



## Planning for a VLAN Configuration

---

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

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

This chapter includes the following sections:

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

## Understanding VLANs on the ASA 5505

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

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

This section includes the following topics:

- [About Physical Ports on the ASA 5505, page 3-2](#)
- [About VLANs, page 3-2](#)

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

## About Physical Ports on the ASA 5505

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

## About VLANs

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

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

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

To impose strict access control and provide protection of sensitive devices, you can apply security policies to VLANs that restrict communications between VLANs. You can also apply security policies to individual ports. You might want to apply security policies at the port level if, for example, there are two ports on the same VLAN connecting devices that you do not want to be able to communicate with each other.

Before you can enable a switch port on the ASA 5505, it must be assigned to a VLAN. With the Base platform, each switch port can be assigned to only one VLAN at a time. With the Security Plus license, you can use a single port to trunk 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	<a href="#">Chapter 5, “Configuring the Adaptive Security Appliance”</a>
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, thus 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.

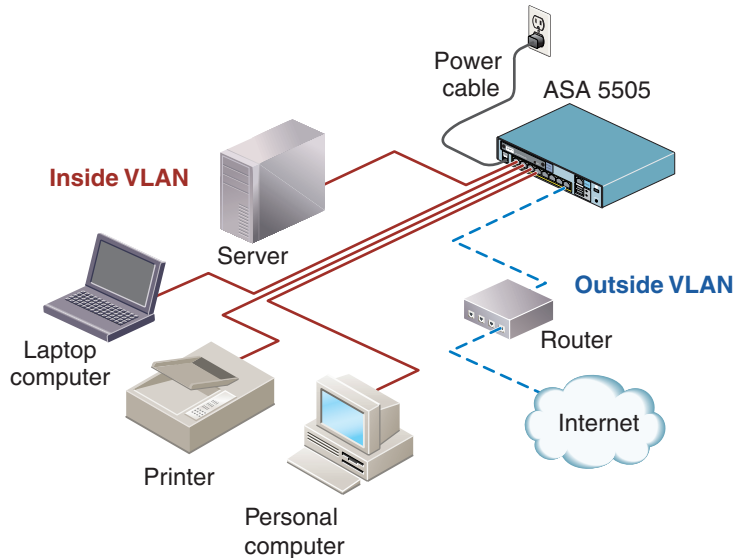
This section includes the following topics:

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

## Basic Deployment Using Two VLANs

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

**Figure 3-1** Deployment Using Two VLANs



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

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

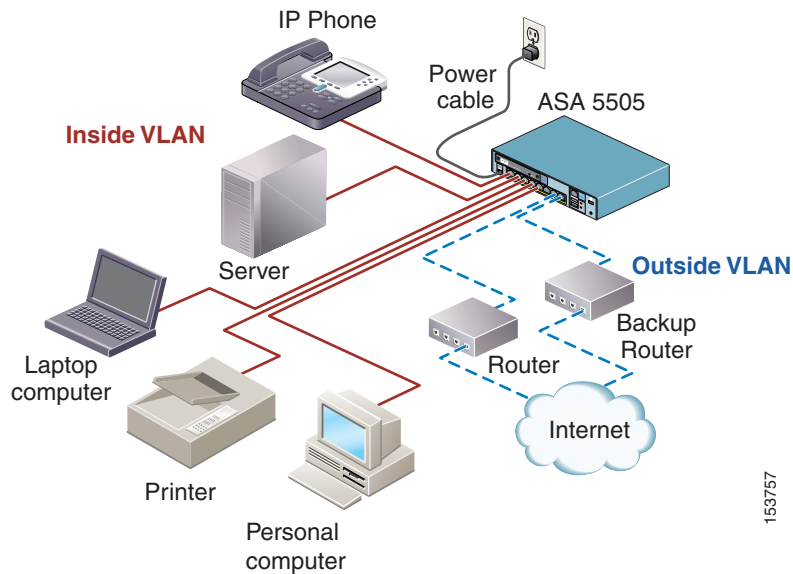
In [Figure 3-1](#), the Inside VLAN uses four switch ports on the ASA 5505 and the Outside VLAN uses only one. Three switch ports are unused.

**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



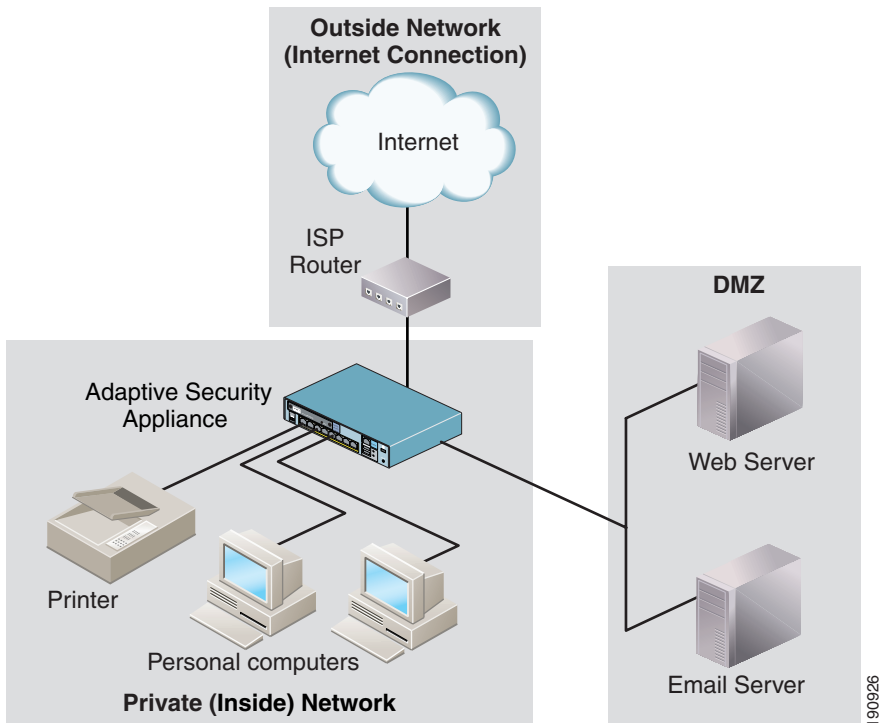
153757

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

## DMZ Deployment

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

**Figure 3-3** Deployment Requiring Three VLANs



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

## Teleworker Deployment Using Three VLANs

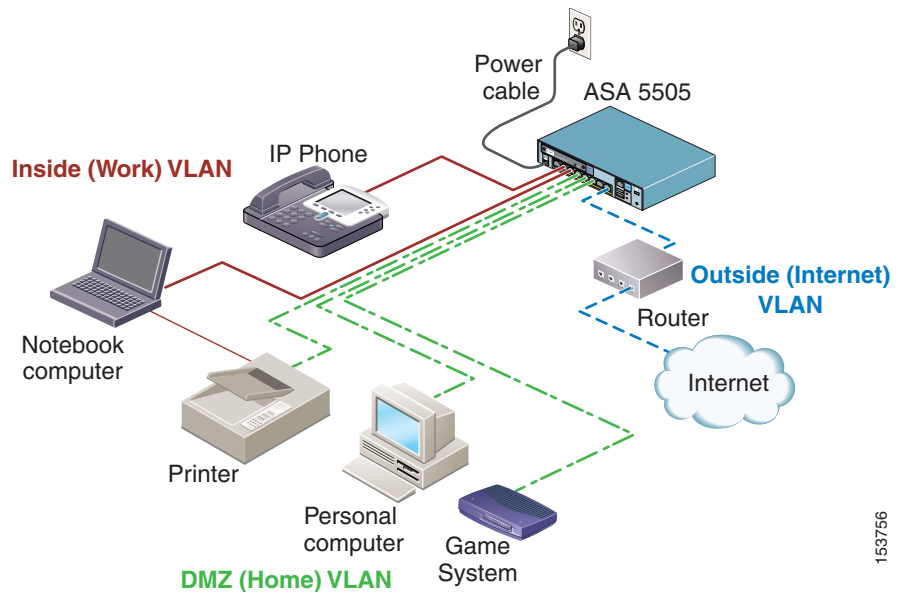
Although not required, using three VLANs can be useful in other situations, such as when deploying a remote VPN hardware client to support a teleworker.

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

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

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

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 more scenarios with VLANs, see the *Cisco Security Appliance Command Line Configuration Guide*.

## What to Do Next

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

