



Cisco ASA 5505 Getting Started Guide

Software Version 8.0

Americas 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: 408 527-0883

Customer Order Number: DOC-78-18003=
Text Part Number: 78-18003-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0704R)



CONTENTS

CHAPTER 1**Before You Begin 1-1**

CHAPTER 2**Deployment Planning 2-3**

- Scenarios for Deployment Planning and Configuration 2-4
- Scenario 1: Private Network with External Connectivity 2-6
- Scenario 2: Basic Installation with DMZ 2-7
- Scenario 3: IPsec Remote-Access VPN 2-9
- Scenario 4: SSL VPN 2-9
- Scenario 5: Site-to-Site VPN 2-10
- Scenario 6: Easy VPN Hardware Client 2-11
- Where to Find Configuration Procedures 2-12
- What to Do Next 2-13

CHAPTER 3**Planning 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

CHAPTER 4

Installing the ASA 5505 4-1

- Verifying the Package Contents 4-1
- PoE Ports and Devices 4-3
- Installing the Chassis 4-4
- Connecting to Network Interfaces 4-4
- Powering on the Cisco ASA 5505 4-6
- Setting Up a PC for System Administration 4-6
- Optional Procedures 4-8
 - Connecting to the Console 4-8
 - Installing a Cable Lock 4-9
- Ports and LEDs 4-9
 - Front Panel Components 4-10
 - Rear Panel Components 4-12
- What to Do Next 4-13

CHAPTER 5

Configuring the Adaptive Security Appliance 5-1

- About the Factory Default Configuration 5-1
- Using the CLI for Configuration 5-3
- Using the Adaptive Security Device Manager for Configuration 5-3
 - Preparing to Use ASDM 5-5
 - Gathering Configuration Information for Initial Setup 5-5
 - Installing the ASDM Launcher 5-6
 - Starting ASDM with a Web Browser 5-9
- Running the ASDM Startup Wizard 5-10
- What to Do Next 5-11

CHAPTER 6

Scenario: DMZ Configuration 6-1

- Basic Network Layout for a DMZ Configuration 6-1

Example DMZ Network Topology	6-2
An Inside User Visits a Web Server on the Internet	6-4
An Internet User Visits the DMZ Web Server	6-6
An Inside User Visits the DMZ Web Server	6-8
Configuring the Security Appliance for a DMZ Deployment	6-10
Configuration Requirements	6-11
Information to Have Available	6-11
Enabling Inside Clients to Communicate with Devices on the Internet	6-12
Enabling Inside Clients to Communicate with the DMZ Web Server	6-12
Translating Internal Client IP Addresses Between the Inside and DMZ Interfaces	6-13
Translating the Public Address of the Web Server to its Real Address on the Inside Interface	6-15
Configuring Static PAT for Public Access to the DMZ Web Server (Port Forwarding)	6-17
Providing Public HTTP Access to the DMZ Web Server	6-21
What to Do Next	6-24

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	7-7
Specifying the VPN Tunnel Group Name and Authentication Method	7-8
Specifying a User Authentication Method	7-9
(Optional) Configuring User Accounts	7-11
Configuring Address Pools	7-12
Configuring Client Attributes	7-13

- Configuring the IKE Policy 7-14
- Configuring IPsec Encryption and Authentication Parameters 7-16
- Specifying Address Translation Exception and Split Tunneling 7-17
- Verifying the Remote-Access VPN Configuration 7-18
- What to Do Next 7-19

CHAPTER 8

Scenario: Configuring Connections for a Cisco AnyConnect VPN Client 8-1

- About SSL VPN Client Connections 8-1
- Obtaining the Cisco AnyConnect VPN Client Software 8-2
- Example Topology Using AnyConnect SSL VPN Clients 8-3
- Implementing the Cisco SSL VPN Scenario 8-3
 - Information to Have Available 8-4
 - Starting ASDM 8-5
 - Configuring the ASA 5505 for the Cisco AnyConnect VPN Client 8-7
 - Specifying the SSL VPN Interface 8-8
 - Specifying a User Authentication Method 8-9
 - Specifying a Group Policy 8-11
 - Configuring the Cisco AnyConnect VPN Client 8-12
 - Verifying the Remote-Access VPN Configuration 8-14
- What to Do Next 8-15

CHAPTER 9

Scenario: SSL VPN Clientless Connections 9-1

- About Clientless SSL VPN 9-1
 - Security Considerations for Clientless SSL VPN Connections 9-2
- Example Network with Browser-Based SSL VPN Access 9-3
- Implementing the Clientless SSL VPN Scenario 9-4
 - Information to Have Available 9-5
 - Starting ASDM 9-5
 - Configuring the ASA 5505 for Browser-Based SSL VPN Connections 9-7

Specifying the SSL VPN Interface	9-8
Specifying a User Authentication Method	9-10
Specifying a Group Policy	9-11
Creating a Bookmark List for Remote Users	9-12
Verifying the Configuration	9-16
What to Do Next	9-18

CHAPTER 10**Scenario: Site-to-Site VPN Configuration** 10-1

Example Site-to-Site VPN Network Topology	10-1
Implementing the Site-to-Site Scenario	10-2
Information to Have Available	10-3
Configuring the Site-to-Site VPN	10-3
Starting ASDM	10-3
Configuring the Security Appliance at the Local Site	10-5
Providing Information About the Remote VPN Peer	10-7
Configuring the IKE Policy	10-9
Configuring IPsec Encryption and Authentication Parameters	10-10
Specifying Hosts and Networks	10-11
Viewing VPN Attributes and Completing the Wizard	10-12
Configuring the Other Side of the VPN Connection	10-14
What to Do Next	10-15

CHAPTER 11**Scenario: Easy VPN Hardware Client Configuration** 11-1

Using an ASA 5505 as an Easy VPN Hardware Client	11-1
Client Mode and Network Extension Mode	11-3
Configuring the Easy VPN Hardware Client	11-5
Starting ASDM With the ASDM Launcher	11-6
Configuring the Hardware Client	11-9
Configuring Advanced Easy VPN Attributes	11-11

What to Do Next 11-12

APPENDIX **A**

Obtaining a 3DES/AES License A-1



CHAPTER 1

Before You Begin

Use the following table to find the installation and configuration steps that are required for your implementation of the Cisco ASA 5505 Adaptive Security Appliance.

To Do This...	See...
Learn about typical deployments of the ASA 5505	Chapter 2, “Deployment Planning”
Learn about VLANs and port allocation on the ASA 5505	Chapter 3, “Planning a VLAN Configuration”
Install the chassis	Chapter 4, “Installing the ASA 5505”
Perform initial setup of the adaptive security appliance	Chapter 5, “Configuring the Adaptive Security Appliance”
Configure the adaptive security appliance for your implementation	Chapter 6, “Scenario: DMZ Configuration”
	Chapter 7, “Scenario: IPsec Remote-Access VPN Configuration”
	Chapter 8, “Scenario: Configuring Connections for a Cisco AnyConnect VPN Client”
	Chapter 9, “Scenario: SSL VPN Clientless Connections”
	Chapter 10, “Scenario: Site-to-Site VPN Configuration”
	Chapter 11, “Scenario: Easy VPN Hardware Client Configuration”

To Do This... (continued)	See...
Refine the configuration	<i>Cisco Security Appliance Command Line Configuration Guide</i>
Configure optional and advanced features	<i>Cisco Security Appliance Command Reference</i>
	<i>Cisco Security Appliance Logging Configuration and System Log Messages</i>



CHAPTER 2

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:

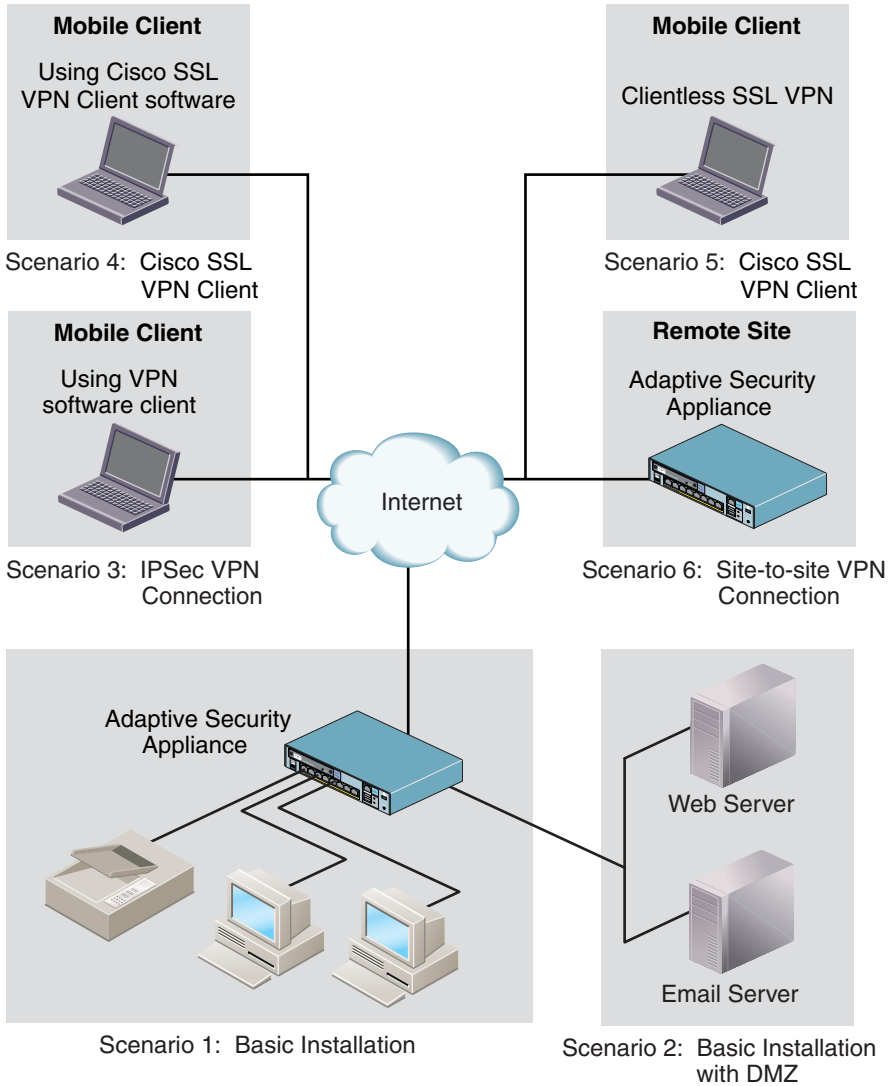
- [Scenarios for Deployment Planning and Configuration, page 2-4](#)
- [Scenario 1: Private Network with External Connectivity, page 2-6](#)
- [Scenario 2: Basic Installation with DMZ, page 2-7](#)
- [Scenario 3: IPsec Remote-Access VPN, page 2-9](#)
- [Scenario 4: SSL VPN, page 2-9](#)
- [Scenario 5: Site-to-Site VPN, page 2-10](#)
- [Scenario 6: Easy VPN Hardware Client, page 2-11](#)
- [Where to Find Configuration Procedures, page 2-12](#)
- [What to Do Next, page 2-13](#)

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 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

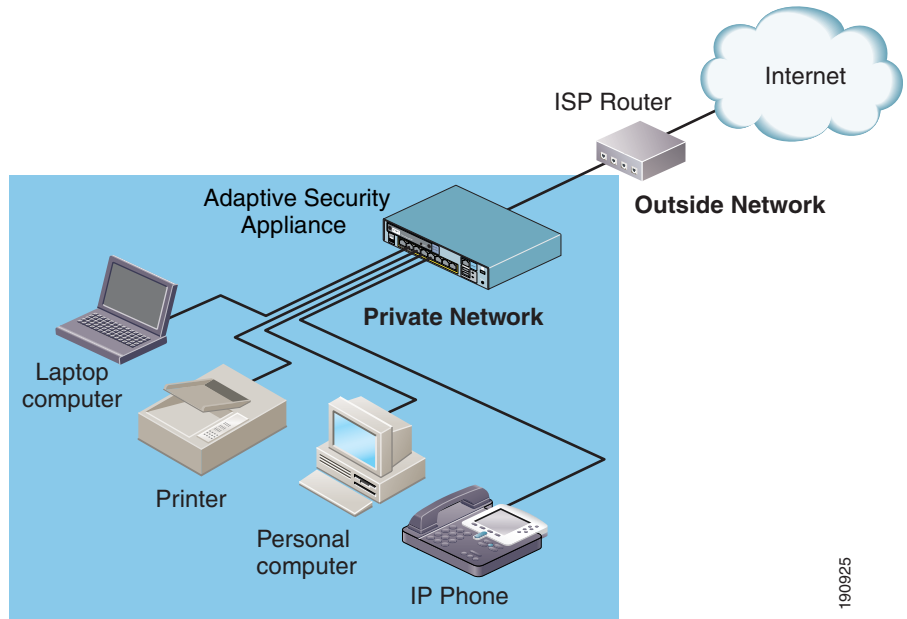


190924

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*



190925

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.

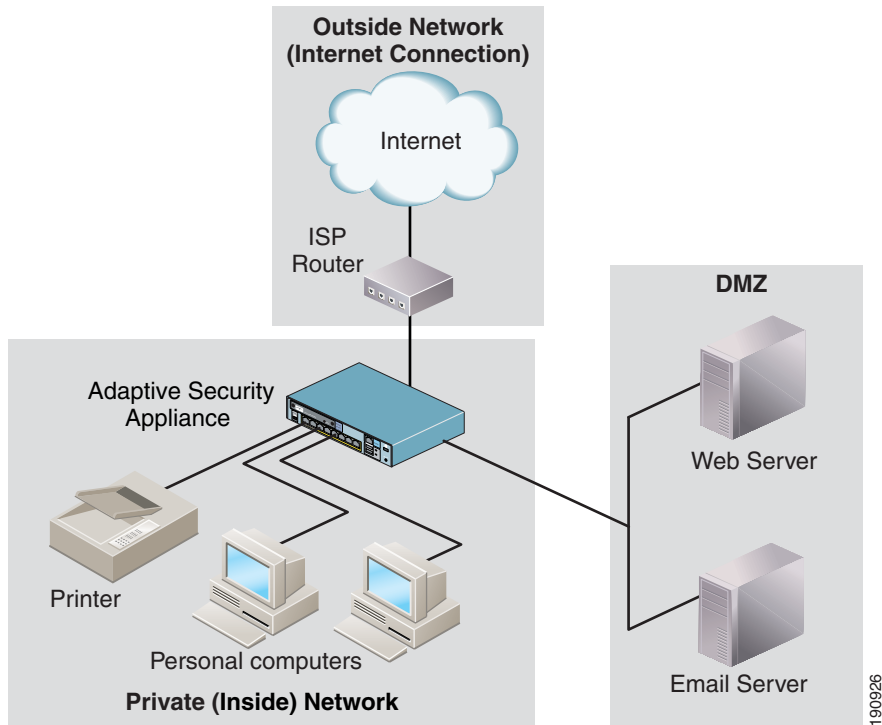
For information about how to configure your adaptive security appliance for this deployment, see [Chapter 5, “Configuring the Adaptive Security Appliance.”](#)

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

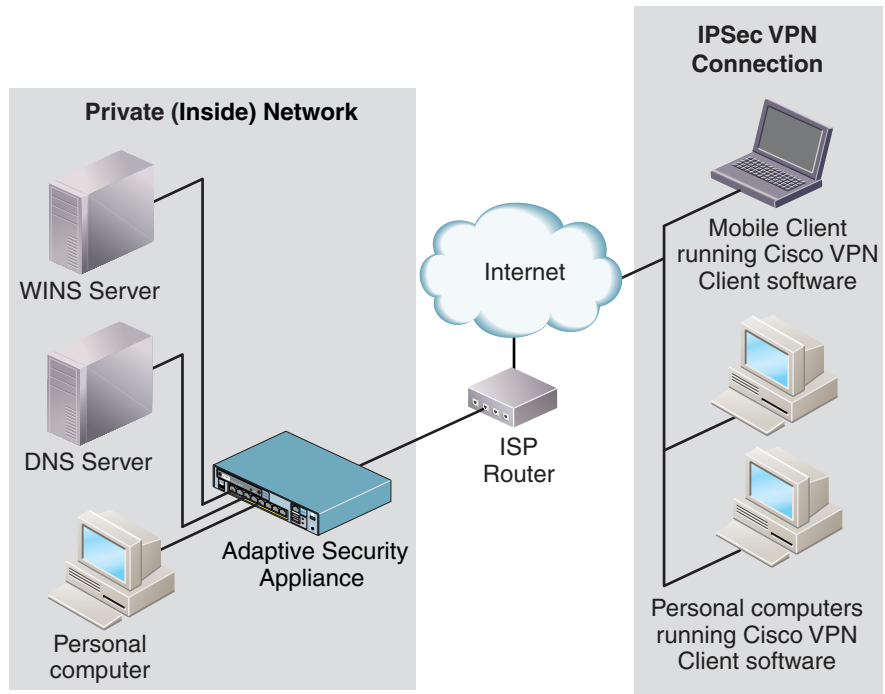


For information about configuring a DMZ deployment, see [Chapter 6, “Scenario: DMZ Configuration.”](#)

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.

Figure 2-4 IPsec Remote-Access VPN Connection



For information about how to configure an IPsec remote-access VPN deployment, see [Chapter 7, “Scenario: IPsec Remote-Access VPN Configuration.”](#)

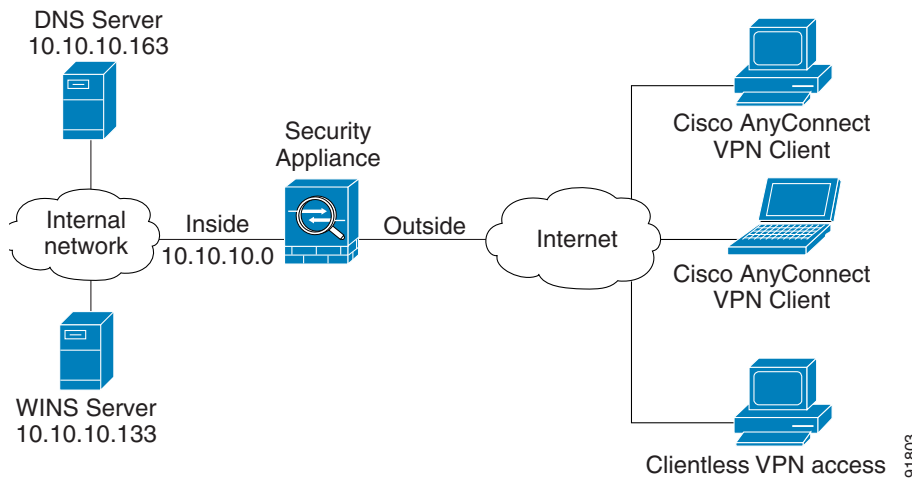
Scenario 4: SSL VPN

The adaptive security appliance supports two types of SSL VPN connections, including:

- Remote clients running the Cisco SSL VPN AnyConnect Client software.
- Clientless SSL VPN connections, that is, SSL VPN connections established with a remote system running a Web browser.

Figure 2-5 shows an adaptive security appliance configured to accept requests for and establish both types of supported SSL VPN connections.

Figure 2-5 Network Layout for SSL VPN Scenario

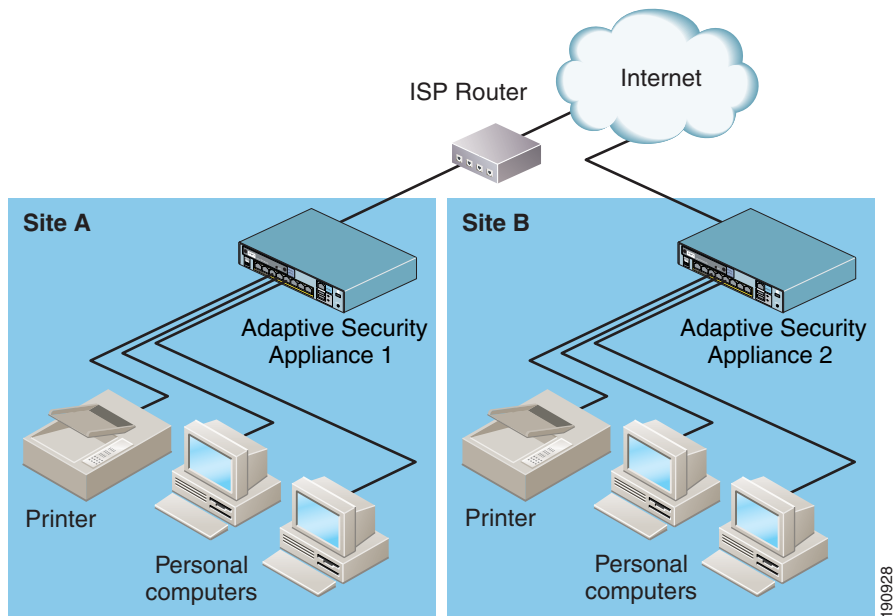


Scenario 5: Site-to-Site VPN

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.

Figure 2-6 Network Layout for Site-to-Site VPN Configuration Scenario



For information about configuring a site-to-site VPN deployment, see [Chapter 10](#), “Scenario: Site-to-Site VPN Configuration.”

Scenario 6: Easy VPN Hardware 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.

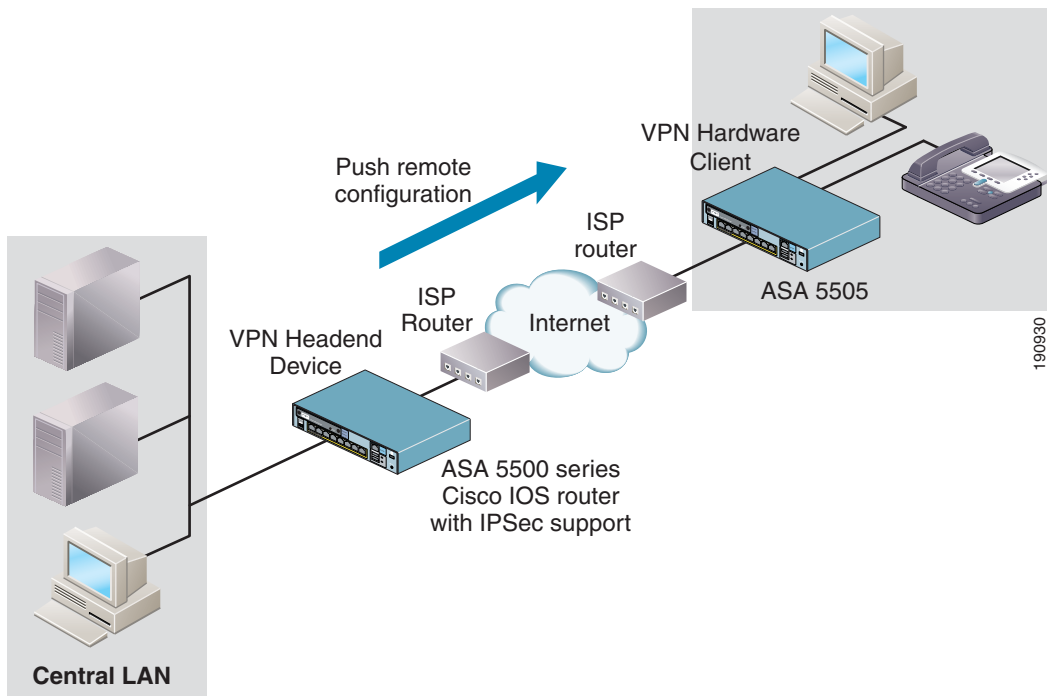
Deploying an Easy VPN solution with hardware clients simplifies the deployment and management of a VPN in the following ways:

- 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 2-7 illustrates how the different Easy VPN components can be deployed.

Figure 2-7 ASA 5505 Installed as VPN Hardware Client



For information about how to configure the ASA 5505 as a VPN hardware client, see [Chapter 11, “Scenario: Easy VPN Hardware Client Configuration.”](#)

Where to Find Configuration Procedures

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.

To Configure the ASA 5505 For This Scenario....	See This Chapter...
Scenario 1: Private Network with External Connectivity	Chapter 5, “Configuring the Adaptive Security Appliance”
Scenario 2: Basic Installation with DMZ	Chapter 6, “Scenario: DMZ Configuration”
Scenario 3: IPsec Remote-Access VPN	Chapter 7, “Scenario: IPsec Remote-Access VPN Configuration”
Scenario 4: SSL VPN	Chapter 8, “Scenario: Configuring Connections for a Cisco AnyConnect VPN Client” Chapter 9, “Scenario: SSL VPN Clientless Connections”
Scenario 5: Site-to-Site VPN	Chapter 10, “Scenario: Site-to-Site VPN Configuration”
Scenario 6: Easy VPN Hardware Client	Chapter 11, “Scenario: Easy VPN Hardware Client Configuration”

What to Do Next

Continue with [Chapter 3, “Planning a VLAN Configuration.”](#)

■ What to Do Next



CHAPTER 3

Planning 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](#)

- [Maximum Number and Types of VLANs, page 3-3](#)

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 protect 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 multiple 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:

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

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 20 VLANs, depending on your license. The security plus license allows you to create up to 20 VLANs in both modes—routed and transparent.

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, thereby enabling a full DMZ configuration.

[Table 3-1](#) lists the number and types of connections supported by each license.

Table 3-1 License Restrictions on Active VLANs

License Type	Mode	Connections
Base Platform	Transparent Mode	Up to two active VLANs.
	Routed Mode	Up to three active VLANs. The DMZ VLAN is restricted from initiating traffic to the inside VLAN.
Security Plus License	Transparent Mode	Up to three active VLANs, one of which must be used for failover.
	Routed Mode	Up to 20 active VLANs. For example, you can allocate each physical port to a separate VLAN, such as Outside, DMZ 1, DMZ 2, Engineering, Sales, Customer Service, Finance, and HR. Because there are only 8 physical ports, the additional VLANs are useful for assigning to trunk ports, which aggregate multiple VLANs on a single physical port.

**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:

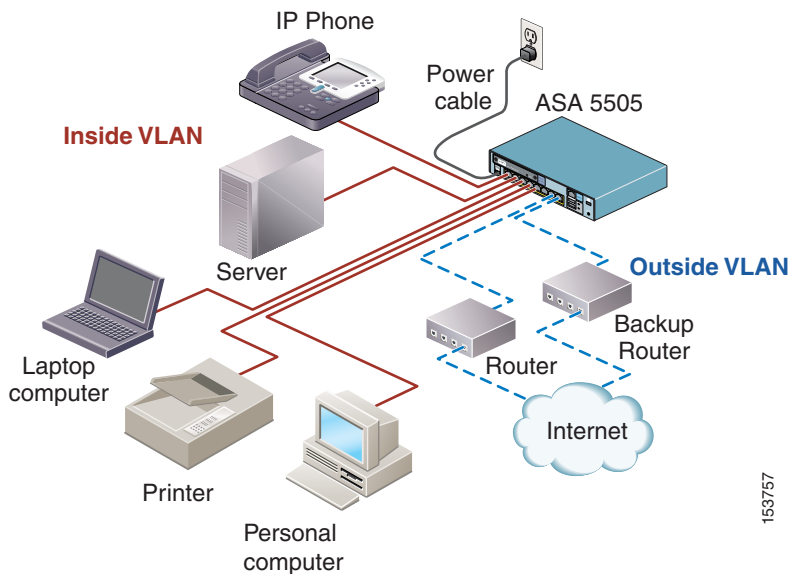
- [Basic Deployment Using Two VLANs, page 3-5](#)
- [DMZ Deployment, page 3-7](#)
- [Teleworker Deployment Using Three VLANs, page 3-8](#)

**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.

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



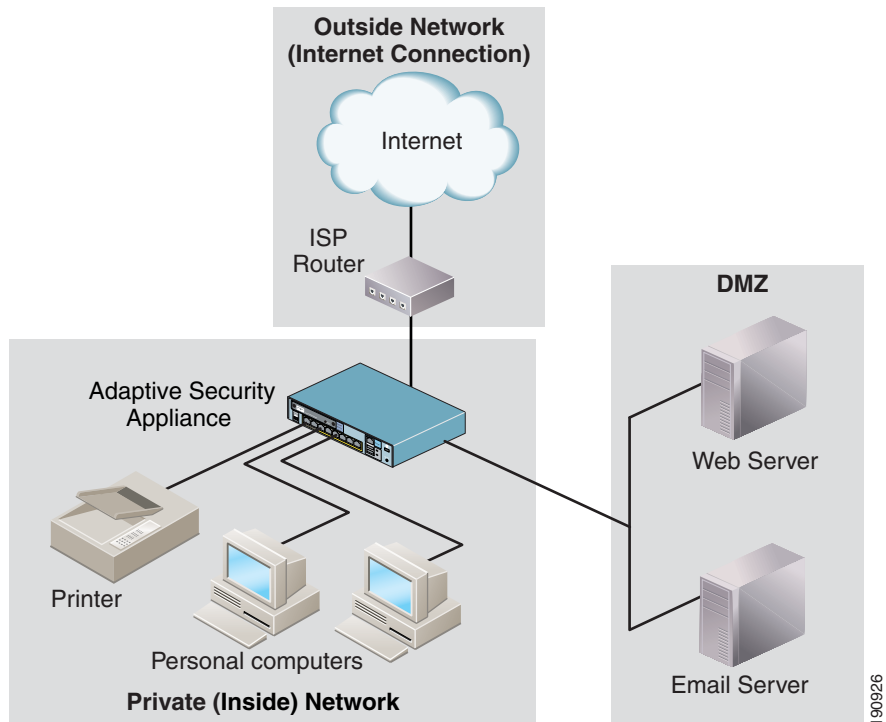
153757

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

DMZ Deployment

The only deployments that require three VLANs are those in which there is a DMZ to protect as well as the 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

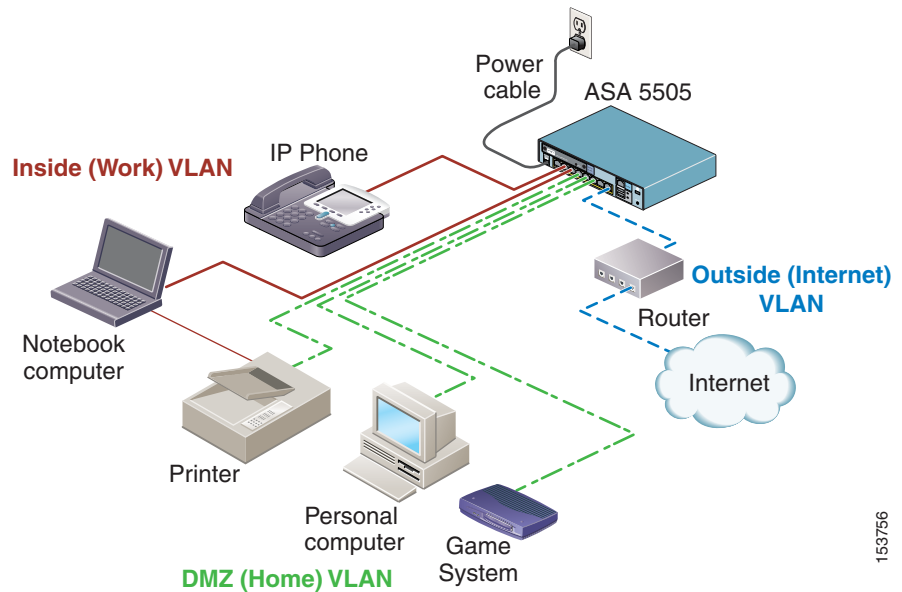
Although not required, using three VLANs can be useful in other situations, such as when deploying a remote VPN hardware client to support a teleworker.

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.

Figure 3-4 Teleworker Deployment Using Three VLANs



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 (Home) 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 additional scenarios with VLANs, see the *Cisco Security Appliance Command Line Configuration Guide*.

What to Do Next

Continue with [Chapter 4, “Installing the ASA 5505.”](#)

■ What to Do Next



CHAPTER 4

Installing the ASA 5505

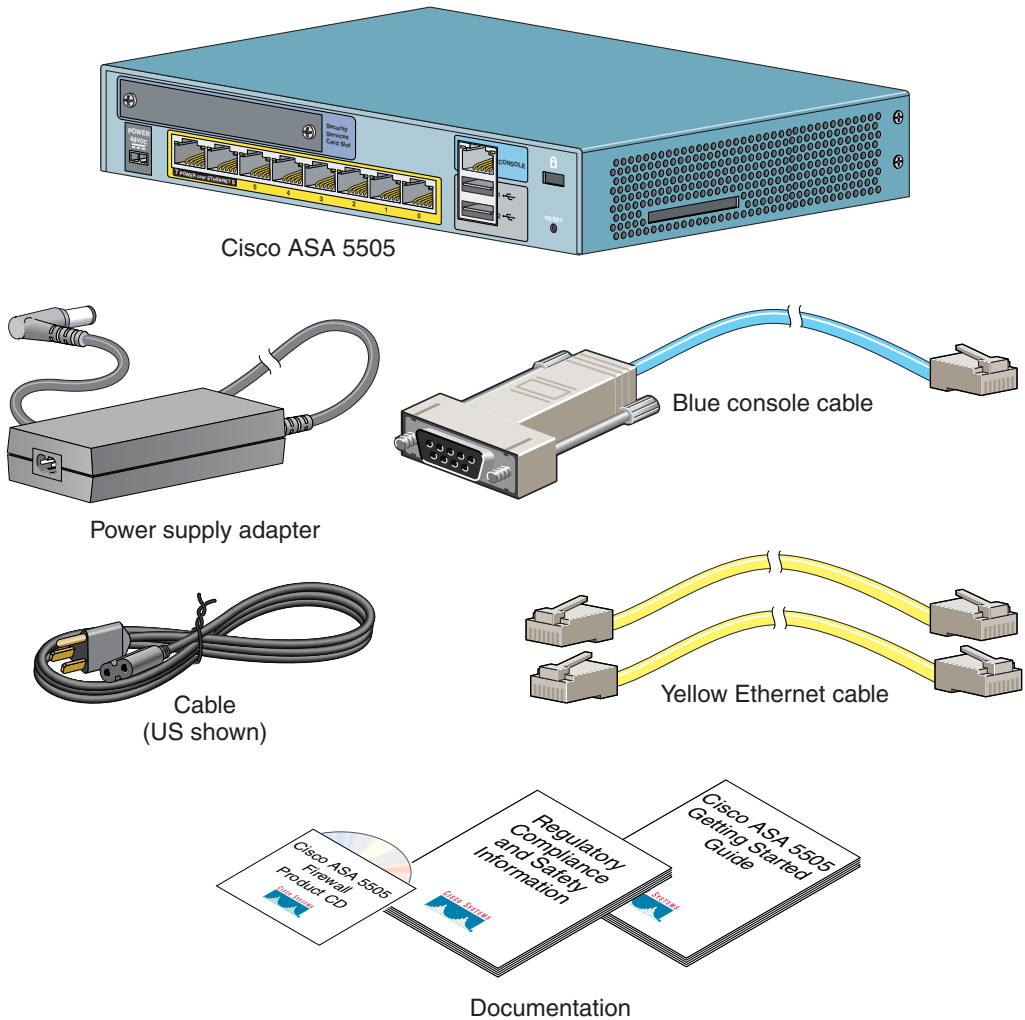
This chapter describes how to install the Cisco ASA 5505 adaptive security appliance. This chapter includes the following sections:

- [Verifying the Package Contents, page 4-1](#)
- [PoE Ports and Devices, page 4-3](#)
- [Installing the Chassis, page 4-4](#)
- [Connecting to Network Interfaces, page 4-4](#)
- [Powering on the Cisco ASA 5505, page 4-6](#)
- [Setting Up a PC for System Administration, page 4-6](#)
- [Optional Procedures, page 4-8](#)
- [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 Cisco ASA 5505 adaptive security appliance, as shown in [Figure 4-1](#).

Figure 4-1 Contents of Cisco ASA 5505 Package



PoE Ports and Devices

On the Cisco 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 and 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 Cisco 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 Cisco 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.

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

Installing the Chassis

You can wall-mount or rack-mount the Cisco ASA 5505. The part number for ordering a wall-mount kit for the Cisco ASA 5505 is ASA-5505-WALL-MNT=, the part number for ordering a rack-mount kit for the Cisco ASA 5505 is ASA5505-RACK-MNT=. For information on wall-mounting or rack-mounting the Cisco ASA 5505, see “[Mounting the ASA 5505 Chassis](#)” section in the *Cisco ASA 5500 Series Hardware Installation Guide*.

To install the Cisco ASA 5505, perform the following steps:

-
- Step 1** Place the chassis on a flat, stable surface.
- Step 2** Connect Port 0 to the public network (that is, the Internet):
- Use a yellow Ethernet cable to connect the device to a switch or hub.
 - 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.

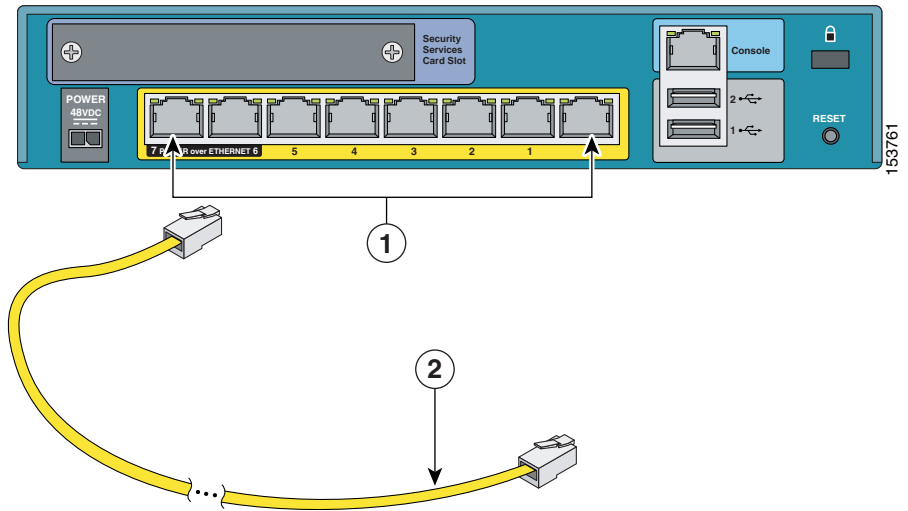
- Step 3** Connect your network devices with an Ethernet cable to one of the remaining seven switched ports (numbered 1 through 7).
- If you are connecting any Power over Ethernet (PoE) devices, connect them to one of the switch ports that support PoE (ports numbered 6 and 7).
-

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.)

Figure 4-2 Connecting to an Ethernet Interface



1	Ethernet switch ports	2	Ethernet cable
----------	-----------------------	----------	----------------

Step 3 Connect the other end of the Ethernet cable to a device, such as a router, desktop computer, or printer.



Note When connecting a computer to an inside port on the rear panel of the adaptive security appliance, use a straight through cable because ports 0 through 5 are switched ports and ports 6 and 7 are PoE ports and both require that you connect a straight through cable.

Powering on the Cisco ASA 5505

To power on the Cisco 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 Cisco 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 4-10](#).
-

Setting Up a PC for System Administration

You can perform setup, configuration and management tasks from a PC using the command-line interface or with 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 Cisco ASA 5505, perform the following steps:

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

By default, the Cisco 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 Cisco ASA 5505), which enables the PC to communicate with the Cisco 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. (Valid addresses are 192.168.1.2 through 192.168.1.254, with a mask of 255.255.255.0 and default route of 192.168.1.1.)

When you connect other devices to any of the inside ports, make sure that they do not have the same IP address.



Note The MGMT interface of the adaptive security appliance is assigned 192.168.1.1 by default, so this address is unavailable.

- Step 3** Use an Ethernet cable to connect the PC to a switched inside port on the rear panel of the Cisco 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 Cisco ASA 5505.

When connectivity is established, the LINK LED on the front panel of the Cisco 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 Cisco ASA 5505.

Optional Procedures

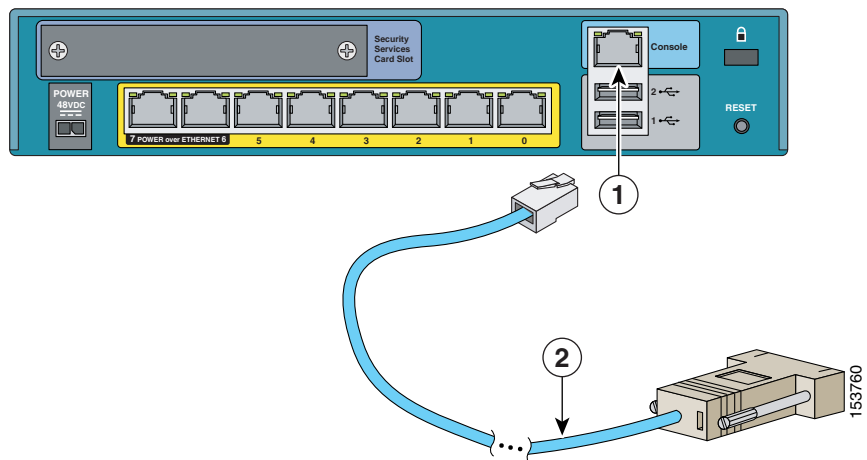
This section describes how to perform tasks that are not required for the initial setup of the Cisco ASA 5505. This section includes the following topics:

- “Connecting to the Console” section on page 4-8
- “Installing a Cable Lock” section on page 4-9

Connecting to the Console

You can access the command line for administration using the console port on the Cisco ASA 5505. To do so, you must run a serial terminal emulator on a PC or workstation, as shown in [Figure 4-3](#).

Figure 4-3 Connecting to the Console



1	Console port	2	Console cable
----------	--------------	----------	---------------

To connect a console for local, command-line administrative access, perform the following steps:

-
- Step 1** Plug one end (DB9) of the PC terminal adapter into a standard 9-pin PC serial port on your PC.
- Step 2** Plug the other end (RJ-45) of the blue console cable into the console port.
- Step 3** 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 Cisco 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 Cisco ASA 5505.
-

Ports and LEDs

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

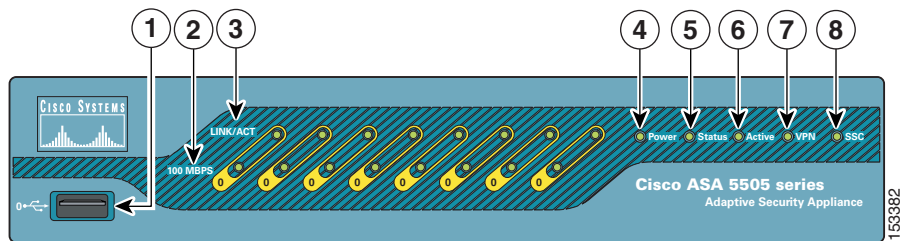
- [Front Panel Components, page 4-10](#)
- [Rear Panel Components, page 4-12](#)

Front Panel Components

The LINK/ACT indicators on the front panel of the Cisco 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 Cisco ASA 5505.

Figure 4-4 ASA 5505 Front Panel



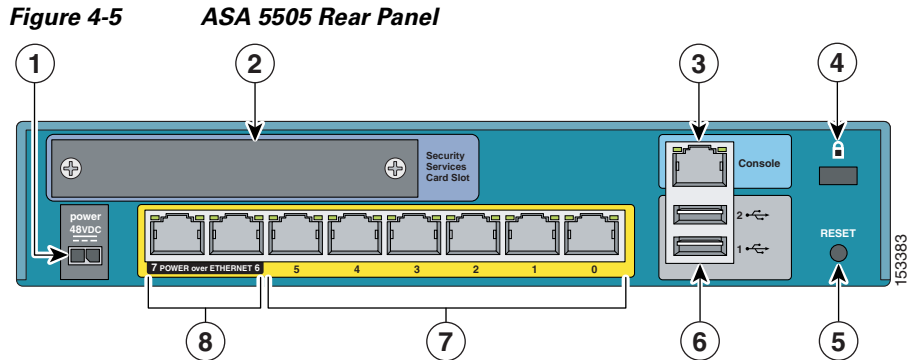
	Port / LED	Color	State	Description
1	USB Port	—	—	Reserved for future use.
2	Speed Indicators	Not lit	—	Network traffic is flowing at 10 Mbps.
		Green	On	Network traffic is flowing at 100 Mbps.
3	Link Activity Indicators	Green	Solid	The physical link established.*
		Green	Flashing	There is network activity.
4	Power	Green	On	The device is powered on.
		Off	—	The device is powered off.
5	Status	Green	Flashing	The power-up diagnostics are running or the system is booting.
			Solid	The system is operational.
		Amber	Solid	The system has encountered a problem.

	Port / LED	Color	State	Description
6	Active	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	VPN	Green	Solid	The VPN tunnel is established.
			Flashing	The system is initiating the VPN tunnel.
		Amber	Solid	The tunnel failed to initiate.
8	SSC	—	—	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 Cisco 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.

Rear Panel Components

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



	Port or LED	Purpose
1	Power connector	Attaching the power cord.
2	Security service card slot	Reserved for future use.
3	Serial console port	Managing the device using the CLI (command-line interface).
4	Lock device	Reserved for future use.
5	RESET button	Reserved for future use.
6	Two USB v2.0 ports	Reserved for future use.
7	Ethernet switch ports 0–7	Layer 2 switch ports that provide flexible VLAN configuration. Note Ethernet switch ports 6 and 7 also support PoE devices. If a PoE device is not attached, power is not supplied to the port and the device must be powered on its own.
8	PoE switch ports 6–7	Can be used for PoE devices, that is, devices that can be powered by the network interface, such as IP phones. These ports are the only ports that can be used 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, as are the ports numbered 0 through 5. If a PoE device is not attached, power is not supplied to the port and the device must be powered on its own.

What to Do Next

Continue with [Chapter 5, “Configuring the Adaptive Security Appliance.”](#)

■ What to Do Next



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](#)
- [Using the CLI for Configuration, page 5-3](#)
- [Using the Adaptive Security Device Manager for Configuration, page 5-3](#)
- [Running the ASDM Startup Wizard, page 5-10](#)
- [What to Do Next, page 5-11](#)

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 the following:

- Two VLANs: VLAN 1 and VLAN2
- VLAN 1 has the following properties:
 - Named “inside”

- Allocated switch ports Ethernet 0/1 through Ethernet 0/7
- 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.

The default configuration that ships with the adaptive security appliance, in most cases, is sufficient for your basic deployment. However, you can modify the default configuration so that you can customize the security policy to suit your deployment. To modify the default settings, you can use the ASDM or the CLI. In ASDM, run the Startup Wizard to change the following settings from their factory default settings:

- Hostname
- Domain name
- Administrative passwords
- IP address of the outside interface
- Interfaces such as DMZ interfaces
- Address translation rules
- Dynamic IP address settings for the inside interface

For more information about configuring the adaptive security appliance by using ASDM, see the online Help.

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

Using the CLI for Configuration

In addition to the ASDM web configuration tool, you can configure the adaptive security appliance by using the command-line interface.

You can get step-by-step examples of how to configure basic remote access and LAN-to-LAN connections in the CLI itself by using the `vpnsetup ipsec-remote-access` steps and `vpnsetup site-to-site` steps commands. For more information about these commands, see the *Cisco Security Appliance Command Reference*.

For step-by-step configuration procedures for all functional areas of the adaptive security appliance, see the *Cisco Security Appliance Command Line Configuration Guide*.

Using the Adaptive Security Device Manager for Configuration

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.

This section includes the following topics:

- [Preparing to Use ASDM, page 5-5](#)
- [Gathering Configuration Information for Initial Setup, page 5-5](#)
- [Installing the ASDM Launcher, page 5-6](#)
- [Starting ASDM with a Web Browser, page 5-9](#)

Preparing to Use ASDM

Before you can use ASDM, perform the following steps:

Step 1 If you have not already done so, connect the MGMT interface to a switch or hub by using the Ethernet cable. To this same switch, connect a PC for configuring the adaptive security appliance.

Step 2 Configure your PC to use DHCP (to receive an IP address automatically from the adaptive security appliance), 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. (Valid addresses are 192.168.1.2 through 192.168.1.254, with a mask of 255.255.255.0 and default route of 192.168.1.1.)

When you connect other devices to any of the inside ports, make sure that they do not have the same IP address.



Note The MGMT interface of the adaptive security appliance is assigned 192.168.1.1 by default, so this address is unavailable.

Step 3 Check the LINK LED on the MGMT interface.

When a connection is established, the LINK LED interface on the adaptive security appliance and the corresponding LINK LED on the switch or hub turn solid green.

Gathering Configuration Information for Initial Setup

Gather 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.)
 - 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.
-

Installing the ASDM Launcher

You can launch ASDM in either of two ways: by downloading the ASDM Launcher software so that ASDM runs locally on your PC, or by enabling Java and JavaScript in your web browser and accessing ASDM remotely from your PC. This procedure describes how to set up your system to run ASDM locally.

To install the ASDM Launcher, perform the following steps:

-
- Step 1** On the PC connected to the switch or hub, launch an Internet browser.
- a. In the address field of the browser, enter this URL:
`https://192.168.1.1/admin.`



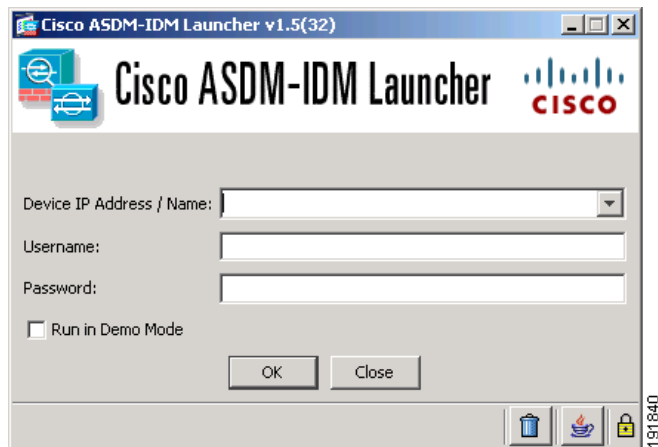
Note The adaptive security appliance ships with a default IP address of 192.168.1.1. Remember to add the “s” in “**https**” or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the adaptive security appliance.

The Cisco ASDM splash screen appears.

- b.** Click **Install ASDM Launcher and Run ASDM**.
- c.** In the dialog box that requires a username and password, leave both fields empty. Click **OK**.
- d.** Click **Yes** to accept the certificates. Click **Yes** for all subsequent authentication and certificate dialog boxes.
- e.** When the File Download dialog box opens, click **Open** to run the installation program directly. It is not necessary to save the installation software to your hard drive.
- f.** When the InstallShield Wizard appears, follow the instructions to install the ASDM Launcher software.

Step 2 From your desktop, start the Cisco ASDM Launcher software.

A dialog box appears.



Step 3 Enter the IP address or the host name of your adaptive security appliance.

Step 4 Leave the Username and Password fields blank.



Note By default, there is no Username and Password set for the Cisco ASDM Launcher.

Step 5 Click OK.

Step 6 If you receive a security warning containing a request to accept a certificate, click **Yes**.

The ASA checks to see if there is updated software and if so, downloads it automatically.

The main ASDM window appears.

The screenshot displays the Cisco ASDM 6.1 for ASA web interface. The main window is titled "Cisco ASDM 6.1 for ASA - 10.86.194.224". The interface is divided into several sections:

- Device Information:** Shows host name (asa2.cisco.com), ASA version (8.0(4)), ASDM version (6.1(3)), firewall mode (Routed), total flash (64 MB), total memory (256 MB), device uptime (46d 15h 59m 34s), device type (ASA 5510), and context mode (Single).
- Interface Status:** A table showing interface details:

Interface	IP Address/Mask	Line	Link	Kbps
faildata	192.168.3.4/24	down	down	0
inside	no ip address	down	down	0
management	192.168.1.1/24	down	down	0
outside	10.86.194.224/23	up	up	120
- System Resources Status:** Shows CPU usage (3%) and Memory usage (132MB).
- Traffic Status:** Displays graphs for "Connections Per Second Usage" and "outside Interface Traffic Usage (Kbps)".
- Latest ASDM Syslog Messages:** A table of recent messages:

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destination	Description
6	Oct 14 2008	13:55:31	725007	171.69.39.67	1748			SSL session with client outside:171.69.39.67/1748 terminated.
6	Oct 14 2008	13:55:31	605005	171.69.39.67	1748	10.86.194.224	https	Login permitted from 171.69.39.67/1748 to outside:10.86.194.224/https for user "enable_15"
6	Oct 14 2008	13:55:31	725002	171.69.39.67	1748			Device completed SSL handshake with client outside:171.69.39.67/1748
6	Oct 14 2008	13:55:31	725003	171.69.39.67	1748			SSL client outside:171.69.39.67/1748 permit to resume previous session

The status bar at the bottom indicates "Device configuration loaded successfully." and the user is logged in as "admin".

ASDM starts and the main window appears.

Starting ASDM with a Web Browser

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.

Running the ASDM Startup Wizard

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

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

-
- Step 1** From the Wizards menu at the top of the ASDM window, choose Startup Wizard.
- Step 2** 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.

**Note**

If you get an error requesting a DES license or a 3DES-AES license, see [Appendix A, “Obtaining a 3DES/AES License”](#) for information.

**Note**

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:

To Do This...	See...
Configure the adaptive security appliance to protect a DMZ web server	Chapter 6, “Scenario: DMZ Configuration”
Configure the adaptive security appliance for remote-access VPN	Chapter 7, “Scenario: IPsec Remote-Access VPN Configuration”
Configure the adaptive security appliance for SSL VPN connections using software clients	Chapter 8, “Scenario: Configuring Connections for a Cisco AnyConnect VPN Client”
Configure the adaptive security appliance for SSL VPN connections using a web browser	Chapter 9, “Scenario: SSL VPN Clientless Connections”
Configure the adaptive security appliance for site-to-site VPN	Chapter 10, “Scenario: Site-to-Site VPN Configuration”
Configure the adaptive security appliance as an Easy VPN remote device	Chapter 11, “Scenario: Easy VPN Hardware Client Configuration”

■ What to Do Next



CHAPTER 6

Scenario: DMZ Configuration



Note

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

A demilitarized zone (DMZ) is a separate network located in the neutral zone between a private (inside) network and a public (outside) network.

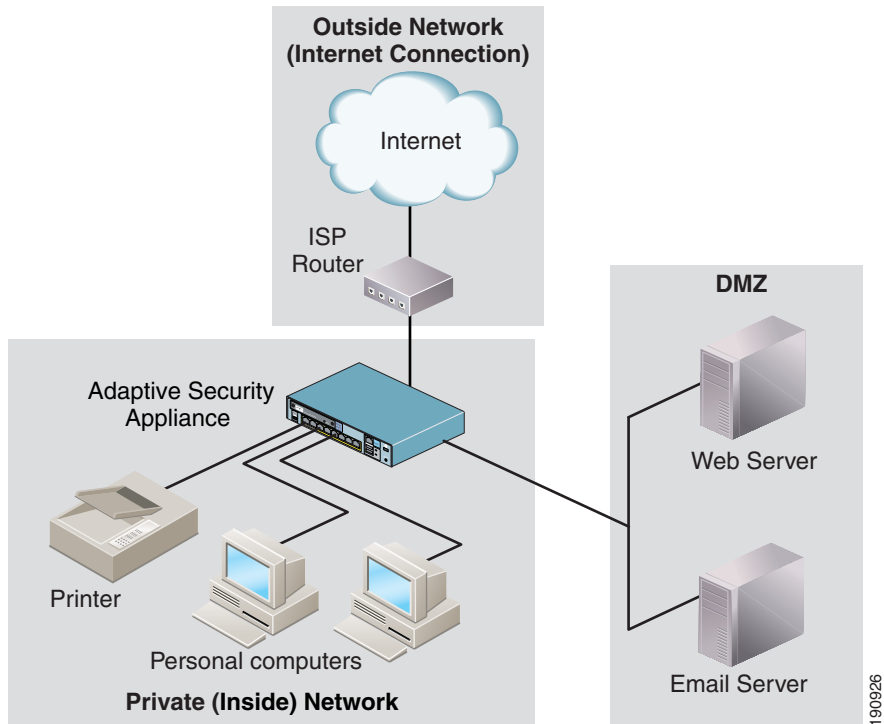
This chapter includes the following sections:

- [Basic Network Layout for a DMZ Configuration, page 6-1](#)
- [Example DMZ Network Topology, page 6-2](#)
- [Configuring the Security Appliance for a DMZ Deployment, page 6-10](#)
- [What to Do Next, page 6-24](#)

Basic Network Layout for a DMZ Configuration

The network topology in [Figure 6-1](#) is typical of most DMZ implementations of the adaptive security appliance. In this deployment, the web server is on the DMZ interface, and HTTP clients from both the inside and outside networks can access the web server.

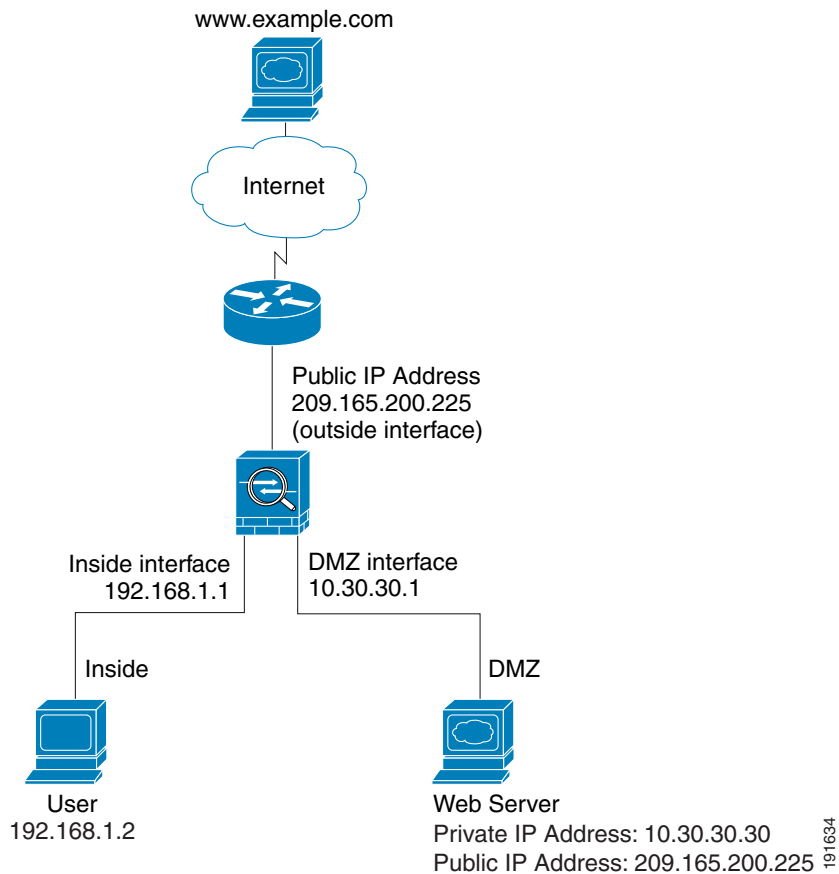
Figure 6-1 Private Network with DMZ



Example DMZ Network Topology

The chapter describes how to configure a DMZ deployment of the adaptive security appliance, as shown in [Figure 6-2](#).

Figure 6-2 Network Layout for DMZ Configuration Scenario



This example scenario has the following characteristics:

- The web server is on the DMZ interface of the adaptive security appliance.
- Clients on the inside 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 coming from the Internet is denied.
- The network has one IP address that is publicly available: the outside interface of the adaptive security appliance (`209.165.200.225`). This public address is shared by the adaptive security appliance and the DMZ web server.

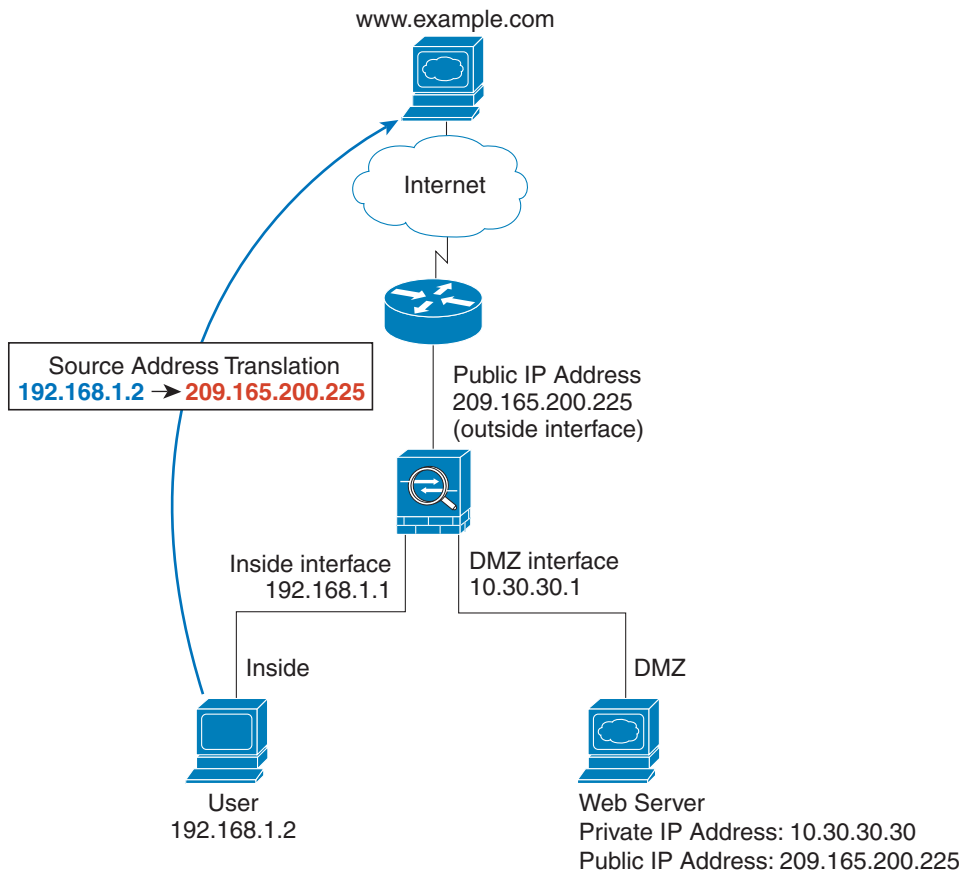
This section includes the following topics:

- [An Inside User Visits a Web Server on the Internet](#), page 6-4
- [An Internet User Visits the DMZ Web Server](#), page 6-6
- [An Inside User Visits the DMZ Web Server](#), page 6-8

An Inside User Visits a Web Server on the Internet

[Figure 6-3](#) shows the traffic flow through the adaptive security appliance when an inside user requests an HTTP page from a web server on the Internet.

Figure 6-3 An Inside User Visits an Internet Web Server



191799

When an inside user requests an HTTP page from a web server on the Internet, data moves through the adaptive security appliance as follows:

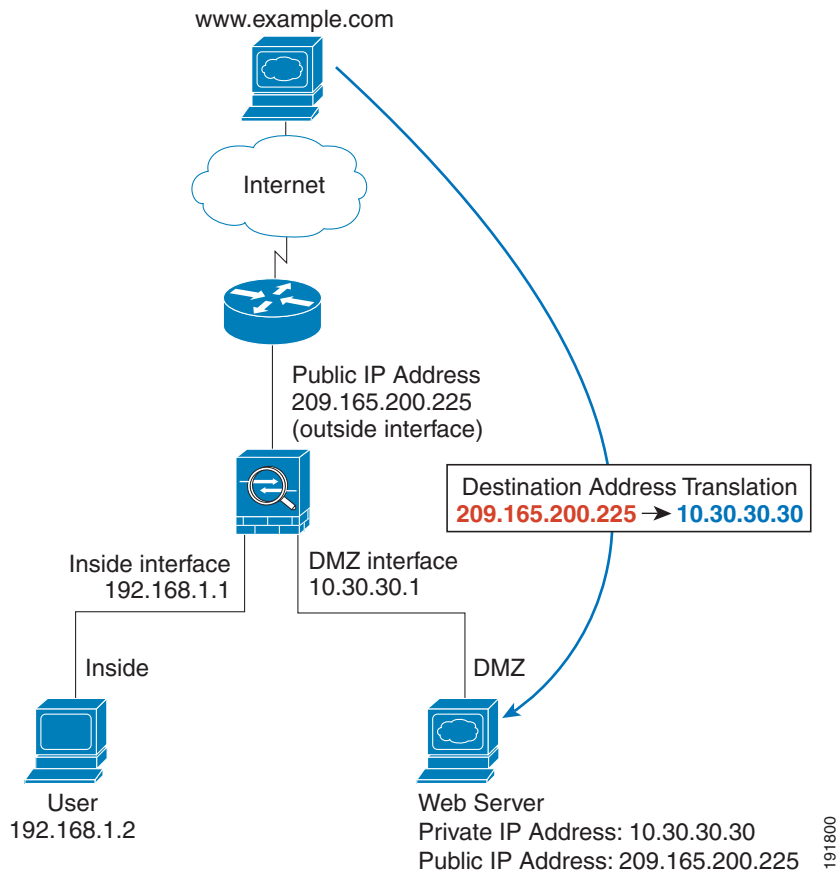
1. The user on the inside network requests a web page from www.example.com.
2. The adaptive security appliance receives the packet and, because it is a new session, verifies that the packet is allowed.
3. The adaptive security appliance performs network address translation (NAT) to translate the local source address (192.168.1.2) to the public address of the outside interface (209.165.200.225).

4. The adaptive security appliance records that a session is established and forwards the packet from the outside interface.
5. When `www.example.com` responds to the request, the packet goes through the adaptive security appliance using the established session.
6. The adaptive security appliance uses NAT to translate the public destination address (209.165.200.225) to the local user address, 192.168.1.2.
7. The adaptive security appliance forwards the packet to the inside user.

An Internet User Visits the DMZ Web Server

Figure 6-4 shows the traffic flow through the adaptive security appliance when a user on the Internet requests a web page from the DMZ web server.

Figure 6-4 An Outside User Visits the DMZ Web Server



When a user on the Internet requests an HTTP page from the DMZ web server, traffic flows through the adaptive security appliance as follows:

1. A user on the outside network requests a web page from the DMZ web server using the public IP address of the adaptive security appliance (209.165.200.225, the IP address of the outside interface).
2. The adaptive security appliance receives the packet and, because it is a new session, verifies that the packet is allowed.

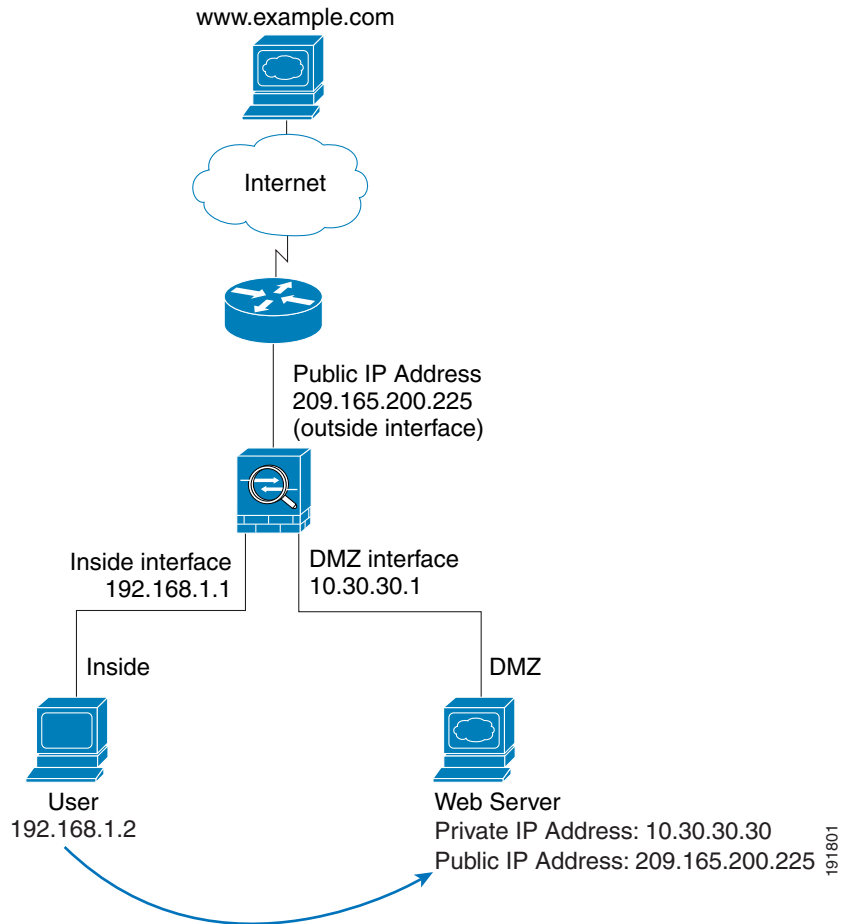
191800

3. The adaptive security appliance translates the destination address to the local address of the DMZ web server (10.30.30.30) and forwards the packet through the DMZ interface.
4. When the DMZ web server responds to the request, the adaptive security appliance translates the local source address to the public address of the DMZ web server (209.165.200.225).
5. The adaptive security appliance forwards the packet to the outside user.

An Inside User Visits the DMZ Web Server

Figure 6-5 shows an inside user accessing the DMZ web server.

Figure 6-5 *An Inside User Visits a Web Server on the DMZ*



In [Figure 6-5](#), 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.

191801

2. The internal client requests a web page from the public IP address of the DMZ web server. The adaptive security appliance receives the request on its inside interface.
3. The adaptive security appliance translates the public IP address of the DMZ web server to its real address (209.165.200.225 -> 10.30.30.30) and forwards the request out of its DMZ interface to the web server.
4. When the DMZ web server responds to the request, the adaptive security appliance receives the data on its DMZ interface and forwards the data out of its inside interface to the user.

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 6-2](#). 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 6-11
- [Information to Have Available](#), page 6-11
- [Enabling Inside Clients to Communicate with Devices on the Internet](#), page 6-12
- [Enabling Inside Clients to Communicate with Devices on the Internet](#), page 6-12

- [Enabling Inside Clients to Communicate with the DMZ Web Server, page 6-12](#)
- [Configuring Static PAT for Public Access to the DMZ Web Server \(Port Forwarding\), page 6-17](#)
- [Providing Public HTTP Access to the DMZ Web Server, page 6-21](#)

The remainder of this chapter provides instructions for how to implement this configuration.

Configuration Requirements

This DMZ deployment of the adaptive security appliance requires the following configuration rules:

So That...	Create These Rules...
Internal clients can request information from web servers on the Internet	The adaptive security appliance comes with a default configuration that permits inside clients access to devices on the Internet. No additional configuration is required.
Internal clients can request information from the DMZ web server	<ul style="list-style-type: none"> • 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 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 DMZ web server (10.30.30.30 to 10.30.30.30).
External clients can request information from the DMZ web server	<ul style="list-style-type: none"> • An address translation rule between the outside and DMZ interfaces that translates the public IP address of the DMZ web server to its private IP address (209.165.200.225 to 10.30.30.30). • An access control rule permitting incoming HTTP traffic that is destined for the DMZ web server.

Information to Have Available

Before you begin this configuration procedure, collect the following information:

- Internal IP address of the server inside the DMZ that you want to make available to clients on the public network (in this scenario, a web server).
- Public IP addresses to be used for servers inside the DMZ. (Clients on the public network will use the public IP address to access the server inside the DMZ.)
- Client IP address to substitute for internal IP addresses in outgoing traffic. (Outgoing client traffic will appear to come from this address so that the internal IP address is not exposed.)

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 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).

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.

**Note**

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.

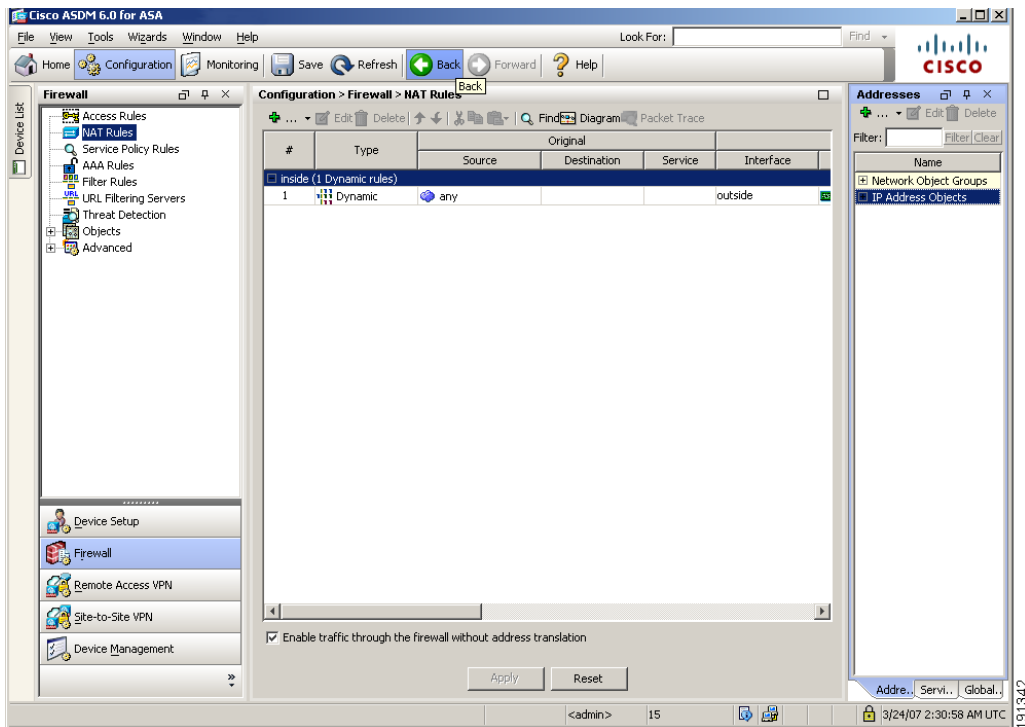
This section includes the following topics:

- [Translating Internal Client IP Addresses Between the Inside and DMZ Interfaces, page 6-13](#)
- [Translating the Public Address of the Web Server to its Real Address on the Inside Interface, page 6-15](#)

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, choose **Configuration > Firewall > NAT Rules**.



Step 2 Click the green **plus (+)** icon and choose **Add Static NAT Rule**.

The Add Static NAT Rule dialog box appears.

- Step 3** In the Original area, specify the IP address to be translated. For this scenario, address translation for inside clients is performed for the entire 192.168.1.0 subnet.
- From the Interface drop-down list, choose the Inside interface.
 - In the Source field, enter the IP address of the client or network. In this scenario, the IP address of the network is 192.168.1.0.
- Step 4** In the Translated area, do the following:
- From the Interface drop-down list, choose the DMZ interface.
 - In the IP Address field, enter the IP address of the internal client or network. In this scenario, the IP address of the network is 192.168.1.0.

Add Static NAT Rule

Original

Interface: inside

Source: 192.168.1.0/24

Translated

Interface: dmz

Use IP Address: 192.168.1.0/24

Use Interface IP Address

Port Address Translation (PAT)

Enable Port Address Translation (PAT)

Protocol: TCP UDP

Original Port:

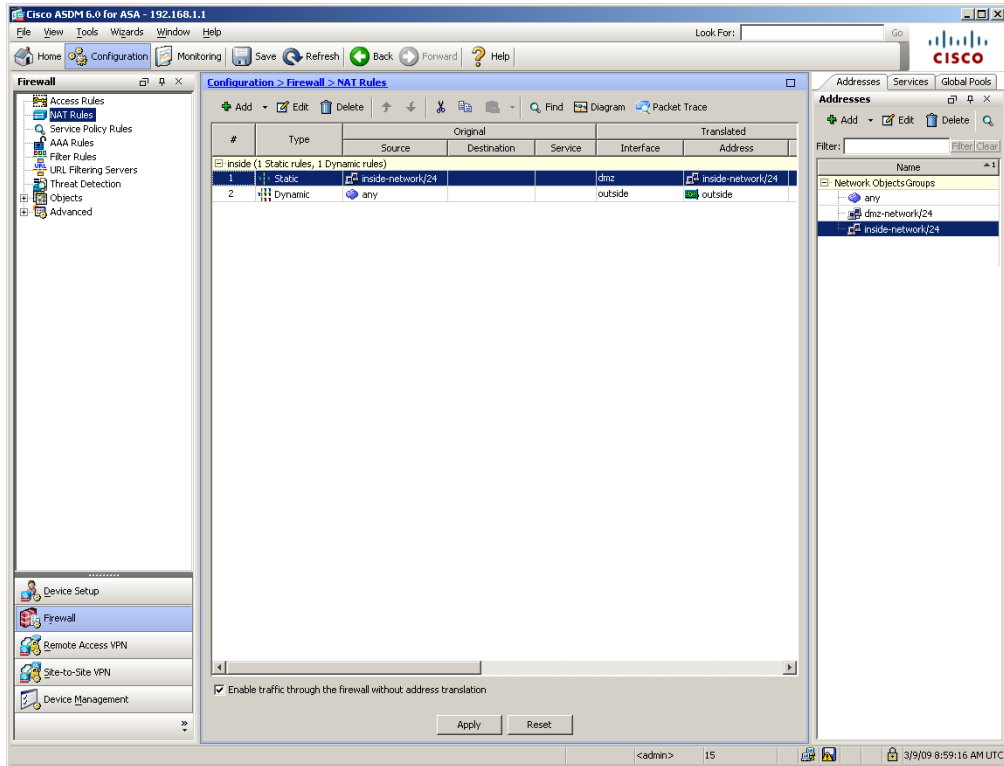
Translated Port:

Connection Settings

OK Cancel Help

- Click **OK** to add the static NAT rule and return to the Configuration > Firewall > NAT Rules pane.

- Step 5** Review the configuration pane to verify that the translation rule appears as you expected. The rule should appear similar to the following:



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

Translating the Public Address of the Web Server to its Real Address on the Inside Interface

To configure a 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 Configuration > Firewall > NAT Rules pane, click the green **plus (+)** icon and choose **Add Static NAT Rule**.

The Add Static NAT Rule dialog box appears.

- Step 2** In the Original area, do the following:
- From the Interface drop-down list, choose DMZ.
 - In the Source field, 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 **10.30.30.30**.
- Step 3** In the Translated area, do the following:
- From the Interface drop-down list, choose Inside.
 - 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 **209.165.200.225**.

Add Static NAT Rule

Original

Interface: DMZ

Source: 10.30.30.30

Translated

Interface: inside

Use IP Address: 209.165.200.225

Use Interface IP Address

Port Address Translation (PAT)

Enable Port Address Translation (PAT)

Protocol: TCP UDP

Original Port:

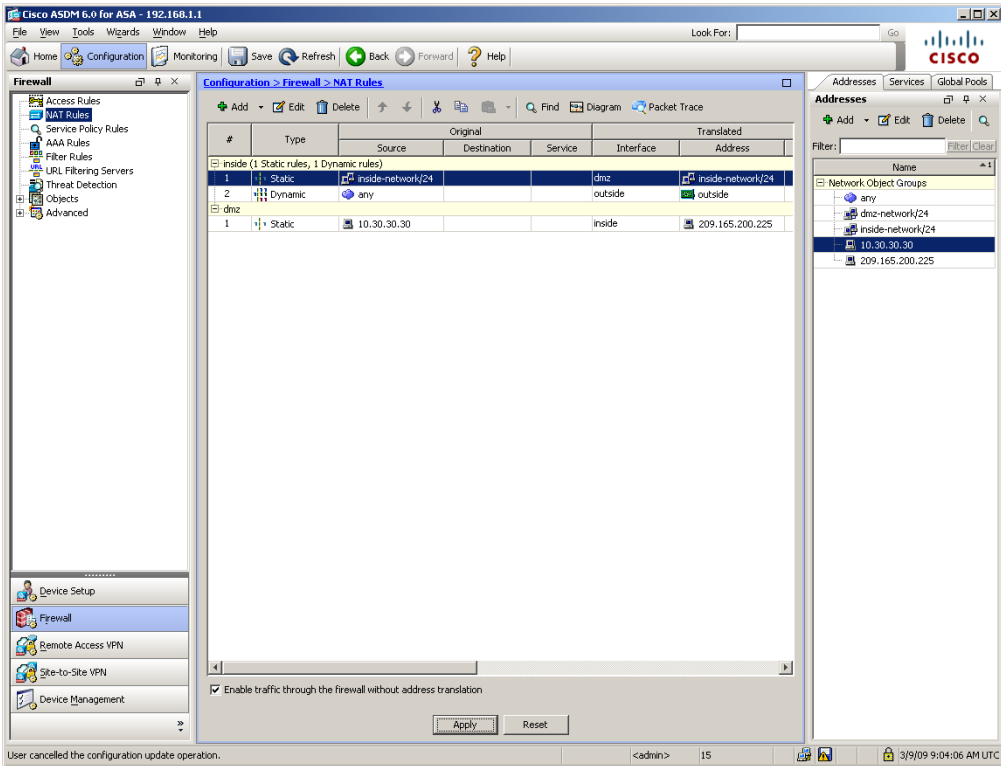
Translated Port:

Connection Settings

OK Cancel Help

191336

- Step 4** Click **OK** to return to the Configuration > Firewall > NAT Rules pane. The configuration should look similar to the following:



- Step 5** Click **Apply** to complete the adaptive security appliance configuration changes.

Configuring Static PAT for Public Access to the DMZ Web Server (Port Forwarding)

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. In this scenario the DMZ web server shares a public IP address with the outside interface of the adaptive security appliance (209.165.200.225).

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 Configuration > Firewall > NAT Rules pane, choose Add Static NAT Rule from the Add drop-down list.
- The Add Static NAT Rule dialog box appears.
- Step 2** In the Original area, specify the real IP address of the web server:
- From the Interface drop-down list, choose the DMZ interface.
 - Enter the real IP address of the DMZ web server. In this scenario, the IP address is **10.30.30.30**.
- Step 3** In the Translated area, specify the public IP address to be used for the web server:
- From the Interface drop-down list, choose Outside.
 - Click the **Use Interface IP Address** radio button, which is the IP address for the specified outside interface, in this case.

The screenshot shows the 'Add Static NAT Rule' dialog box. It has a title bar with a close button. The dialog is organized into several sections:

- Original:** Interface: dmz; Source: 10.30.30.30
- Translated:** Interface: outside; Use IP Address: (empty); Use Interface IP Address: (selected)
- Port Address Translation (PAT):** Enable Port Address Translation (PAT): (checked); Protocol: TCP (selected), UDP (unselected); Original Port: 80; Translated Port: 80
- Connection Settings:** (collapsed)
- Buttons:** OK, Cancel, Help

Step 4 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 IP address (IP address of the Outside interface) of the adaptive security appliance. To configure Port Address Translation, perform the following steps:

- a. Check the **Enable Port Address Translation** check box.
- b. Click the **TCP Protocol** radio button.
- 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).

Configuring the Security Appliance for a DMZ Deployment

Step 5 Confirm that the rule was created the way you expected. The displayed configuration should be similar to the following:

The screenshot shows the Cisco ASDM 6.0 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Firewall > NAT Rules". The left sidebar shows the "Firewall" tree with "NAT Rules" selected. The main pane displays a table of NAT rules:

#	Type	Source	Destination	Service	Interface	Translated Address
inside (1 Static rules, 1 Dynamic rules)						
1	Static	inside-network/24			dmz	inside-network/24
2	Dynamic	any			outside	outside
dmz						
1	Static	10.30.30.30		http	outside	209.165.200.225
2	Static	10.30.30.30			inside	209.165.200.225

Below the table, the checkbox "Enable traffic through the firewall without address translation" is checked. At the bottom of the main pane are "Apply" and "Reset" buttons. The right pane shows the "Addresses" section with a list of "Network Object Groups" including "any", "dmz-network/24", "inside-network/24", "10.30.30.30", and "209.165.200.225". The status bar at the bottom indicates "Configuration changes saved successfully." and the user is logged in as "admin".

Step 6 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.

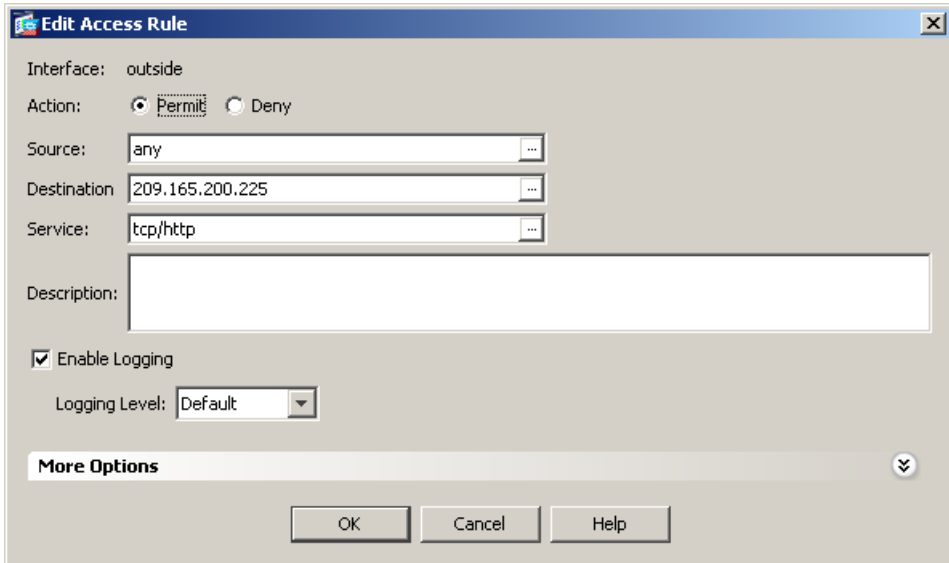
In this section, you create an access rule that permits incoming HTTP traffic originating from any host or network on the Internet, if the destination of the traffic is the web server on the DMZ network. All other traffic coming in from the public network is denied.

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

-
- Step 1** In the ASDM main window, do the following:
- Choose **Configuration > Firewall > Access Rules**.
 - Click the green **plus (+)** icon, then choose **Add Access Rule**.
The Add Access Rule dialog box appears.

- Step 2** In the Add Access Rule dialog box, do the following:
- From the Interface pull-down list, choose **Outside**.
 - Click the **Permit Action** radio button.
 - In the Source field, enter **Any**.
 - In the Destination field, enter the public IP address of the web server (**209.165.200.225**).
 - In the Service field, enter **TCP/HTTP**.

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

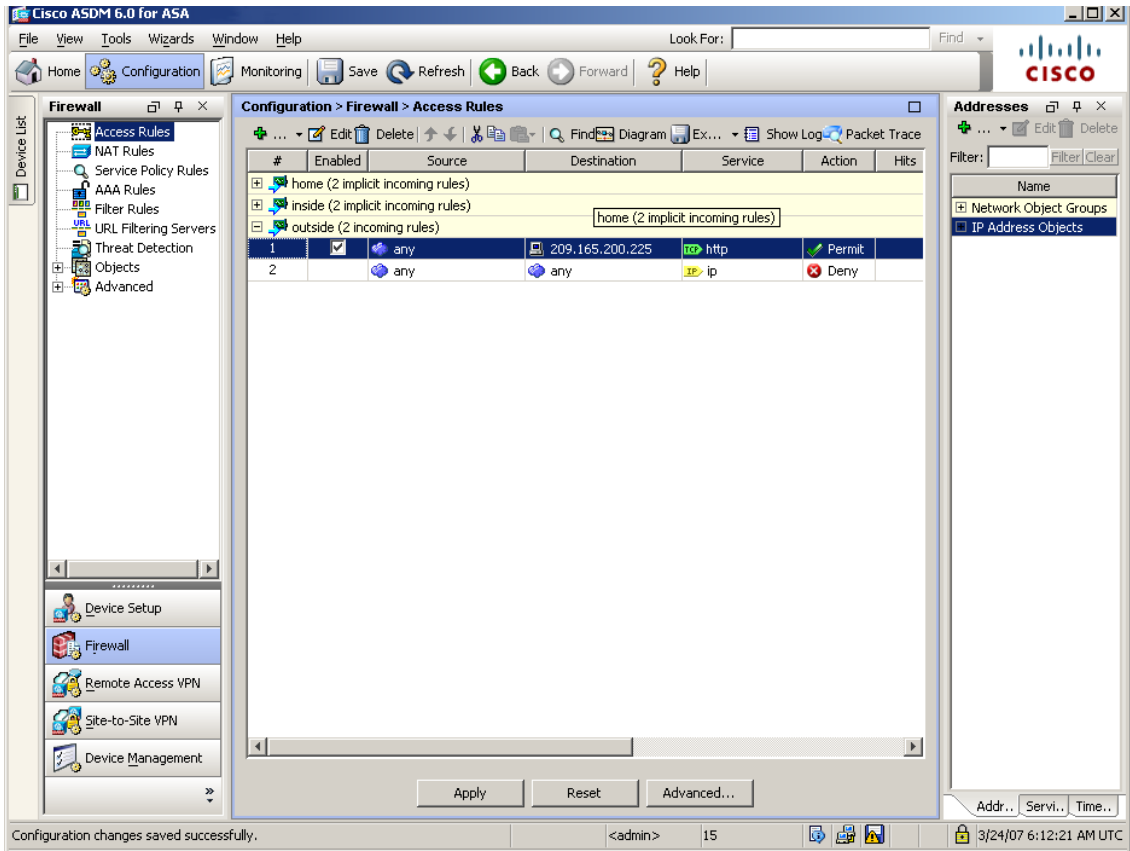


The screenshot shows the 'Edit Access Rule' dialog box with the following configuration:

- Interface: outside
- Action: Permit Deny
- Source: any
- Destination: 209.165.200.225
- Service: tcp/http
- Description: (empty text box)
- Enable Logging
- Logging Level: Default
- More Options: (collapsed)

Buttons: OK, Cancel, Help

- f. Click **OK** to return to the Security Policy > Access Rules pane.
The displayed configuration should be similar to the following:



- g. Verify that the information you entered is accurate.
- h. Click **Apply** to save the configuration changes to the configuration that the adaptive security appliance is currently running.

With this setting, clients on the public network can resolve HTTP requests for content from the DMZ web server, while keeping the private network secure.

- Step 3** 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, choose **Save**.

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

If you do not save the configuration changes, the previous configuration takes effect the next time that 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:

To Do This...	See...
Refine configuration and configure optional and advanced features	<i>Cisco Security Appliance Command Line Configuration Guide</i>
Learn about daily operations	<i>Cisco Security Appliance Command Reference</i> <i>Cisco Security Appliance System Log Messages Guide</i>

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.

To Do This...	See...
Configure a remote-access VPN	Chapter 7, “Scenario: IPsec Remote-Access VPN Configuration”
Configure an SSL VPN for Cisco AnyConnect software clients	Chapter 8, “Scenario: Configuring Connections for a Cisco AnyConnect VPN Client”
Configure a browser-based SSL VPN	Chapter 9, “Scenario: SSL VPN Clientless Connections”
Configure a site-to-site VPN	Chapter 10, “Scenario: Site-to-Site VPN Configuration”



CHAPTER 7

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. In this type of VPN configuration, remote users must be running the Cisco VPN client to connect to the adaptive security appliance.

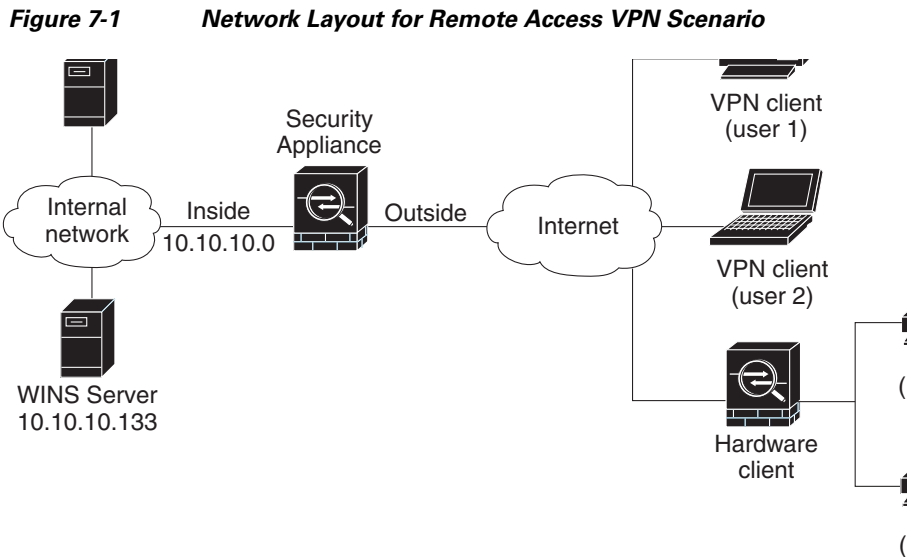
If you are implementing an Easy VPN solution, this chapter describes how to configure the Easy VPN server (sometimes called a headend device).

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 7-19](#)

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 7-7](#)
- [Specifying the VPN Tunnel Group Name and Authentication Method, page 7-8](#)

- [Specifying a User Authentication Method, page 7-9](#)
- [\(Optional\) Configuring User Accounts, page 7-11](#)
- [Configuring Address Pools, page 7-12](#)
- [Configuring Client Attributes, page 7-13](#)
- [Configuring the IKE Policy, page 7-14](#)
- [Configuring IPsec Encryption and Authentication Parameters, page 7-16](#)
- [Specifying Address Translation Exception and Split Tunneling, page 7-17](#)
- [Verifying the Remote-Access VPN Configuration, page 7-18](#)

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 a 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

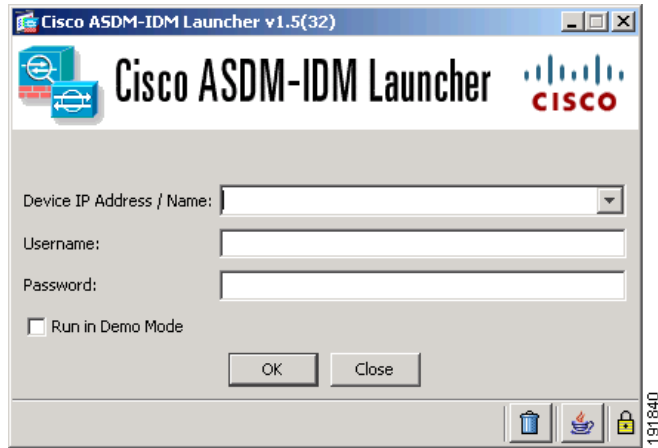
Starting ASDM

This section describes how to start ASDM using the ASDM Launcher software. If you have not installed the ASDM Launcher software, see [Installing the ASDM Launcher, page 5-6](#).

If you prefer to access ASDM directly with a web browser or using Java Web Start, see [Starting ASDM with a Web Browser, page 5-9](#).

To start ASDM using the ASDM Launcher software, perform the following steps:

- Step 1** From your desktop, start the Cisco ASDM Launcher software.
The Cisco ASDM-IDM Launcher dialog box appears.



- Step 2** Enter the IP address or the host name of your adaptive security appliance.
Step 3 Leave the Username and Password fields blank.



Note By default, no Username or Password is set for the Cisco ASDM Launcher.

- Step 4** Click **OK**.
Step 5 If you receive a security warning that includes a request to accept a certificate, click **Yes**.

The adaptive security appliance checks to see if there is updated software and if so, downloads it automatically.

The ASDM main window appears.

The screenshot displays the Cisco ASDM 6.1 for ASA interface for device 10.86.194.224. The interface is divided into several sections:

- Device Information:**
 - Host Name: asa2.cisco.com
 - ASA Version: 8.0(4)
 - ASDM Version: 6.1(3)
 - Firewall Mode: Routed
 - Total Flash: 64 MB
 - Device Uptime: 46d 15h 59m 34s
 - Device Type: ASA 5510
 - Context Mode: Single
 - Total Memory: 256 MB
- Interface Status:**

Interface	IP Address/Mask	Line	Link	Kbps
fa/ldata	192.168.3.4/24	down	down	0
inside	no ip address	down	down	0
management	192.168.1.1/24	down	down	0
outside	10.86.194.224/23	up	up	120
- VPN Sessions:**
 - IPSec: 0
 - Clientless SSL VPN: 0
 - SSL VPN Client: 0
- System Resources Status:**
 - CPU Usage (percent):** 3%
 - Memory Usage (MB):** 13 MB
- Traffic Status:**
 - Connections Per Second Usage:** Graph showing UDP (0), TCP (0), and Total (0) connections per second.
 - 'outside' Interface Traffic Usage (Kbps):** Graph showing traffic usage on the outside interface.
- Latest ASDM Syslog Messages:**

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
6	Oct 14 2008	13:55:31	725007	171.69.39.67	1748			SSL session with client outside:171.69.39.67/1748 terminated.
6	Oct 14 2008	13:55:31	605005	171.69.39.67	1748	10.86.194.224	https	Login permitted from 171.69.39.67/1748 to outside:10.86.194.224/https for user "enable_15"
6	Oct 14 2008	13:55:31	725002	171.69.39.67	1748			Device completed SSL handshake with client outside:171.69.39.67/1748
6	Oct 14 2008	13:55:31	725003	171.69.39.67	1748			SSL client outside:171.69.39.67/1748 permitted to resume previous session.

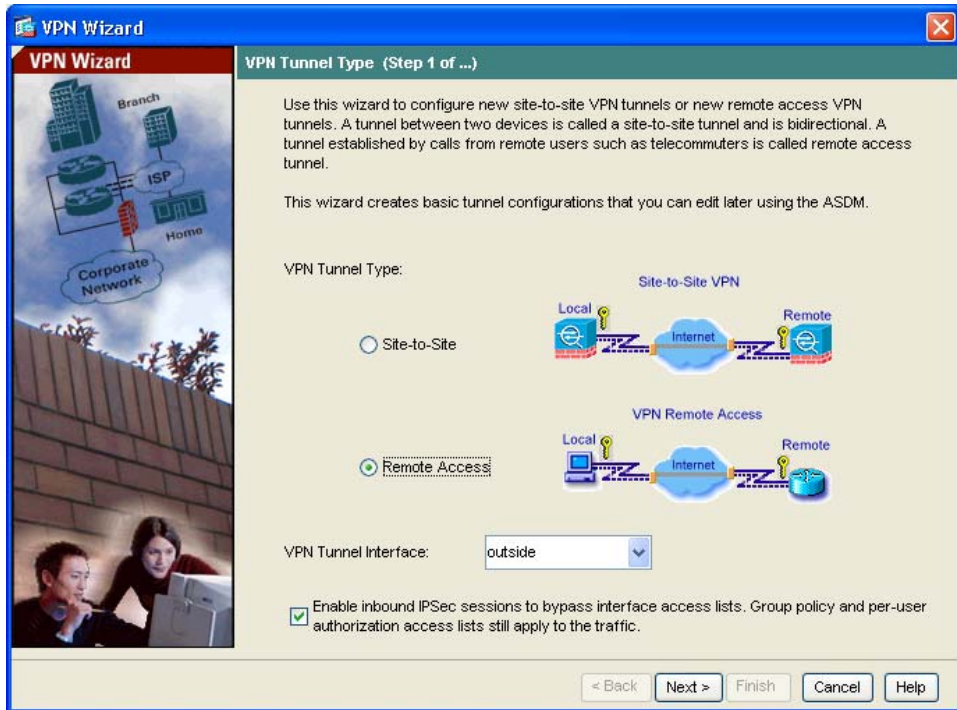
Device configuration loaded successfully. Status: <admin> 15. Time: 10/14/08 1:55:28 PM EDT.

Configuring the ASA 5505 for an IPsec Remote-Access VPN

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

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

Implementing the IPsec Remote-Access VPN Scenario



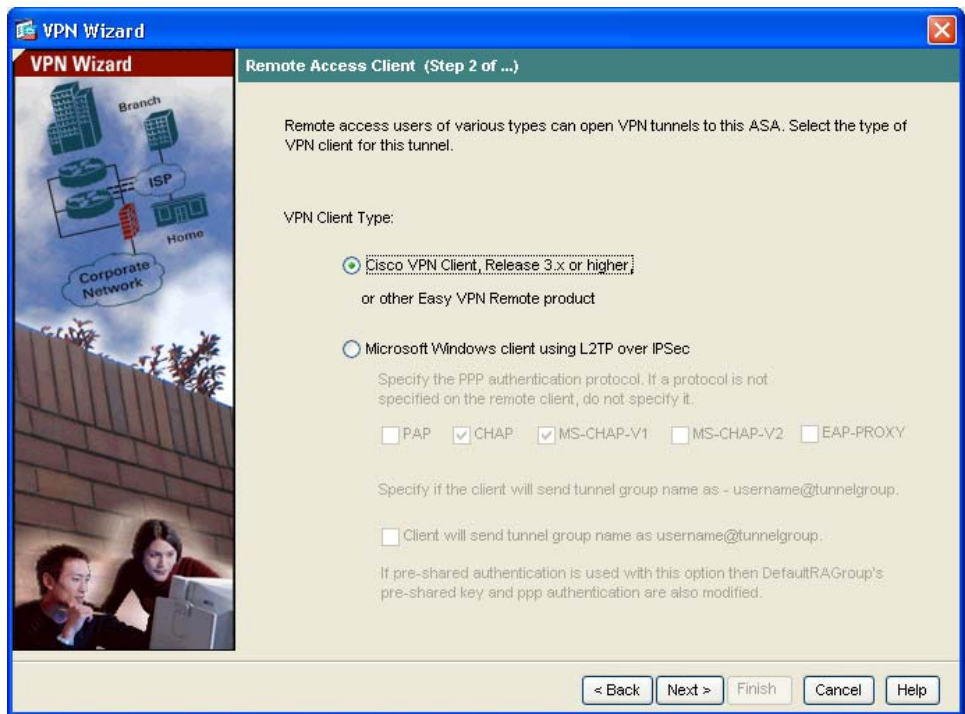
- Step 2** In Step 1 of the VPN Wizard, perform the following steps:
- a. Click the **Remote Access** radio button.
 - b. From the drop-down list, choose **Outside** as the enabled interface for the incoming VPN tunnels.
 - c. Click **Next** to continue.

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

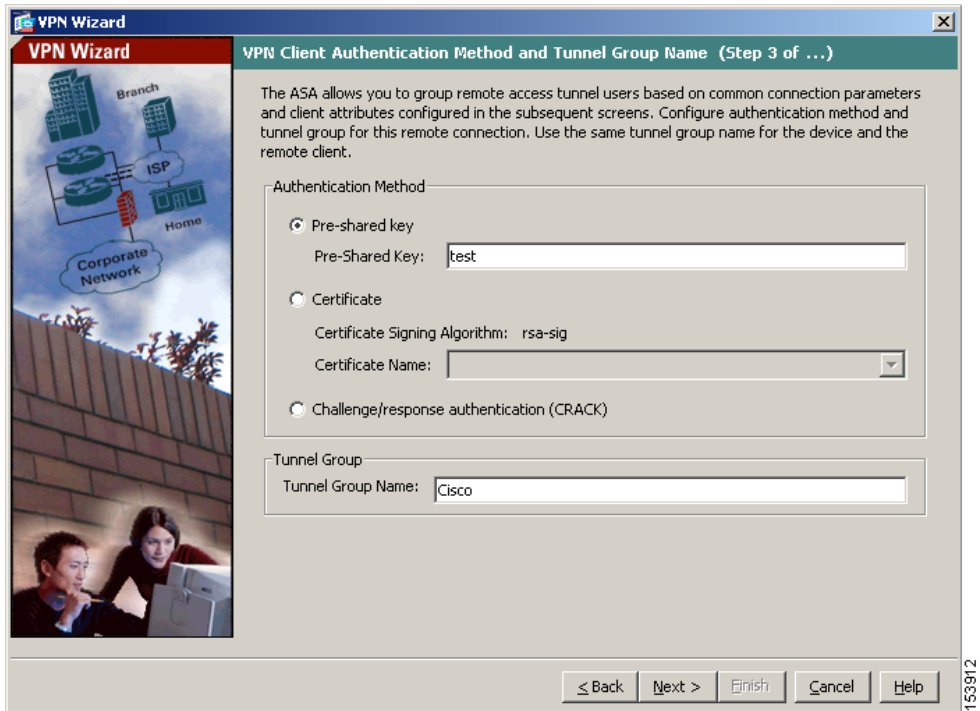
In Step 3 of the VPN Wizard, perform the following steps:

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.



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.

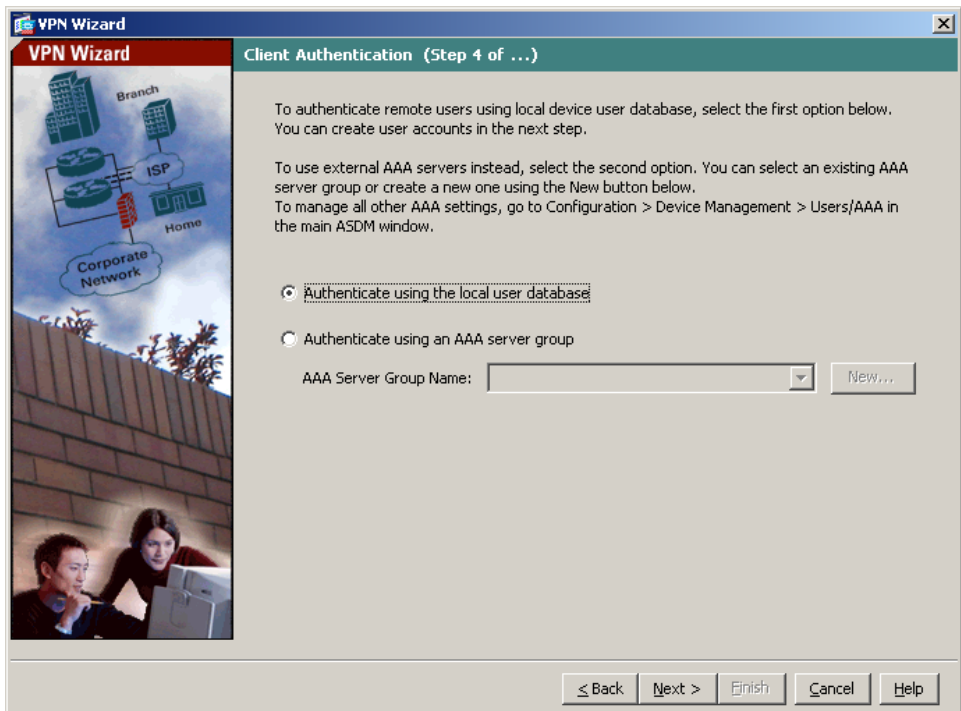
Specifying a User Authentication Method

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).

Implementing the IPsec Remote-Access VPN Scenario

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:
- Click the **Authenticate Using an AAA Server Group** radio button.
 - 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.



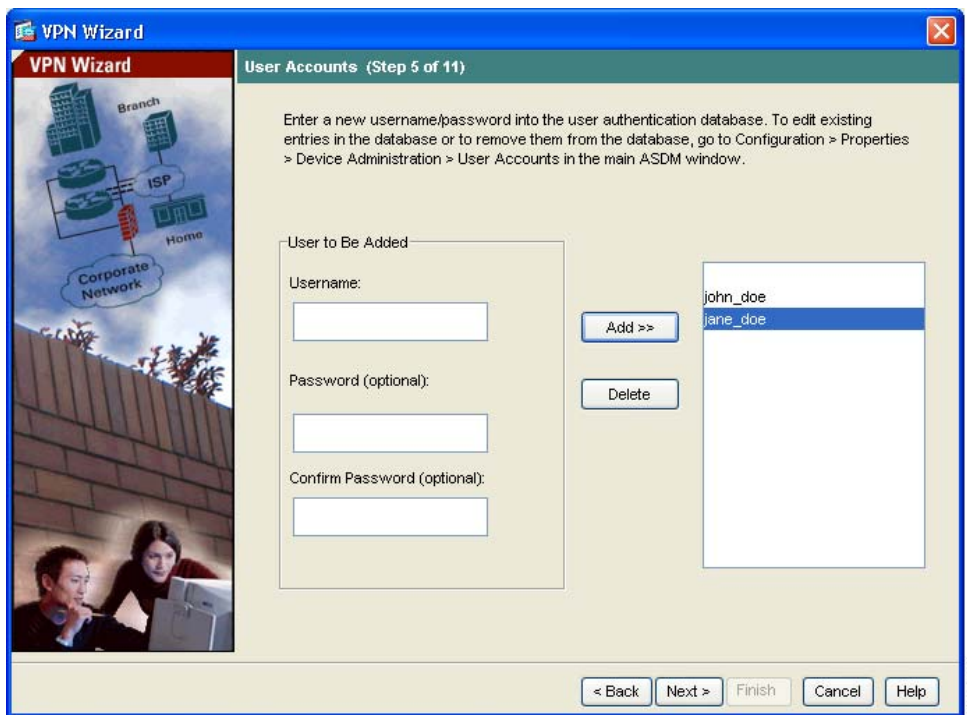
- Step 3** Click **Next** to continue.

(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**.



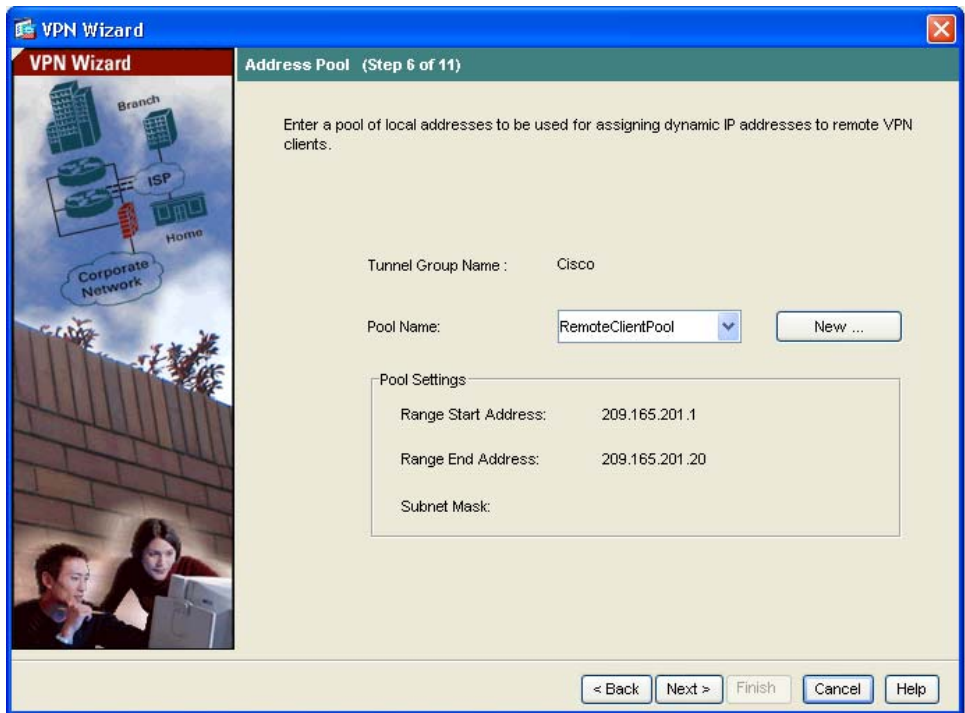
- Step 2** When you have finished adding new users, click **Next** to continue.

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 209.165.201.1–209.165.201.20.

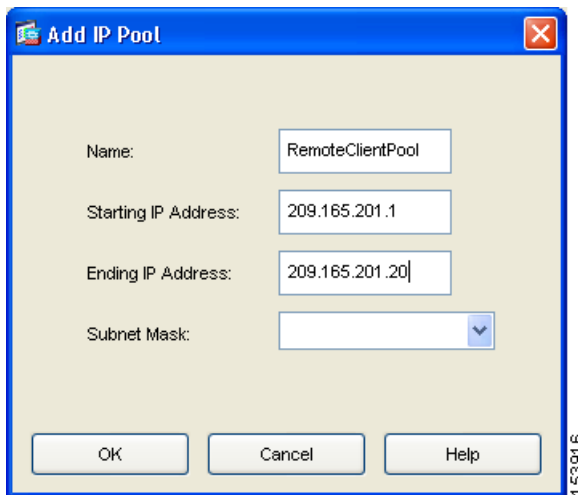
In Step 6 of the VPN Wizard, perform the following steps:

- Step 1** Enter a pool name or choose a preconfigured pool from the Pool 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:
- Enter the Starting IP address and Ending IP address of the range.
 - (Optional) Enter a subnet mask or choose a subnet mask for the range of IP addresses from the Subnet Mask drop-down list.
 - Click **OK** to return to Step 6 of the VPN Wizard.
- Step 3** Click **Next** to continue.
-

Configuring Client Attributes

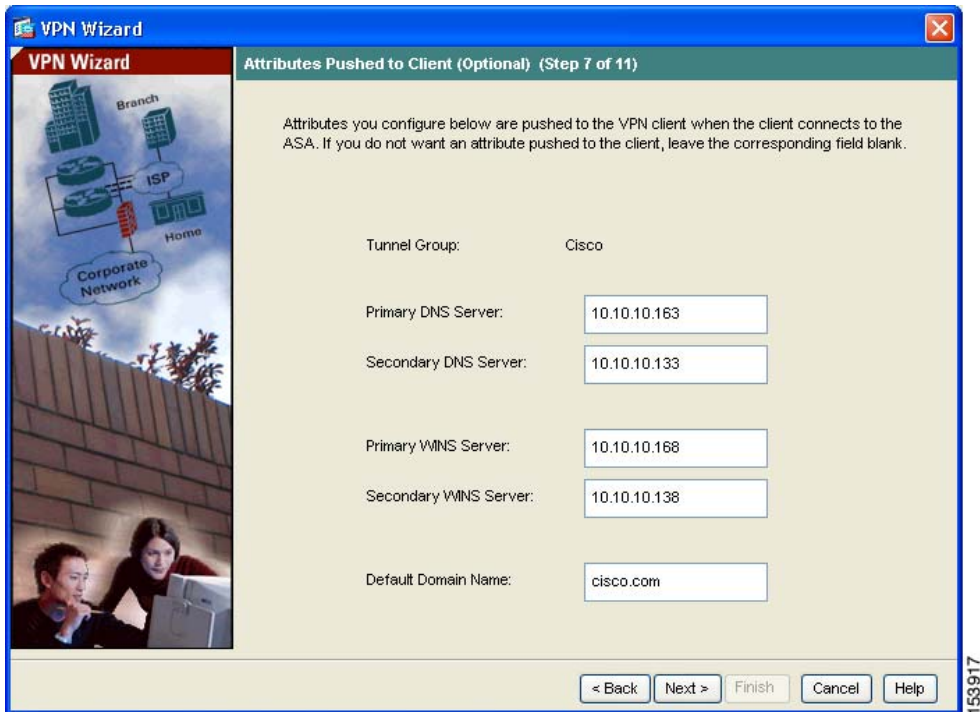
To access your network, each remote access client needs basic network configuration information, such as which DNS and WINS servers to use and the default domain name. Instead of configuring each remote client individually, you can provide the client information to ASDM. The adaptive security appliance 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.



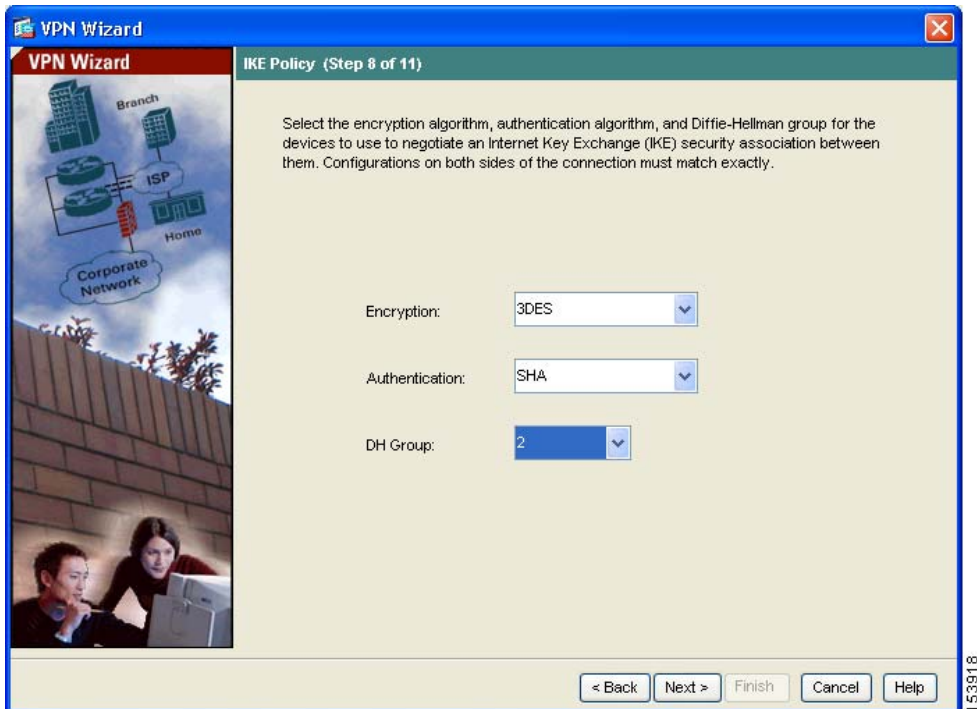
- Step 2** Click Next to continue.

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.

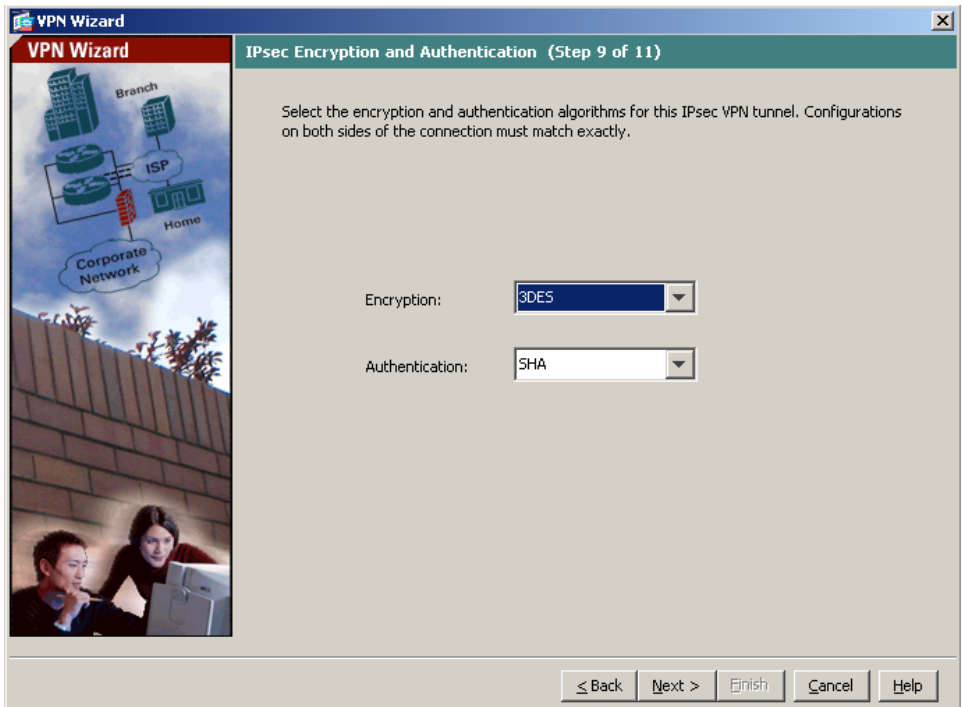


- Step 2** Click **Next** to continue.

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 area, click **Add** or **Delete**, respectively.

VPN Wizard

VPN Wizard

Address Translation Exemption and Split Tunneling (Optional) (Step 10 of 11)

Network Address Translation (NAT) is used to hide the internal network from outside users. You can make exceptions to NAT to expose the entire or part of the internal network to authenticated remote users protected by VPN.

To expose the entire network behind the most secure interface to remote VPN users without NAT, leave the selection list blank.

Host/Network

Interface:

Address:

Add

Delete

Selected Hosts/Networks:

10.10.10.0

Enable split tunneling to let remote users have simultaneous encrypted access to the resources defined above, and unencrypted access to the internet.

< Back Next > Finish Cancel Help

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:

VPN Wizard

Summary (Step 11 of 11)

You have created a Remote Access VPN tunnel with the following attributes:

- VPN Tunnel Interface: outside
- IPsec authentication uses pre-shared key: test
- Tunnel Group Name: Cisco
- Default Group Policy: Cisco
- User authentication using local user database
- New users created in the local database: john_doe jane_smith
- Pool of IP addresses for VPN clients: IPsecClientPool (209.165.201.1 - 209.165.201.20)
- Primary DNS: 10.10.10.163
- Secondary DNS: 10.10.10.168
- Primary WINS: 10.10.10.133
- Secondary WINS: 10.10.10.138
- Default Domain Name: cisco.com
- IKE Policy Encryption / Authentication / DHGroup: 3DES / SHA / Group 2
- IPsec ESP Encryption / ESP Authentication: 3DES / SHA
- Internal network elements exposed to remote VPN users without NAT: 10.10.10.0
- Split tunneling: enabled

< Back Next > Finish Cancel Help

153921

- 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 that 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 that 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.

For more information about the Cisco Systems VPN client, see the following URL:

<http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html>

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:

To Do This...	See...
Refine configuration and configure optional and advanced features	<i>Cisco Security Appliance Command Line Configuration Guide</i>
Learn about daily operations	<i>Cisco Security Appliance Command Reference</i> <i>Cisco Security Appliance System Log Messages Guide</i>

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.

To Do This...	See...
Configure the adaptive security appliance to protect a web server in a DMZ	Chapter 6, “Scenario: DMZ Configuration”
Configure an SSL VPN for the Cisco AnyConnect software client	Chapter 8, “Scenario: Configuring Connections for a Cisco AnyConnect VPN Client”
Configure a clientless (browser-based) SSL VPN	Chapter 9, “Scenario: SSL VPN Clientless Connections”
Configure a site-to-site VPN	Chapter 10, “Scenario: Site-to-Site VPN Configuration”



CHAPTER 8

Scenario: Configuring Connections for a Cisco AnyConnect VPN Client

This chapter describes how to configure the adaptive security appliance so that remote users can establish SSL connections using a Cisco AnyConnect VPN Client.

This chapter includes the following sections:

- [About SSL VPN Client Connections, page 8-1](#)
- [Obtaining the Cisco AnyConnect VPN Client Software, page 8-2](#)
- [Example Topology Using AnyConnect SSL VPN Clients, page 8-3](#)
- [Implementing the Cisco SSL VPN Scenario, page 8-3](#)
- [What to Do Next, page 8-15](#)

About SSL VPN Client Connections

To begin the process of using the SSL VPN Client (AnyConnect), remote users enter in their browser the IP address or FQDN of the SSL VPN interface of the adaptive security appliance. The browser connects to the SSL VPN-enabled interface and displays the login screen.



Note

Administrative rights are required the first time the Cisco AnyConnect VPN Client is installed or downloaded.

After downloading, the client installs and configures itself and then establishes a secure SSL connection. When the connection terminates, the client software either remains or uninstalls itself, depending on how you configure the adaptive security appliance.

If a remote user has previously established an SSL VPN connection and the client software is not instructed to uninstall itself, when the user authenticates, the adaptive security appliance examines the client version and upgrades if it necessary.

Obtaining the Cisco AnyConnect VPN Client Software

The adaptive security appliance obtains the AnyConnect VPN Client software from the Cisco website. This chapter provides instructions for configuring the SSL VPN using a configuration Wizard. You can download the Cisco SSL VPN software during the configuration process.

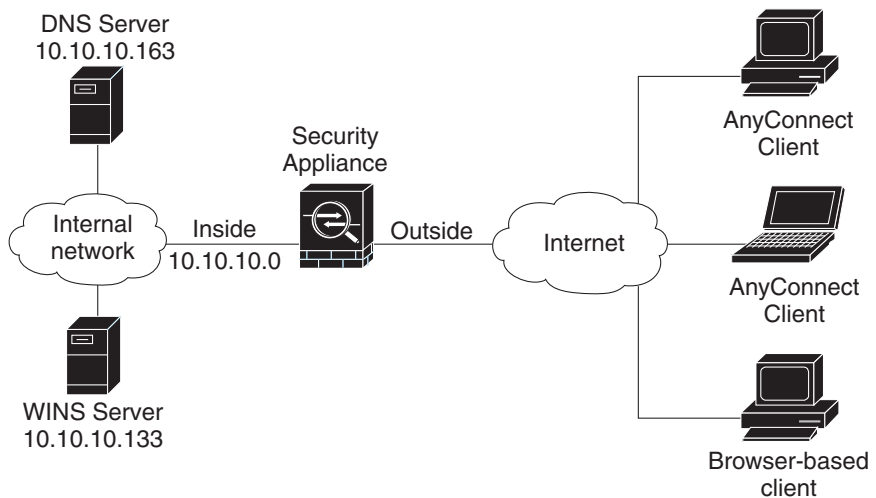
Users can download the AnyConnect VPN Client from the adaptive security appliance, or it can be installed manually on the remote PC by the system administrator. For more information about installing the client software manually, see the *Cisco AnyConnect VPN Client Administrator Guide*.

The adaptive security appliance pushes the client software based on the group policy or username attributes of the user establishing the connection. You can configure the adaptive security appliance to automatically push the client each time the user establishes a connection, or you can configure it to prompt the remote user to specify whether to download the client. In the latter case, if the user does not respond, you can configure the adaptive security appliance either to push the client after a timeout period or present the SSL VPN login screen.

Example Topology Using AnyConnect SSL VPN Clients

Figure 8-1 shows an adaptive security appliance configured to accept requests for and establish SSL connections from clients running the AnyConnect SSL VPN software. The adaptive security appliance can support connections to both clients running the AnyConnect VPN software and browser-based clients.

Figure 8-1 Network Layout for SSL VPN Scenario



Implementing the Cisco SSL VPN Scenario

This section describes how to configure the adaptive security appliance to accept Cisco AnyConnect SSL VPN connections. Values for example configuration settings are taken from the SSL VPN scenario illustrated in Figure 8-1.

This section includes the following topics:

- [Information to Have Available](#), page 8-4
- [Starting ASDM](#), page 8-5

- [Configuring the ASA 5505 for the Cisco AnyConnect VPN Client, page 8-7](#)
- [Specifying the SSL VPN Interface, page 8-8](#)
- [Specifying a User Authentication Method, page 8-9](#)
- [Specifying a Group Policy, page 8-11](#)
- [Configuring the Cisco AnyConnect VPN Client, page 8-12](#)
- [Verifying the Remote-Access VPN Configuration, page 8-14](#)

Information to Have Available

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

- Name of the interface on the adaptive security appliance to which remote users will connect.
- Digital certificate
The ASA 5505 generates a self-signed certificate by default. However, for enhanced security you may want to purchase a publicly trusted SSL VPN certificate before putting the system in a production environment.
- Range of IP addresses to be used in an IP pool. These addresses are assigned to SSL AnyConnect VPN clients as they are successfully connected.
- List of users to be used in creating a local authentication database, unless you are using a AAA server for authentication.
- If you are using a AAA server for authentication:
 - AAA Server group name
 - Authentication protocol to be used (TACACS, SDI, NT, Kerberos, LDAP)
 - IP address of the AAA server
 - Interface of the adaptive security appliance to be used for authentication
 - Secret key to authenticate with the AAA server

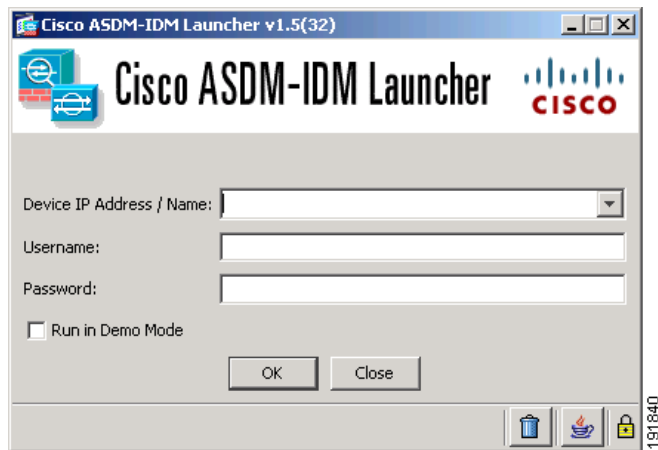
Starting ASDM

This section describes how to start ASDM using the ASDM Launcher software. If you have not installed the ASDM Launcher software, see [Installing the ASDM Launcher](#), page 5-6.

If you prefer to access ASDM directly with a web browser or using Java, see [Starting ASDM with a Web Browser](#), page 5-9.

To start ASDM using the ASDM Launcher software, perform the following steps:

-
- Step 1** From your desktop, start the Cisco ASDM Launcher software.
A dialog box appears.



- Step 2** Enter the IP address or the host name of your adaptive security appliance.
- Step 3** Leave the Username and Password fields blank.



Note By default, there is no Username and Password set for the Cisco ASDM Launcher.

- Step 4** Click OK.
- Step 5** If you receive a security warning containing a request to accept a certificate, click Yes.

Implementing the Cisco SSL VPN Scenario

The ASA checks to see if there is updated software and if so, downloads it automatically.

The main ASDM window appears.

The screenshot displays the Cisco ASDM 6.1 for ASA interface. The main window is titled "Cisco ASDM 6.1 for ASA - 10.86.194.224". The interface includes a menu bar (File, View, Tools, Wizards, Window, Help) and a toolbar with icons for Home, Configuration, Monitoring, Save, Refresh, Back, Forward, and Help. The main content area is divided into several sections:

- Device Information:** Shows general information for the ASA device, including Host Name (asa2.cisco.com), ASA Version (8.0(4)), ASDM Version (6.1(3)), Firewall Mode (Routed), Total Flash (64 MB), Device Uptime (46d 15h 59m 34s), Device Type (ASA 5510), Context Mode (Single), and Total Memory (256 MB).
- Interface Status:** A table showing the status of various interfaces:

Interface	IP Address/Mask	Line	Link	Kbps
fa/ldata	192.168.3.4/24	down	down	0
inside	no ip address	down	down	0
management	192.168.1.1/24	down	down	0
outside	10.86.194.224/23	up	up	120

- VPN Sessions:** Shows 0 IPsec, 0 Clientless SSL VPN, and 0 SSL VPN Client sessions.
- System Resources Status:** Displays CPU usage (3%) and Memory usage (12 MB).
- Traffic Status:** Shows Connections Per Second Usage and 'outside' Interface Traffic Usage (Kbps).
- Latest ASDM Syslog Messages:** A table showing recent system messages:

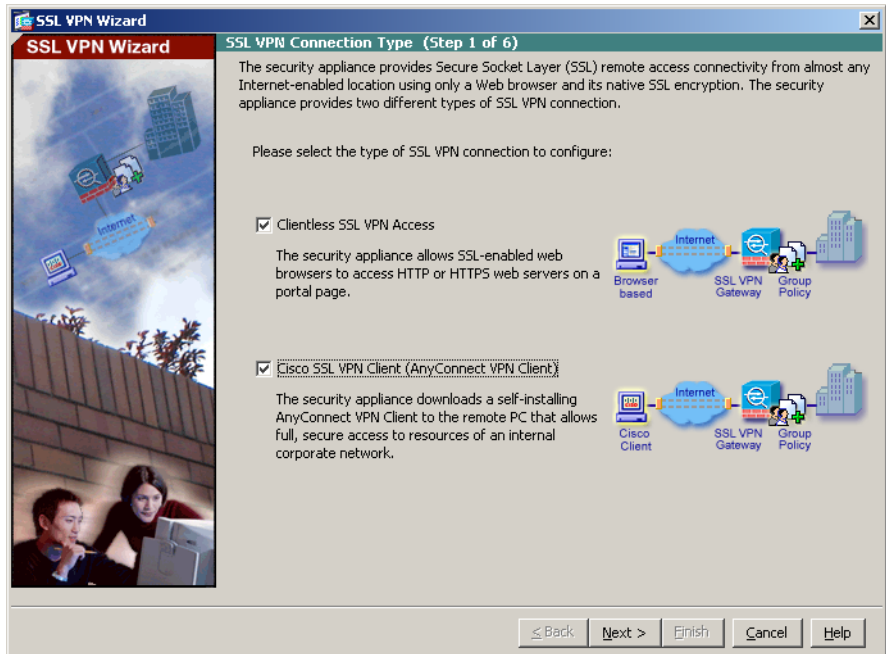
Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destination	Description
6	Oct 14 2008	13:55:31	725007	171.69.39.67	1748	10.86.194.224	https	SSL session with client outside:171.69.39.67/1748 terminated.
6	Oct 14 2008	13:55:31	605005	171.69.39.67	1748	10.86.194.224	https	Login permitted from 171.69.39.67/1748 to outside:10.86.194.224/https for user "enable_15"
6	Oct 14 2008	13:55:31	725002	171.69.39.67	1748			Device completed SSL handshake with client outside:171.69.39.67/1748
6	Oct 14 2008	13:55:31	725003	171.69.39.67	1748			SSL client outside:171.69.39.67/1748 request to resume previous session

The bottom status bar indicates "Device configuration loaded successfully." and shows the user "admin" with ID 15. The system clock shows 10/14/08 1:55:28 PM E.

Configuring the ASA 5505 for the Cisco AnyConnect VPN Client

To begin the configuration process, perform the following steps:

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



- Step 2** In Step 1 of the SSL VPN Wizard, perform the following steps:
- Check the **Cisco SSL VPN Client** check box.
 - Click **Next** to continue.

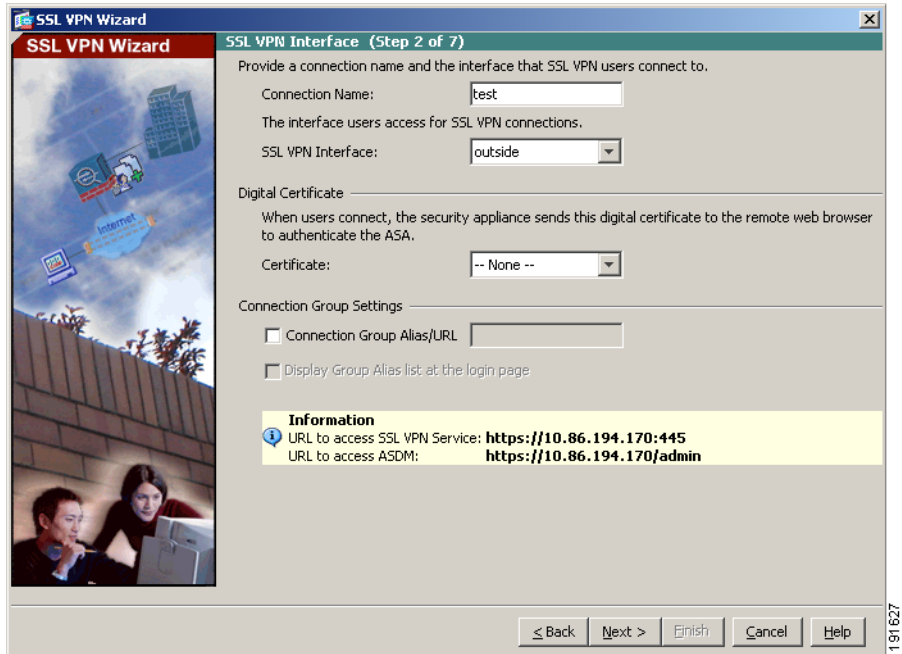
Specifying the SSL VPN Interface

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

-
- Step 1** Specify a Connection Name to which remote users connect.
 - Step 2** From the SSL VPN Interface drop-down list, choose the interface to which remote users connect. When users establish a connection to this interface, the SSL VPN portal page is displayed.
 - Step 3** From the Certificate drop-down list, choose the certificate the ASA sends to the remote user to authenticate the ASA.



Note The ASA 5505 generates a self-signed certificate by default. However, for enhanced security you may want to purchase a publicly trusted SSL VPN certificate before putting the system in a production environment.

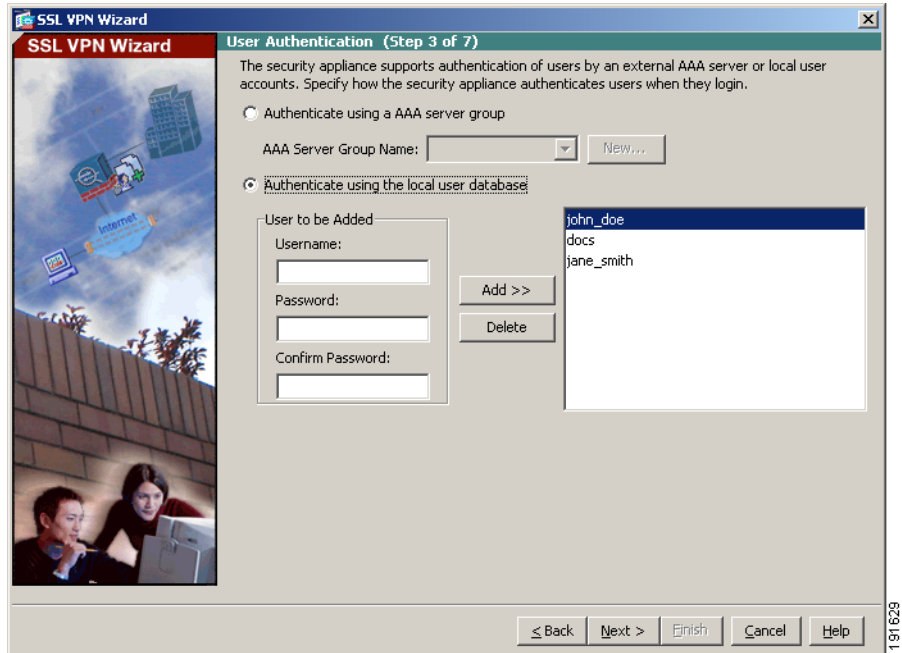


Step 4 Click Next to continue.

Specifying a User Authentication Method

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

- Step 1** If you are using a AAA server or server group for authentication, perform the following steps:
- Click the **Authenticate using a AAA server group** radio button.



- b. Specify a AAA Server Group Name.
- c. You can either choose an existing AAA server group name from the drop down list, or you can create a new server group by clicking **New**.

To create a new AAA Server Group, click **New**. The New Authentication Server Group dialog box appears.

In this dialog box, specify the following:

- A server group name
- The Authentication Protocol to be used (RADIUS, TACACS, SDI, NT, Kerberos, LDAP)
- IP address of the AAA server
- Interface of the adaptive security appliance
- Secret key to be used when communicating with the AAA server

Click OK.

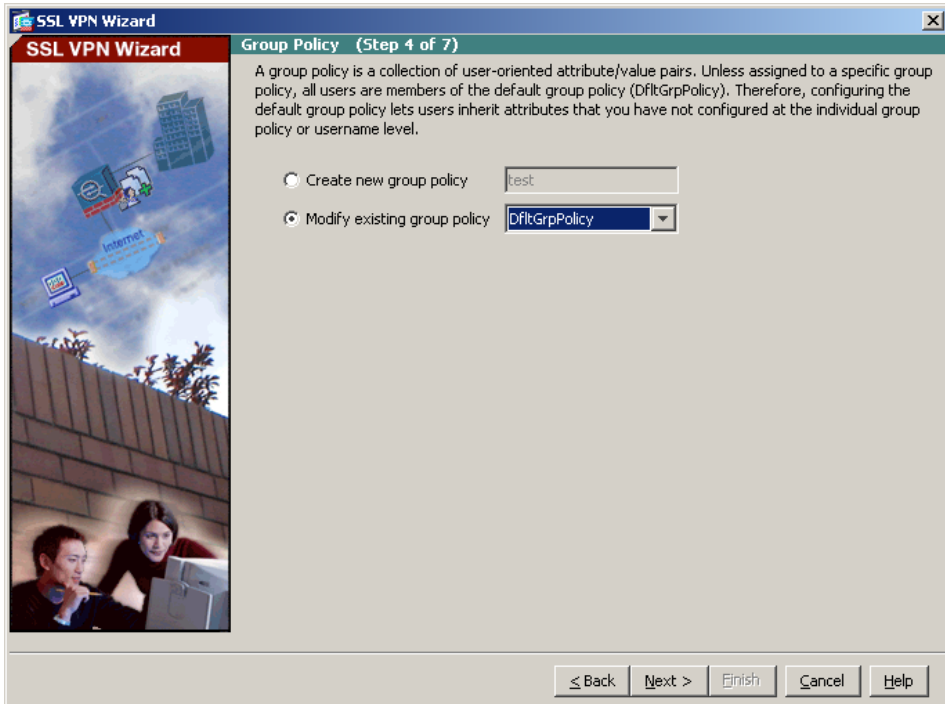
- Step 2** If you have chosen to authenticate users with the local user database, you can create new user accounts here. You can also add users later using the ASDM configuration interface.
- To add a new user, enter a username and password, and then click **Add**.
- Step 3** When you have finished adding new users, click **Next** to continue.
-

Specifying a Group Policy

In Step 4 of the SSL VPN Wizard, specify a group policy by performing the following steps:

-
- Step 1** Click the **Create new group policy** radio button and specify a group name.
- OR
- Step 2** Click the **Modify an existing group policy** radio button and choose a group from the drop-down list.

Implementing the Cisco SSL VPN Scenario



Step 3 Click **Next**.

Step 4 Step 5 of the SSL VPN Wizard appears. This step does not apply to AnyConnect VPN client connections, so click **Next** again.

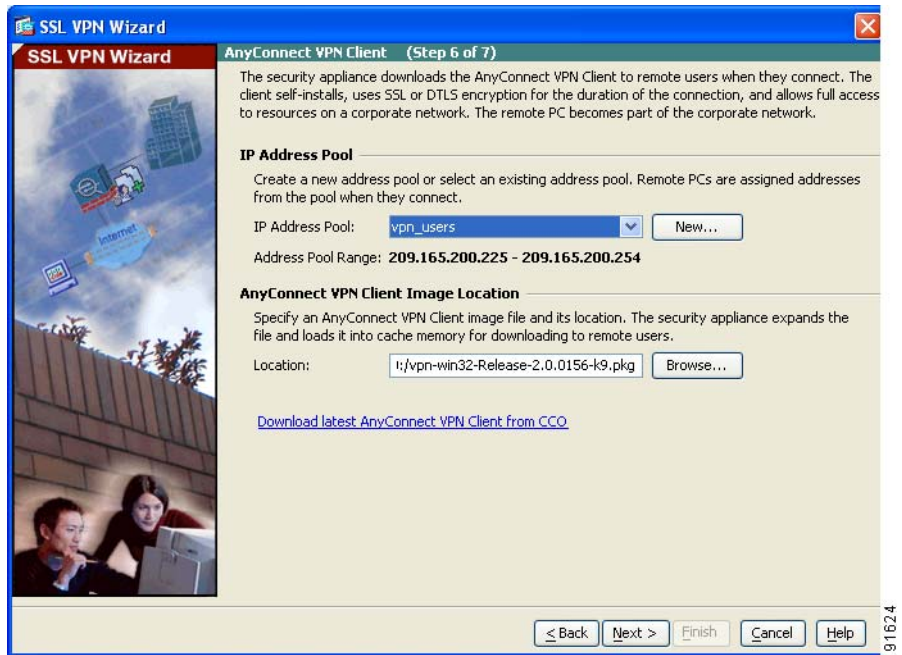
Configuring the Cisco AnyConnect VPN Client

For remote clients to gain access to your network with a Cisco VPN Client, 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.

You must also specify the location of the AnyConnect software so that the adaptive security appliance can push it to users.

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

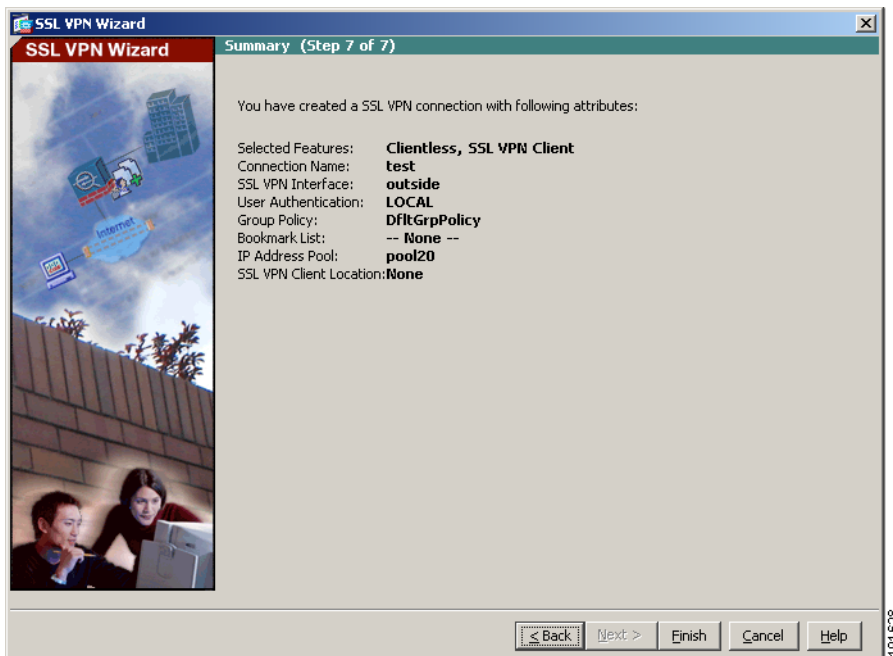
- Step 1** To use a preconfigured address pool, choose the name of the pool from the IP Address Pool drop-down list.



- Step 2** Alternatively, click **New** to create a new address pool.
- Step 3** Specify the location of the AnyConnect VPN Client software image.
To obtain the most current version of the software, click **Download Latest AnyConnect VPN Client from cisco.com**. This downloads the client software to your PC.
- Step 4** Click **Next** to continue.

Verifying the Remote-Access VPN Configuration

In Step 7 of the SSL VPN Wizard, review the configuration settings to ensure that they are correct. The displayed configuration should be similar to the following:



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

If you are deploying the adaptive security appliance solely to support AnyConnect VPN connections, you have completed the initial configuration. In addition, you may want to consider performing some of the following steps:

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

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.

To Do This...	See...
Configure the adaptive security appliance to protect a web server in a DMZ	Chapter 6, “Scenario: DMZ Configuration”
Configure a site-to-site VPN	Chapter 10, “Scenario: Site-to-Site VPN Configuration”
Configure a remote-access IPSec VPN	Chapter 7, “Scenario: IPSec Remote-Access VPN Configuration”
Configure clientless (browser-based) SSL VPN	Chapter 9, “Scenario: SSL VPN Clientless Connections”

■ What to Do Next



CHAPTER 9

Scenario: SSL VPN Clientless Connections

This chapter describes how to use the adaptive security appliance to accept remote access SSL VPN connections without a software client (clientless). A clientless SSL VPN allows you to create secure connections, or tunnels, across the Internet using a web browser. This provides secure access to off-site users without a software client or hardware client.

This chapter includes the following sections:

- [About Clientless SSL VPN, page 9-1](#)
- [Example Network with Browser-Based SSL VPN Access, page 9-3](#)
- [Implementing the Clientless SSL VPN Scenario, page 9-4](#)
- [What to Do Next, page 9-18](#)

About Clientless SSL VPN

Clientless SSL VPN connections enable secure and easy access to a broad range of web resources and web-enabled applications from almost any computer on the Internet. They include:

- Internal websites
- Web-enabled applications
- NT/Active Directory and FTP file shares
- E-mail proxies, including POP3S, IMAP4S, and SMTPS

- MS Outlook Web Access
- MAPI
- Application Access (that is, port forwarding for access to other TCP-based applications) and Smart Tunnels

Clientless SSL VPN uses the Secure Sockets Layer Protocol (SSL) and its successor, Transport Layer Security (TLS), to provide the secure connection between remote users and specific, supported internal resources that you configure at a central site. The adaptive security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

The network administrator provides access to resources by users of Clientless SSL VPN on a group basis.

Security Considerations for Clientless SSL VPN Connections

Clientless SSL VPN connections on the adaptive security appliance differ from remote access IPsec connections, particularly with respect to how they interact with SSL-enabled servers and the validation of certificates.

In a Clientless SSL VPN connection, the adaptive security appliance acts as a proxy between the end user web browser and target web servers. When a user connects to an SSL-enabled web server, the adaptive security appliance establishes a secure connection and validates the server SSL certificate. The end user browser never receives the presented certificate, so therefore it cannot examine and validate the certificate.

The current implementation of Clientless SSL VPN on the adaptive security appliance does not permit communication with sites that present expired certificates. Nor does the adaptive security appliance perform trusted CA certificate validation. Therefore, users cannot analyze the certificate an SSL-enabled web-server presents before communicating with it.

To minimize the risks involved with SSL certificates:

1. Configure a group policy that consists of all users who need Clientless SSL VPN access and enable it only for that group policy.

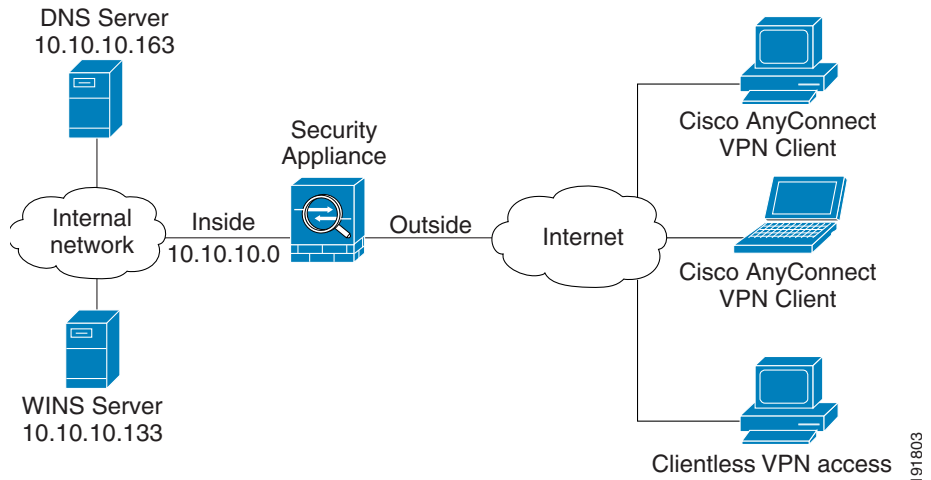
2. Limit Internet access for Clientless SSL VPN users, for example, by limiting which resources a user can access using a clientless SSL VPN connection. To do this, you could restrict the user from accessing general content on the Internet. Then, you could configure links to specific targets on the internal network that you want users of Clientless SSL VPN to be able to access.
3. Educate users. If an SSL-enabled site is not inside the private network, users should not visit this site over a Clientless SSL VPN connection. They should open a separate browser window to visit such sites, and use that browser to view the presented certificate.

The adaptive security appliance does not support the following features for Clientless SSL VPN connections:

- NAT, reducing the need for globally unique IP addresses.
- PAT, permitting multiple outbound sessions appear to originate from a single IP address.

Example Network with Browser-Based SSL VPN Access

Figure 9-1 shows an adaptive security appliance configured to accept SSL VPN connection requests over the Internet using a web browser.

Figure 9-1 Network Layout for SSL VPN Connections

Implementing the Clientless SSL VPN Scenario

This section describes how to configure the adaptive security appliance to accept SSL VPN requests from web browsers. Values for example configuration settings are taken from the remote-access scenario illustrated in [Figure 9-1](#).

This section includes the following topics:

- [Information to Have Available](#), page 9-5
- [Starting ASDM](#), page 9-5
- [Configuring the ASA 5505 for Browser-Based SSL VPN Connections](#), page 9-7
- [Specifying the SSL VPN Interface](#), page 9-8
- [Specifying a User Authentication Method](#), page 9-10
- [Specifying a Group Policy](#), page 9-11
- [Creating a Bookmark List for Remote Users](#), page 9-12
- [Verifying the Configuration](#), page 9-16

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:

- Name of the interface on the adaptive security appliance to which remote users will connect. When remote users connect to this interface, the SSL VPN Portal Page is displayed.

- Digital certificate

The ASA 5505 generates a self-signed certificate by default. For improved security and to eliminate browser warning messages, you may want to purchase a publicly trusted SSL VPN certificate before putting the system in a production environment.

- List of users to be used in creating a local authentication database, unless you are using a AAA server for authentication.
- If you are using a AAA server for authentication, the AAA Server Group Name
- The following information about group policies on the AAA server:
 - Server group name
 - Authentication protocol to be used (TACACS, SDI, NT, Kerberos, LDAP)
 - IP address of the AAA server
 - Interface of the adaptive security appliance to be used for authentication
 - Secret key to authenticate with the AAA server
- List of internal websites or pages you want to appear on the SSL VPN portal page when remote users establish a connection. Because this is the page users see when they first establish a connection, it should contain the most frequently used targets for remote users.

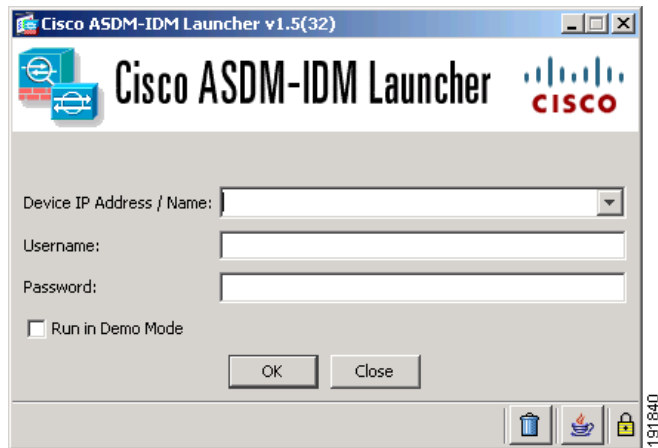
Starting ASDM

This section describes how to start ASDM using the ASDM Launcher software. If you have not installed the ASDM Launcher software, see [Installing the ASDM Launcher, page 5-6](#).

If you prefer to access ASDM directly with a web browser or using Java, see [Starting ASDM with a Web Browser, page 5-9](#).

To start ASDM using the ASDM Launcher software, perform the following steps:

- Step 1** From your desktop, start the Cisco ASDM Launcher software.
A dialog box appears.



- Step 2** Enter the IP address or the host name of your adaptive security appliance.
Step 3 Leave the Username and Password fields blank.



Note By default, there is no Username and Password set for the Cisco ASDM Launcher.

- Step 4** Click OK.
Step 5 If you receive a security warning containing a request to accept a certificate, click **Yes**.

The ASA checks to see if there is updated software and if so, downloads it automatically.

The main ASDM window appears.

Device Information

General	License
Host Name: asa2.cisco.com	
ASA Version: 8.0(4)	Device Uptime: 46d 15h 59m 34s
ASDM Version: 6.1(3)	Device Type: ASA 5510
Firewall Mode: Routed	Context Mode: Single
Total Flash: 64 MB	Total Memory: 256 MB

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
fa/ldata	192.168.3.4/24	down	down	0
inside	no ip address	down	down	0
management	192.168.1.1/24	down	down	0
outside	10.86.194.224/23	up	up	120

Select an interface to view input and output Kbps

VPN Sessions

IPSec: 0 Clientless SSL VPN: 0 SSL VPN Client: 0 [Details](#)

System Resources Status

CPU Usage (percent): 3% (at 13:55:28)

Memory Usage (MB): 127MB

Traffic Status

Connections Per Second Usage

'outside' Interface Traffic Usage (Kbps)

Latest ASDM Syslog Messages

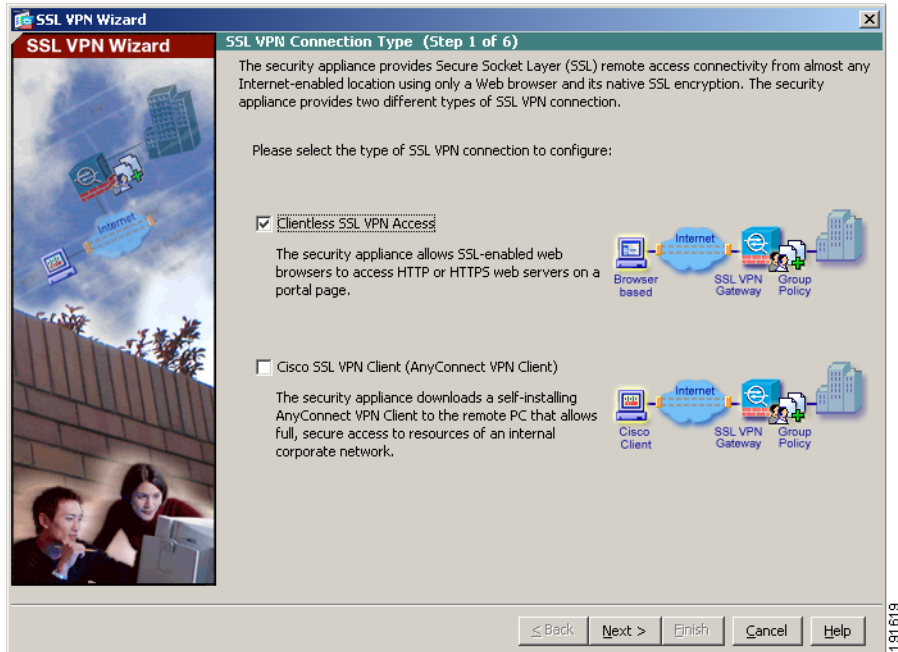
Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destination	Description
6	Oct 14 2008	13:55:31	725007	171.69.39.67	1748			SSL session with client outside:171.69.39.67/1748 terminated.
6	Oct 14 2008	13:55:31	605005	171.69.39.67	1748	10.86.194.224	https	Login permitted from 171.69.39.67/1748 to outside:10.86.194.224/https for user "enable_15"
6	Oct 14 2008	13:55:31	725002	171.69.39.67	1748			Device completed SSL handshake with client outside:171.69.39.67/1748
6	Oct 14 2008	13:55:31	725003	171.69.39.67	1748			SSL client outside:171.69.39.67/1748 permit to resume previous session

Device configuration loaded successfully. <admin> 15 10/14/08 1:55:28 PM E

Configuring the ASA 5505 for Browser-Based SSL VPN Connections

To begin the process for configuring a browser-based SSL VPN, perform the following steps:

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

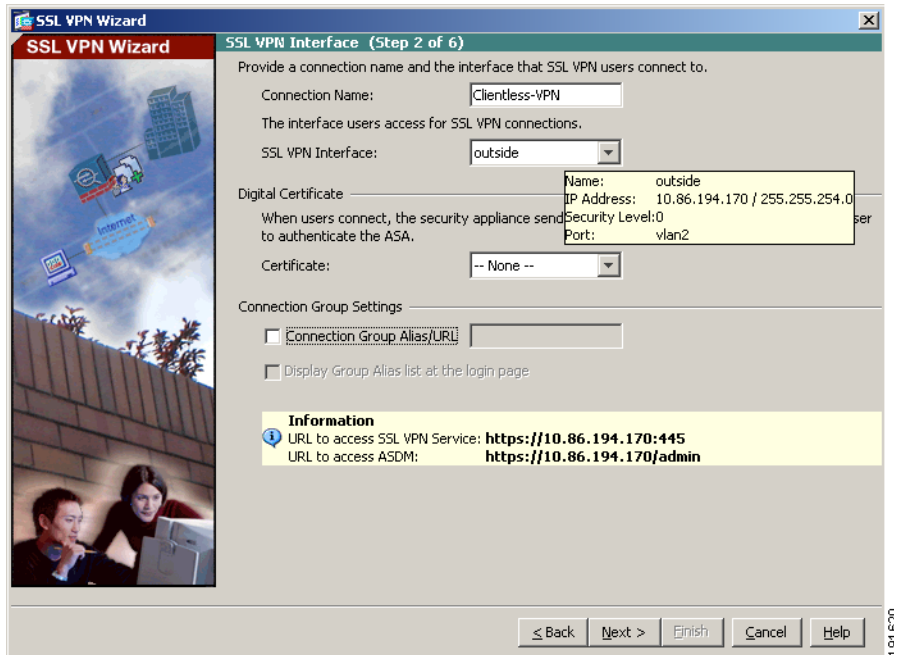


- Step 2** In Step 1 of the SSL VPN Wizard, perform the following steps:
- a. Check the **Browser-based SSL VPN (Web VPN)** check box.
 - b. Click **Next** to continue.

Specifying the SSL VPN Interface

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

- Step 1** Specify a Connection Name to which remote users connect.



- Step 2** From the SSL VPN Interface drop-down list, choose the interface to which remote users connect. When users establish a connection to this interface, the SSL VPN portal page is displayed.
- Step 3** From the Certificate drop-down list, choose the certificate the ASA sends to the remote user to authenticate the ASA.

**Note**

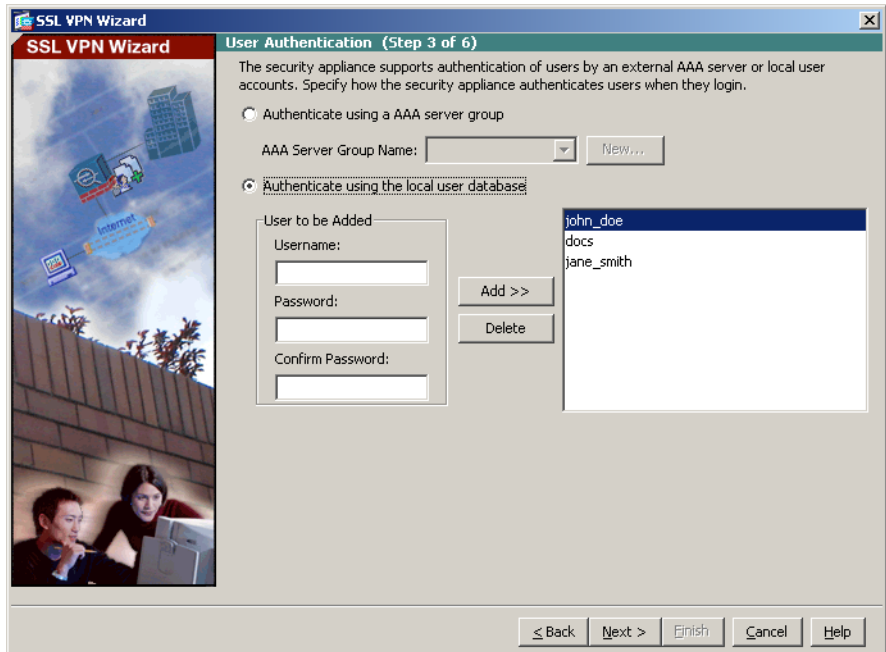
The ASA 5505 generates a self-signed certificate by default. For improved security and to eliminate browser warning messages, you may want to purchase a publicly trusted SSL VPN certificate before putting the system in a production environment.

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 3 of the SSL VPN Wizard, perform the following steps:

- Step 1** If you are using a AAA server or server group for authentication, perform the following steps:
- a. Click the **Authenticate using a 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. To create a new AAA Server Group, click **New**. The New Authentication Server Group dialog box appears.

In this dialog box, specify the following:

- A server group name
- The Authentication Protocol to be used (TACACS, SDI, NT, Kerberos, LDAP)
- IP address of the AAA server
- Interface of the adaptive security appliance
- Secret key to be used when communicating with the AAA server

Click OK.

Step 2 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.

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

Step 3 When you have finished adding new users, click **Next** to continue.

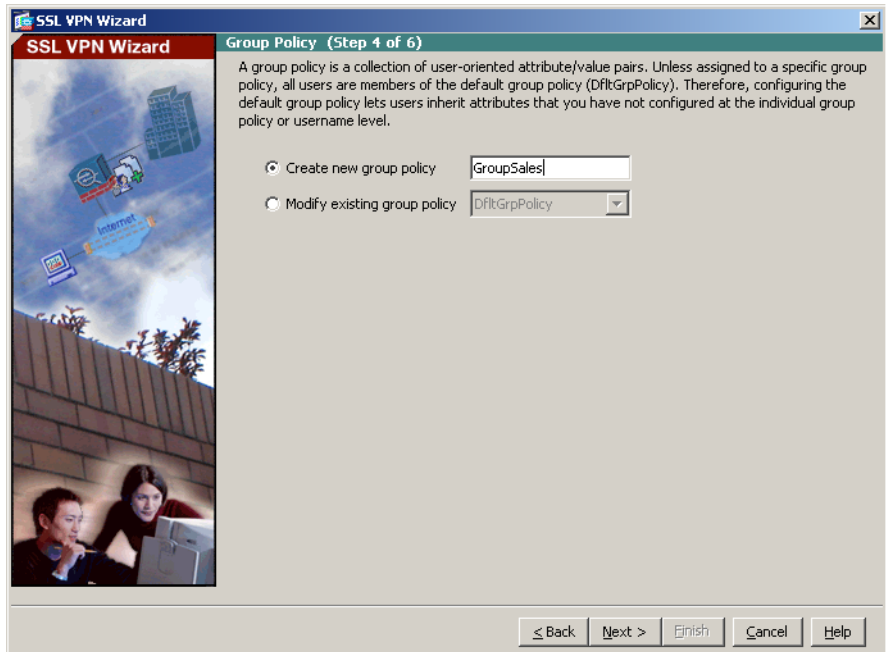
Specifying a Group Policy

In Step 4 of the SSL VPN Wizard, specify a group policy by performing the following steps:

Step 1 Click the **Create new group policy** radio button and specify a group name.

OR

Click the **Modify an existing group policy** radio button and choose a group from the drop-down list.



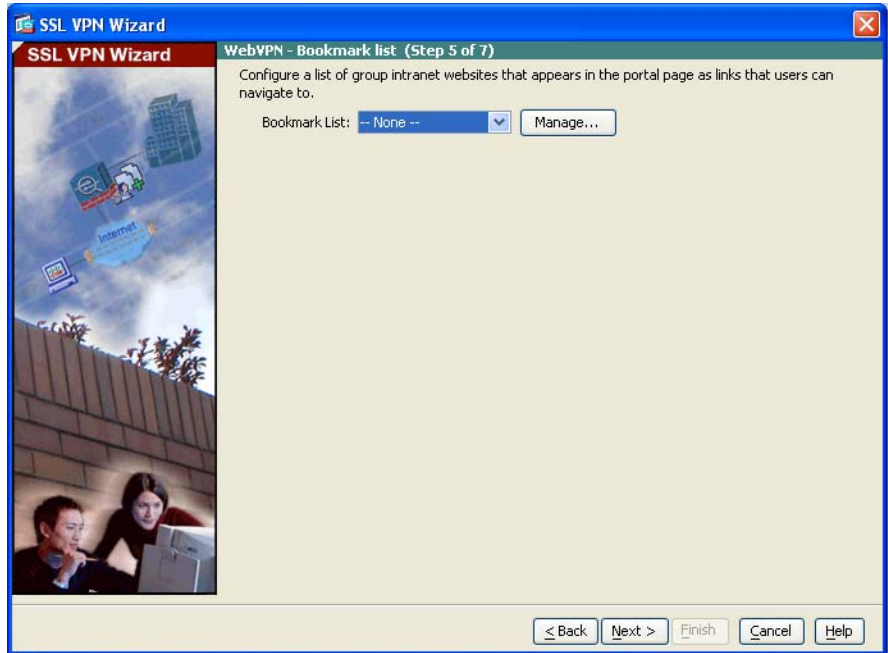
Step 2 Click Next.

Creating a Bookmark List for Remote Users

You can create a portal page, a special web page that comes up when browser-based clients establish VPN connections to the adaptive security appliance, by specifying a list of URLs to which users should have easy access.

In Step 5 of the SSL VPN Wizard, specify URLs to appear on the VPN portal page by performing the following steps:

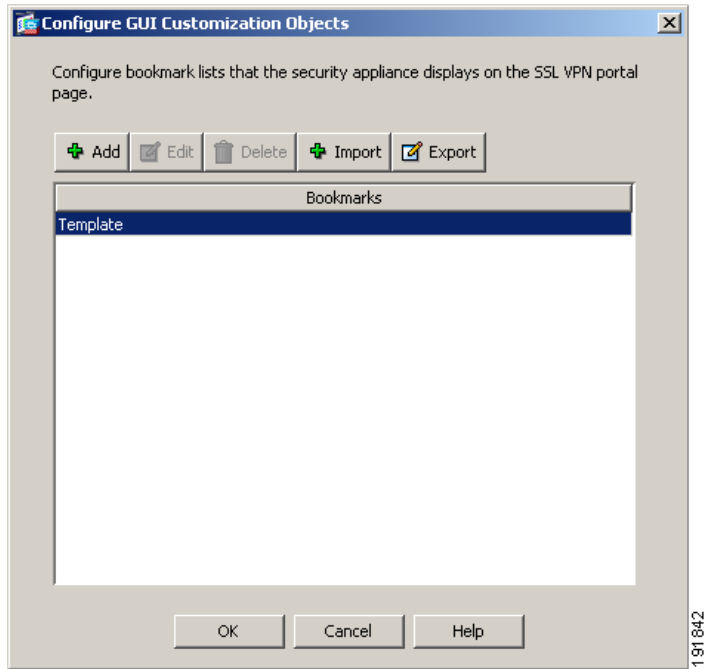
Step 1 To specify an existing bookmark list, choose the Bookmark List name from the drop-down list.



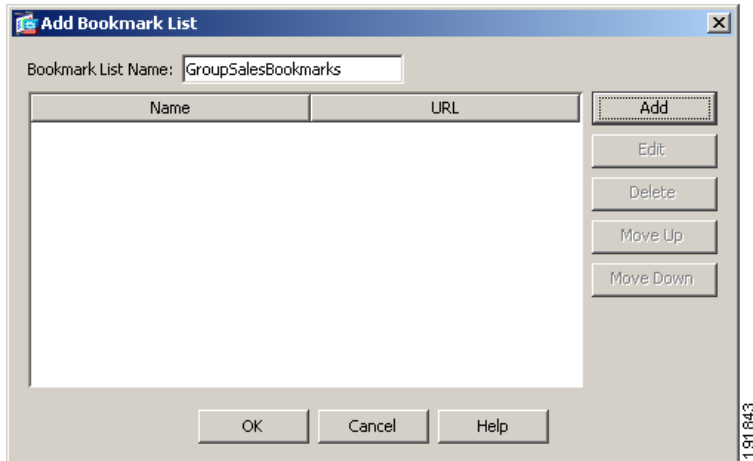
To add a new list or edit an existing list, click **Manage**.

The Configure GUI Customization Objects dialog box appears.

■ Implementing the Clientless SSL VPN Scenario



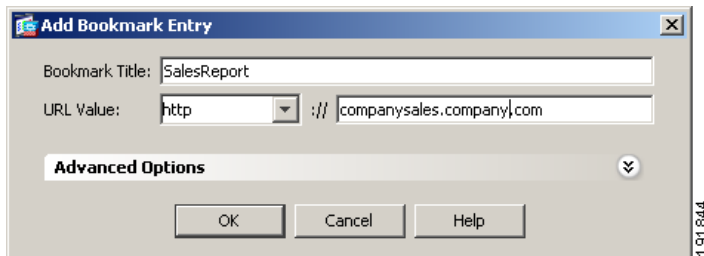
- Step 2** To create a new bookmark list, click **Add**.
- To edit an existing bookmark list, choose the list and click **Edit**.
- The Add Bookmark List dialog box appears.



Step 3 In the URL List Name box, specify a name for the list of bookmarks you are creating. This is used as the title for your VPN portal page.

Step 4 Click **Add** to add a new URL to the bookmark list.

The Add Bookmark Entry dialog box appears.



Step 5 Specify a title for the list in the Bookmark Title field.

Step 6 From the URL Value drop-down list, choose the type of URL you are specifying. For example, choose http, https, ftp, and so on.

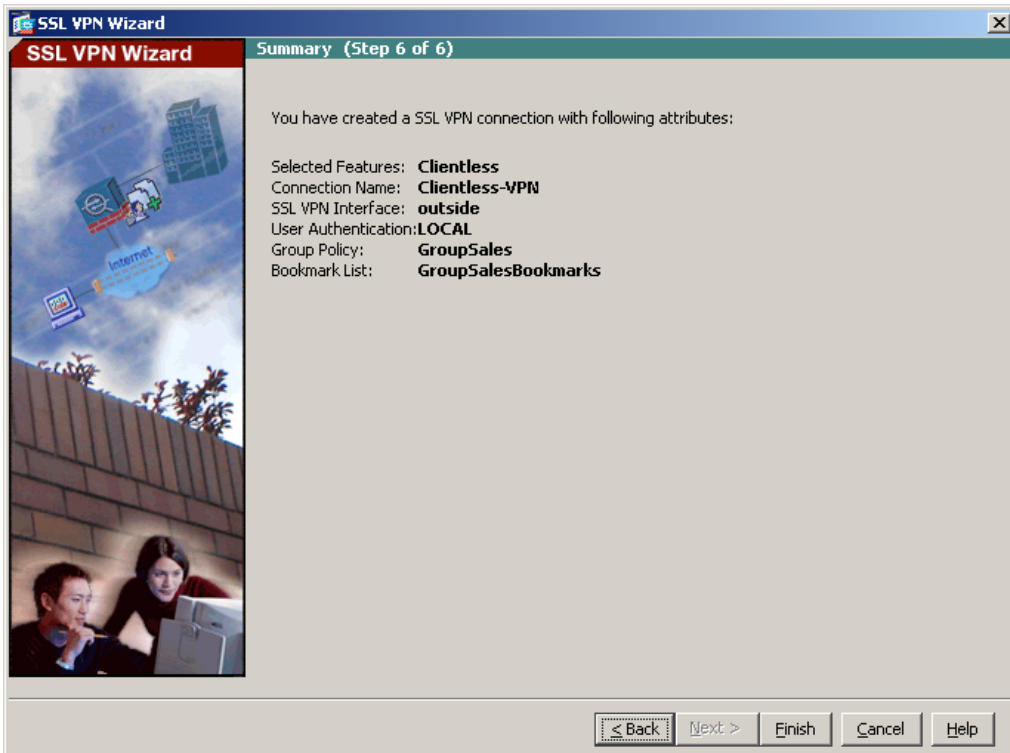
Then, specify the complete URL for the page.

Step 7 Click **OK** to return to the Add Bookmark List dialog box.

- Step 8** If you are finished adding bookmark lists, click **OK** to return to the Configure GUI Customization Objects dialog box.
 - Step 9** When you are finished adding and editing bookmark lists, click **OK** to return to Step 5 of the SSL VPN Wizard.
 - Step 10** Choose the name of the bookmark list for this VPN group from the Bookmark List drop-down list.
 - Step 11** Click **Next** to continue.
-

Verifying the Configuration

In Step 7 of the SSL VPN Wizard, review the configuration settings to ensure that they are correct. The displayed configuration should be similar to the following:



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

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

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

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.

To Do This...	See...
Configure the adaptive security appliance to protect a web server in a DMZ	Chapter 6, “Scenario: DMZ Configuration”
Configure a remote-access VPN	Chapter 7, “Scenario: IPsec Remote-Access VPN Configuration”
Configure an AnyConnect VPN	Chapter 8, “Scenario: Configuring Connections for a Cisco AnyConnect VPN Client”
Configure a site-to-site VPN	Chapter 10, “Scenario: Site-to-Site VPN Configuration”



CHAPTER 10

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.

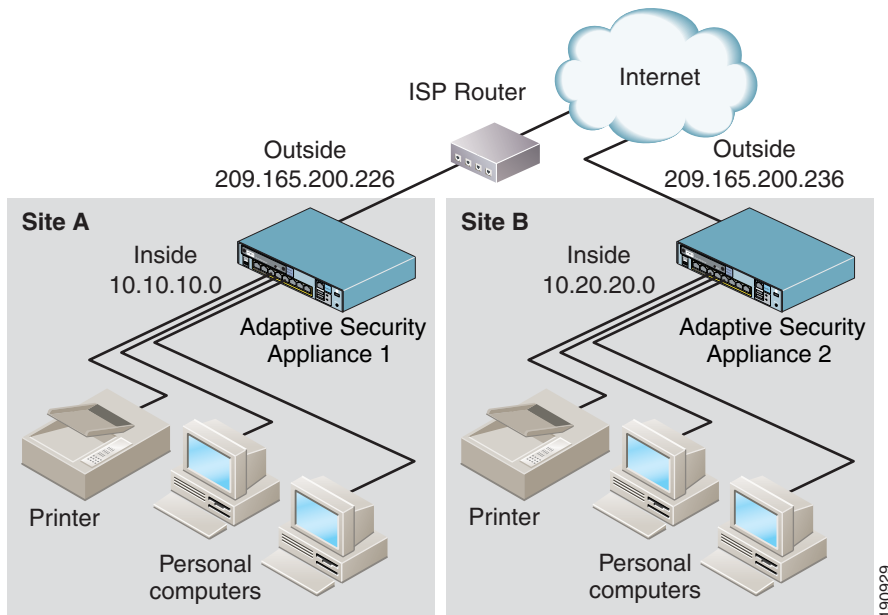
This chapter includes the following sections:

- [Example Site-to-Site VPN Network Topology, page 10-1](#)
- [Implementing the Site-to-Site Scenario, page 10-2](#)
- [Configuring the Other Side of the VPN Connection, page 10-14](#)
- [What to Do Next, page 10-15](#)

Example Site-to-Site VPN Network Topology

[Figure 10-1](#) shows an example VPN tunnel between two adaptive security appliances.

Figure 10-1 Network Layout for Site-to-Site VPN Configuration Scenario



Creating a VPN site-to-site deployment such as the one in [Figure 10-1](#) 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 10-1](#).

This section includes the following topics:

- [Information to Have Available, page 10-3](#)
- [Configuring the Site-to-Site VPN, page 10-3](#)

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 at 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 10-3](#)
- [Configuring the Security Appliance at the Local Site, page 10-5](#)
- [Providing Information About the Remote VPN Peer, page 10-7](#)
- [Configuring the IKE Policy, page 10-9](#)
- [Configuring IPsec Encryption and Authentication Parameters, page 10-10](#)
- [Specifying Hosts and Networks, page 10-11](#)
- [Viewing VPN Attributes and Completing the Wizard, page 10-12](#)

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

Starting ASDM

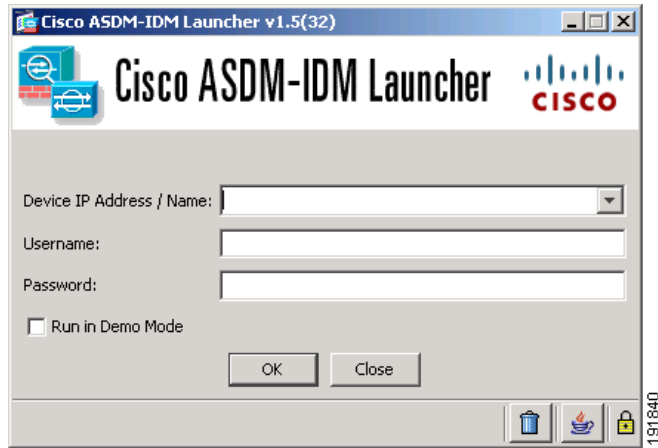
This section describes how to start ASDM using the ASDM Launcher software. If you have not installed the ASDM Launcher software, see [Installing the ASDM Launcher, page 5-6](#).

If you prefer to access ASDM directly with a web browser or using Java Web Start, see [Starting ASDM with a Web Browser, page 5-9](#).

To start ASDM using the ASDM Launcher software, perform the following steps:

Implementing the Site-to-Site Scenario

- Step 1** From your desktop, double-click the Cisco ASDM-IDM Launcher icon. The Cisco ASDM-IDM Launcher dialog box appears.



- Step 2** Enter the IP address or the hostname of your adaptive security appliance.
- Step 3** Leave the Username and Password fields blank.



Note By default, there is no Username and Password set for the Cisco ASDM Launcher.

- Step 4** Click OK.
- Step 5** If you receive a security warning containing a request to accept a certificate, click **Yes**.

The adaptive security appliance checks to see if there is updated software and if so, downloads it automatically.

The ASDM main window appears.

The screenshot displays the Cisco ASDM 6.1 interface for an ASA device at 10.86.194.224. The main window is divided into several sections:

- Device Information:** Host Name: asa2.cisco.com, ASA Version: 8.0(4), ASDM Version: 6.1(3), Firewall Mode: Routed, Total Flash: 64 MB, Total Memory: 256 MB.
- Interface Status:** A table showing the status of interfaces:

Interface	IP Address/Mask	Line	Link	Kbps
fa1data	192.168.3.4/24	down	down	0
inside	no ip address	down	down	0
management	192.168.1.1/24	down	down	0
outside	10.86.194.224/23	up	up	120
- VPN Sessions:** IPsec: 0, Clientless SSL VPN: 0, SSL VPN Client: 0.
- System Resources Status:** CPU usage is 3%, Memory usage is 1.2 MB.
- Traffic Status:** Shows connections per second usage and interface traffic usage for the 'outside' interface.
- Latest ASDM Syslog Messages:**

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
6	Oct 14 2008	13:55:31	725007	171.69.39.67	1748			SSL session with client outside:171.69.39.67/1748 terminated.
6	Oct 14 2008	13:55:31	605005	171.69.39.67	1748	10.86.194.224	https	Login permitted from 171.69.39.67/1748 to outside:10.86.194.224/https for user "enable_15"
6	Oct 14 2008	13:55:31	725002	171.69.39.67	1748			Device completed SSL handshake with client outside:171.69.39.67/1748
6	Oct 14 2008	13:55:31	725003	171.69.39.67	1748			SSL client outside:171.69.39.67/1748 connect to resume previous session.

Configuring the Security Appliance at the Local Site



Note

In this scenario, the adaptive security appliance at the local site (Site A) is referred to as Security Appliance 1.

To configure Security Appliance 1, perform the following steps:

- Step 1** In the ASDM main window, choose the IPsec VPN Wizard option from the Wizards drop-down menu. ASDM opens the first VPN Wizard screen.

Implementing the Site-to-Site Scenario

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

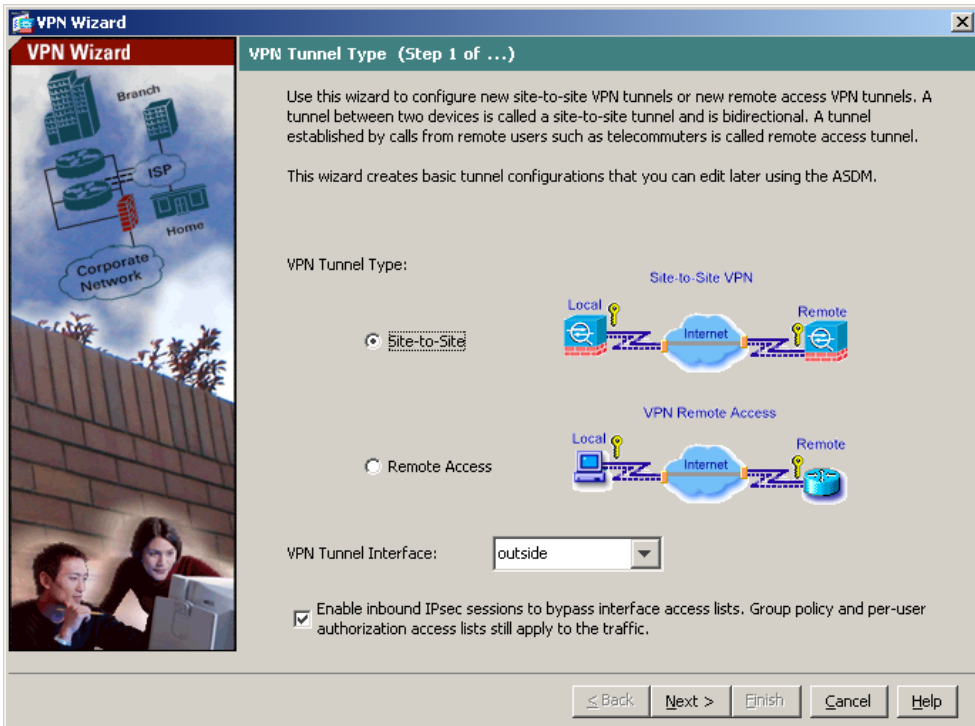
- a. In the VPN Tunnel Type area, click the **Site-to-Site** radio button.



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 VPN peer at the remote site (Site B) is referred to as Security Appliance 2.

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

-
- Step 1** Enter the remote VPN peer IP address (209.165.200.236) and a tunnel group name.
- 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.
 - 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 choosing one of the other two options. You can revise the authentication configuration later using the same ASDM panes.
- To use the CRACK method of authentication, click the **Challenge/Response Authentication** radio button.

Implementing the Site-to-Site Scenario

Step 3 In the Tunnel Group Name field, enter the IP address of the peer or peer hostname.



Note For site-to-site connections with pre-shared key authentication such as this scenario, the tunnel group name must be the same as either the IP address of the peer or the peer hostname, whichever is used as the peer identity.

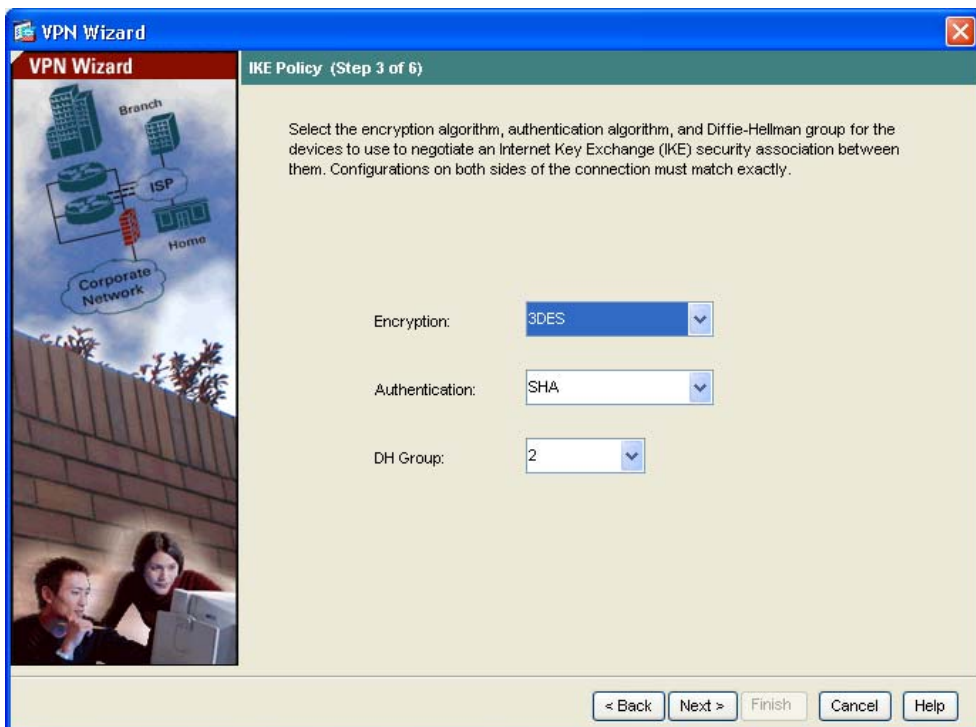
Step 4 Click **Next** to continue.

Configuring the IKE Policy

IKE is a negotiation protocol that includes an encryption method to protect data integrity through secure VPN tunnels 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.



153906



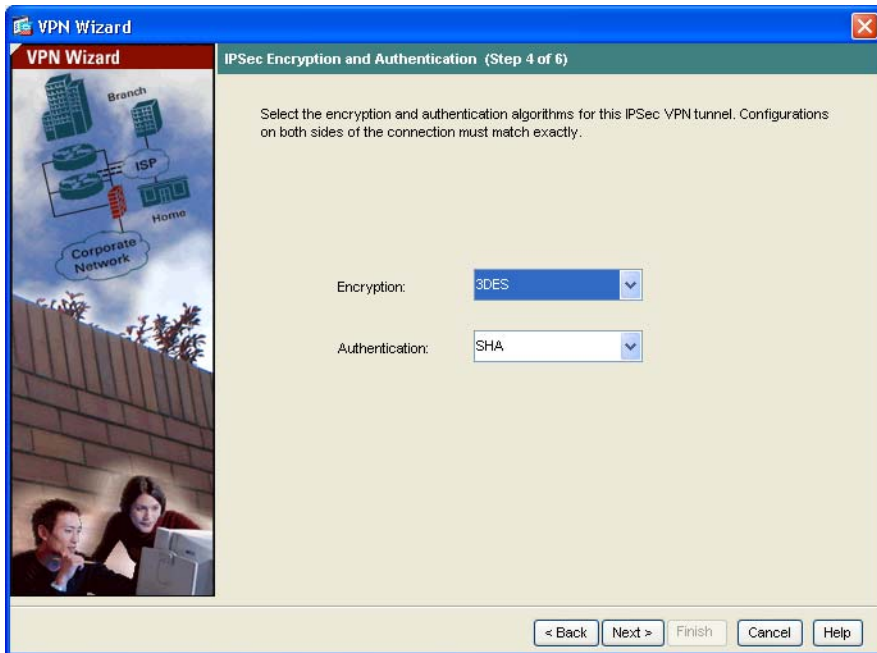
Note When configuring Security Appliance 2, enter the same values for each of the options that you chose for Security Appliance 1, with the exception of local hosts and networks. Encryption mismatches are a common cause of VPN tunnel failures and can slow down the configuration process.

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.

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 Site 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 Site 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:



Note

In this context, protection provides encryption to preserve data integrity between two hosts through a secure VPN tunnel. Information that is being sent from one host to another as plain text, without encryption through an unsecured connection, is considered unprotected data. Tampering may occur when you send unprotected data through unsecured connections.

- Step 1** Enter the IP address of local networks to be protected or not protected, or click the ellipsis (...) button to select from a list of hosts and networks.
- Step 2** Enter the IP address of remote networks to be protected or not protected, or click the ellipsis (...) button to select from a list of hosts and networks.



Note

If a remote peer has a dynamic IP address, you can use the hostname as the peer IP address.

Implementing the Site-to-Site Scenario

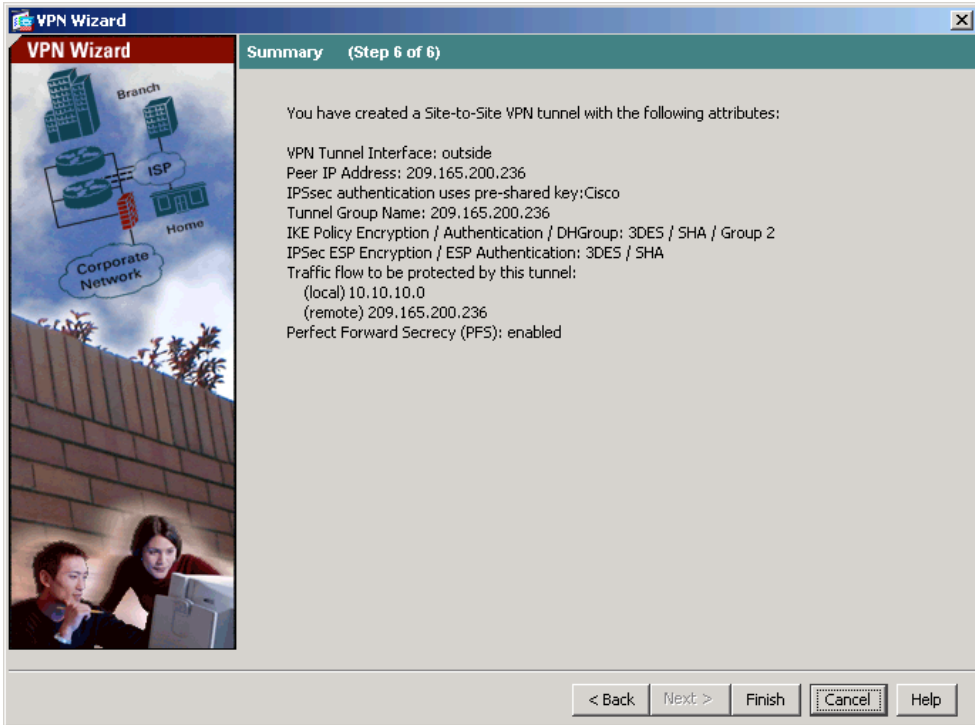
Step 3 If you are not using NAT or PAT, check the **Exempt ASA side host network from address translation** check box and choose the inside interface from the drop-down list.

Step 4 Click **Next** to continue.

Viewing VPN Attributes and Completing the Wizard

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

Step 1 Review the configuration summary for the site-to-site VPN tunnel that you have just created.



Step 2 If you are satisfied with the configuration, click **Finish** to apply the changes to the adaptive security appliance.

Step 3 Choose one of the following:

- 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 previous configuration takes effect the next time that the device starts.

This concludes the configuration process for Security Appliance 1.

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 (Security Appliance 2) to serve as a remote VPN peer. Use the same procedure that you used to configure the local adaptive security appliance, starting with “[Configuring the Security Appliance at the Local Site](#)” section on page 10-5 and finishing with “[Viewing VPN Attributes and Completing the Wizard](#)” section on page 10-12.

**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.

For information about verifying or troubleshooting the configuration for the Site-to-Site VPN, see the section “Troubleshooting the Security Appliance” in the *Cisco Security Appliance Command Line Configuration Guide*.

For specific troubleshooting issues, see the Troubleshooting Technotes at the following location:

http://www.cisco.com/en/US/products/ps6120/prod_tech_notes_list.html

For help troubleshooting configuration issues, see the Configuration Examples and TechNotes at the following location:

http://www.cisco.com/en/US/products/ps6120/prod_configuration_examples_list.html

In particular, see the technotes for Site to Site VPN (L2L) with ASA in the Troubleshooting Technotes. The troubleshooting technotes walk you through using commands like the following to troubleshoot the Site-to-site VPN configuration:

- **show run isakmp**
- **show run ipsec**
- **show run tunnel-group**
- **show run crypto map**
- **debug crypto ipsec sa**

- `debug crypto isakmp sa`

See also the *Cisco Security Appliance Command Reference* for detailed information about each of these commands.

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:

To Do This...	See...
Refine configuration and configure optional and advanced features	<i>Cisco Security Appliance Command Line Configuration Guide</i>
Learn about daily operations	<i>Cisco Security Appliance Command Reference</i> <i>Cisco Security Appliance System Log Messages Guide</i>

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.

To Do This...	See...
Configure the adaptive security appliance to protect a web server in a DMZ	Chapter 6, “Scenario: DMZ Configuration”
Configure a remote-access VPN	Chapter 7, “Scenario: IPsec Remote-Access VPN Configuration”
Configure a clientless (browser-based) SSL VPN	Chapter 9, “Scenario: SSL VPN Clientless Connections”
Configure an SSL VPN for the Cisco AnyConnect software client	Chapter 8, “Scenario: Configuring Connections for a Cisco AnyConnect VPN Client”

■ What to Do Next



CHAPTER 11

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 11-1](#)
- [Client Mode and Network Extension Mode, page 11-3](#)
- [Configuring the Easy VPN Hardware Client, page 11-5](#)
- [Configuring Advanced Easy VPN Attributes, page 11-11](#)
- [What to Do Next, page 11-12](#)

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.

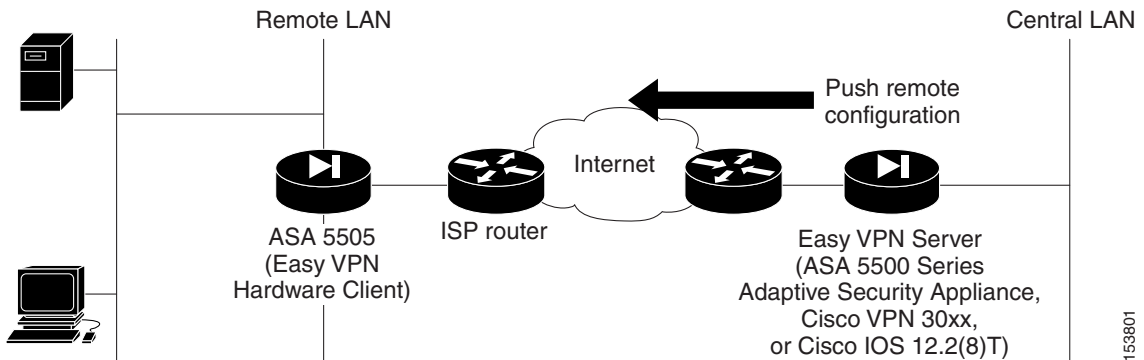
The Cisco ASA 5505 can function as a Cisco Easy VPN hardware client or as a Cisco Easy VPN server (sometimes called a “headend device”), but not both at the same time.

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 11-1 illustrates how Easy VPN components can be deployed to create a VPN.

Figure 11-1 Easy VPN Components in a Virtual Private Network



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.



Note

Load balancing is supported with VPN remote sessions that are initiated with the ASA 5505 when it is acting as an Easy VPN client.

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.

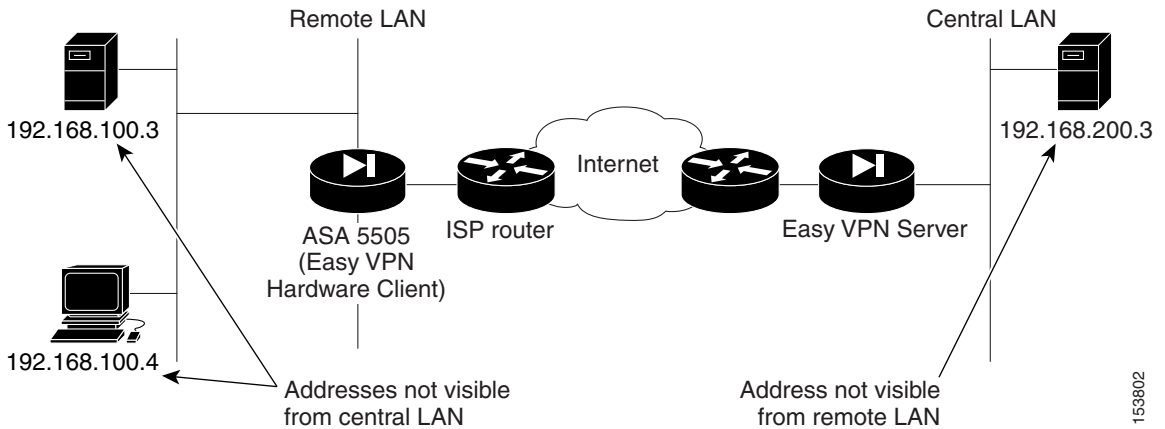
NEM makes the inside interface and all inside hosts routable across the enterprise network over the tunnel. Hosts on the inside network obtain their IP addresses from an accessible subnet (statically or with DHCP) that is preconfigured with static IP addresses. PAT does not apply to VPN traffic in NEM. 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 11-2](#) 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.

Figure 11-2 Topology with ASA 5505 in Client Mode



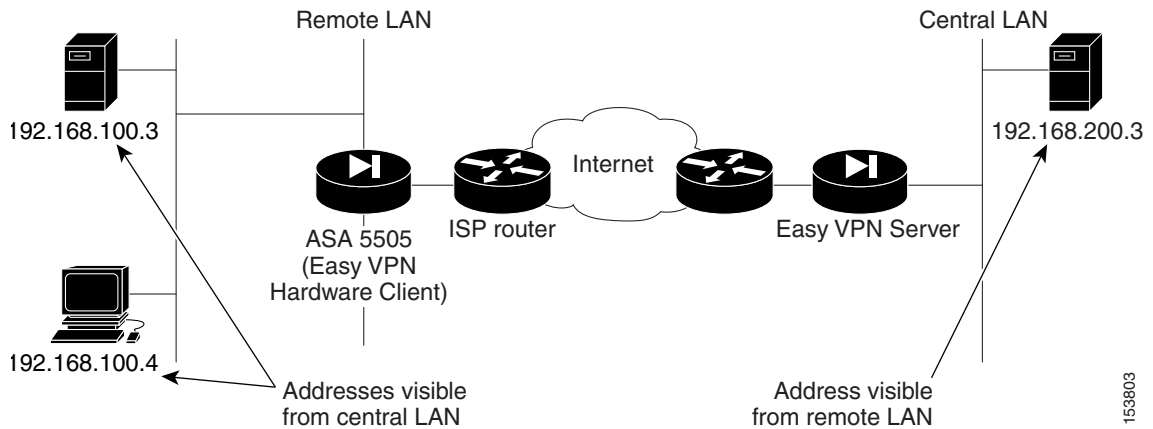
153802

When configured in 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 the network behind the Easy VPN server.

Figure 11-3 shows a sample network topology with the ASA 5505 running in Network Extension Mode.

Figure 11-3 Network Topology with ASA 5505 Running in Network Extension Mode



Use the following guidelines when deciding whether to configure the ASA 5505 in 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.

You can perform this configuration procedure by using ASDM or by using the command-line interface.

This section includes the following topics:

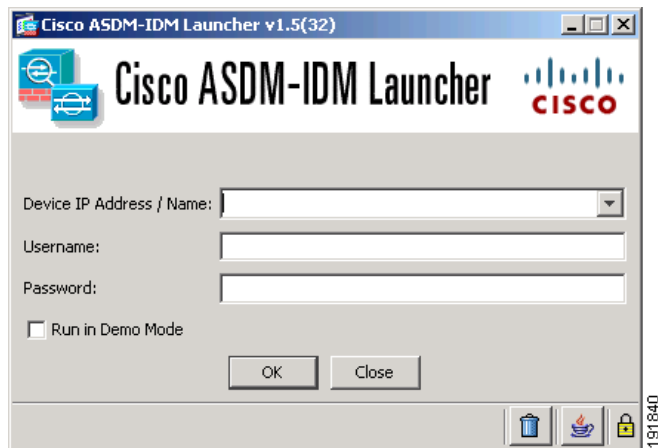
- [Starting ASDM With the ASDM Launcher, page 11-6](#)
- [Configuring the Hardware Client, page 11-9](#)

Starting ASDM With the ASDM Launcher

This section describes how to start ASDM using the ASDM Launcher software. If you have not installed the ASDM Launcher software, see [Installing the ASDM Launcher, page 5-6](#). If you prefer to access ASDM directly with a web browser or using Java, see [Starting ASDM with a Web Browser, page 5-9](#).

To start ASDM, perform the following steps:

-
- Step 1** From your desktop, double-click the Cisco ASDM Launcher icon. The Cisco ASDM-IDM Launcher dialog box appears.



- Step 2** Enter the IP address or the device name of the adaptive security appliance.
- Step 3** Leave the Username and Password fields blank.



Note By default, no Username and Password are set for the Cisco ASDM-IDM Launcher.

Step 4 Click **OK**.

Step 5 Click **Yes** to accept the certificates.

The adaptive security appliance checks to see if updated software is available and if so, downloads it automatically.

Step 6 Click **Yes** to all subsequent authentication and certificate dialog boxes.

The ASDM main window appears.

Configuring the Easy VPN Hardware Client

Cisco ASDM 6.1 for ASA - 10.86.194.224

File View Tools Wizards Window Help Look For: Go

Home Configuration Monitoring Save Refresh Back Forward Help

CISCO

Home

Device Dashboard Firewall Dashboard

Device Information

General License

Host Name: **asa2.cisco.com**

ASA Version: **8.0(4)** Device Uptime: **46d 15h 59m 34s**

ASDM Version: **6.1(3)** Device Type: **ASA 5510**

Firewall Mode: **Routed** Context Mode: **Single**

Total Flash: **64 MB** Total Memory: **256 MB**

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
fa/0/24	192.168.3.4/24	down	down	0
inside	no ip address	down	down	0
management	192.168.1.1/24	down	down	0
outside	10.86.194.224/23	up	up	120

Select an interface to view input and output Kbps

VPN Sessions

IPSec: 0 Clientless SSL VPN: 0 SSL VPN Client: 0 [Details](#)

Traffic Status

-Connections Per Second Usage

Legend: UDP: 0 TCP: 0 Total: 0

-'outside' Interface Traffic Usage (Kbps)

System Resources Status

CPU — CPU Usage (percent)

3%

Memory — Memory Usage (MB)

137MB

Latest ASDM Syslog Messages

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
6	Oct 14 2008	13:55:31	725007	171.69.39.67	1748			SSL session with client outside:171.69.39.67/1748 terminated.
6	Oct 14 2008	13:55:31	605005	171.69.39.67	1748	10.86.194.224	https	Login permitted from 171.69.39.67/1748 to outside:10.86.194.224/https for user "enable_15"
6	Oct 14 2008	13:55:31	725002	171.69.39.67	1748			Device completed SSL handshake with client outside:171.69.39.67/1748
6	Oct 14 2008	13:55:31	725003	171.69.39.67	1748			SSL client outside:171.69.39.67/1748 permitted to resume previous session.

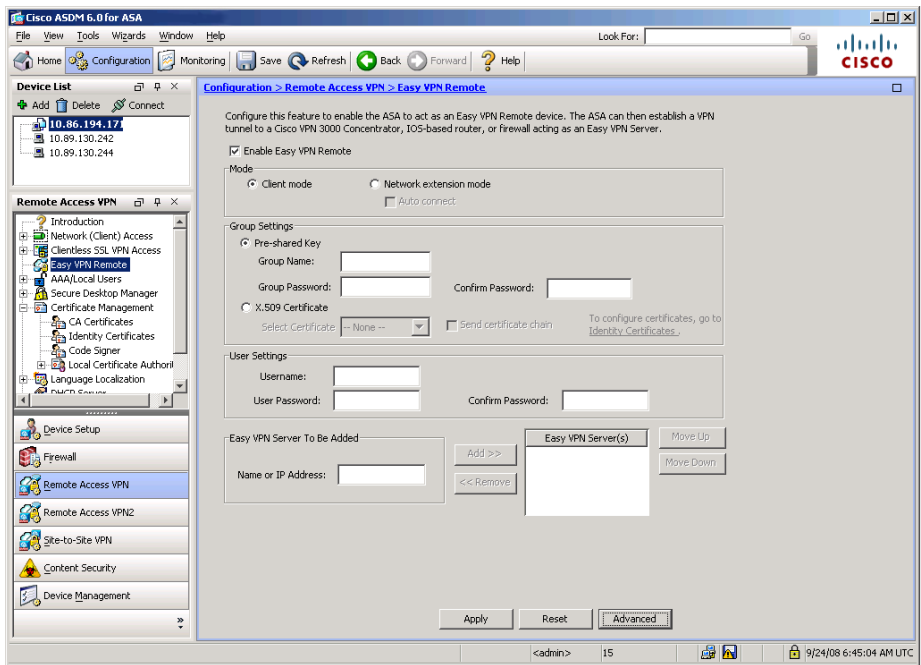
Device configuration loaded successfully. <admin> 15 10/14/08 1:55:28 PM EDT

Configuring the Hardware Client

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

Step 1 In the ASDM main window, choose **Configuration > Remote Access VPN > Easy VPN Remote**.

The Easy VPN Remote pane appears.



Step 2 Check the **Enable Easy VPN Remote** check box to enable Easy VPN on the device. 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 want to disable the Easy VPN client temporarily.



Note When Easy VPN Remote is enabled, you cannot make any configuration changes to IPsec rules, tunnel policy, IKE, or SSL VPN settings.

- Step 3** In the Mode area, to specify which mode the Easy VPN remote hardware client should run in, click the **Client Mode** or **Network Extension Mode** radio button.
- Step 4** To have the Easy VPN remote hardware client automatically run in Network Extension Mode, check the **Auto Connect** check box.
- Step 5** In the Group Settings area, specify the type of authentication that the VPN devices should use by choosing one of the following options.
- To use a pre-shared key for authentication, click the **Pre shared key** radio button and enter a Group Name and Group Password.
 - To use an X.509 certificate for authentication, click the **X.509 Certificate** radio button. Choose the certificate from the drop-down list, check the **Send certificate chain** check box, and click the **Identity Certificates** link to open the Certificate Management pane, from which you can configure and manage certificates. For more information about managing certificates, see the ASDM online help.
- Step 6** In the User Settings area, specify the User Name and User Password to be used by the ASA 5505 when establishing a VPN connection.
- Step 7** Specify one or more Easy VPN servers from which this device obtains VPN security policies.
- a. In the Easy VPN server To Be Added area, enter the hostname or IP address of an Easy VPN server. You must add at least one Easy VPN server.
 - b. Click **Add** or **Remove** to add or remove servers from the Easy VPN servers list. The first server on the list is used as the primary server. Other servers on the list provide redundancy. To change the order of the list, click **Move Up** or **Move Down**. You can specify up to nine backup servers, for a total of ten servers.
- Step 8** Click **Apply** to push the configuration to the adaptive security appliance.
- Step 9** To save the configuration, click **Save** on the toolbar.
-

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 cannot perform authentication, and therefore cannot participate 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 are allowed to manage the Easy VPN connection through the tunnel.



Note

When behind a NAT device, the public address of the ASA 5505 is not accessible unless you add static NAT mappings on the NAT device.

To configure these attributes, click **Advanced** in the Easy VPN Remote configuration pane to open the Advanced Easy VPN Properties pane. For specific information about configuration settings for this pane, see the ASDM online help.

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:

To Do This...	See...
Refine configuration and configure optional and advanced features	<i>Cisco Security Appliance Command Line Configuration Guide</i>
Learn about daily operations	<i>Cisco Security Appliance Command Reference</i> <i>Cisco Security Appliance System Log Messages Guide</i>



APPENDIX **A**

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 about activation key examples or software upgrades, see the *Cisco Security Appliance Command Line Configuration Guide*.

To use the activation key, perform the following steps:

	Command	Purpose
Step 1	hostname# show version	Shows the software release, hardware configuration, license key, and related uptime data.
Step 2	hostname# configure terminal	Enters global configuration mode.
Step 3	hostname(config)# activation-key <i>activation-5-tuple-key</i>	Updates the encryption activation key by replacing the <i>activation-4-tuple-key</i> variable with the activation key obtained with your new license. The <i>activation-5-tuple-key</i> 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.
Step 4	hostname(config)# exit	Exits global configuration mode.
Step 5	hostname# copy running-config startup-config	Saves the configuration.
Step 6	hostname# reload	Reboots the adaptive security appliance and reloads the configuration.