



## Deployment Planning

---

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

This chapter includes the following sections:

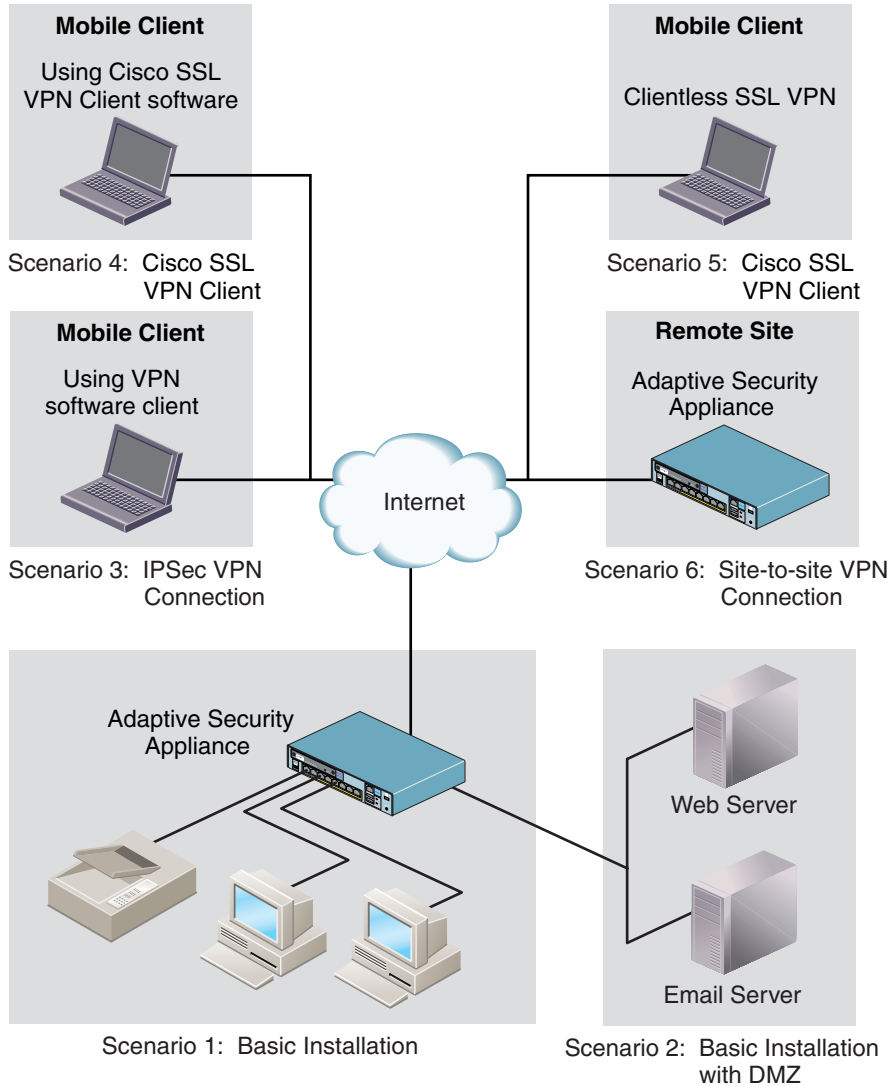
- [Scenarios for Deployment Planning and Configuration, page 2-1](#)
- [Scenario 1: Private Network with External Connectivity, page 2-3](#)
- [Scenario 2: Basic Installation with DMZ, page 2-4](#)
- [Scenario 3: IPSec Remote-Access VPN, page 2-5](#)
- [Scenario 4: Site-to-Site VPN, page 2-6](#)
- [Scenario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

## Scenarios for Deployment Planning and Configuration

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

[Figure 2-1](#) illustrates an extended network that includes most of the deployment and configuration scenarios included in this document.

Figure 2-1 Extended Network Deployment

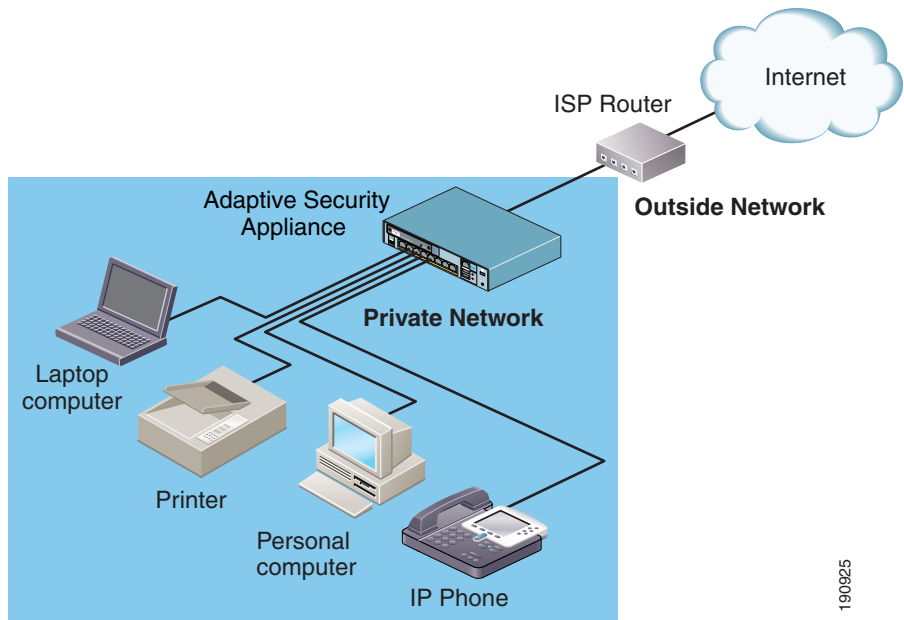


190924

# 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



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.

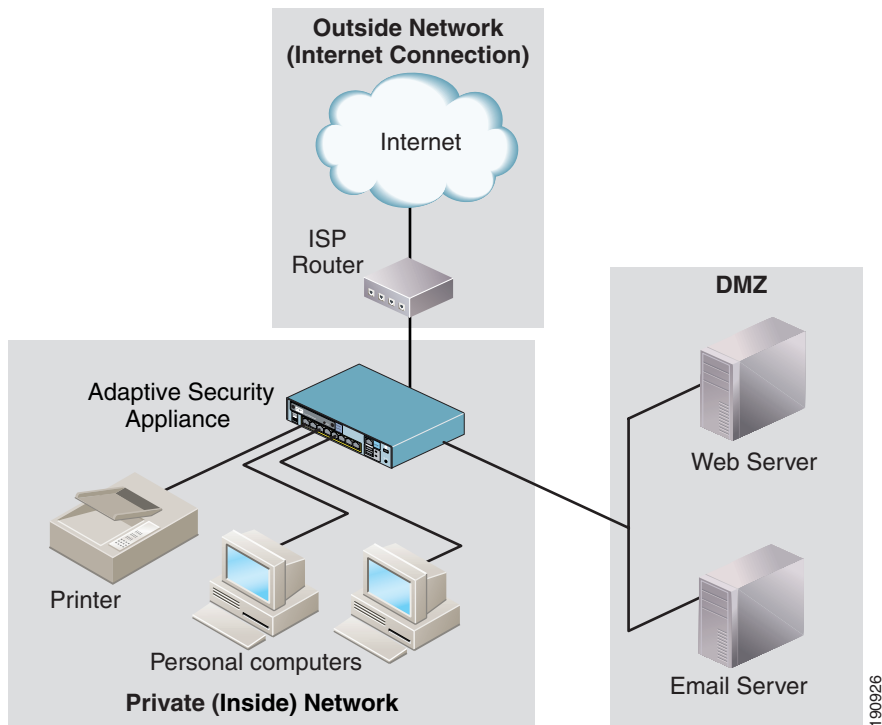
For information about how to configure your adaptive security appliance for this deployment, see [Chapter 5, “Configuring the Adaptive Security Appliance.”](#)

## 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

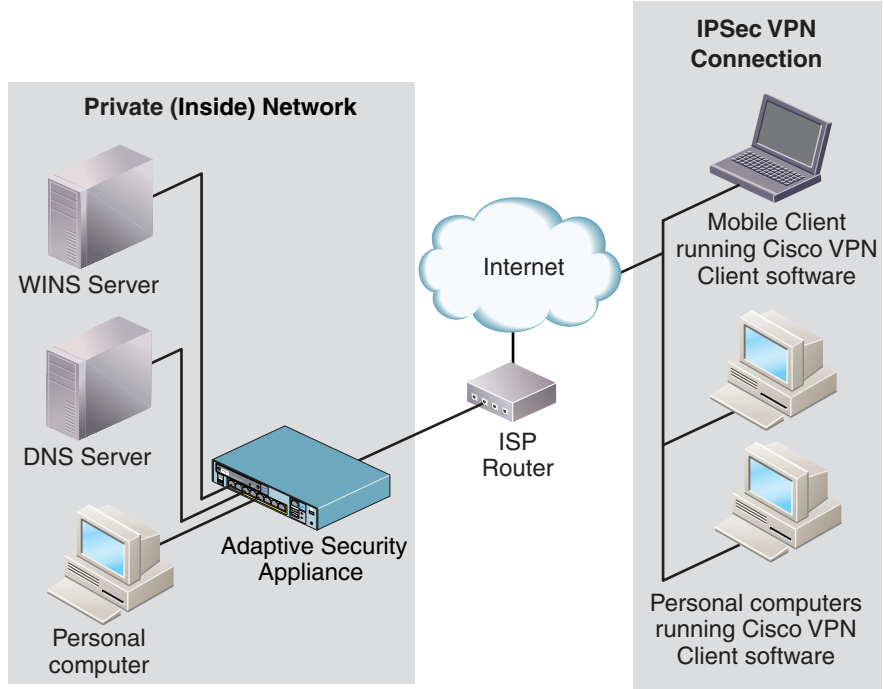


For information about configuring a DMZ deployment, see [Chapter 6, “Scenario: DMZ Configuration.”](#)

## 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*



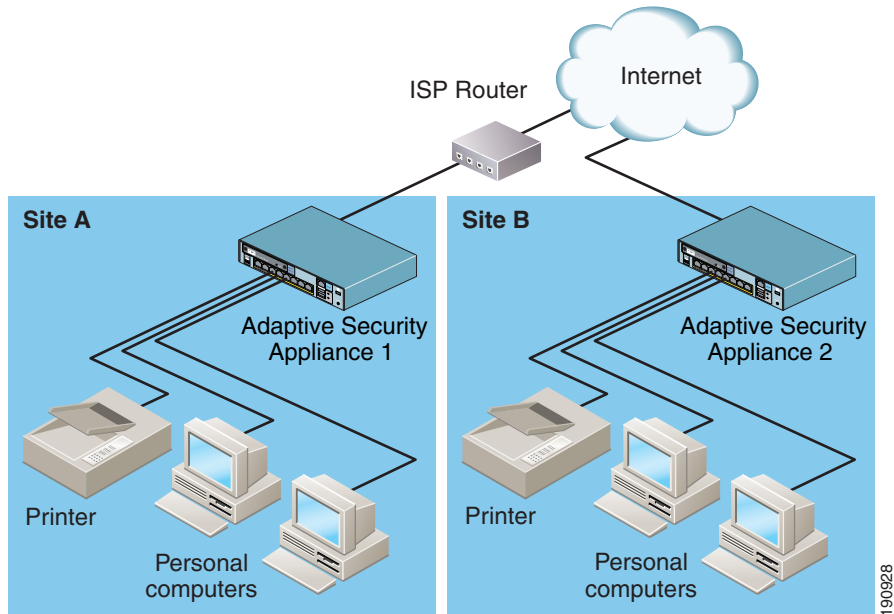
For information about how to configure an IPSec remote-access VPN deployment, see [Chapter 7, “Scenario: IPSec Remote-Access VPN Configuration.”](#)

## Scenario 4: 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 2-5** Network Layout for Site-to-Site VPN Configuration Scenario



For information about configuring a site-to-site VPN deployment, see [Chapter 8](#), “Scenario: Site-to-Site VPN Configuration.”

# Scenario 5: ASA 5505 Deployed as a Hardware VPN Client

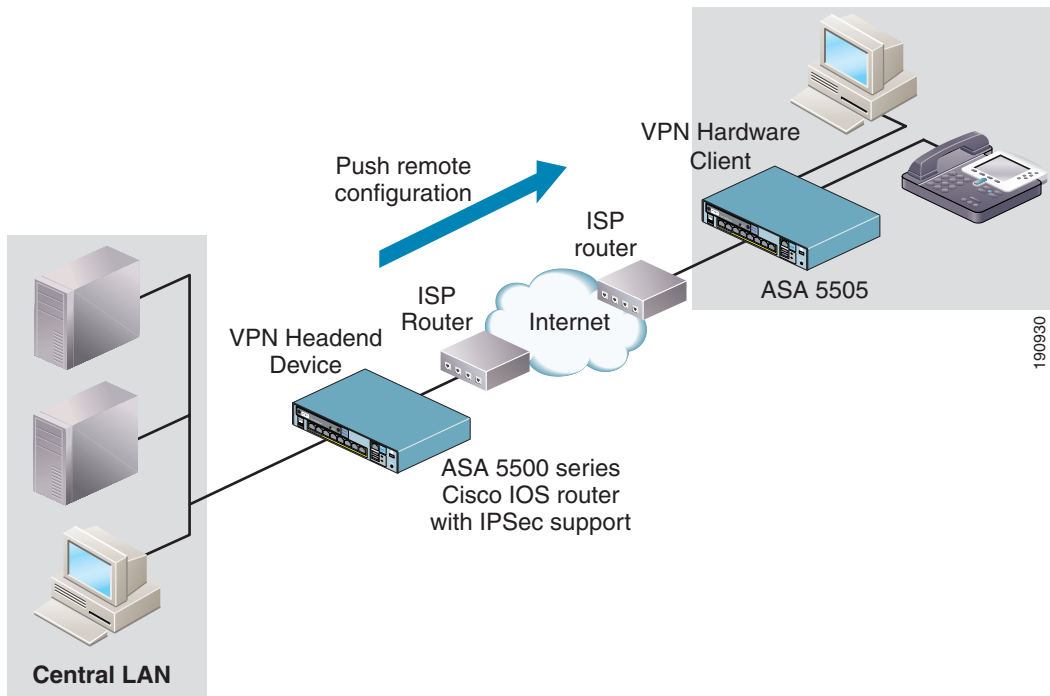
In this scenario, an ASA 5505 is deployed as a hardware client (sometimes called a remote device). Deploying one or more VPN hardware clients in conjunction with a VPN headend device enables companies with multiple sites to establish secure communications among them and share network resources.

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

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

[Figure 2-6](#) illustrates how the different Easy VPN components can be deployed.

**Figure 2-6** ASA 5505 Installed as VPN Hardware Client



For information about how to configure the ASA 5505 as a VPN hardware client, see [Chapter 9, “Scenario: Easy VPN Hardware Client Configuration.”](#)

## Configuration Procedures for Scenarios

Each deployment scenario in this chapter has a corresponding configuration chapter in this document that describes how to configure the ASA 5505 for that type of deployment.

To Configure the ASA 5505 For This Scenario....	See This Chapter...
<a href="#">Scenario 1: Private Network with External Connectivity</a>	Chapter 5, “Configuring the Adaptive Security Appliance”
<a href="#">Scenario 2: Basic Installation with DMZ</a>	Chapter 6, “Scenario: DMZ Configuration”
<a href="#">Scenario 3: IPSec Remote-Access VPN</a>	Chapter 7, “Scenario: IPSec Remote-Access VPN Configuration”
<a href="#">Scenario 4: Site-to-Site VPN</a>	Chapter 8, “Scenario: Site-to-Site VPN Configuration”
<a href="#">Scenario 5: ASA 5505 Deployed as a Hardware VPN Client</a>	Chapter 9, “Scenario: Easy VPN Hardware Client Configuration”

## What to Do Next

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

