



# Server Room

## Technology Design Guide

August 2014 Series



# Table of Contents

---

<b>Preface</b> .....	<b>1</b>
<b>CVD Navigator</b> .....	<b>2</b>
Use Cases .....	2
Scope .....	2
Proficiency .....	2
<b>Introduction</b> .....	<b>3</b>
Technology Use Cases .....	5
Use Case: Deploy Server Room LAN in Central and Remote Locations .....	5
Use Case: Secure Server Room Resources with Cisco ASA .....	5
Design Overview .....	6
Server Room Ethernet LAN .....	6
Server Room Security .....	7
<b>Server Room Ethernet LAN</b> .....	<b>8</b>
Design Overview.....	8
Deployment Details .....	9
Configuring the Server Room Ethernet LAN .....	10
<b>Server Room Security</b> .....	<b>22</b>
Design Overview.....	22
Security Topology Design .....	23
Security Policy Development.....	24
Deployment Details .....	25
Configuring Firewall Connectivity for the Server Room.....	26
Configuring the Server Room Firewall.....	30
Configuring Firewall High Availability .....	35
Evaluating and Deploying Firewall Security Policy .....	37
Deploying Firewall Intrusion Prevention Systems (IPS) .....	44
<b>Appendix A: Product List</b> .....	<b>59</b>
<b>Appendix B: Configuration Examples</b> .....	<b>60</b>
Cisco Catalyst 3850 Switch Stack .....	60
Cisco ASA 5500-X Firewall—Primary and Secondary .....	71
Cisco ASA 5500-X IPS—Primary.....	76
Cisco ASA 5500-X IPS—Secondary .....	78
<b>Appendix C: Changes</b> .....	<b>81</b>

# Preface

---

Cisco Validated Designs (CVDs) present systems that are based on common use cases or engineering priorities. CVDs incorporate a broad set of technologies, features, and applications that address customer needs. Cisco engineers have comprehensively tested and documented each design in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested design details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate existing CVDs but also include product features and functionality across Cisco products and sometimes include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems.

## CVD Foundation Series

This CVD Foundation guide is a part of the *August 2014 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit [the CVD Foundation web site](#).

## Comments and Questions

If you would like to comment on a guide or ask questions, please use the [feedback form](#).

# CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

## Use Cases

This guide addresses the following technology use cases:

- **Deploy Server Room LAN in Central and Remote Locations**—Organizations have requirements to house applications and servers in a secure and resilient manner in central and remote locations.
- **Secure Server Room Resources with Cisco ASA**—Securing critical applications and resources within the server room is a growing concern for organizations.

For more information, see the "Use Cases" section in this guide.

## Scope

This guide covers the following areas of technology and products:

- Design and configuration of server room LAN switches
- Design and configuration of Cisco Adaptive Security Appliance (ASA) firewall with integrated intrusion prevention systems (IPS) in order to protect servers and applications
- Server room LAN quality of service (QoS) design and configuration

For more information, see the "Design Overview" section in this guide.

## Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Routing and Switching**—1 to 3 years installing, configuring, and maintaining routed and switched networks
- **CCNA Security**—1 to 3 years installing, monitoring, and troubleshooting network devices to maintain integrity, confidentiality, and availability of data and devices

### Related CVD Guides



Campus Wired LAN  
Technology Design Guide



Firewall and IPS Technology  
Design Guide

To view the related CVD guides, click the titles or visit [the CVD Foundation web site](#).

# Introduction

---

This guide is designed to provide a growing organization its first formal foundation for centralizing up to 24 physical servers in a secure and resilient environment. It can also be used to provide a server room deployment for a regional site or in-country location for a larger organization. This guide is a prescriptive design based on the [Campus Wired LAN Design Guide](#) so that you can use the Layer 3 services of your Cisco Validated Design (CVD) LAN distribution layer for routing traffic to and from the IP subnets in the server room.

CVD incorporates LAN, WAN, wireless, security, WAN optimization, and unified communication technologies tested together as a solution. The CVD server room is part of the larger CVD design and incorporates the same equipment, processes, and procedures as the CVD campus design in order to provide seamless extension of service for the servers and appliances in the server room.

This guide, *Server Room Design Guide*, includes the following chapters:

- “Server Room Ethernet LAN” includes guidance for the configuration of server ports on the switches, VLAN usage and trunking, resiliency, and connectivity to the LAN distribution layer or collapsed LAN core.
- “Server Room Security” focuses on the deployment of firewalls and intrusion prevention systems (IPS) in order to help protect the information assets of your organization.
- The appendices provides the complete list of products used in the lab testing of this design, software revisions used on the products in the system, a summary of changes to this guide since it was last published, and configuration examples for the products used.

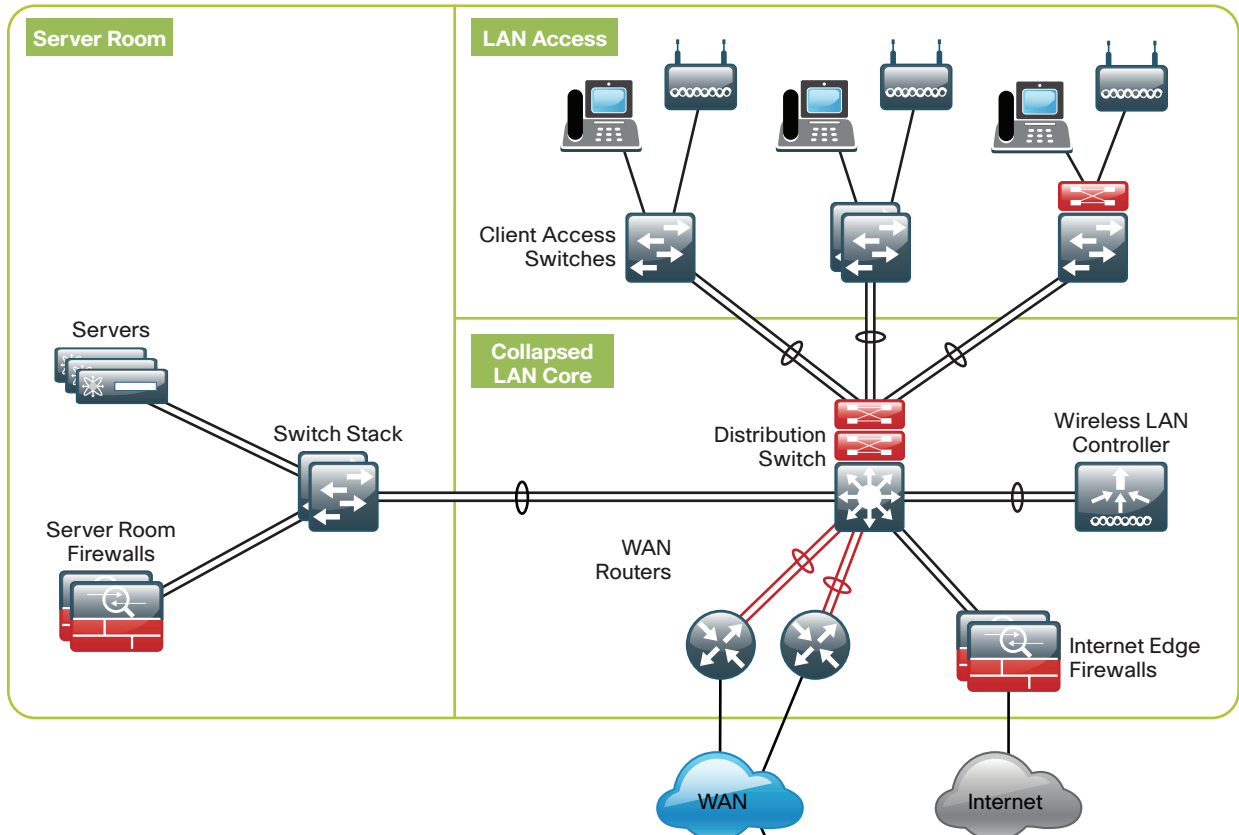
As organizations scale beyond the server room to data centers with many application servers and larger storage environments, the [Data Center Technology Design Guide](#) provides a methodology for a smooth transition.



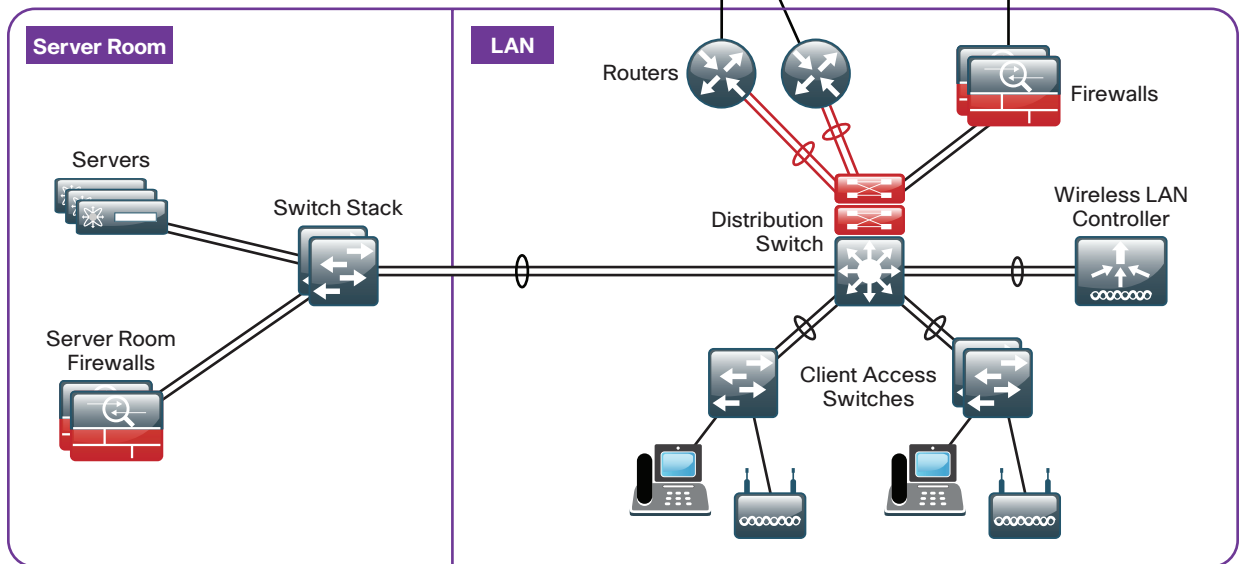
Figure 1 illustrates typical scenarios where the CVD server room would apply.

Figure 1 - Typical CVD server room deployment scenarios

### Headquarters



### Regional Site



3022

# Technology Use Cases

The *Server Room Design Guide* is designed to address two primary use cases:

- Deploy Server Room LAN for central and remote locations
- Secure server room resources with Cisco ASA

The design illustrates how to cleanly integrate network security capabilities such as firewall and intrusion prevention, while protecting areas of the network housing critical server and storage resources. The architecture provides the flexibility to secure specific portions of the server room or insert firewall capability between tiers of a multi-tier application, according to the security policy agreed upon by the organization.

## Use Case: Deploy Server Room LAN in Central and Remote Locations

Organizations and businesses often begin their IT practices with application servers sitting under desks or in closets with switches—and perhaps some storage tapes for ad hoc backups stacked on top. As the organization grows and its reliance on data grows, so does the need to provide a more stable environment for its critical applications. Whether it is the fear of an outage delaying productivity, data loss that could harm the perception of an organization, or regulatory compliance, the IT person or group is forced to build a more suitable environment.

The server room represents the first move into a serious IT environment onsite with the business. An example environment will have controlled cooling and power, two to three equipment racks for application servers, supporting network connectivity, and a small backup system.

Also, many organizations have large remote-site locations that might house hundreds of employees and require local processing for communication services, file sharing, and low-latency access to information. Organizations extending their presence to a global reach often require regional offices located in a foreign country in order to focus on geographic and business requirements. These remote-site locations often require an IT environment for their local servers in order to provide high availability and security for the applications being used. The *Server Room Design Guide* provides a foundation for housing those applications and servers in a secure and resilient manner.

This guide enables the following server room capabilities:

- Deployment of up to 24 physical servers in central or remote locations
- Establishment of resilient 1GE server connections using dual server access layer switches
- Deployment of Layer 2 switches using Cisco StackWise Plus, 802.1Q trunks, Link Aggregation Control Protocol (LACP), and quality of service (QoS) for server access environments

## Use Case: Secure Server Room Resources with Cisco ASA

With communication and commerce in the world becoming increasingly Internet-based, network security quickly becomes a primary concern in a growing organization. Often organizations will begin by securing their Internet edge connection, considering the internal network a trusted entity. However, an Internet firewall is only one component of building security into the network infrastructure.

Frequently, threats to an organization's data may come from within the internal network. This may come in the form of onsite vendors, contaminated employee laptops, or existing servers that have already become compromised and may be used as a platform to launch further attacks. With the centralized repository of the organization's most critical data typically being the data center, security is no longer considered an optional component of a complete data center architecture plan.

The server room of a small organization contains some of the organization's most valuable assets. Customer and personnel records, financial data, email stores, and intellectual property must be maintained in a secure environment to ensure confidentiality and availability. Additionally, portions of networks in specific business sectors may be subject to industry or government regulations that mandate specific security controls in order to protect customer or client information. Some regional offices may require a server room for in-country operation where the need to protect customer and business information dictates local security measures.

This guide enables the following server room capabilities:

- Deployment of Cisco ASA Firewalls in active-standby configuration
- Deployment of a basic firewall security policy to protect server room resources
- Deployment of an integrated Cisco ASA Intrusion Prevention System (IPS) in an in-line configuration
- Deployment of in-line IPS security policy to protect server room resources

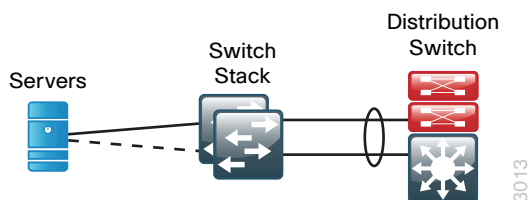
## Design Overview

The chapters in this guide describe a design that enables communications across the organization. This section provides architectural guidance specific to the network components or services you need to deploy.

### Server Room Ethernet LAN

The server room switches provide network connectivity for servers and appliances that offer network and user services to a variety of devices in the network. The server room design has two product lines to choose from: Cisco Catalyst 3850 Series and Cisco Catalyst 3650 Series switches. Cisco Catalyst 3850 Series offers flexible port density and server port connection speeds from 10-Mb Ethernet to 1-Gigabit Ethernet. With a Cisco Catalyst 3850 Series switch stack, you can build in fault tolerance by dual-homing servers to the server room and dual-homing the server room to the LAN distribution layer with redundant Gigabit Ethernet or 10-Gigabit Ethernet links in an EtherChannel. Cisco Catalyst 3850 Series provides platform resilience when stacked through Cisco StackWise480, which allows the control plane for the server room Ethernet switches to reside on either of the Catalyst 3850 Series switches and fail over in the event of a failure. Cisco StackPower on the Catalyst 3850 Series switch provides the ability to spread the power load over multiple power supplies in each chassis for diversity and resilience. The Cisco Catalyst 3650 Series switch offers a lower-cost option for applications where Ethernet LAN switch resiliency is not a priority.

Figure 2 - Resilience in the server room design



Both the server room and the client LAN access methods connect devices to the network; the difference between the two methods that changes the switch model is the requirement in the LAN access for Power over Ethernet (PoE). Although PoE-capable devices are not typical in the server room, using PoE-capable switches offers a benefit worth considering: the minor initial cost savings of a non-PoE switch may not be worth the benefits of using the same switch across multiple modules of your local LAN. Although configurations differ between LAN access switches and server room switches, the ability to use a single switch type between multiple modules can lower operational costs by allowing for simpler sparing and management, as well as provide a better chance of reuse as the organization grows.

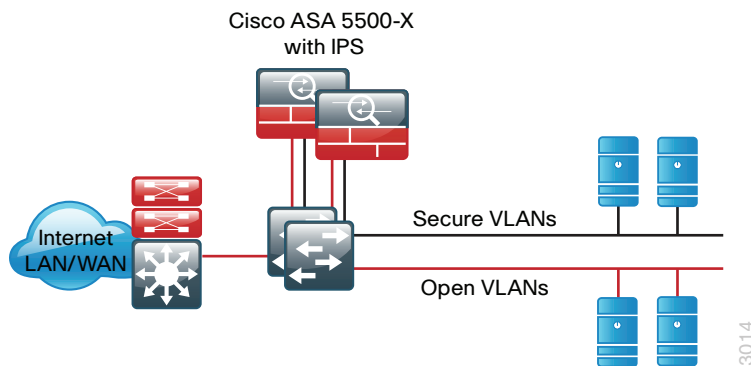


## Server Room Security

Within the design, there are many requirements and opportunities to include or improve security. At the headquarters, there is a layer of security to protect the business information assets. These devices help provide direct and indirect protection against potential threats. The first product in the server room security perimeter is Cisco ASA 5500-X Series Midrange Adaptive Security Appliance (ASA). Cisco ASA 5500-X Series is a next-generation multifunction appliance providing multi-gigabit firewall capability and intrusion prevention or intrusion detection services in a compact 1RU form-factor. Cisco ASA 5500-X Series runs the same base firewall and IPS software as the ASA 5500 Series, making transition and operational support easy for existing ASA customers.

Dedicated IPS hardware acceleration adds the ability to inspect application-layer data for attacks and to block malicious traffic based on the content of the packet or the reputation of the sender without additional hardware requirements.

Figure 3 - Secure server room with firewall and IPS-secured VLANs



The indirect security is established by the use of an intrusion detection system (IDS). This is a passive method for monitoring threats. After a threat is detected, mitigation steps can be taken. Cisco IPS allows your organization to continuously monitor the network traffic destined for protected VLANs for potential threats. When a threat is detected, the system sends an alert to the appropriate monitoring resource, and engineering or operational staff take action to resolve the issue. The IPS service can also be deployed inline in IPS mode in order to fully engage intrusion prevention capabilities, wherein they will block malicious traffic before it reaches its destination. The ability to run in IDS mode or IPS mode is highly configurable to allow the maximum flexibility in meeting a specific security policy.

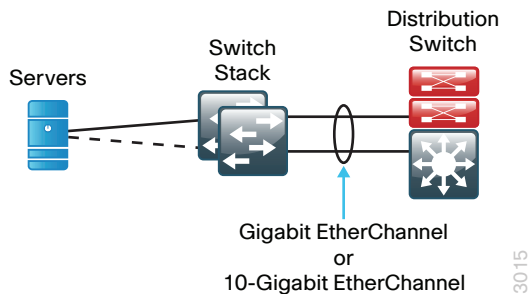
# Server Room Ethernet LAN

## Design Overview

In CVD, the server room provides basic compute capability for business operations and is designed to accommodate up to 24 physical servers. The design uses the Cisco Catalyst 3650 standalone switch and Cisco Catalyst 3850 Series stackable access switches, with 10/100/1000 support to accommodate a wide range of server Ethernet interface speeds, as well as wired and wireless network convergence.

The Cisco StackWise-480 feature of Cisco Catalyst 3850 Series provides a resilient, high-speed backplane for the server room environment and the ability to dual-home servers to the server room LAN for increased resiliency. With two switches in the stack and dual homing to servers and the LAN core switches, your server room is protected from single points of failure. The Catalyst 3850 Series switches in a stack provide automated control plane failover in the event that the active switch experiences an issue. The option of dual power supplies and Cisco StackPower with the Catalyst 3850 Series switches provides more resiliency to the server room design. Cisco Catalyst 3650 Series does not provide the same level of resiliency as Cisco Catalyst 3850 Series, but it is suitable for single connected servers and less-critical systems.

Figure 4 - Server room switch or switch stack with EtherChannel uplinks



In this CVD, the server room switches are connected to the collapsed core or distribution layer with an EtherChannel so that two 10-Gigabit Ethernet ports combine to make a single 20-Gigabit Ethernet channel. It is possible to increase the number of links to the core from the server room to four or eight for more bandwidth if needed.

# Deployment Details

## How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

```
class-map [highest class name]
```

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined.

Enter them as one command:

```
police rate 10000 pps burst 10000  
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

```
interface Vlan64  
ip address 10.5.204.5 255.255.255.0
```

This section includes the procedures you need to perform in order to configure your server room Ethernet LAN connectivity. As you review the *Server Room Design Guide*, you may find it useful to understand the following tables, which list the IP addressing and VLAN assignments used in CVD server room deployments. Because the server room can be deployed at the main site or a remote site, this guide contains two models for addressing. This guide will use the remote-site addressing. Your design requirements for IP addressing and VLAN numbering may differ.

Table 1 - Design guide addressing for main-site deployment

VLAN	IP address range	Usage
148	10.4.48.x /24	Server VLAN #1
149	10.4.49.x /24	Server VLAN #2
115	10.4.15.x /25	Management VLAN from LAN core

Table 2 - Design guide addressing for remote-site deployment

VLAN	IP address range	Usage
148	10.5.24.x /24	Server VLAN #1
149	10.5.25.x /24	Server VLAN #2
106	10.5.7.x /25	Management VLAN from LAN core

## Configuring the Server Room Ethernet LAN

1. Configure the platform
2. Configure switch universal settings
3. Apply the switch global configuration
4. Configure server room uplink ports
5. Configure server access ports
6. Configure LAN distribution layer downlinks

The following procedures are designed to configure a standalone Cisco Catalyst 3650 Series server room switch or a stack of two Catalyst 3850 Series switches used for the server room Ethernet LAN.

### Procedure 1 Configure the platform

**Step 1:** To configure a Cisco Catalyst 3650 or 3850 stack, use the command-line interface (CLI) global exec mode (not configuration mode) to set the preferred active switch.

```
switch [switch number] priority 15
```

When there are multiple Cisco Catalyst 3650 or 3850 Series switches configured in a stack, one of the switches takes the ACTIVE switch role, and another member takes the HOT-STANDBY role. Upon reload, the switch configured with the highest priority assumes the active role. If this is a new configuration, only the active switch console is active during the initial configuration. When two or more switches are configured as a stack, configure the active switch functionality on a switch of your preference.

**Step 2:** For each platform, define two macros that you will use in later procedures to apply the platform-specific QoS configuration. This makes consistent deployment of QoS easier.

#### Tech Tip

The match statements in the class-maps can be combined into one line. However, listing them separately provides additional per-DSCP counters available from SNMP and from the following verification command.

```
show policy-map interface
```

```
class-map match-any PRIORITY-QUEUE
  match dscp ef
class-map match-any VIDEO-PRIORITY-QUEUE
  match dscp cs5
  match dscp cs4
class-map match-any CONTROL-MGMT-QUEUE
  match dscp cs7
  match dscp cs6
  match dscp cs3
  match dscp cs2
```

```

class-map match-any MULTIMEDIA-CONFERENCING-QUEUE
  match dscp af41
  match dscp af42
  match dscp af43
class-map match-any MULTIMEDIA-STREAMING-QUEUE
  match dscp af31
  match dscp af32
  match dscp af33
class-map match-any TRANSACTIONAL-DATA-QUEUE
  match dscp af21
  match dscp af22
  match dscp af23
class-map match-any BULK-SCAVENGER-DATA-QUEUE
  match dscp af11
  match dscp af12
  match dscp af13
  match dscp cs1
!
policy-map 2P6Q3T
  class PRIORITY-QUEUE
    priority level 1 percent 10
  class VIDEO-PRIORITY-QUEUE
    priority level 2 percent 20
  class CONTROL-MGMT-QUEUE
    bandwidth remaining percent 10
    queue-buffers ratio 10
  class MULTIMEDIA-CONFERENCING-QUEUE
    bandwidth remaining percent 10
    queue-buffers ratio 10
    queue-limit dscp af43 percent 80
    queue-limit dscp af42 percent 90
    queue-limit dscp af41 percent 100
  class MULTIMEDIA-STREAMING-QUEUE
    bandwidth remaining percent 10
    queue-buffers ratio 10
    queue-limit dscp af33 percent 80
    queue-limit dscp af32 percent 90
    queue-limit dscp af31 percent 100
  class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 10
    queue-buffers ratio 10
    queue-limit dscp af23 percent 80
    queue-limit dscp af22 percent 90
    queue-limit dscp af21 percent 100
  class BULK-SCAVENGER-DATA-QUEUE
    bandwidth remaining percent 5
    queue-buffers ratio 10

```



```

class class-default
  bandwidth remaining percent 25
  queue-buffers ratio 25
!
macro name AccessEdgeQoS
  auto qos voip cisco-phone
@
!
macro name EgressQoS
  service-policy output 2P6Q3T
@

```

## Procedure 2 Configure switch universal settings

This procedure configures system settings that simplify and secure the management of the switch. The values and actual settings in the examples provided will depend on your current network configuration.

Table 3 - Common network services used in the deployment examples

Service	Address
Domain name	cisco.local
Active Directory, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) server	10.4.48.10
Cisco Secure Access Control System (Secure ACS) server	10.4.48.15
Network Time Protocol (NTP) server	10.4.48.17

**Step 1:** Configure the device host name.

```
hostname [hostname]
```

**Step 2:** Configure VLAN Trunking Protocol (VTP) transparent mode. This deployment uses VTP transparent mode because the benefits of the alternative mode—dynamic propagation of VLAN information across the network—are not worth the potential for unexpected behavior that is due to operational error.

VTP allows network managers to configure a VLAN in one location of the network and have that configuration dynamically propagate out to other network devices. However, in most cases, VLANs are defined once during switch setup with few, if any, additional modifications.

```
vtp mode transparent
```

**Step 3:** Enable Rapid Per-VLAN Spanning-Tree (PVST+). Rapid PVST+ provides an instance of Rapid Spanning Tree Protocol (802.1w) per VLAN. Rapid PVST+ greatly improves the detection of indirect failures or linkup restoration events over classic spanning tree (802.1D).

Although this architecture is built without any Layer 2 loops, you must still enable spanning tree. By enabling spanning tree, you ensure that if any physical or logical loops are accidentally configured, no actual Layer 2 loops will occur.

```
spanning-tree mode rapid-pvst
```

**Step 4:** Enable Unidirectional Link Detection Protocol (UDLD).

*UDLD* is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. When UDLD detects a unidirectional link, it disables the affected interface and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree loops, black holes, and non-deterministic forwarding. In addition, UDLD enables faster link failure detection and quick reconvergence of interface trunks, especially with fiber-optic cables, which can be susceptible to unidirectional failures.

```
udld enable
```

**Step 5:** Enable the recovery mechanism to allow ports disabled as a result of errors to automatically clear the err-disable status and attempt a recovery to operational behavior and connected status. Enabling the recovery mechanism avoids requiring manual intervention; instead, you use the CLI to shut down and enable the port after the cause of the error is cleared. By default, the recovery mechanism waits five minutes to attempt clearing of the interface err-disable status.

```
errdisable recovery cause all
```

**Step 6:** Set EtherChannels to use the traffic source and destination IP address when calculating which link to send the traffic across. This normalizes the method in which traffic is load-shared across the member links of the EtherChannel. EtherChannels are used extensively in this design because they add resiliency to the network.

```
port-channel load-balance src-dst-ip
```

**Step 7:** Configure DNS for host lookup.

At the command line of a Cisco IOS device, it is helpful to be able to type a domain name instead of the IP address for a destination.

```
ip name-server 10.4.48.10
```

**Step 8:** Configure device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) are more secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

The SSH and HTTPS protocols enable secure management of the LAN device. Both protocols are encrypted for privacy, and the unencrypted protocols, Telnet and HTTP, are turned off. Enabling HTTPS automatically generates a cryptographic key to use the service. When SSH is configured after HTTPS, you do not have to explicitly generate the cryptographic key that SSH requires, unless you wish to change the default key size.

Secure Copy (SCP) provides a secure and authenticated method for copying configuration and image files by making use of SSH as a secure transport. To avoid the use of less secure protocols such as TFTP and FTP, enable SCP. This allows secure file management with the device.

Specify the transport **preferred none** on vty lines in order to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name server is unreachable, long timeout delays may occur for mistyped commands.

```
no ip http server
ip http secure-server
ip domain-name cisco.local
ip ssh version 2
ip scp server enable
!
line vty 0 15
```

```
transport input ssh
transport preferred none
```

**Step 9:** Enable Simple Network Management Protocol (SNMP), and then configure SNMPv2c both for a read-only and a read-write community string.

```
snmp-server community [SNMP RO string] RO
snmp-server community [SNMP RW string] RW
```

**Step 10:** If network operational support is centralized in your network, you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class 55 in vrf-also
!
snmp-server community [SNMP RO string] RO 55
snmp-server community [SNMP RW string] RW 55
```



### Caution

If you configure an access list on the vty interface, you may lose the ability to use SSH to log in from one router to the next for hop-by-hop troubleshooting.

**Step 11:** Configure the local login and password.

The local login account and password provide basic device access authentication in order to view platform operation. The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the use of plaintext passwords when viewing configuration files.

```
username admin password [password]
enable secret [password]
service password-encryption
aaa new-model
```

By default, HTTPS access to the switch uses the enable password for authentication.

**Step 12:** If you want to reduce operational tasks per device, configure centralized user authentication by using the TACACS+ protocol to authenticate management logins on the infrastructure devices to the authentication, authorization, and accounting (AAA) server.

As networks scale in the number of devices to maintain, the operational burden to maintain local user accounts on every device also scales. A centralized AAA service reduces operational tasks per device and provides an audit log of user access for security compliance and root-cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined in Step 11 on each network infrastructure device in order to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key [key]
```

```

!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa

```

**Step 13:** Configure a synchronized clock by programming network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. Configure console messages, logs, and debug output to provide time stamps on output, which allows cross-referencing of events in a network.

```

ntp server 10.4.48.17
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime

```

### Procedure 3 Apply the switch global configuration

Configure VLANs on the switch for all VLANs to which the server needs connectivity. Configure the switch management VLAN to match the CVD LAN foundation management VLAN in use at the location of this server room deployment.

**Step 1:** Configure the server and management VLANs.

```

vlan [VLAN number]
name Server_VLAN_1
vlan [VLAN number]
name Server_VLAN_2
vlan [VLAN number]
name Management

```

**Step 2:** Configure the switch with an IP address so that it can be managed via in-band connectivity, and then assign an IP default gateway.

```

interface vlan [management VLAN]
ip address [IP address] [mask]
no shutdown
ip default-gateway [default router]

```

**Step 3:** Configure bridge protocol data unit (BPDU) Guard globally. This protects PortFast-enabled interfaces by disabling the port if another switch is plugged into the port.

```

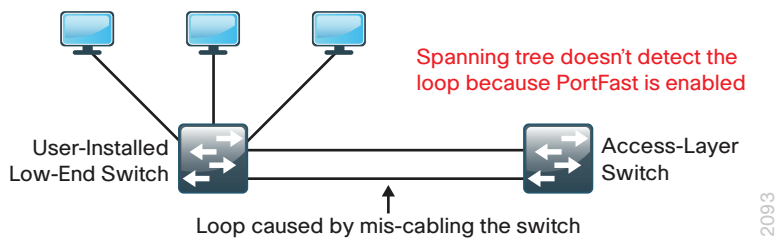
spanning-tree portfast bpduguard default

```

BPDU Guard protects against a user plugging a switch into an access port, which could cause a catastrophic undetected spanning-tree loop.

A PortFast-enabled interface receives a BPDU when an invalid configuration exists, such as when an unauthorized device is connected. The BPDU Guard feature prevents loops by moving a nontrunking interface into an errdisable state when a BPDU is received on an interface when PortFast is enabled.

Figure 5 - Scenario that BPDU Guard protects against



## Example

```

vlan 148
name Server_VLAN_1
vlan 149
name Server_VLAN_2
vlan 106
name Management
!
interface vlan 106
ip address 10.5.7.4 255.255.255.128
no shutdown
ip default-gateway 10.5.7.1

```

## Procedure 4 Configure server room uplink ports

This procedure details how to connect a server room switch to the distribution layer or collapsed LAN core.

Configure the physical interfaces that are members of a Layer 2 EtherChannel prior to configuring the logical port-channel interface. This sequence allows for minimal configuration because most of the commands entered to a port-channel interface are copied to its members' interfaces and do not require manual replication.

**Step 1:** Configure the EtherChannel member interfaces.

Set Link Aggregation Control Protocol (LACP) negotiation to **active** on both sides to ensure a proper EtherChannel is formed. Also, apply the egress QoS macro that was defined in Procedure 1, "Configure the platform," in order to ensure traffic is prioritized appropriately.

```

interface [interface type] [port 1]
description Link to Core port 1
interface [interface type] [port 2]
description Link to Core port 2
interface range [interface type] [port 1], [interface type] [port 2]
switchport
macro apply EgressQoS
channel-protocol lacp
channel-group [number] mode active

```



```

logging event link-status
logging event trunk-status
logging event bundle-status

```

**Step 2:** Configure the 802.1Q trunk.

An 802.1Q trunk is used for the connection to this upstream device, which allows the uplink to provide Layer 3 services to all the VLANs defined on the server room switch. Prune the VLANs allowed on the trunk to only the VLANs that are active on the server room switch. When using EtherChannel, the interface type is port-channel, and the number must match the channel-group configured in Step 1.

```

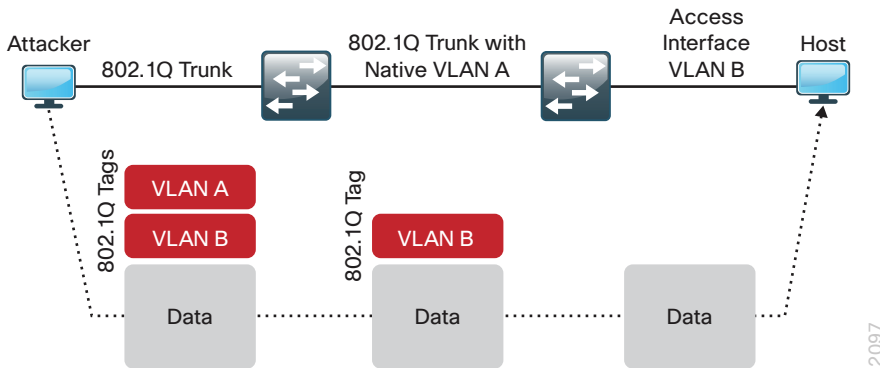
interface Port-channel [number]
  description EtherChannel Link to Core
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan [server VLAN 1], [server VLAN 2], [management VLAN]
  switchport mode trunk
  logging event link-status
  no shutdown

```

Next, mitigate the remote risk of a VLAN hopping attack on the trunk.

There is a remote possibility that an attacker can create a double 802.1Q encapsulated packet. If the attacker has specific knowledge of the 802.1Q native VLAN, a packet could be crafted that when processed, the first or outermost tag is removed when the packet is switched onto the untagged native VLAN. When the packet reaches the target switch, the inner or second tag is then processed and the potentially malicious packet is switched to the target VLAN.

Figure 6 - VLAN hopping attack



At first glance, this appears to be a serious risk. However, the traffic in this attack scenario is in a single direction, and no return traffic can be switched by this mechanism. Additionally, this attack cannot work unless the attacker knows the native VLAN ID.

**Step 3:** Configure an unused VLAN on the switch-to-switch 802.1Q trunk link from the server room to the distribution layer. Using a hard-to-guess, unused VLAN for the native VLAN reduces the possibility that a double 802.1Q-tagged packet can hop VLANs. If you are running the recommended EtherChannel uplink to the LAN access layer switch, configure the **switchport trunk native vlan** on the port-channel interface.

```

vlan 999
!
interface Port-channel [number]
  switchport trunk native vlan 999

```

## Example

```
interface TenGigabitEthernet1/1/3
  description Link to LAN Core 1
interface TenGigabitEthernet2/1/3
  description Link to LAN Core 2
interface range TenGigabitEthernet 1/1/3, TenGigabitEthernet 2/1/3
  channel-protocol lacp
  channel-group 20 mode active
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
!
interface Port-channel 20
  description EtherChannel Link to LAN Core
  switchport trunk allowed vlan 148-149,106
  switchport mode trunk
  logging event link-status
  no shutdown
!
vlan 999
!
interface Port-channel 20
  switchport trunk native vlan 999
```

### Procedure 5 Configure server access ports

To make configuration easier when the same configuration will be applied to multiple interfaces on the switch, use the **interface range** command. This command allows you to issue a command once and have it apply to many interfaces at the same time.

**Step 1:** Configure switch interfaces to offer basic server connectivity.

```
interface range [interface type] [port number]-[port number]
  switchport access vlan [server VLAN 1]
  switchport mode access
```

**Step 2:** Shorten the time it takes for a port to go into the forwarding state by setting the switchport to mode host.

```
switchport host
```

**Step 3:** If you want to trust the QoS markings on the traffic from the servers based on the QoS macro configuration, enter the following command.

```
macro apply EgressQoS
```



## Reader Tip

It is possible that your server or application may require special configuration like trunking or port channeling. Refer to vendor documentation for this information.

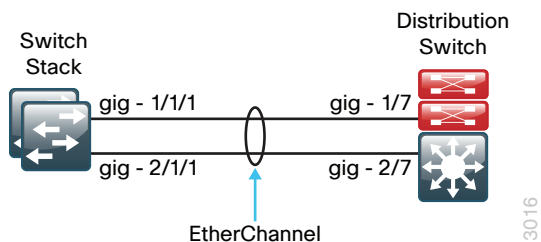
**Step 4:** Save the running configuration that you have entered. It will be used as the startup configuration file when your switch is rebooted or power-cycled.

```
copy running-config startup-config
```

## Procedure 6 Configure LAN distribution layer downlinks

The links to the server room switch are Layer 2 EtherChannels. Connect the server room EtherChannel uplinks to separate stack members or interface modules on the distribution layer switch.

Figure 7 - EtherChannel with stack member or switch blade diversity



**Step 1:** Add the VLANs to the core switch's VLAN database that the downlink will carry.

```

vlan [vlan number]
name Server_VLAN_1
vlan [vlan number]
name Server_VLAN_2

```

**Step 2:** Configure the EtherChannel member interfaces. Set LACP negotiation to **active** on both sides to ensure a proper EtherChannel is formed. Also, apply the egress QoS macro that is configured on the CVD LAN distribution layer in order to ensure traffic is prioritized appropriately.

```

interface [interface type] [port 1]
  description Link to Server Room port 1
interface [interface type] [port 2]
  description Link to Server Room 2
interface range [interface type] [port 1], [interface type] [port 2]
  switchport
  macro apply EgressQoS
  channel-protocol lacp
  channel-group [number] mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status

```

**Step 3:** Configure the trunk.

An 802.1Q trunk is used for the connection to the server room switch, which allows the uplink to provide Layer 3 services to all the VLANs defined in the server room. Prune the VLANs allowed on the trunk to only the VLANs that are active on the server room switch. When using EtherChannel, the interface type is port-channel, and the number must match the channel-group configured in Step 2.

```
interface Port-Channel [number]
  description EtherChannel Link to Server Room
  switchport trunk allowed vlan [server VLAN 1] , [server VLAN 2] , [mgmt VLAN]
  switchport mode trunk
  logging event link-status
  no shutdown
```

**Step 4:** Add VLAN-hopping mitigation for the trunk.

```
interface Port-channel [number]
  switchport trunk native vlan 999
```

**Step 5:** If the VLANs for the server room did not already exist on the core switch, add a switched virtual interface (SVI) for every server room VLAN so that the VLANs can route to the rest of the network.

If you are using DHCP to assign IP addresses for servers in the server room, use the **ip helper-address** command to allow remote DHCP servers to provide IP addresses for this network. The address to which the helper command points is the DHCP server; if you have more than one DHCP server, multiple helper commands can be listed on an interface.

```
interface vlan [number]
  ip address [IP address] [mask]
  ip helper-address [DHCP server IP address]
  ip pim sparse-mode
  no shutdown
```

### Example

```
vlan 148
name Server_VLAN_1
vlan 149
name Server_VLAN_2
!
interface TenGigabitEthernet1/1/5
  description Link to Server Room port 1
interface TenGigabitEthernet2/1/5
  description Link to Server Room port 2
interface range TenGigabitEthernet 1/1/5, TenGigabitEthernet 2/1/5
  channel-protocol lacp
  channel-group 20 mode active
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
!
```

```
interface Port-channel 20
  description EtherChannel Link to Server Room
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 148-149,106
  switchport mode trunk
  logging event link-status
  no shutdown
!
interface Port-channel 20
  switchport trunk native vlan 999
!
interface vlan 148
  ip address 10.5.24.1 255.255.255.0
  ip pim sparse-mode
  no shutdown
interface vlan 149
  ip address 10.5.25.1 255.255.255.0
  ip pim sparse-mode
  no shutdown
```

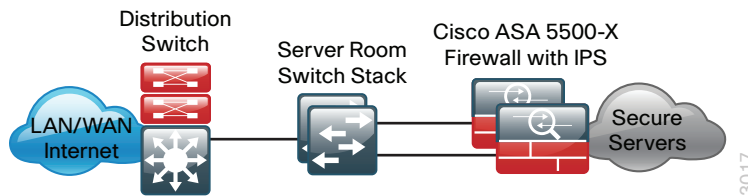


# Server Room Security

## Design Overview

To minimize the impact of unwanted network intrusions, you should deploy firewalls and intrusion prevention systems (IPSs) between clients and centralized data resources.

Figure 8 - Deploy firewall inline to help protect data resources



Because everything else outside the protected VLANs hosting the server room resources can be a threat, the security policy associated with protecting those resources has to include the following potential threat vectors (the data center threat landscape):

- Internet
- Remote access and teleworker VPN hosts
- Remote office and branch networks
- Business partner connections
- Campus networks
- Unprotected server room networks
- Other protected server room networks

The server room security design employs a pair of Cisco ASA 5500-X Series Midrange Security Appliances. Cisco ASA 5500-X is a next-generation security appliance that provides a context-aware approach to security. Cisco ASA 5500-X is available in multiple models to scale from 1 Gbps to 4 Gbps of firewall throughput, and 250 Mbps to 1.3 Gbps of firewall + IPS throughput.

Each of the Cisco ASA firewalls are homed to one of the server room Cisco Catalyst switches using two 1-Gigabit Ethernet links. The first 1-Gigabit Ethernet link on each Cisco ASA is configured to carry traffic from the CVD LAN distribution layer. This link is designated as the outside VLAN for the firewall, and any hosts or servers that reside in that VLAN are outside the firewall and therefore receive no protection from Cisco ASA for attacks originating from anywhere else in the organization's network. The second 1-Gigabit Ethernet link on each Cisco ASA is configured as a VLAN trunk to transport server room VLANs designated as being firewalled from all the other server room threat vectors or firewalled with additional IPS services.

The pair of Cisco ASAs is configured for firewall active/standby high availability operation to ensure that access to the server room is only minimally impacted by outages caused by software maintenance or hardware failure. When Cisco ASAs are configured in active/standby mode, the standby appliance does not handle traffic, so the ASAs must be sized so that either appliance can provide enough throughput to address connectivity requirements between the LAN and the server room. Although the IPS modules do not actively exchange state traffic, they participate in the firewall appliances' active/standby status by way of reporting their status to the firewall's status monitor. A firewall failover will occur if either the appliance itself has an issue or the IPS module becomes unavailable.

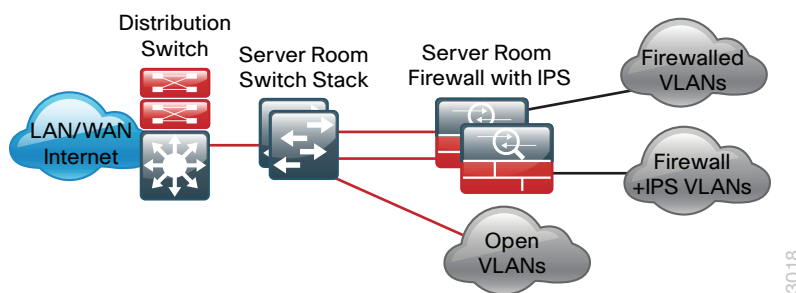
Cisco ASAs are configured in routing mode; as a result, the secure network must be in a separate subnet from the client subnets. IP subnet allocation would be simplified if the appliance were deployed in transparent mode; however, hosts might inadvertently be connected to the wrong VLAN, where they would still be able to communicate with the network, incurring an unwanted security exposure.

The server room IPS monitors for and mitigates potential malicious activity that is contained within traffic allowed by the security policy defined on Cisco ASA. The IPS sensors can be deployed in promiscuous, or *IDS*, mode so that they only monitor and alert for abnormal traffic. The IPS sensors can be deployed in inline, or *IPS*, mode in order to fully engage their intrusion prevention capabilities, wherein they will block malicious traffic before it reaches its destination. The choice to have the sensor drop traffic or not is one that is influenced by several factors: risk tolerance for having a security incident, risk aversion for inadvertently dropping valid traffic, and other possibly externally driven reasons such as compliance requirements for IPS. The ability to run in IDS or IPS mode is highly configurable to allow the maximum flexibility in meeting a specific security policy.

## Security Topology Design

The CVD server room security design provides two secure VLANs for application servers. The number of secure VLANs is arbitrary; the design is an example of how to create multiple secured networks to host services that require separation. High-value applications, such as Enterprise Resource Planning and Customer Relationship Management, may need to be separated from other applications in their own VLAN.

Figure 9 - Example design with secure VLANs



As another example, services that are indirectly exposed to the Internet (via a web server or other application servers in the Internet demilitarized zone) should be separated from other services, if possible, to prevent Internet-borne compromise of some servers from spreading to other services that are not exposed. Traffic between VLANs should be kept to a minimum, unless your security policy dictates service separation. Keeping traffic between servers intra-VLAN will improve performance and reduce the load on network devices.

For this deployment, devices that need an access policy will be deployed on a VLAN behind the firewalls. Devices that require both an access policy and IPS traffic inspection will be deployed on a different VLAN that exists logically behind Cisco ASAs. Because the Cisco ASAs are physically attached only to the server room switches, these protected VLANs will also exist at Layer 2 on the server room switches. All protected VLANs are logically connected via Layer 3 to the rest of the network through Cisco ASA and, therefore, are reachable only by traversing Cisco ASA.

## Security Policy Development

An organization should have an IT security policy as a starting point in defining its firewall policy. If there is no organization-wide security policy, it will be very difficult to define an effective policy for the organization while maintaining a secure computing environment.

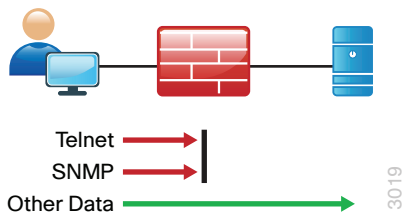


### Reader Tip

A detailed examination of regulatory compliance considerations exceeds the scope of this document. You should include industry regulation in your network security design. Noncompliance may result in regulatory penalties such as fines or suspension of business activity.

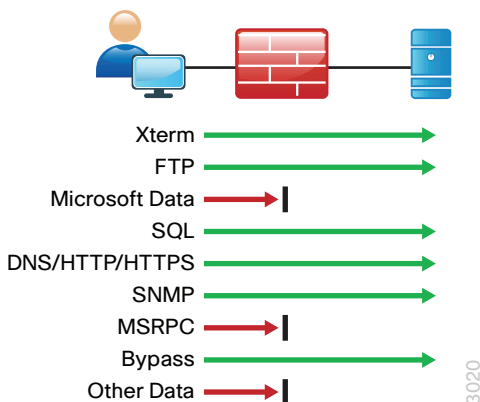
Network security policies can be broken down into two basic categories: whitelist policies and blacklist policies. A *blacklist policy* denies traffic that specifically poses the greatest risk to network resources.

Figure 10 - Blacklist security policy



Inversely, a *whitelist policy* offers a higher implicit security posture, blocking all traffic except that which must be allowed (at a sufficiently granular level) to enable applications. Other traffic is blocked and does not need to be monitored to ensure that unwanted activity is not occurring; this reduces the volume of data that will be forwarded to an IDS or IPS and minimizes the number of log entries that must be reviewed in the event of an intrusion or data loss.

Figure 11 - Whitelist security policy



Whitelist policies can be identified by the last rule of the policy rule-set: whitelist policies always end with a rule to deny any traffic that has not been denied or allowed by previous rules. Cisco ASA firewalls implicitly add a deny-all rule at the end of an access list. Blacklist policies include an explicit rule, prior to the implicit deny-all rule, to allow any traffic that is not explicitly allowed or denied.

A blacklist policy is simpler to maintain and less likely to interfere with network applications. A whitelist policy is the best-practice option if you have the opportunity to examine the network's requirements and adjust the policy to avoid interfering with desired network activity. Whitelist policies are generally better positioned to meet regulatory requirements because only traffic that must be allowed in order to conduct business is allowed.

Whether you choose a whitelist or blacklist policy basis, IDS or IPS can monitor malicious activity on otherwise trustworthy application traffic. At a minimum, IDS or IPS can aid with forensics to determine the origin of a data breach. IPS can detect and prevent known attacks as they occur and provide detailed information to track the malicious activity to its source. IDS or IPS may also be required by the regulatory oversight to which a network is subject (for example, PCI 2.0).

A blacklist policy that blocks high-risk traffic offers a lower-impact, less-secure option (as compared to a whitelist policy) in cases where either:

- A detailed study of the network's application activity is impractical.
- The network availability requirements prohibit application troubleshooting.

If identifying all of the application requirements is not practical, an organization can apply a blacklist policy with logging enabled to develop a detailed study of the policy. With details about its network's behavior in hand, an organization can more easily develop an effective whitelist policy.

## Deployment Details

For deployment in the server room, Cisco ASA 5500-X firewall with IPS will be deployed to enforce the security policy between the network core and the application server network, and between the different application server networks.

Cisco ASA is set up as a highly available active/standby pair. Active/standby:

- Is much simpler than an active/active configuration.
- Allows the use of the same appliance for firewall and VPN (VPN functionality is disabled when Cisco ASA is configured as active/active).

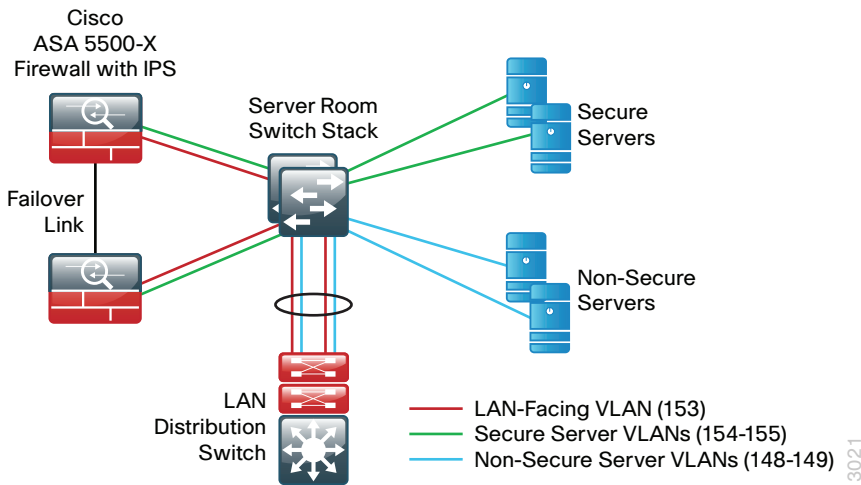
The performance needs in this design do not surpass the performance of a single appliance.

In the event that the active appliance fails or needs to be taken out of service for maintenance, the secondary appliance will take over all firewall and IPS functions.

Cisco ASA is statically routed to the CVD LAN distribution on the outside interface in order to simplify the routing configuration. A second interface is trunked to the server room switch with a VLAN interface for each application server network.

This design applies the following topology for Cisco ASA firewall connectivity.

Figure 12 - Cisco ASA connectivity for the server room



PROCESS

## Configuring Firewall Connectivity for the Server Room

1. Configure the LAN distribution layer
2. Configure the server room switch

Complete each of the following procedures in order to configure a resilient pair of Cisco ASA 5500-X for the server room. The Cisco ASA's network ports are connected as follows:

- GigabitEthernet 0/0 connects to a VLAN trunk port offering connectivity to secure server-room LANs
- GigabitEthernet 0/2 connects via a crossover or straight-through Ethernet cable to the other Cisco ASA for the failover link
- GigabitEthernet 0/3 connects to an access port on the server room switch for the outside or untrusted-VLAN

Connect all of the ports for each firewall to a different switch in the Cisco Catalyst 3750-X Series switch stack for resilience.

As described earlier in the Server Room Ethernet LAN Deployment Details, because the server room can be deployed at the main site or a remote site, this guide contains two models for IP addressing. This guide will use the remote-site addressing. Your design requirements for IP addressing and VLAN numbering may differ.

Table 4 - Server room firewall IP addressing for main-site deployment

VLAN	IP address	Trust state	Use
153	10.4.53.1 /25	Untrusted	Firewall to core LAN routing
154	10.4.54.X /24	Trusted	Firewall-protected VLAN
155	10.4.55.X /24	Trusted	Firewall and IPS-protected VLAN



Table 5 - Server room firewall IP addressing for remote-site deployment

VLAN	IP address	Trust state	Use
153	10.5.26.1 /25	Untrusted	Firewall to core LAN routing
154	10.5.27.X /24	Trusted	Firewall-protected VLAN
155	10.5.28.X /24	Trusted	Firewall and IPS-protected VLAN

Table 6 - Common network services used in the deployment examples

Service	Address
Domain name	cisco.local
Active Directory, DNS, DHCP server	10.4.48.10
Cisco Secure ACS	10.4.48.15
NTP server	10.4.48.17

## Procedure 1 Configure the LAN distribution layer

Configure the LAN distribution layer or collapsed core switch that will provide Layer 3 routing for the server room Cisco ASAs' LAN-side (untrusted) interfaces and to forward traffic destined to trusted subnets to the firewall.

**Step 1:** Define the outside (untrusted) VLAN.

```
vlan 153
name FirewallOutsideVLAN
```

**Step 2:** Configure the Layer 3 SVI.

```
interface Vlan 153
description SR Firewall Outside SVI
ip address 10.5.26.1 255.255.255.128
no shutdown
```

**Step 3:** Configure the EtherChannel trunk to the server room switch to carry the outside VLAN. This design adds the VLAN to the EtherChannel link that connects the LAN distribution-layer switch to the server-room switch, configured in Procedure 6, "Configure LAN distribution layer downlinks."

```
interface Port-channel 20
switchport trunk allowed vlan add 153
```

**Step 4:** Configure static routes pointing to the trusted subnets behind the Cisco ASA firewalls.

```
ip route 10.5.27.0 255.255.255.0 Vlan 153 10.5.26.126
ip route 10.5.28.0 255.255.255.0 Vlan 153 10.5.26.126
```

**Step 5:** Redistribute the trusted subnets into the existing Enhanced Interior Gateway Routing Protocol (EIGRP) routing process. This design uses route maps in order to control which static routes are redistributed.

```
ip access-list standard trusted_subnets
permit 10.5.27.0 0.0.0.255
permit 10.5.28.0 0.0.0.255
```

```

!
route-map static-to-eigrp permit 10
  match ip address trusted_subnets
  set metric 1000000 10 255 1 1500
!
router eigrp LAN
  address-family ipv4 unicast autonomous-system 100
  topology base
  redistribute static route-map static-to-eigrp

```

## Procedure 2 Configure the server room switch

This procedure will create all VLANs required for the server room firewall deployment, configure the trunk to the LAN distribution layer to carry the outside VLAN, configure the outside (untrusted) VLAN ports for connectivity to the Cisco ASA firewalls, and configure the inside (trusted) VLAN trunk to connect to the ASA firewalls.

For resilience, you configure all of the ports for each firewall to a different switch in the Cisco Catalyst 3750-X Series switch stack.

**Step 1:** Configure the untrusted and trusted VLANs.

```

vlan 153
  name FirewallOutsideVLAN
vlan 154
  name FirewallSecVLAN
vlan 155
  name FirewallIPSSecVLAN

```

**Step 2:** Configure the server-room switch EtherChannel trunk to the LAN distribution-layer switch so that it carries the outside VLAN. This design adds the VLAN to the EtherChannel trunk between the server room switch and LAN distribution-layer switch, configured in Procedure 4, “Configure server room uplink ports.”

```

interface Port-channel 20
  switchport trunk allowed vlan add 153

```

**Step 3:** If the existing switch ports are set up with a server room client edge port configuration, use the **default interface** command prior to setting up the ports for connection to Cisco ASAs. This clears any existing configuration on the port.

```

default interface GigabitEthernet [slot/port]

```

**Step 4:** Configure a pair of Ethernet ports on the server room switch to connect to the Cisco ASAs’ LAN-side (untrusted) interfaces. The first or primary appliance will be on switch 1, and the secondary appliance will be on switch 2 of the Catalyst 3850 Series switch stack.

```

interface GigabitEthernet1/0/47
  description SR-ASA5500a outside gi 0/3
!
interface GigabitEthernet2/0/47
  description SR-ASA5500b outside gi 0/3
!
interface range GigabitEthernet1/0/47,GigabitEthernet2/0/47

```

```
switchport
switchport access vlan 153
switchport mode access
spanning-tree portfast
macro apply EgressQoS
```

In this configuration, multiple VLAN subinterfaces are trunked from the Cisco ASA units' GigabitEthernet 0/0 inside interfaces to the server room switches. VLANs 154 and 155 provide connections for two different application server networks, with different security policy requirements for each.

**Step 5:** Configure the server room switch to be the spanning-tree root for the inside (trusted) VLANs. Because the VLANs do not trunk to the LAN distribution layer, the server room switch will be the spanning-tree root.

```
spanning-tree vlan 154-155 root primary
```

**Step 6:** Configure server room switch interfaces to connect to the inside interfaces of the Cisco ASA server room firewall.

```
interface GigabitEthernet1/0/48
  description SR-ASA5500a inside gi 0/0
!
interface GigabitEthernet2/0/48
  description SR-ASA5500b inside gi 0/0
!
interface range GigabitEthernet1/0/48,GigabitEthernet2/0/48
  switchportswitchport trunk allowed vlan 154-155
  switchport mode trunk
  spanning-tree portfast trunk
  macro apply EgressQoS
```

## Configuring the Server Room Firewall

1. Apply Cisco ASA initial configuration
2. Configure the firewall outside port
3. Configure user authentication
4. Configure time synchronization and logging
5. Configure device management protocols
6. Configure the Cisco ASAs' inside interfaces
7. Configure the firewall static route
8. Disable proxy ARP

Configuration for this process is applied using CLI through the console port on the Cisco ASA firewall that is the primary unit of the high-availability pair. The standby unit synchronizes the configuration from the primary unit when it is programmed in the next process, "Configuring Firewall High Availability."

The factory default password for enable mode is <CR>.

Table 7 - Cisco ASA 5500X firewall and IPS module IP addressing

Cisco ASA firewall failover assignment	ASA firewall IP address	IPS module management interface IP address
Primary	10.5.26.126 /25	10.5.7.21 /25
Secondary	10.5.26.125 /25	10.5.7.22 /25

### Procedure 1 Apply Cisco ASA initial configuration

Initial configuration is applied using the CLI on the primary Cisco ASA (of the high-availability pair) only.

**Step 1:** In response to the prompt, "Pre-configure Firewall now through interactive prompts," answer **no**. This prompt appears on new Cisco ASAs that have never been configured.

```
Pre-configure Firewall now through interactive prompts [yes]? no
```

**Step 2:** Enter configuration mode.

```
configure terminal
```

**Step 3:** You are given a choice to enable anonymous reporting of error and health information to Cisco. Select the choice appropriate for your organization's security policy.

```
***** NOTICE *****
Help to improve the ASA platform by enabling anonymous reporting, which allows
Cisco to securely receive minimal error and health information from the device.
To learn more about this feature, please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help improve the product?
[Y]es, [N]o, [A]sk later:N
```

**Step 4:** Configure the host name for Cisco ASA.

```
hostname SR-ASA5500X
```

**Step 5:** Enable the dedicated management interface, and then remove any IP address for use as the IPS management port.

```
interface Management0/0
  nameif IPS-mgmt
  no ip address
  no shutdown
```

**Step 6:** Configure an administrative username and password.

```
username admin password [password] privilege 15
```

### Tech Tip

All passwords in this document are examples and should not be used in production configurations. Follow your company's policy, or—if no policy exists—create a password using a minimum of eight characters with a combination of uppercase, lowercase, and numbers.

## **Procedure 2** Configure the firewall outside port

Next, you configure the firewall so that the interfaces connected to the server room switch are the untrusted side of the firewall connected to the server room switch ports that have been configured for the outside VLAN.

**Step 1:** Configure Ethernet 0/3 as the outside interface connected to the server room switch outside interfaces. The default outside security-level setting, 0, is applied automatically.

```
interface GigabitEthernet0/3
  nameif outside
  ip address 10.5.26.126 255.255.255.128 standby 10.5.26.125
  no shutdown
```

All Cisco ASA interfaces have a security-level setting. The higher the number, the more secure the interface. Inside interfaces are typically assigned 100, the highest security level. Outside interfaces are always assigned 0.

By default, traffic can pass from a high-security interface to a lower-security interface. In other words, traffic from an inside network is permitted to an outside network, but not conversely.

### Tech Tip

The interfaces have a standby IP address in addition to the main IP address. This is part of the firewall failover configuration that is used to determine whether the interface is connected and available to the network. Interfaces that will not be monitored do not need a standby address.

### Procedure 3 Configure user authentication

#### (Optional)

If you want to reduce operational tasks per device, configure centralized user authentication by using the TACACS+ protocol to authenticate management logins on the infrastructure devices to the AAA server.

As networks scale in the number of devices to maintain, the operational burden to maintain local user accounts on every device also scales. A centralized AAA service reduces operational tasks per device and provides an audit log of user access for security compliance and root-cause analysis. When AAA is enabled for access control, it controls all management access to the network infrastructure devices (SSH and HTTPS).

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database was defined already in order to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

**Step 1:** Configure the TACACS+ server.

```
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (outside) host 10.4.48.15 [key]
```

**Step 2:** Configure the appliance's management authentication to use the TACACS+ server first and then use the local user database if the TACACS+ server is unavailable.

```
aaa authentication enable console AAA-SERVER LOCAL
aaa authentication ssh console AAA-SERVER LOCAL
aaa authentication http console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
```

**Step 3:** Configure the appliance to use AAA to authorize management users.

```
aaa authorization exec authentication-server
```



#### Tech Tip

User authorization on the Cisco ASA firewall (unlike Cisco IOS devices) does not automatically present the user with the enable prompt if they have a privilege level of 15.

### Procedure 4 Configure time synchronization and logging

Logging and monitoring are critical aspects of network security devices to support troubleshooting and policy-compliance auditing.

The Network Time Protocol (NTP) is designed to synchronize time across a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organization's network.

Network devices should be programmed to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source.

There is a range of detail that can be logged on the appliance. Informational-level logging provides the ideal balance between detail and log-message volume. Lower log levels produce fewer messages, but they do not produce enough detail to effectively audit network activity. Higher log levels produce a larger volume of messages, but they do not add sufficient value to justify the number of messages logged.

**Step 1:** Configure the NTP server IP address.

```
ntp server 10.4.48.17
```

**Step 2:** Configure the time zone.

```
clock timezone PST -8 0
clock summer-time PDT recurring
```

**Step 3:** Configure which logs to store on the appliance.

```
logging enable
logging buffered informational
```

## Procedure 5 Configure device management protocols

Cisco Adaptive Security Device Manager (Cisco ASDM) requires that the appliance's HTTPS server be available. Be sure that the configuration includes networks where administrative staff has access to the device through Cisco ASDM; the appliance can offer controlled Cisco ASDM access for a single address or management subnet (in this case, 10.4.48.0/24).

HTTPS and SSH are more secure replacements for the HTTP and Telnet protocols. They use SSL and TLS to provide device authentication and data encryption.

Use SSH and HTTPS protocols in order to more securely manage the device. Both protocols are encrypted for privacy, and the insecure protocols (Telnet and HTTP) are turned off.

SNMP is enabled to allow the network infrastructure devices to be managed by a network management system (NMS). SNMPv2c is configured for a read-only community string.

**Step 1:** Allow internal administrators to remotely manage the appliance over HTTPS and SSH.

```
domain-name cisco.local
http server enable
http 10.4.48.0 255.255.255.0 outside
ssh 10.4.48.0 255.255.255.0 outside
ssh version 2
```

**Step 2:** Specify the list of supported SSL encryption algorithms for Cisco ASDM.

```
ssl encryption aes256-sha1 aes128-sha1 3des-sha1
```

**Step 3:** Configure the appliance to allow SNMP polling from the NMS.

```
snmp-server host outside 10.4.48.35 community [SNMP RO string]
snmp-server community [SNMP RO string]
```

## Procedure 6 Configure the Cisco ASAs' inside interfaces

A pair of Ethernet VLAN trunks is used to connect the Cisco ASAs' inside interfaces to the server room switch ports configured for the inside VLANs in Step 6 of Procedure 2, "Configure the server room switch." VLAN trunks allow flexibility to offer connectivity for multiple trusted VLANs, as needed. The firewalls carry two inside subinterfaces, VLAN 154 and VLAN 155, on the interface.

**Step 1:** Clear any name, security-level, and IP address settings, and then enable the interface.

```
interface GigabitEthernet0/0
  no nameif
  no security-level
  no ip address
  no shutdown
```

**Step 2:** Configure the firewalls' inside subinterfaces for connectivity to the trusted VLANs on the LAN core switch.

```
interface GigabitEthernet0/0.154
  vlan 154
  nameif SRVLAN154
  security-level 100
  ip address 10.5.27.1 255.255.255.0 standby 10.5.27.2
!
interface GigabitEthernet0/0.155
  vlan 155
  nameif SRVLAN155
  security-level 100
  ip address 10.5.28.1 255.255.255.0 standby 10.5.28.2
```

## Procedure 7 Configure the firewall static route

The server room Cisco ASA unit will be the default router for the internal application server networks and will statically route to the core network on the outside interface for networks outside of the server room.

**Step 1:** On the Cisco ASA, configure a static route pointing to the VLAN 153 SVI address of the LAN distribution layer, configured in Step 2 of Procedure 1, "Configure the LAN distribution layer."

```
route outside 0.0.0.0 0.0.0.0 10.5.26.1 1
```

## Procedure 8 Disable proxy ARP

**Step 1:** Proxy ARP is enabled by default on the ASA appliance. Because proxy ARP is not in use in this design, it is disabled as a best practice.

**Step 2:** Disable proxy ARP on all interfaces.

```
sysopt noproxyarp SRVLAN154
sysopt noproxyarp SRVLAN155
sysopt noproxyarp outside
```



## Configuring Firewall High Availability

1. Configure HA on the primary appliance
2. Configure HA on the secondary appliance

Cisco ASAs are set up as a highly available active/standby pair. Active/standby is used, rather than an active/active configuration, because this allows the same appliance to be used for firewall and VPN services if required in the future (VPN functionality is disabled on the appliance in active/active configuration). In the event that the active appliance fails or needs to be taken out of service for maintenance, the secondary appliance assumes all active firewall and IPS functions. In an active/standby configuration, only one device is passing traffic at a time; thus, Cisco ASAs must be sized so that the entire traffic load can be handled by either device in the pair.

Both units in the failover pair must be the same model, with identical feature licenses and IPS modules (if the software module is installed). For failover to be enabled, the secondary Cisco ASA unit needs to be powered up and cabled to the same networks as the primary unit.

One interface on each Cisco ASA is configured as the state-synchronization interface, which the appliances use to share configuration updates, determine which device in the high-availability pair is active, and exchange state information for active connections. The failover interface carries the state synchronization information. All session state data is replicated from the active to the standby unit through this interface. There can be a substantial amount of data, and it is recommended that this be a dedicated interface.

By default, the appliance can take from 2 to 25 seconds to recover from a failure. Tuning the failover poll times can reduce that to 0.5 to 5 seconds. On an appropriately sized Cisco ASA unit, the poll times can be tuned down without performance impact to the appliance, which minimizes the downtime a user experiences during failover. It is recommended that you do not reduce the failover timer intervals below the values in this guide.

### Procedure 1 Configure HA on the primary appliance

**Step 1:** Enable failover on the primary Cisco ASA unit, and then assign it as the primary unit.

```
failover
failover lan unit primary
```

**Step 2:** Configure the failover interface.

```
failover lan interface failover GigabitEthernet0/2
failover replication http
failover key [key]
failover link failover GigabitEthernet0/2
```

**Step 3:** If you want to speed up failover in the event of a device or link failure, tune the failover timers. With the default setting, depending on the failure, Cisco ASA can take from 2 to 25 seconds to fail over to the standby unit. Tuning the failover poll times can reduce that to 0.5 to 5 seconds, depending on the failure.

```
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
```

**Step 4:** Configure the failover interface IP address.

```
failover interface ip failover 10.5.26.130 255.255.255.252 standby 10.5.26.129
```

**Step 5:** Enable the failover interface.

```
interface GigabitEthernet0/2
  no shutdown
```

**Step 6:** Configure failover to monitor the outside interface.

```
monitor-interface outside
```

**Step 7:** Configure failover to monitor the inside interfaces.

```
monitor-interface SRVLAN154
monitor-interface SRVLAN155
```

## Procedure 2 Configure HA on the secondary appliance

**Step 1:** On the secondary Cisco ASA unit, enable failover, and then assign it as the secondary unit.

```
failover
failover lan unit secondary
```

**Step 2:** Configure the failover interface.

```
failover lan interface failover GigabitEthernet0/2
failover replication http
failover key [key]
failover link failover GigabitEthernet0/2
```

**Step 3:** Configure the failover interface IP address.

```
failover interface ip failover 10.5.26.130 255.255.255.252 standby 10.5.26.129
```

**Step 4:** Enable the failover interface. The Cisco ASA units synchronize their configuration from the primary unit to the secondary.

```
interface GigabitEthernet0/2
  no shutdown
```

**Step 5:** Verify standby synchronization between the Cisco ASA units. On the primary appliance, in the command-line interface, issue the **show failover state** command.

```
SR-ASA5500X# show failover state
```

	State	Last Failure Reason	Date/Time
This host -	Primary		
	Active	None	
Other host -	Secondary		
	Standby Ready	None	

```
====Configuration State====
```

```
Sync Done
```

```
====Communication State====
```

```
Mac set
```

**Step 6:** On the primary appliance, save your Cisco ASA firewall configuration. This will save the configuration on the primary and secondary ASA firewalls.

```
copy running-config startup-config
```

## PROCESS

### Evaluating and Deploying Firewall Security Policy

1. Evaluate security policy requirements
2. Define policy objects
3. Deploy the appropriate security policy

This process describes the steps required to evaluate which type of policy fits an organization's security requirements for a server room, and the procedures apply these policies.

#### Procedure 1 Evaluate security policy requirements

**Step 1:** Evaluate security policy requirements by answering the following questions:

- What applications will be served from the secure server room?
- Can the applications' traffic be characterized at the protocol level?
- Is a detailed description of application behavior available to facilitate troubleshooting if the security policy interferes with the application?
- What is the network's baseline performance expectation between the controlled and uncontrolled portions of the network?
- What is the peak level of throughput that security controls will be expected to handle, including bandwidth-intensive activity such as workstation backups or data transfers to a secondary data replication site?

**Step 2:** For each server room VLAN, determine which security policy enables application requirements. Each firewall VLAN requires either a permissive (blacklist) or restrictive (whitelist) security policy.

#### Procedure 2 Define policy objects

Network security policy configuration can vary greatly among organizations and is dependent on the policy and management requirements of the organization. Thus, examples here should be used as a basis for security policy configuration.

After the system setup and high availability is complete via CLI, you will use the integrated GUI management tool, Cisco ASDM, to program the following security policies:

- Network objects such as hosts and IP subnets
- Firewall access rules

First, to simplify the configuration of the security policy, you create the network objects that are used in the firewall policies.

Table 8 - Firewall network objects

Network object name	Object type	IP address	Description
IT_Web_Server	Host	10.5.27.80	IT Dept server
Finance_Web_Server	Host	10.5.27.81	Finance Dept server
HR_Web_Server	Host	10.5.28.80	HR Dept server
Research_Web_Server	Host	10.5.28.81	Research Dept server
IT_Management_Host_Range	Network	10.4.48.224–254	IT Management Systems

**Step 1:** Using a secure HTTP session (Example: <https://10.5.26.126>), navigate to the Cisco ASA firewall outside interface programmed in Procedure 2 “Configure the firewall outside port,” and then click **Run ASDM**. Cisco ASDM starts from a Java Web Start application.

**Step 2:** Enter the username and password configured for the Cisco ASA firewall in Step 6 of Procedure 1, “Apply Cisco ASA initial configuration.”

**Step 3:** In the Cisco ASDM work pane, navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

**Step 4:** Repeat Step 5 through Step 10 for each object listed in Table 8. If an object already exists, then skip to the next object listed in the table.

**Step 5:** Click **Add > Network Object**.

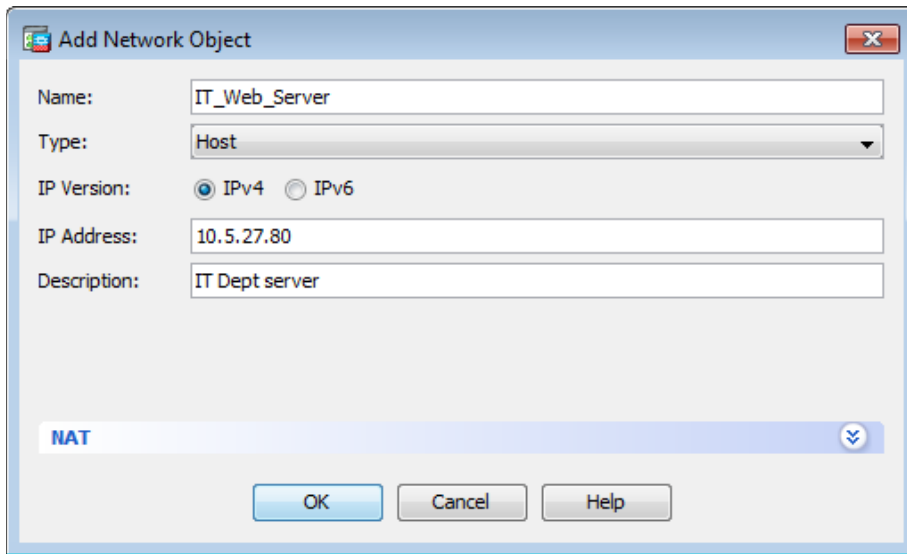
**Step 6:** The Add Network Object dialog box appears.

**Step 7:** In the **Name** box, enter the name. (Example: IT\_Web\_Server)

**Step 8:** In the **Type** list, choose the object type. (Example: Host).

**Step 9:** In the **IP Address** box, enter the address. (Example: 10.5.27.80)

**Step 10:** In the **Description** box, enter a useful description, and then click **OK**. (Example: IT Dept server)



The screenshot shows a dialog box titled "Add Network Object". It has a close button in the top right corner. The fields are as follows:

- Name: IT\_Web\_Server
- Type: Host
- IP Version: IPv4 (selected), IPv6
- IP Address: 10.5.27.80
- Description: IT Dept server

At the bottom, there is a "NAT" section with a dropdown arrow and three buttons: "OK", "Cancel", and "Help".

**Step 11:** After adding all of the objects listed in Table 8, on the Network Objects/Groups pane, click **Apply**.

Next, specify which resources certain users (for example, IT management staff or network users) can use to access management resources. In this example, management hosts in the IP address range 10.4.48.224–254 are allowed SSH and SNMP access to server room subnets.

**Step 12:** Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

**Step 13:** Click **Add > Network Object**.

**Step 14:** The Add Access Rule dialog box appears.

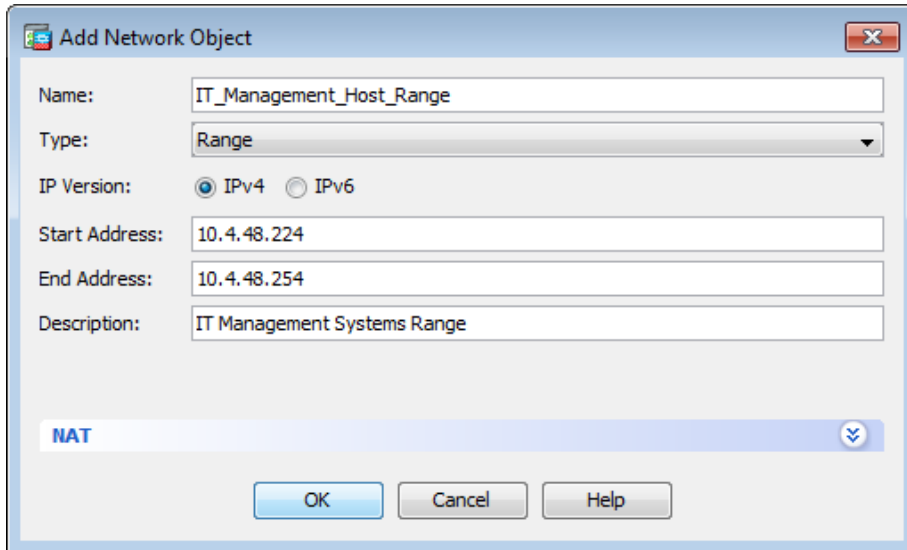
**Step 15:** In the **Name** box, enter the name. (Example: IT\_Management\_Host\_Range)

**Step 16:** In the **Type** list, choose **Range**.

**Step 17:** In the **Start Address** box, enter the first address in the range. (Example: 10.4.48.224)

**Step 18:** In the **End Address** box, enter the last address in the range. (Example: 10.4.48.254)

**Step 19:** In the **Description** box, enter a useful description, and then click **OK**. (Example: IT Management Systems Range)



The screenshot shows a dialog box titled "Add Network Object". It contains the following fields and controls:

- Name:** IT\_Management\_Host\_Range
- Type:** Range
- IP Version:** IPv4 (selected), IPv6
- Start Address:** 10.4.48.224
- End Address:** 10.4.48.254
- Description:** IT Management Systems Range
- NAT:** A section with a dropdown arrow.
- Buttons:** OK, Cancel, Help

Next you will create a service group containing SSH and SNMP protocols, and you create an access list to permit the SSH and SNMP traffic service group from the network management range to the server subnets.

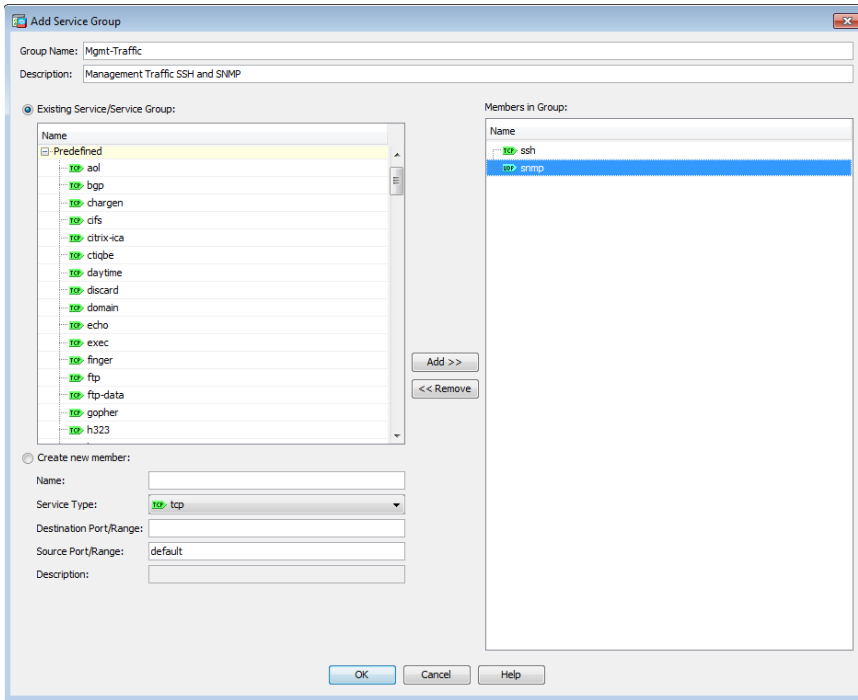
**Step 20:** Navigate to **Configuration > Firewall > Objects > Service Objects/Groups**.

**Step 21:** Click **Add > Service Group**.

**Step 22:** In the **Group Name** box, enter the name. (Example: Mgmt-Traffic)

**Step 23:** In the **Description** box, enter a useful description. (Example: Management Traffic SSH and SNMP)

**Step 24:** In the Existing Service/Service Group list, choose **tcp > ssh** and **udp > snmp**, click **Add**, and then click **OK**.



### Procedure 3 Deploy the appropriate security policy

If you are deploying a whitelist security policy, complete Option 1 of this procedure. If you are deploying a blacklist security policy, complete Option 2 of this procedure.

#### Option 1: Deploy a whitelist security policy

To allow common business services such as HTTP and HTTPS access to your servers, you can apply a basic whitelist data-service policy.

**Step 1:** Navigate to **Configuration > Firewall > Access Rules**.

Table 9 - Sample whitelist firewall policy rules

Interface	Action	Source	Destination	Service	Description	Logging Enable / Level
Any	Permit	any4	IT_Web_Server	tcp/http, tcp/https	Inbound web to IT Dept Server	Selected / Default
Any	Permit	any4	Finance_Web_Server	tcp/http, tcp/https	Inbound web to Finance Dept Server	Selected / Default
Any	Permit	any4	HR_Web_Server	tcp/http, tcp/https	Inbound web to HR Dept Server	Selected / Default
Any	Permit	any4	Research_Web_Server	tcp/http, tcp/https	Inbound web to Research Dept Server	Selected / Default
Outside	Permit	IT_Management_Host_Range	SRVLAN154-network, SRVLAN155-network	tcp/ssh, udp/snmp	Management access to servers	Selected / Default

**Step 2:** Repeat Step 3 through Step 11 for all rules listed in Table 9.

**Step 3:** Click **Add > Add Access Rule**.

The Add Access Rule dialog box appears.

**Step 4:** In the **Interface** list, choose the interface. (Example: Any)

**Step 5:** For the **Action** option, select the action. (Example: Permit)

**Step 6:** In the **Source** box, choose the source. (Example: any4)

**Step 7:** In the **Destination** box, choose the destination. (Example: IT\_Web\_Server)

**Step 8:** In the **Service** box, enter the service. (Example: tcp/http, tcp/https)

**Step 9:** In the **Description** box, enter a useful description. (Example: Inbound web to IT Dept Server)

**Step 10:** Select or clear **Enable Logging**. (Example: Selected)

**Step 11:** In the **Logging Level** list, choose the logging level value, and then click **OK**. (Example: Default)

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

- Interface:** -- Any --
- Action:**  Permit  Deny
- Source Criteria:**
  - Source:** any4
  - User:** (empty)
  - Security Group:** (empty)
- Destination Criteria:**
  - Destination:** IT\_Web\_Server
  - Security Group:** (empty)
  - Service:** tcp/http, tcp/https
- Description:** HTTP and HTTPS to IT Web Server
- Enable Logging:**
- Logging Level:** Default
- More Options:** (expanded)
- Buttons:** OK, Cancel, Help



**Step 12:** After adding all of the rules in Table 9, in the order listed, click **Apply** on the Access Rules pane.

#	Enabled	Source Criteria:			Destination Criteria:		Service	Action
		Source	User	Security Group	Destination	Security Group		
<b>outside (1 incoming rule)</b>								
1	<input checked="" type="checkbox"/>	IT_Management_H...			SRVLAN154-network.. SRVLAN155-network..		Mgmt-Traffic	Permit
<b>Global (5 rules)</b>								
1	<input checked="" type="checkbox"/>	any4			IT_Web_Server		tcp http tcp https	Permit
2	<input checked="" type="checkbox"/>	any4			Finance_Web_Server		tcp http tcp https	Permit
3	<input checked="" type="checkbox"/>	any4			Hr_Web_Server		tcp http tcp https	Permit
4	<input checked="" type="checkbox"/>	any4			Research_Web_Se...		tcp http tcp https	Permit
5	<input checked="" type="checkbox"/>	any			any		ip ip	Deny

## Option 2: Deploy a blacklist security policy

If an organization does not have the desire or resources to maintain a granular, restrictive policy to control access between centralized data and the user community, a simpler, easy-to-deploy policy that limits only the highest-risk traffic may be more attractive. This policy is typically configured such that only specific services' access is blocked; all other traffic is permitted.

In this example, you allow SNMP queries and SSH requests from a specific address range that is allocated for IT staff. Network administrative users may need to issue SNMP queries from desktop computers to monitor network activity and SSH to connect to devices.

**Step 1:** Navigate to **Configuration > Firewall > Access Rules**.

Table 10 - Sample blacklist firewall policy rules

Interface	Action	Source	Destination	Service	Description	Logging Enable / Level
Outside	Permit	IT_Management_ Host_Range	SRVLAN154-network, SRVLAN155-network	tcp/ssh, udp/ snmp	Management access to servers	Selected / Default
Any	Deny	any4	any	tcp/ssh, udp/ snmp	Deny SSH and SNMP from all other hosts	Selected / Default
Any	Permit	any4	SRVLAN154-network, SRVLAN155-network	ip	Permit all other traffic to SR Secure VLANs	Selected / Default

**Step 2:** Repeat Step 3 through Step 11 for all rules listed in Table 10.

**Step 3:** Click **Add > Add Access Rule**

The Add Access Rule dialog box appears.

**Step 4:** In the **Interface** list, choose the interface. (Example: Outside)

**Step 5:** For the **Action** option, select the action. (Example: Permit)

**Step 6:** In the **Source** box, choose the source. (Example: IT\_Management\_Host\_Range)

**Step 7:** In the **Destination** box, choose the destination. (Example: SRVLAN154-network, SRVLAN155-network)

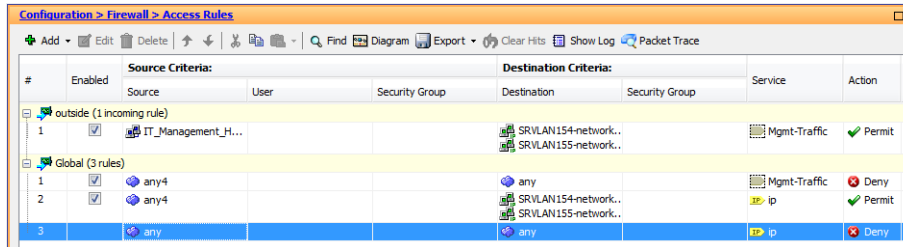
**Step 8:** In the **Service** box, enter the service. (Example: Mgmt-Traffic)

**Step 9:** In the **Description** box, enter a useful description. (Example: Management access to servers)

**Step 10:** Select or clear **Enable Logging**. (Example: Selected)

**Step 11:** In the **Logging Level** list, choose the logging level value, and then click **OK**. (Example: Default)

**Step 12:** After adding all of the rules in Table 10, in the order listed, click **Apply** on the Access Rules pane.



#	Enabled	Source Criteria:			Destination Criteria:		Service	Action
		Source	User	Security Group	Destination	Security Group		
outside (1 incoming rule)								
1	<input checked="" type="checkbox"/>	IT_Management_H...			SRVLAN154-network.. SRVLAN155-network..		Mgmt-Traffic	Permit
Global (3 rules)								
1	<input checked="" type="checkbox"/>	any4			any		Mgmt-Traffic	Deny
2	<input checked="" type="checkbox"/>	any4			SRVLAN154-network.. SRVLAN155-network..		ip	Permit
3	<input type="checkbox"/>	any			any		ip	Deny

## PROCESS

### Deploying Firewall Intrusion Prevention Systems (IPS)

1. Configure the LAN switch access port
2. Initialize the IPS module
3. Apply initial configuration
4. Complete basic configuration
5. Modify the inline security policy

From a security standpoint, intrusion detection systems (IDS) and intrusion prevention systems (IPS) are complementary to firewalls because firewalls are generally access-control devices that are built to block access to an application or host. In this way, a firewall can be used to remove access to a large number of application ports, reducing the threat to the servers. IDS and IPS sensors look for attacks in network and application traffic that is permitted to go through the firewall. If an IDS-configured sensor detects an attack, it generates an alert to inform the organization about the activity. An IPS-configured sensor is similar in that it generates alerts due to malicious activity and, additionally, it can apply an action to block the attack before it reaches the destination.

## Promiscuous versus Inline Deployment Modes

There are two primary deployment modes when using IPS sensors: *promiscuous* (IDS) or *inline* (IPS). There are specific reasons for each deployment model, based on risk tolerance and fault tolerance:

- In promiscuous mode (IDS), the sensor inspects copies of packets, which prevents it from being able to stop a malicious packet when it sees one. An IDS sensor must use another inline enforcement device in order to stop malicious traffic. This means that for activity such as single-packet attacks (for example, slammer worm over User Datagram Protocol [UDP]), an IDS sensor could not prevent the attack from occurring. However, an IDS sensor can offer great value when identifying and cleaning up infected hosts.
- In an inline (IPS) deployment, because the packet flow is sent through the sensor and returned to Cisco ASA, the sensor inspects the actual data packets. The advantage IPS mode offers is that when the sensor detects malicious behavior, the sensor can simply drop the malicious packet. This allows the IPS device a much greater capacity to actually prevent attacks.

## Deployment Considerations

Use IDS when you do not want to impact the availability of the network or create latency issues. Use IPS when you need higher security than IDS can provide and when you need the ability to drop malicious data packets.

The secure server room design using Cisco ASA 5500-X Series with IPS implements a policy for IPS, which sends all traffic to the IPS module inline.

Your organization may choose an IPS or IDS deployment, depending on regulatory and application requirements. It is very easy to initially deploy an IDS, or *promiscuous*, design and then move to IPS after you understand the traffic and performance profile of your network and you are comfortable that production traffic will not be affected.

### Procedure 1 Configure the LAN switch access port

A LAN switch port on the server room switch provides connectivity for the IPS sensor's management interface.

**Step 1:** Configure an access port to the management VLAN on the server room switch where each IPS device's management port will be connected. On Cisco ASA 5500X Series firewalls, the firewall and IPS modules share a single management interface. This deployment uses the management interface for IPS module access only. The server room management VLAN was defined in Procedure 3, "Apply the switch global configuration," in the "Server Room Ethernet LAN" chapter of this guide.

```
interface GigabitEthernet1/0/6
  description SR-5500X-IPSa
  !
interface GigabitEthernet2/0/6
  description SR-5500X-IPSB
  !
Interface range GigabitEthernet1/0/6, GigabitEthernet2/0/6
  switchport
  switchport access vlan 106
  switchport mode access
  switchport host
```



## Tech Tip

The IPS module and Cisco ASA share the same physical port for management traffic. In this deployment, Cisco ASA is managed in-band, and the IPS, either module or appliance, is always managed from the dedicated management port.

## Procedure 2 Initialize the IPS module

When a Cisco ASA 5500-X Series with IPS is initially deployed, the software IPS module may not be initialized, resulting in the Cisco ASA firewall being unaware of what code version to boot for the IPS module. Verify the IPS module status and prepare for configuration by following this procedure.

**Step 1:** From the Cisco ASA command line, check the status of the IPS module software.

```
SR-ASA5500X# show module ips detail
```

**Step 2:** If the status shown below is **Up**, the IPS module software has already been loaded. Skip to Procedure 3.

```
SR-ASA5500X# sh module ips detail
```

```
Getting details from the Service Module, please wait...
```

```
Card Type:          ASA 5555-X IPS Security Services Processor
Model:              ASA5555-IPS
Hardware version:   N/A
Serial Number:      FCH162377L4
Firmware version:   N/A
Software version:   7.3(2)E4
MAC Address Range:  a493.4caa.6f47 to a493.4caa.6f47
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.3(2)E4
Data Plane Status:  Up
Status:             Up
```

If the status shown below is **Status: Unresponsive No Image Present**, the IPS module software has never been loaded. Proceed to the next step.

```
SR-ASA5500X# show module ips detail
```

```
Getting details from the Service Module, please wait...
```

```
Unable to read details from module ips
```

```
Card Type:          Unknown
Model:              N/A
Hardware version:   N/A
Serial Number:      FCH162377L4
Firmware version:   N/A
Software version:
```

```
MAC Address Range: a493.4caa.6f47 to a493.4caa.6f47
Data Plane Status: Not Applicable
Status: Unresponsive No Image Present
...
```

**Step 3:** Verify that you have the correct IPS image on the Cisco ASA firewall disk0:

**i** Tech Tip

IPS recovery requires an image with file extension .aip

IPS upgrades require an image with file extension .pkg

The two image types are incompatible, and the correct type must be used for each type of operation.

Software installation and upgrade information for Cisco ASA-5500X Series can be found at:

<http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/release/notes/asarn91.html>

```
SR-ASA5500X# dir

Directory of disk0:/

11    drwx  4096      23:34:46 Jun 11 2012  log
24    drwx  4096      23:35:00 Jun 11 2012  crypto_archive
162   -rwx 37822464    13:40:42 Apr 25 2014  asa915-smp-k8.bin
163   -rwx 23374256    13:41:54 Apr 25 2014  asdm-716.bin
168   -rwx 47536128    11:10:18 Jul 11 2014  IPS-SSP_5555-K9-sys-1.1-a-7.3-
2-E4.aip
```

**Step 4:** Configure the IPS module to load the software on disk0:, and then boot with that software.

```
SR-ASA5500X# sw-module module ips recover configure image disk0:/ IPS-SSP_5555-
K9-sys-1.1-a-7.3-2-E4.aip
SR-ASA5500X# sw-module module ips recover boot
```

Module ips will be recovered. This may erase all configuration and all data on that device and attempt to download/install a new image for it. This may take several minutes.

```
Recover module ips? [confirm]y
```

```
Recover issued for module ips.
```

The recovery process takes several minutes to complete.

**Step 5:** Check that the module was loaded correctly.

```
SR-ASA5500X# show module ips detail
```

The output should display the line **Status: Up**.

### Procedure 3 Apply initial configuration

Use the sensor's CLI in order to set up basic networking information, specifically: the IP address, gateway address, and access lists that allow remote access. After these critical pieces of data are entered, the rest of the configuration is accomplished by using Cisco Adaptive Security Device Manager/IPS Device Manager (ASDM/IDM), the embedded GUI console.

Table 11 - IP addressing for the Cisco ASA 5500X Series IPS module

Cisco ASA firewall failover assignment	IPS module management interface IP address
Primary	10.5.7.21 /25
Secondary	10.5.7.22 /25

**Step 1:** From Cisco ASA, open a session into the module.

After logging into the Cisco ASA firewall appliance, access the IPS module.

```
SR-ASA5500X# session ips
Opening command session with module ips.
Connected to module ips. Escape character sequence is 'CTRL-^X'.
```

**Step 2:** Log in to the IPS module. The default username and password are both cisco.

```
login: cisco
Password: [password]
```

If this is the first time the sensor has been logged into, you are prompted to change the password. Enter the current password, and then input a new password. Change the password to a value that complies with the security policy of your organization.

**Step 3:** Begin entering setup script information. If this is the first configuration on the IPS system, it will automatically begin the setup script.

If the unit does not automatically begin the setup script, at the IPS module's CLI, launch the System Configuration Dialogue by typing **setup**.

```
sensor# setup
```

The IPS module enters interactive setup.

**Step 4:** Define the IPS module's host name.

```
--- Basic Setup ---
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '['].
Current time: Fri Jul 11 11:13:57 2014
Setup Configuration last modified: Mon Apr 28 07:13:55 2014
Enter host name [sensor]: SR-IPS-A
```

**Step 5:** Define the IP address and gateway address for the IPS module's external management port.

```
Enter IP interface [192.168.1.62/24,192.168.1.250]: 10.5.7.21/25,10.5.7.1
```

**Step 6:** Define the access list, and then press **Enter**. This controls management access to the IPS module. Press **Enter** at a blank Permit: prompt to go to the next step.

```
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.4.48.0/24
```

**Step 7:** Define the DNS server address and then accept the default answer (no) for the next two questions.

```
Use DNS server for Auto-Updates from www.cisco.com and Global Correlation?[yes]:
yes
DNS server IP address[]: 10.4.48.10
Use HTTP proxy server for Auto-Updates from www.cisco.com and Global
Correlation?[no]: no
Modify system clock settings?[no]: no
```

Note the following:

- An HTTP proxy server address is not needed for a network that is configured according to this guide.
- You will configure time details in the IPS module's GUI console.

**Step 8:** For the option to participate in the SensorBase Network, enter **partial** and agree to participate based on your security policy.

```
Participation in the SensorBase Network allows Cisco to collect aggregated
statistics about traffic sent to your IPS.
SensorBase Network Participation level? [off]: partial
....
Do you agree to participate in the SensorBase Network?[no]: yes
....
```

The IPS module displays your configuration and a brief menu with four options.

**Step 9:** In the System Configuration dialog, save your configuration and exit setup by entering **2**.

```
The following configuration was entered.
service host
network-settings
host-ip 10.5.7.21/25,10.5.7.1
host-name SR-IPS-A
telnet-option disabled
sshv1-fallback disabled
access-list 10.4.48.0/24
ftp-timeout 300
no login-banner-text
dns-primary-server enabled
address 10.4.48.10
exithttp-proxy no-proxy
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
```

```
exit
summertime-option disabled
ntp-option disabled
exit
service global-correlation
network-participation partial
exit
```

- [0] Go to the command prompt without saving this config.
- [1] Return to setup without saving this config.
- [2] Save this configuration and exit setup.
- [3] Continue to Advanced setup.

Enter your selection[3]: **2**

Warning: DNS or HTTP proxy is required for global correlation inspection and reputation filtering, but no DNS or proxy servers are defined.

--- Configuration Saved ---

Complete the advanced setup using CLI or IDM.

To use IDM, point your web browser at <https://<sensor-ip-address>>.

**Step 10:** To return to the Cisco ASA command line, type **exit**.

**Step 11:** Repeat Step 1 through Step 10, for the IPS sensor installed in the other Cisco ASA chassis. In Step 4, assign a unique host name (Example: SR-IPS-B), and then in Step 5, be sure to use a different IP address (Example: 10.5.7.22) on the other sensor's management interface.

#### **Procedure 4** Complete basic configuration

After the basic setup in the System Configuration Dialog is complete, you will use the startup wizard in the integrated management tool, Cisco ASDM/IDM, to complete the following tasks in order to complete a basic IPS configuration:

- Configure time settings
- Configure DNS and NTP servers
- Define a basic IDS configuration
- Configure inspection service rule policy
- Assign interfaces to virtual sensors

Using Cisco ASDM to configure the IPS module operation allows the GUI to set up the communications path from the Cisco ASA firewall to the IPS module, as well as configure the IPS module settings.

**Step 1:** Using a secure HTTP session (<https://10.5.26.126>), navigate to the Cisco ASA firewall outside interface programmed in Procedure 2, "Configure the firewall outside port," and then click **Run ASDM**. Cisco ASDM starts from a Java Web Start application.

**Step 2:** Enter the username and password configured for the Cisco ASA firewall in Step 6 of Procedure 1, "Apply Cisco ASA initial configuration."



**Step 3:** In the Cisco ASDM work pane, click the **Intrusion Prevention** tab, enter the IP address, username, and password that you configured for IPS-A access, and then click **Continue**.

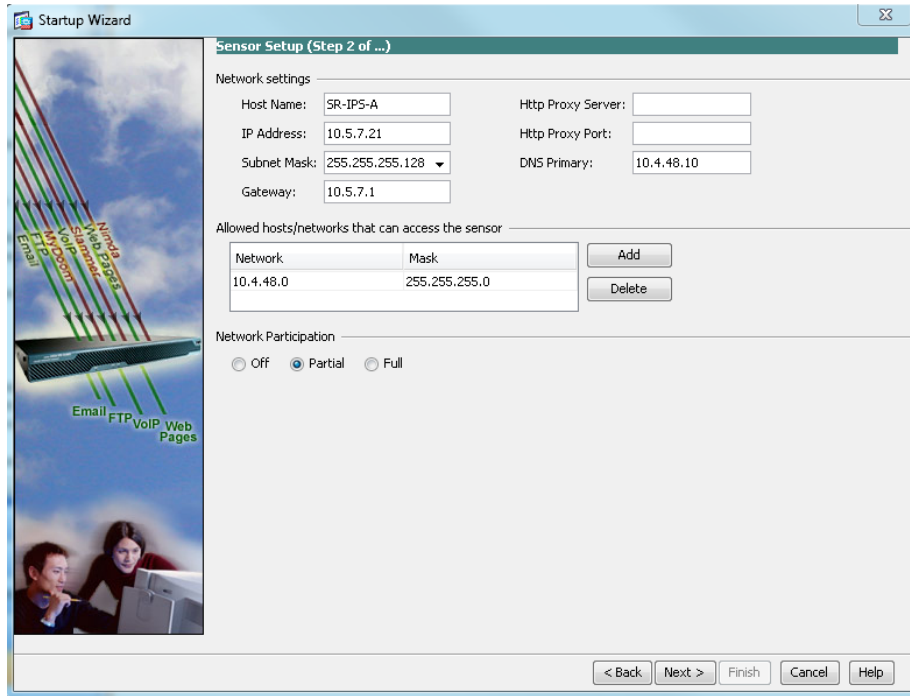
Cisco ASDM downloads the IPS information from the appliance for SR-IPS-A.

**Step 4:** Click **Configuration**, navigate to the **IPS** tab, and then click **Launch Startup Wizard**.

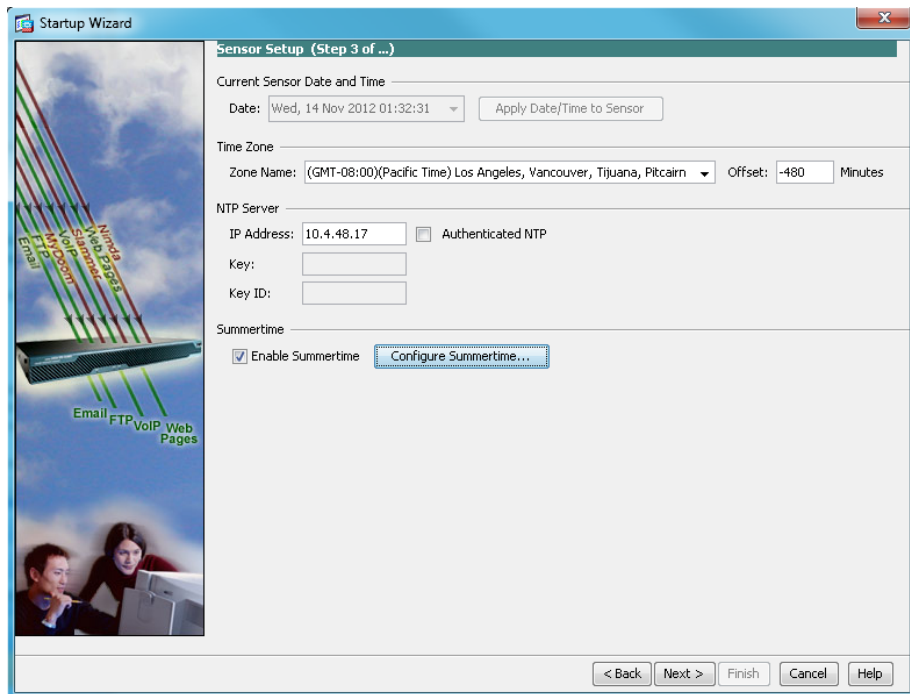


**Step 5:** Follow the instructions in the wizard. Note the following:

- On the **Sensor Setup** page, verify the settings, and then click **Next**.



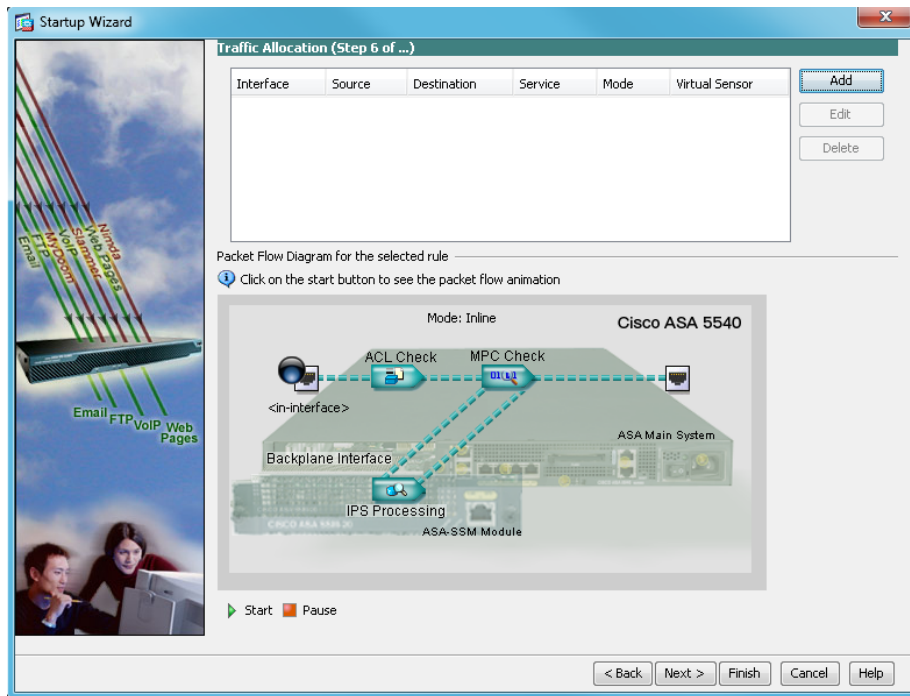
- On the next **Sensor Setup** page, in the **Zone Name** list, select the appropriate time zone. Enter the NTP Server IP address (Example: 10.4.48.17), ensure the **Authenticated NTP** is cleared, set the summertime settings, and then click **Next**.



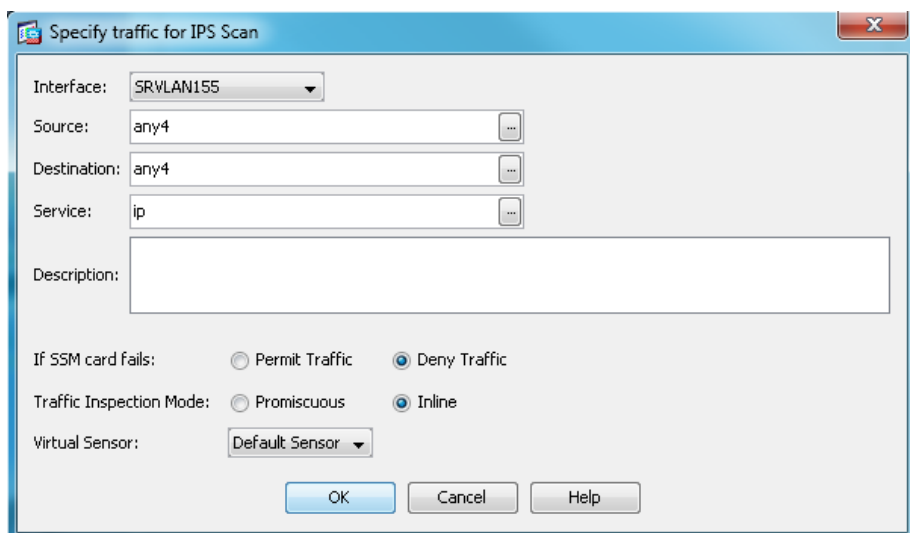
## Tech Tip

NTP is particularly important for security event correlation if you use a Security Event Information Manager product to monitor security activity on your network.

- On the Virtual Sensors page, click **Next**.
- On the Signatures page, click **Next**.
- On the Traffic Allocation page, click **Add**.



In the Specify traffic for IPS Scan dialog box, in the **Interface** list, choose **SRVLAN155**, and next to Traffic Inspection Mode, select **Inline**, and then click **OK**.



At the bottom of the Traffic Allocation page, click **Next**.

- Configure the IPS device to automatically pull updates from Cisco.com. On the Auto Update page, select **Enable Signature and Engine Updates**. Provide a valid cisco.com username and password that holds entitlement to download IPS software updates. Select **Daily**, enter a time between 12:00 AM and 4:00 AM for the update **Start Time**, and then select **Every Day**. Click **Finish**.

**Step 6:** When you are prompted if you want to commit your changes to the sensor, click **Yes**. ASDM/IDM applies your changes and replies with a message that a reboot is required.

**Step 7:** Click **OK**. Do not reboot the IPS sensor yet.

Next, you assign interfaces to the virtual sensor.

**Step 8:** Navigate to **Sensor Setup > Policies > IPS Policies**.

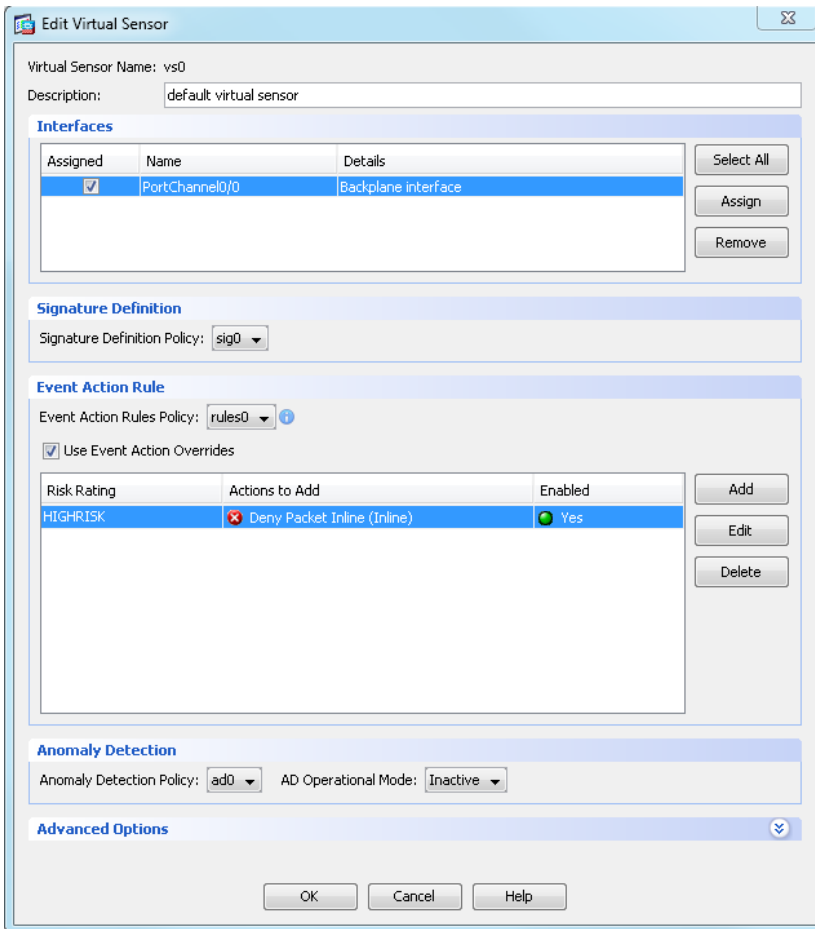


#### Tech Tip

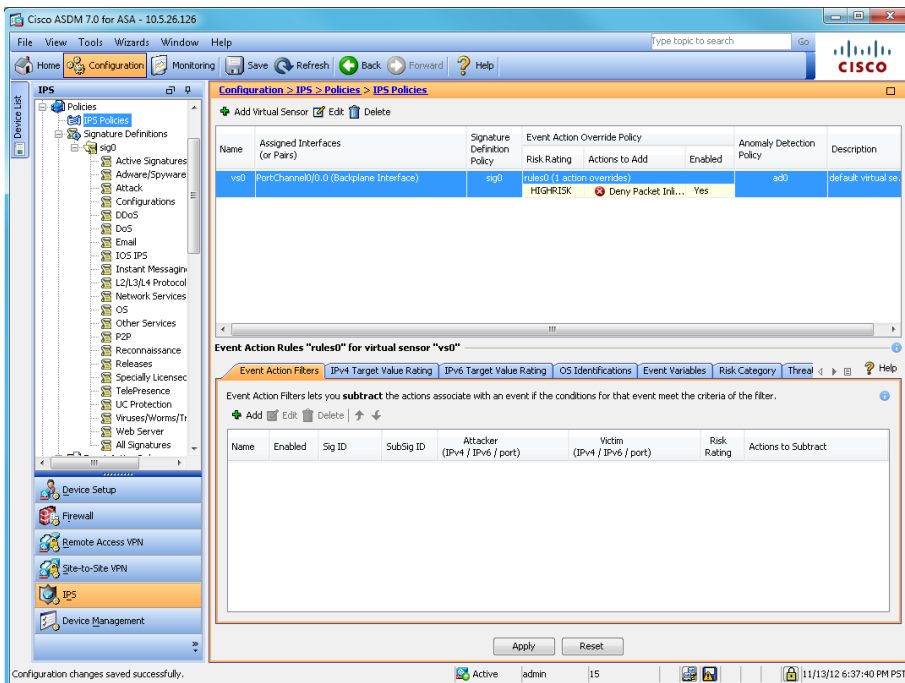
With certain versions of Java, ASDM does not properly load the IPS Policies configuration section. If you are unable to load the IPS Policies configuration section in ASDM, use IDM. To launch IDM, enter the management IP address of the IPS module in a web browser (Example: <https://10.5.7.21>). Navigate to **Configuration > Policies > IPS Policies**. The following steps apply to both ASDM and IDM.

**Step 9:** Highlight the vs0 virtual sensor, and then click **Edit**.

Step 10: In the Edit Virtual Sensor dialog box, for the PortChannel0/0 interface, select **Assigned**, and then click **OK**.



Step 11: Click **Apply**.



Next, you reboot the sensor.

**Step 12:** Navigate to **Sensor Management > Reboot Sensor**, click **Reboot Sensor**, and then click **OK** to approve.

**Step 13:** Repeat the steps in this procedure for the IPS module in the second Cisco ASA firewall. There is no configuration synchronization between the two IPS modules like there is between the Cisco ASA firewalls. Note that in Step 1, navigate to the second firewall's outside IP address, and then launch Cisco ASDM. (Example: <https://10.5.26.125>).

### Tech Tip

Do not attempt to modify the firewall configuration on the standby appliance.  
Configuration changes are only made on the primary appliance.

## Procedure 5 Modify the inline security policy

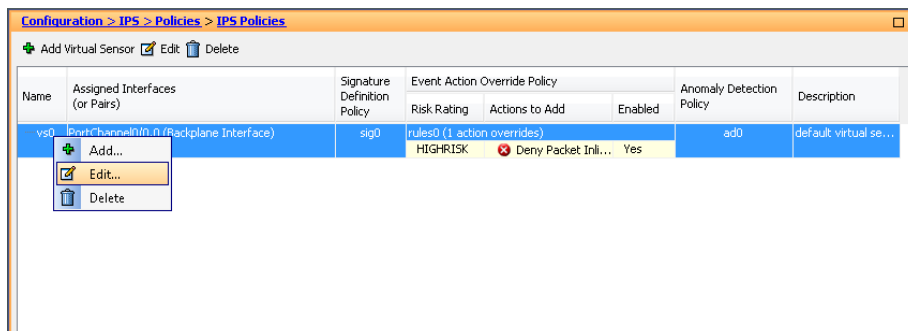
### (Optional)

If you opted to run inline mode on an IPS device, the sensor is configured to drop high-risk traffic. By default, this means that if an alert fires with a risk rating of at least 90 or if the traffic comes from an IP address with a negative reputation that raises the risk rating to 90 or higher, the sensor drops the traffic. If the risk rating is raised to 100 because of the source address reputation score, then the sensor drops all traffic from that IP address.

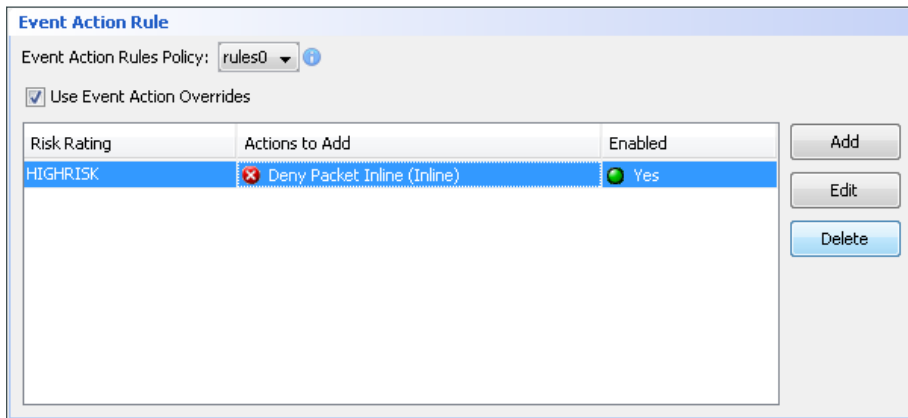
The chances of the IPS dropping traffic that is not malicious when using a risk threshold of 90 is very low. However, if you want to adopt a more conservative policy, for the risk threshold, raise the value to 100.

**Step 1:** In Cisco ASDM, navigate to **Configuration > IPS > Policies > IPS Policies**.

**Step 2:** In the Virtual Sensor panel, right-click the **vs0** entry, and then select **Edit**.

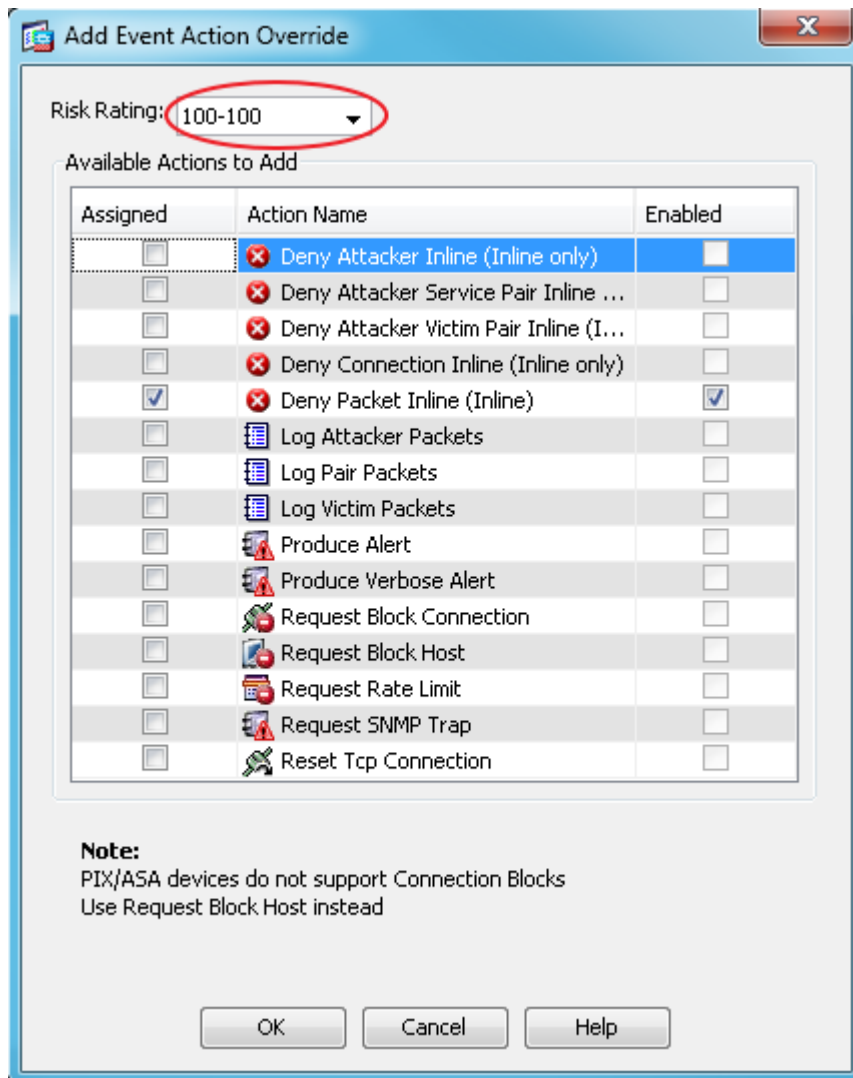


**Step 3:** In the Event Action Rule work pane, click **Deny Packet Inline (Inline)**, and then click **Delete**.



**Step 4:** In the Event Action Rule work pane, Click **Add**.

**Step 5:** In the Add Event Action Override dialog box, in the **Risk Rating** list, enter new value of **100-100**, select **Deny Packet Inline**, and then click **OK**.



**Step 6:** In the Edit Virtual Sensor pane, click **OK**.

**Step 7:** Click **Apply**.

**Step 8:** For the secondary sensor, repeat Step 1 through Step 7.

There is no configuration synchronization between the two sensors.



# Appendix A: Product List

## Server Room

Functional Area	Product Description	Part Numbers	Software
Firewall	ASA 5555-X IPS Edition - security appliance	ASA5555-IPS-K9	ASA 9.1(5) IPS 7.3(2) E4
	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	

## LAN Access Layer

Functional Area	Product Description	Part Numbers	Software	
Stackable Access Layer Switch	Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.3.3SE(15.0.1EZ3) IP Base feature set	
	Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports	WS-C3850-24P		
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G		
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G		
	Standalone Access Layer Switch	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 2x10GE or 4x1GE Uplink	WS-C3650-24PD	3.3.3SE(15.0.1EZ3) IP Base feature set
		Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 4x1GE Uplink	WS-C3650-24PS	
		Cisco Catalyst 3650 Series Stack Module	C3650-STACK	

# Appendix B: Configuration Examples

## Cisco Catalyst 3850 Switch Stack

The server room Cisco Catalyst 3850 switch operates in a stack configuration of two switches to provide a resilient Ethernet LAN.

```
!  
version 15.0  
no service pad  
service timestamps debug datetime msec localtime  
service timestamps log datetime msec localtime  
service password-encryption  
service compress-config  
!  
hostname RS200-SR3850  
!  
boot-start-marker  
boot-end-marker  
!  
!  
vrf definition Mgmt-vrf  
!  
  address-family ipv4  
  exit-address-family  
!  
  address-family ipv6  
  exit-address-family  
!  
enable secret 5 <removed>  
!  
username admin password 7 <removed>  
aaa new-model  
!  
!  
aaa group server tacacs+ TACACS-SERVERS  
  server name TACACS-SERVER-1  
!  
aaa authentication login default group TACACS-SERVERS local  
aaa authorization console  
aaa authorization exec default group TACACS-SERVERS local  
!
```

```

!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
switch 1 provision ws-c3850-48t
switch 2 provision ws-c3850-48t
!
ip domain-name cisco.local
ip name-server 10.4.48.10
ip device tracking
!
!
vtp domain ltdfin
vtp mode transparent
udld enable

!
crypto pki trustpoint TP-self-signed-1981248194
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-1981248194
  revocation-check none
  rsakeypair TP-self-signed-1981248194
!
!
crypto pki certificate chain TP-self-signed-1981248194
  certificate self-signed 02
    <output omitted>
!
!
!
!
!
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig (STP)
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause l2ptguard
errdisable recovery cause psecure-violation

```

```

errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause pppoe-ia-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause inline-power
errdisable recovery cause arp-inspection
errdisable recovery cause loopback
errdisable recovery cause psp
diagnostic bootup level minimal
port-channel load-balance src-dst-ip
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 154-155 priority 24576
!
redundancy
  mode sso
!
!
vlan 106
  name Management
!
vlan 148
  name Server_VLAN_1
!
vlan 149
  name Server_VLAN_2
!
vlan 153
  name FirewallOutsideVLAN
!
vlan 154
  name FirewallSecVLAN
!
vlan 155
  name FirewallIPSSecVLAN
!
vlan 999
!
ip ssh version 2
ip scp server enable
!
class-map match-any MULTIMEDIA-STREAMING-QUEUE
  match dscp af31

```

```

    match dscp af32
    match dscp af33
class-map match-any CONTROL-MGMT-QUEUE
    match dscp cs7
    match dscp cs6
    match dscp cs3
    match dscp cs2
class-map match-any TRANSACTIONAL-DATA-QUEUE
    match dscp af21
    match dscp af22
    match dscp af23
class-map match-any VIDEO-PRIORITY-QUEUE
    match dscp cs5
    match dscp cs4
class-map match-any BULK-SCAVENGER-DATA-QUEUE
    match dscp af11
    match dscp af12
    match dscp af13
    match dscp cs1
class-map match-any MULTIMEDIA-CONFERENCING-QUEUE
    match dscp af41
    match dscp af42
    match dscp af43
class-map match-any non-client-nrt-class
    match non-client-nrt
class-map match-any PRIORITY-QUEUE
    match dscp ef
!
policy-map port_child_policy
    class non-client-nrt-class
        bandwidth remaining ratio 10
policy-map 2P6Q3T
    class PRIORITY-QUEUE
        priority level 1 percent 10
    class VIDEO-PRIORITY-QUEUE
        priority level 2 percent 20
    class CONTROL-MGMT-QUEUE
        bandwidth remaining percent 10
        queue-buffers ratio 10
    class MULTIMEDIA-CONFERENCING-QUEUE
        bandwidth remaining percent 10
        queue-buffers ratio 10
        queue-limit dscp af41 percent 100
        queue-limit dscp af42 percent 90
        queue-limit dscp af43 percent 80
    class MULTIMEDIA-STREAMING-QUEUE
        bandwidth remaining percent 10

```

```

    queue-buffers ratio 10
    queue-limit dscp af31 percent 100
    queue-limit dscp af32 percent 90
    queue-limit dscp af33 percent 80
class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 10
    queue-buffers ratio 10
    queue-limit dscp af21 percent 100
    queue-limit dscp af22 percent 90
    queue-limit dscp af23 percent 80
class BULK-SCAVENGER-DATA-QUEUE
    bandwidth remaining percent 5
    queue-buffers ratio 10
class class-default
    bandwidth remaining percent 25
    queue-buffers ratio 25
!
!
!
!
macro name AccessEdgeQoS
    auto qos voip cisco-phone
@
macro name EgressQoS
    service-policy output 2P6Q3T
@
!
interface Port-channel1
    description EtherChannel link to RS200-3925-VG
    switchport access vlan 148
    switchport mode access
    spanning-tree portfast
!
interface Port-channel20
    description EtherChannel to RS200-D4500X
    switchport trunk native vlan 999
    switchport trunk allowed vlan 106,148,149,153
    switchport mode trunk
    logging event link-status
!
interface GigabitEthernet0/0
    vrf forwarding Mgmt-vrf
    no ip address
    negotiation auto
!
interface GigabitEthernet1/0/1
    switchport access vlan 148

```

```

switchport mode access
macro description EgressQoS
spanning-tree portfast
service-policy output 2P6Q3T
!
interface GigabitEthernet1/0/2
description RS200-ESXi2 Server Room VLANs (vmmnic4)
switchport access vlan 148
switchport trunk allowed vlan 148,149
switchport mode trunk
macro description EgressQoS
spanning-tree portfast
service-policy output 2P6Q3T
!
interface GigabitEthernet1/0/3
switchport access vlan 148
switchport mode access
macro description EgressQoS
spanning-tree portfast
service-policy output 2P6Q3T
!
interface GigabitEthernet1/0/4
switchport access vlan 148
switchport mode access
macro description EgressQoS
spanning-tree portfast
service-policy output 2P6Q3T
!
interface GigabitEthernet1/0/5
description RS200-ESXi1 CIMC
switchport access vlan 148
switchport mode access
macro description EgressQoS
spanning-tree portfast
service-policy output 2P6Q3T
!
interface GigabitEthernet1/0/6
description SR-5500X-IPSa
switchport access vlan 106
switchport mode access
macro description EgressQoS
spanning-tree portfast
service-policy output 2P6Q3T
!
interface GigabitEthernet1/0/7
description RS200-3925-VG Gig0/1
switchport access vlan 148

```

```

switchport mode access
macro description EgressQoS
channel-group 1 mode on
spanning-tree portfast
service-policy output 2P6Q3T
!
interface GigabitEthernet1/0/8
switchport access vlan 148
switchport mode access
macro description EgressQoS
spanning-tree portfast
service-policy output 2P6Q3T
!
!*****
! Interfaces GigabitEthernet 1/0/9 to 1/0/46 are
! configured the same way and have been removed for brevity
!*****
!
interface GigabitEthernet1/0/47
description SR-ASA5500a outside gi 0/3
switchport access vlan 153
switchport mode access
macro description EgressQoS
spanning-tree portfast
service-policy output 2P6Q3T
!
interface GigabitEthernet1/0/48
description SR-ASA5500a inside gi 0/0
switchport access vlan 148
switchport trunk allowed vlan 154,155
switchport mode trunk
macro description EgressQoS
spanning-tree portfast trunk
service-policy output 2P6Q3T
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface TenGigabitEthernet1/1/1
!
interface TenGigabitEthernet1/1/2
!

```



```

interface TenGigabitEthernet1/1/3
  description Link to RS200-D4500X Ten1/1/5
  switchport trunk native vlan 999
  switchport trunk allowed vlan 106,148,149,153
  switchport mode trunk
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  macro description EgressQoS
  channel-protocol lacp
  channel-group 20 mode active
  service-policy output 2P6Q3T
!
interface TenGigabitEthernet1/1/4
!
interface GigabitEthernet2/0/1
  switchport access vlan 148
  switchport mode access
  macro description EgressQoS
  spanning-tree portfast
  service-policy output 2P6Q3T
!
interface GigabitEthernet2/0/2
  description RS200-ESXi2 Server Room VLANs (vmnic5)
  switchport access vlan 148
  switchport trunk allowed vlan 148,149
  switchport mode trunk
  macro description EgressQoS
  spanning-tree portfast
  service-policy output 2P6Q3T
!
interface GigabitEthernet2/0/3
  switchport access vlan 148
  switchport mode access
  macro description EgressQoS
  spanning-tree portfast
  service-policy output 2P6Q3T
!
interface GigabitEthernet2/0/4
  switchport access vlan 148
  switchport mode access
  macro description EgressQoS
  spanning-tree portfast
  service-policy output 2P6Q3T
!
interface GigabitEthernet2/0/5
  description RS200-ESXi2 CIMC

```

```

switchport access vlan 148
switchport mode access
macro description EgressQoS
spanning-tree portfast
service-policy output 2P6Q3T
!
interface GigabitEthernet2/0/6
description SR-5500X-IPsb
switchport access vlan 106
switchport mode access
macro description EgressQoS
spanning-tree portfast
service-policy output 2P6Q3T
!
interface GigabitEthernet2/0/7
description RS200-3925-VG Gig0/2
switchport access vlan 148
switchport mode access
macro description EgressQoS
channel-group 1 mode on
spanning-tree portfast
service-policy output 2P6Q3T
!
interface GigabitEthernet2/0/8
switchport access vlan 148
switchport mode access
macro description EgressQoS
spanning-tree portfast
service-policy output 2P6Q3T
!
!*****
! Interfaces GigabitEthernet 2/0/9 to 2/0/46 are
! configured the same way and have been removed for brevity
!*****
!
interface GigabitEthernet2/0/47
description SR-ASA5500b outside gi 0/3
switchport access vlan 153
switchport mode access
macro description EgressQoS
spanning-tree portfast
service-policy output 2P6Q3T
!
interface GigabitEthernet2/0/48
description SR-ASA5500b inside gi 0/0
switchport access vlan 148
switchport trunk allowed vlan 154,155

```

```

switchport mode trunk
macro description EgressQoS
spanning-tree portfast trunk
service-policy output 2P6Q3T
!
interface GigabitEthernet2/1/1
!
interface GigabitEthernet2/1/2
!
interface GigabitEthernet2/1/3
!
interface GigabitEthernet2/1/4
!
interface TenGigabitEthernet2/1/1
!
interface TenGigabitEthernet2/1/2
!
interface TenGigabitEthernet2/1/3
description Link to RS200-D4500X Ten2/1/5
switchport trunk native vlan 999
switchport trunk allowed vlan 106,148,149,153
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
macro description EgressQoS
channel-protocol lacp
channel-group 20 mode active
service-policy output 2P6Q3T
!
interface TenGigabitEthernet2/1/4
!
interface Vlan1
no ip address
shutdown
!
interface Vlan106
ip address 10.5.7.4 255.255.255.128
!
ip default-gateway 10.5.7.1
no ip http server
ip http authentication aaa
ip http secure-server
!
!
!
access-list 55 permit 10.4.48.0 0.0.0.255

```

```

!
snmp-server community <removed> RO 55
snmp-server community <removed> RW 55
!
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key 7 <removed>
!
!
!
!
line con 0
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  access-class 55 in vrf-also
  transport preferred none
  transport input ssh
line vty 5 15
  access-class 55 in vrf-also
  transport preferred none
  transport input ssh
!
ntp server 10.4.48.17
wsma agent exec
  profile httplistener
  profile httpslistener
wsma agent config
  profile httplistener
  profile httpslistener
wsma agent filesys
  profile httplistener
  profile httpslistener
wsma agent notify
  profile httplistener
  profile httpslistener
!
wsma profile listener httplistener
  transport http
!
wsma profile listener httpslistener
  transport https
ap group default-group
end

```

# Cisco ASA 5500-X Firewall—Primary and Secondary

To provide resilience, the server room primary and secondary Cisco ASA 5500-X firewalls are configured as an active/standby pair. The configurations of the primary and secondary Cisco ASA are identical, with one important exception:

- The primary firewall configuration includes the command **failover lan unit primary**.
- The secondary firewall configuration includes the command **failover lan unit secondary**.

Both lines are highlighted in the configuration shown below; however, on the primary and secondary firewalls, only the applicable command is configured.

```
:
ASA Version 9.1(5)
!
hostname SR-ASA5500X
domain-name cisco.local
enable password <removed> encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd <removed> encrypted
names
!
interface GigabitEthernet0/0
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/0.154
  vlan 154
  nameif SRVLAN154
  security-level 100
  ip address 10.5.27.1 255.255.255.0 standby 10.5.27.2
!
interface GigabitEthernet0/0.155
  vlan 155
  nameif SRVLAN155
  security-level 100
  ip address 10.5.28.1 255.255.255.0 standby 10.5.28.2
!
interface GigabitEthernet0/1
  shutdown
  no nameif
```

```

no security-level
no ip address
!
interface GigabitEthernet0/2
description LAN/STATE Failover Interface
!
interface GigabitEthernet0/3
nameif outside
security-level 0
ip address 10.5.26.126 255.255.255.128 standby 10.5.26.125
!
interface GigabitEthernet0/4
shutdown
no nameif
no security-level
no ip address
!
!*****
! Interfaces GigabitEthernet0/5 to 0/7 are
! configured the same way and have been removed for brevity
!*****
!
interface Management0/0
management-only
nameif IPS-mgmt
security-level 0
no ip address
!
boot system disk0:/asa915-smp-k8.bin
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns server-group DefaultDNS
domain-name cisco.local
object network IT_Web_Server
host 10.5.27.80
description IT Web Server
object network Finance_Web_Server
host 10.5.27.81
description Finance Web Server
object network Hr_Web_Server
host 10.5.28.80
description Hr Web Server
object network Research_Web_Server
host 10.5.28.81
description Research Web Server
object network IT_Management_Host_Range

```

```

range 10.4.48.224 10.4.48.254
description IT Management System Range
object-group service DM_INLINE_TCP_1 tcp
port-object eq www
port-object eq https
object-group service DM_INLINE_TCP_2 tcp
port-object eq www
port-object eq https
object-group service DM_INLINE_TCP_3 tcp
port-object eq www
port-object eq https
object-group service DM_INLINE_TCP_4 tcp
port-object eq www
port-object eq https
object-group service Mgmt-Traffic
description Management Traffic SSH and SNMP
service-object tcp destination eq smtp
service-object tcp destination eq ssh
object-group network DM_INLINE_NETWORK_1
network-object 10.5.27.0 255.255.255.0
network-object 10.5.28.0 255.255.255.0
access-list global_access remark HTTP and HTTPS to IT Web Sever
access-list global_access extended permit tcp any4 object IT Web Server object-group
DM_INLINE_TCP_1
access-list global_access remark HTTP and HTTPS to IT Web Server
access-list global_access extended permit tcp any4 object Finance Web Server object-
group DM_INLINE_TCP_2
access-list global_access remark HTTP and HTTPS to IT Web Server
access-list global_access extended permit tcp any4 object Hr Web Server object-group
DM_INLINE_TCP_3
access-list global_access remark HTTP and HTTPS to IT Web Server
access-list global_access extended permit tcp any4 object Research Web Server object-
group DM_INLINE_TCP_4
access-list outside_access_in remark Permit Mgmt Traffic from MgmtRange to SR VLANs
access-list outside_access_in extended permit object-group Mgmt-Traffic object IT
Management Host Range object-group DM_INLINE_NETWORK_1
access-list SRVLAN155_mpc extended permit ip any4 any4
pager lines 24
logging enable
logging buffered informational
mtu SRVLAN154 1500
mtu SRVLAN155 1500
mtu outside 1500
mtu IPS-mgmt 1500
failover
failover lan unit primary
failover lan unit secondary

```

```

failover lan interface failover GigabitEthernet0/2
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key *****
failover replication http
failover link failover GigabitEthernet0/2
failover interface ip failover 10.5.26.130 255.255.255.252 standby 10.5.26.129
monitor-interface SRVLAN154
monitor-interface SRVLAN155
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-716.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group outside_access_in in interface outside
access-group global_access global
route outside 0.0.0.0 0.0.0.0 10.5.26.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (outside) host 10.4.48.15
  key *****
user-identity default-domain LOCAL
aaa authentication enable console AAA-SERVER LOCAL
aaa authentication ssh console AAA-SERVER LOCAL
aaa authentication http console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
aaa authorization exec authentication-server
http server enable
http 10.4.48.0 255.255.255.0 outside
snmp-server host outside 10.4.48.35 community *****
no snmp-server location
no snmp-server contact
snmp-server community *****
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
sysopt noproxyarp SRVLAN154
sysopt noproxyarp SRVLAN155
sysopt noproxyarp outside
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy

```



```

telnet timeout 5
ssh stricthostkeycheck
ssh 10.4.48.0 255.255.255.0 outside
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group1-sha1
console timeout 0
!
tls-proxy maximum-session 1000
!
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 10.4.48.17
ssl encryption aes256-sha1 aes128-sha1 3des-sha1
webvpn
  anyconnect-essentials
username admin password <removed> encrypted privilege 15
!
class-map SRVLAN155-class
  match access-list SRVLAN155_mpc
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
policy-map SRVLAN155-policy
  class SRVLAN155-class
    ips inline fail-close
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip

```

```

inspect xdmcp
!
service-policy global_policy global
service-policy SRVLAN155-policy interface SRVLAN155
prompt hostname context
no call-home reporting anonymous
call-home
  profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/
DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly 8
  subscribe-to-alert-group configuration periodic monthly 8
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:05be392a212bb81aa75237751553d8cb
: end

```

## Cisco ASA 5500-X IPS-Primary

The server room Cisco ASA 5500-X primary IPS operates as an active/standby pair with the second Cisco ASA 5500-X IPS.

```

! Version 7.3(2)
! Host:
!   Realm Keys          key1.0
! Signature Definition:
!   Signature Update    S773.0   2014-02-18
!   Threat Profile Version 6! -----
service interface
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 100-100
exit
exit
! -----
service host
network-settings
host-ip 10.5.7.21/25,10.5.7.1

```

```

host-name SR-IPS-A
telnet-option disabled
access-list 10.4.48.0/24
dns-primary-server enabled
address 10.4.48.10
exit
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset -480
standard-time-zone-name GMT-08:00
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 10.4.48.17
exit
summertime-option recurring
summertime-zone-name UTC
exit
exit
! -----
service logger
exit
! -----
service network-access
exit
! -----
service notification
exit
! -----
service signature-definition sig0
exit
! -----
service ssh-known-hosts
exit
! -----
service trusted-certificates
exit
! -----
service web-server
websession-inactivity-timeout 3600
exit
! -----
service anomaly-detection ad0
exit
! -----
service external-product-interface

```

```

exit
! -----
service health-monitor
exit
! -----
service global-correlation
network-participation partial
exit
! -----
service aaa
exit
! -----
service analysis-engine
virtual-sensor vs0
physical-interface PortChannel0/0
exit

```

## Cisco ASA 5500-X IPS-Secondary

The server room Cisco ASA 5500-X secondary IPS operates as an active/standby pair with the primary Cisco ASA 5500-X IPS.

```

! Version 7.3(2)
! Host:
!   Realm Keys           key1.0
! Signature Definition:
!   Signature Update      S773.0   2014-02-18
!   Threat Profile Version 6service interface
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 100-100
exit
exit
! -----
service host
network-settings
host-ip 10.5.7.22/25,10.5.7.1
host-name SR-IPS-B
telnet-option disabled
access-list 10.4.48.0/24
dns-primary-server enabled
address 10.4.48.10

```

```

exit
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset -480
standard-time-zone-name GMT-08:00
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 10.4.48.17
exit
summertime-option recurring
summertime-zone-name UTC
exit
! -----
service logger
exit
! -----
service network-access
exit
! -----
service notification
exit
! -----
service signature-definition sig0
exit
! -----
service ssh-known-hosts
exit
! -----
service trusted-certificates
exit
! -----
service web-server
  websession-inactivity-timeout 3600
exit
! -----
service anomaly-detection ad0
exit
! -----
service external-product-interface
exit
! -----
service health-monitor
exit
! -----
service global-correlation

```

```
network-participation partial
exit
! -----
service aaa
exit
! -----
service analysis-engine
virtual-sensor vs0
physical-interface PortChannel0/0
exit
```

# Appendix C: Changes

---

This appendix summarizes the changes Cisco made to this guide since its last edition.

- We replaced the Cisco Catalyst 3560-X switch with the Cisco Catalyst 3650 switch running IOS XE 03.03.03.SE
- We replaced the Cisco Catalyst 3750-X switch with the Cisco Catalyst 3850 switch running IOS XE 03.03.03.SE
- We updated Cisco ASA 5500 series firewalls to Cisco ASA 9.1(5) and Cisco IPS 7.3(2)E4

## Feedback

Please use the [feedback form](#) to send comments and suggestions about this guide.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY 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 THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2014 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)