Step 1** Specify hosts, groups, and networks that should be in the list of internal resources made accessible to authenticated remote users.

To add or remove hosts, groups, and networks dynamically from the Selected Hosts/Networks pane, click **Add** or **Delete**, respectively.
Chapter 7      Scenario: IPSec Remote-Access VPN Configuration

Implementing the IPSec Remote-Access VPN Scenario

Note
Enable split tunneling by checking the Enable Split Tunneling ... check box at the bottom of the screen. Split tunneling allows traffic outside the configured networks to be sent out directly to the Internet instead of over the encrypted VPN tunnel.

Step 2
Click Next to continue.

Verifying the Remote-Access VPN Configuration

In Step 11 of the VPN Wizard, review the configuration attributes for the new VPN tunnel. The displayed configuration should be similar to the following:

![Summary of the IPSec Remote-Access VPN Configuration](image)
If you are satisfied with the configuration, click Finish to apply the changes to the adaptive security appliance.

If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, click Save. Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the old configuration takes effect the next time the device starts.

---

**What to Do Next**

To establish end-to-end, encrypted VPN tunnels for secure connectivity for mobile employees or teleworkers, obtain the Cisco VPN client software.


If you are deploying the adaptive security appliance solely in a remote-access VPN environment, you have completed the initial configuration. In addition, you may want to consider performing some of the following steps:

<table>
<thead>
<tr>
<th>To Do This...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refine configuration and configure optional and advanced features</td>
<td><em>Cisco Security Appliance Command Line Configuration Guide</em></td>
</tr>
<tr>
<td>Learn about daily operations</td>
<td><em>Cisco Security Appliance Command Reference</em></td>
</tr>
<tr>
<td></td>
<td><em>Cisco Security Appliance Logging Configuration and System Log Messages</em></td>
</tr>
</tbody>
</table>

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.
Chapter 7      Scenario: IPSec Remote-Access VPN Configuration

What to Do Next

<table>
<thead>
<tr>
<th>To Do This...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the adaptive security appliance to protect a web server in a DMZ</td>
<td>Chapter 6, “Scenario: DMZ Configuration”</td>
</tr>
<tr>
<td>Configure a site-to-site VPN</td>
<td>Chapter 8, “Scenario: Site-to-Site VPN Configuration”</td>
</tr>
</tbody>
</table>
Scenario: Site-to-Site VPN Configuration

This chapter describes how to use the adaptive security appliance to create a site-to-site VPN.

Site-to-site VPN features provided by the adaptive security appliance enable businesses to extend their networks across low-cost public Internet connections to business partners and remote offices worldwide while maintaining their network security. A VPN connection enables you to send data from one location to another over a secure connection, or tunnel, first by authenticating both ends of the connection, and then by automatically encrypting all data sent between the two sites.

This chapter includes the following sections:
- Example Site-to-Site VPN Network Topology, page 8-1
- Implementing the Site-to-Site Scenario, page 8-2
- Configuring the Other Side of the VPN Connection, page 8-13
- What to Do Next, page 8-13

Example Site-to-Site VPN Network Topology

Figure 8-1 shows an example VPN tunnel between two adaptive security appliances.
Creating a VPN site-to-site deployment such as the one in Figure 8-1 requires you to configure two adaptive security appliances, one on each side of the connection.

## Implementing the Site-to-Site Scenario

This section describes how to configure the adaptive security appliance in a site-to-site VPN deployment, using example parameters from the remote-access scenario shown in Figure 8-1.

This section includes the following topics:

- Information to Have Available, page 8-3
- Configuring the Site-to-Site VPN, page 8-3
Information to Have Available

Before you begin the configuration procedure, obtain the following information:

- IP address of the remote adaptive security appliance peer
- IP addresses of local hosts and networks permitted to use the tunnel to communicate with resources on the remote site
- IP addresses of remote hosts and networks permitted to use the tunnel to communicate with local resources

Configuring the Site-to-Site VPN

This section describes how to use the ASDM VPN Wizard to configure the adaptive security appliance for a site-to-site VPN.

This section includes the following topics:

- Starting ASDM, page 8-3
- Configuring the Security Appliance at the Local Site, page 8-4
- Providing Information About the Remote VPN Peer, page 8-6
- Configuring the IKE Policy, page 8-7
- Configuring IPSec Encryption and Authentication Parameters, page 8-9
- Specifying Hosts and Networks, page 8-10
- Viewing VPN Attributes and Completing the Wizard, page 8-11

The following sections provide detailed instructions for how to perform each configuration step.

Starting ASDM

To run ASDM in a web browser, enter the factory default IP address in the address field: https://192.168.1.1/admin/.

Note Remember to add the “s” in “https” or the connection fails. HTTP over SSL (HTTPS) provides a secure connection between your browser and the adaptive security appliance.
The Main ASDM window appears.

Configuring the Security Appliance at the Local Site

**Note**
The adaptive security appliance at the first site is referred to as Security Appliance 1 in this scenario.

To configure the Security Appliance 1, perform the following steps:

**Step 1**
In the main ASDM window, choose the VPN Wizard option from the Wizards drop-down menu. ASDM opens the first VPN Wizard screen.
In Step 1 of the VPN Wizard, perform the following steps:

a. Click the Site-to-Site VPN radio button.

**Note** The Site-to-Site VPN option connects two IPSec security gateways, which can include adaptive security appliances, VPN concentrators, or other devices that support site-to-site IPSec connectivity.

b. From the VPN tunnel Interface drop-down list, choose Outside as the enabled interface for the current VPN tunnel.

c. Click Next to continue.
Providing Information About the Remote VPN Peer

The VPN peer is the system on the other end of the connection that you are configuring, usually at a remote site.

Note

In this scenario, the remote VPN peer is referred to as Security Appliance 2.

In Step 2 of the VPN Wizard, perform the following steps:

Step 1
Enter the Peer IP Address (the IP address of Security Appliance 2, in this scenario 209.165.200.236) and a Tunnel Group Name (for example “Cisco”).

Step 2
Specify the type of authentication that you want to use by selecting one of the following authentication methods:

- To use a static preshared key for authentication, click the Pre-Shared Key radio button and enter a preshared key (for example, “Cisco”). This key is used for IPSec negotiations between the adaptive security appliances.

  Note
  When using preshared key authentication, the Tunnel Group Name must be the IP address of the peer.

- To use digital certificates for authentication, click the Certificate radio button, choose the certificate signing algorithm from the Certificate Signing Algorithm drop-down list, and then choose a preconfigured trustpoint name from the Trustpoint Name drop-down list.

  If you want to use digital certificates for authentication but have not yet configured a trustpoint name, you can continue with the Wizard by using one of the other two options. You can revise the authentication configuration later using the standard ASDM screens.

  Click the Challenge/Response Authentication radio button to use that method of authentication.
Chapter 8  Scenario: Site-to-Site VPN Configuration

Implementing the Site-to-Site Scenario

Step 3  Click Next to continue.

Configuring the IKE Policy

IKE is a negotiation protocol that includes an encryption method to protect data and ensure privacy; it also provides authentication to ensure the identity of the peers. In most cases, the ASDM default values are sufficient to establish secure VPN tunnels between two peers.

In Step 3 of the VPN Wizard, perform the following steps:

Step 1  Click the Encryption (DES/3DES/AES), authentication algorithms (MD5/SHA), and the Diffie-Hellman group (1/2/5) used by the adaptive security appliance during an IKE security association.
Implementing the Site-to-Site Scenario

Note
When configuring Security Appliance 2, enter the exact values for each of the options that you chose for Security Appliance 1. Encryption mismatches are a common cause of VPN tunnel failures and can slow down the process.

Step 2
Click Next to continue.
Configuring IPSec Encryption and Authentication Parameters

In Step 4 of the VPN Wizard, perform the following steps:

**Step 1**  Choose the encryption algorithm (DES/3DES/AES) from the Encryption drop-down list, and the authentication algorithm (MD5/SHA) from the Authentication drop-down list.

**Step 2**  Click Next to continue.
Implementing the Site-to-Site Scenario

Specifying Hosts and Networks

Identify hosts and networks at the local site that are permitted to use this IPSec tunnel to communicate with hosts and networks on the other side of the tunnel. Specify hosts and networks that are permitted access to the tunnel by clicking Add or Delete. In the current scenario, traffic from Network A (10.10.10.0) is encrypted by Security Appliance 1 and transmitted through the VPN tunnel.

In addition, identify hosts and networks at the remote site to be allowed to use this IPSec tunnel to access local hosts and networks. Add or remove hosts and networks dynamically by clicking Add or Delete respectively. In this scenario, for Security Appliance 1, the remote network is Network B (10.20.20.0), so traffic encrypted from this network is permitted through the tunnel.

In Step 5 of the VPN Wizard, perform the following steps:

Step 1
In the Source area, choose IP Address from the Type drop-down list.

Step 2
Enter the local IP Address and Netmask.

Step 3
In the Destination area, choose IP Address from the Type drop-down list.

Step 4
Enter the IP address and Netmask for the remote host or network.
Step 5  Click **Next** to continue.

**Viewing VPN Attributes and Completing the Wizard**

In Step 6 of the VPN Wizard, review the configuration list for the VPN tunnel you just created. If you are satisfied with the configuration, click **Finish** to apply the changes to the adaptive security appliance.
Step 6  If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, click **Save**.

Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the old configuration takes effect the next time the device starts.

This concludes the configuration process for Security Appliance 1.
Chapter 8  Scenario: Site-to-Site VPN Configuration

Configuring the Other Side of the VPN Connection

You have just configured the local adaptive security appliance. Next, you need to configure the adaptive security appliance at the remote site.

At the remote site, configure the second adaptive security appliance to serve as a VPN peer. Use the procedure you used to configure the local adaptive security appliance, starting with “Configuring the Security Appliance at the Local Site” section on page 8-4 and finishing with “Viewing VPN Attributes and Completing the Wizard” section on page 8-11.

Note

When configuring Security Appliance 2, use the same values for each of the options that you selected for Security Appliance 1, with the exception of local hosts and networks. Mismatches are a common cause of VPN configuration failures.

What to Do Next

If you are deploying the adaptive security appliance only in a site-to-site VPN environment, then you have completed the initial configuration. In addition, you may want to consider performing some of the following steps:

<table>
<thead>
<tr>
<th>To Do This...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refine configuration and configure optional and advanced features</td>
<td><em>Cisco Security Appliance Command Line Configuration Guide</em></td>
</tr>
<tr>
<td>Learn about daily operations</td>
<td><em>Cisco Security Appliance Command Reference</em></td>
</tr>
<tr>
<td></td>
<td><em>Cisco Security Appliance Logging Configuration and System Log Messages</em></td>
</tr>
</tbody>
</table>
You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

<table>
<thead>
<tr>
<th>To Do This...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the adaptive security appliance to protect a web server in a DMZ</td>
<td>Chapter 6, “Scenario: DMZ Configuration”</td>
</tr>
<tr>
<td>Configure a remote-access VPN</td>
<td>Chapter 7, “Scenario: IPSec Remote-Access VPN Configuration”</td>
</tr>
</tbody>
</table>
Scenario: Easy VPN Hardware Client Configuration

This chapter describes how to configure the ASA 5505 to function as an Easy VPN hardware client. The ASA 5505 can be used as part of an Easy VPN deployment consisting of multiple devices that make up a Virtual Private Network (VPN).

This chapter includes the following sections:

- Using an ASA 5505 as an Easy VPN Hardware Client, page 9-1
- Client Mode and Network Extension Mode, page 9-2
- Configuring the Easy VPN Hardware Client, page 9-5
- What to Do Next, page 9-9

Using an ASA 5505 as an Easy VPN Hardware Client

A Cisco Easy VPN hardware client (sometimes called an “Easy VPN remote device”) enables companies with multiple sites to establish secure communications among them and share resources. A Cisco Easy VPN solution consists of an Easy VPN server at the main site and Easy VPN hardware clients at the remote offices.

The Cisco ASA 5505 can function as a Cisco Easy VPN hardware client or as a Cisco Easy VPN server (sometimes called a “headend device”), but not both at the same time.
Using an Easy VPN solution simplifies the deployment and management of a VPN in the following ways:

- Hosts at remote sites no longer have to run VPN client software.
- Security policies reside on a central server and are pushed to the remote hardware clients when a VPN connection is established.
- Few configuration parameters need to be set locally, minimizing the need for on-site administration.

Figure 9-1 illustrates how Easy VPN components can be deployed to create a VPN.

When used as an Easy VPN hardware client, the ASA 5505 can also be configured to perform basic firewall services, such as protecting devices in a DMZ from unauthorized access. However, if the ASA 5505 is configured to function as an Easy VPN hardware client, it cannot establish other types of tunnels. For example, the ASA 5505 cannot function simultaneously as an Easy VPN hardware client and as one end of a standard peer-to-peer VPN deployment.

Client Mode and Network Extension Mode

The Easy VPN hardware client supports one of two modes of operation: Client Mode or Network Extension Mode (NEM). The mode of operation determines whether the hosts behind the Easy VPN hardware client are accessible from the enterprise network over the tunnel.
Client Mode, also called Port Address Translation (PAT) mode, isolates all devices on the Easy VPN client private network from those on the enterprise network. The Easy VPN client performs PAT for all VPN traffic for its inside hosts. IP address management is neither required for the Easy VPN client inside interface or the inside hosts.

NEM makes the inside interface and all inside hosts routable across the enterprise network over the tunnel. Hosts on the inside network obtain their IP addresses from an accessible subnet (statically or with DHCP) that is preconfigured with static IP addresses. PAT does not apply to VPN traffic in NEM. This mode does not require a VPN configuration for each client. The ASA 5505 configured for NEM mode supports automatic tunnel initiation. The configuration must store the group name, username, and password.

Automatic tunnel initiation is disabled if secure unit authentication is enabled. The network and addresses on the private side of the Easy VPN client are hidden, and cannot be accessed directly.

The Easy VPN hardware client does not have a default mode. However, if you do not specify the mode in ASDM, ASDM automatically selects client mode. When you configure the Easy VPN hardware client using the CLI, you must specify a mode.

Figure 9-2 shows a sample network topology with the ASA 5505 running in Easy VPN Client Mode. When configured in Client Mode, devices on the inside interface of the ASA 5505 cannot be accessed by devices behind the Easy VPN server.
When configured in Easy VPN Network Extension Mode, the ASA 5505 does not hide the IP addresses of local hosts by substituting a public IP address. Therefore, hosts on the other side of the VPN connection can communicate directly with hosts on the local network.

When configuring NEM, the network behind the Easy VPN client should not overlap your the network behind the Easy VPN server.

Figure 9-3 shows a sample network topology with the ASA 5505 running in Network Extension Mode.
Use the following guidelines when deciding whether to configure the ASA 5505 in Easy VPN Client Mode or Network Extension Mode.

Use Client Mode if:
- You want VPN connections to be initiated when a device behind the Easy VPN hardware client attempts to access a device on the enterprise network.
- You do not want devices behind the Easy VPN hardware client to be accessible by devices on the enterprise network.

Use Network Extension Mode if:
- You want VPN connections to be established automatically and to remain open even when not required for transmitting traffic.
- You want remote devices to be able to access hosts behind the Easy VPN hardware client.

**Configuring the Easy VPN Hardware Client**

The Easy VPN server controls the security policies enforced on the ASA 5505 Easy VPN hardware client. However, to establish the initial connection to the Easy VPN server, you must complete some configuration locally.
Chapter 9  Scenario: Easy VPN Hardware Client Configuration

Configuring the Easy VPN Hardware Client

You can perform this configuration procedure by using ASDM or by using the command-line interface. This section describes how to perform the configuration using ASDM.

To configure the ASA 5505 as an Easy VPN hardware client, perform the following steps:

**Step 1**  At a PC that has access to the inside interface of the ASA 5505, start ASDM.

a. Start a web browser.

b. In the address field of the browser, enter the factory default IP address in the address field: https://192.168.1.1/.

   **Note**  Remember to add the “s” in “https” or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the adaptive security appliance.

c. In the window that requires you to choose the method you want to use to run the ASDM software, choose either to download the ASDM Launcher or to run the ASDM software as a Java applet.

**Step 2**  In the ASDM window, click the **Configuration** tool.

**Step 3**  Click the **VPN** tool, and then check the Enable **Easy VPN Remote** check box.

If you check the Enable Easy VPN Remote check box, Easy VPN is enabled on the device when you click Apply. If you uncheck it, when you apply the configuration changes, you are prompted to specify if you want to clear the entire Easy VPN configuration or whether you just want to disable the Easy VPN client temporarily.

The Easy VPN Remote configuration pane appears.
Step 4  Check the **Enable Easy VPN Remote** check box.

Step 5  To specify which mode the Easy VPN remote hardware client should run in, click **Client Mode** or **Network Extension Mode** radio button.

Step 6  In the Group Settings area, specify the type of authentication the VPN devices should use.

- To specify that the VPN devices should use a text password for authentication, click the **Group Password** radio button and enter a Group Name and Group Password.

Step 7  In the User Settings area, specify the User Name and User Password to be used by the ASA 5505 when establishing a VPN connection.
Configuring Advanced Easy VPN Attributes

You might need to perform some advanced configuration tasks if your network meets any of the following conditions:

- Your network includes devices that are incapable of performing authentication, and therefore are incapable of participating in individual unit authentication. Such devices include Cisco IP Phones, printers, and the like.

  To accommodate these devices, you can enable the device pass-through feature.

- Your ASA 5505 is operating behind a NAT device.

  In this case, you must use tunneled management attributes to specify whether device management should occur in the clear or through the tunnel and the network or networks allowed to manage the Easy VPN connection through the tunnel.

  **Note** The public address of the ASA 5505 is not accessible when behind the NAT device unless you add static NAT mappings on the NAT device.
To configure these attributes, click **Advanced** in the Easy VPN Remote configuration pane. See the online help for specific information about configuration settings.

**What to Do Next**

If you are deploying the adaptive security appliance only as an Easy VPN hardware client, you have completed the initial configuration. You may want to consider performing some of the following additional steps:

<table>
<thead>
<tr>
<th>To Do This...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the ASA 5505 to protect a DMZ web server</td>
<td>Chapter 6, “Scenario: DMZ Configuration”</td>
</tr>
<tr>
<td>Refine configuration and configure optional and advanced features</td>
<td>Cisco Security Appliance Command Line Configuration Guide</td>
</tr>
</tbody>
</table>
| Learn about daily operations                      | Cisco Security Appliance Command Reference  
Cisco Security Appliance Logging Configuration and System Log Messages |
What to Do Next
Obtaining a 3DES/AES License

The Cisco ASA 5505 adaptive security appliance comes with a DES license that provides encryption. You can obtain a 3DES-AES license that provides encryption technology to enable specific features, such as secure remote management (SSH, ASDM, and so on), site-to-site VPN, and remote access VPN. You need an encryption license key to enable this license.

If you are a registered user of Cisco.com and would like to obtain a 3DES/AES encryption license, go to the following website:

http://www.cisco.com/go/license

If you are not a registered user of Cisco.com, go to the following website:

https://tools.cisco.com/SWIFT/Licensing/RegistrationServlet

Provide your name, e-mail address, and the serial number for the adaptive security appliance as it appears in the `show version` command output.

Note

You will receive the new activation key for your adaptive security appliance within two hours of requesting the license upgrade.

For more information on activation key examples or upgrading software, see the Cisco Security Appliance Command Line Configuration Guide.
To use the activation key, perform the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>hostname# show version</strong> Shows the software release, hardware configuration, license key, and related uptime data.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>hostname# configure terminal</strong> Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>hostname(config)# activation-key</strong> Updates the encryption activation key by replacing the <em>activation-4-tuple-key</em> variable with the activation key obtained with your new license. The <em>activation-5-tuple-key</em> variable is a five-element hexadecimal string with one space between each element. An example is 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e. The “0x” is optional; all values are assumed to be hexadecimal.</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>hostname(config)# exit</strong> Exits global configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>hostname# copy running-config startup-config</strong> Saves the configuration.</td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>hostname# reload</strong> Reboots the adaptive security appliance and reloads the configuration.</td>
</tr>
</tbody>
</table>