Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

SBA

DATA CENTER

DEPLOYMENT GUIDE

Server Room Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2012 are the "August 2012 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

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

Comments and Questions

If you would like to comment on a guide or ask questions, please use the SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What’s In This SBA Guide

Cisco SBA Data Center

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization’s problems—without worrying about the technical complexity.

Cisco SBA Data Center is a comprehensive design that scales from a server room to a data center for networks with up to 10,000 connected users. This design incorporates compute resources, security, application resiliency, and virtualization.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

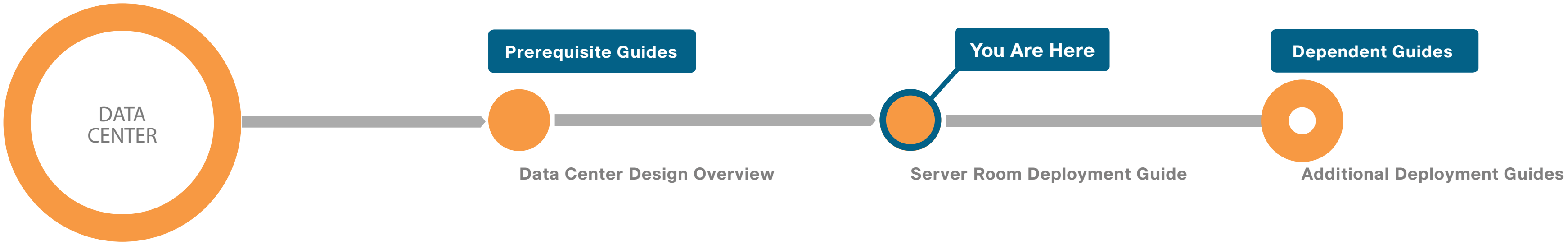
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- Business Overview—Describes the business use case for the design. Business decision makers may find this section especially useful.
- Technology Overview—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- Deployment Details—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel


DATA CENTER
Prerequisite Guides
You Are Here
Dependent Guides
Data Center Design Overview
Server Room Deployment Guide
Additional Deployment Guides

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. This guide 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 *Cisco SBA—Borderless Networks LAN Deployment Guide* so that you can use the Layer 3 services of your Cisco Smart Business Architecture (SBA) LAN distribution layer for routing traffic to and from the IP subnets in the server room.

Cisco SBA is a comprehensive design for networks with up to 10,000 users. This out-of-the-box design is simple, fast, affordable, scalable, and flexible.

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

The *Server Room Deployment Guide* includes the following chapters:

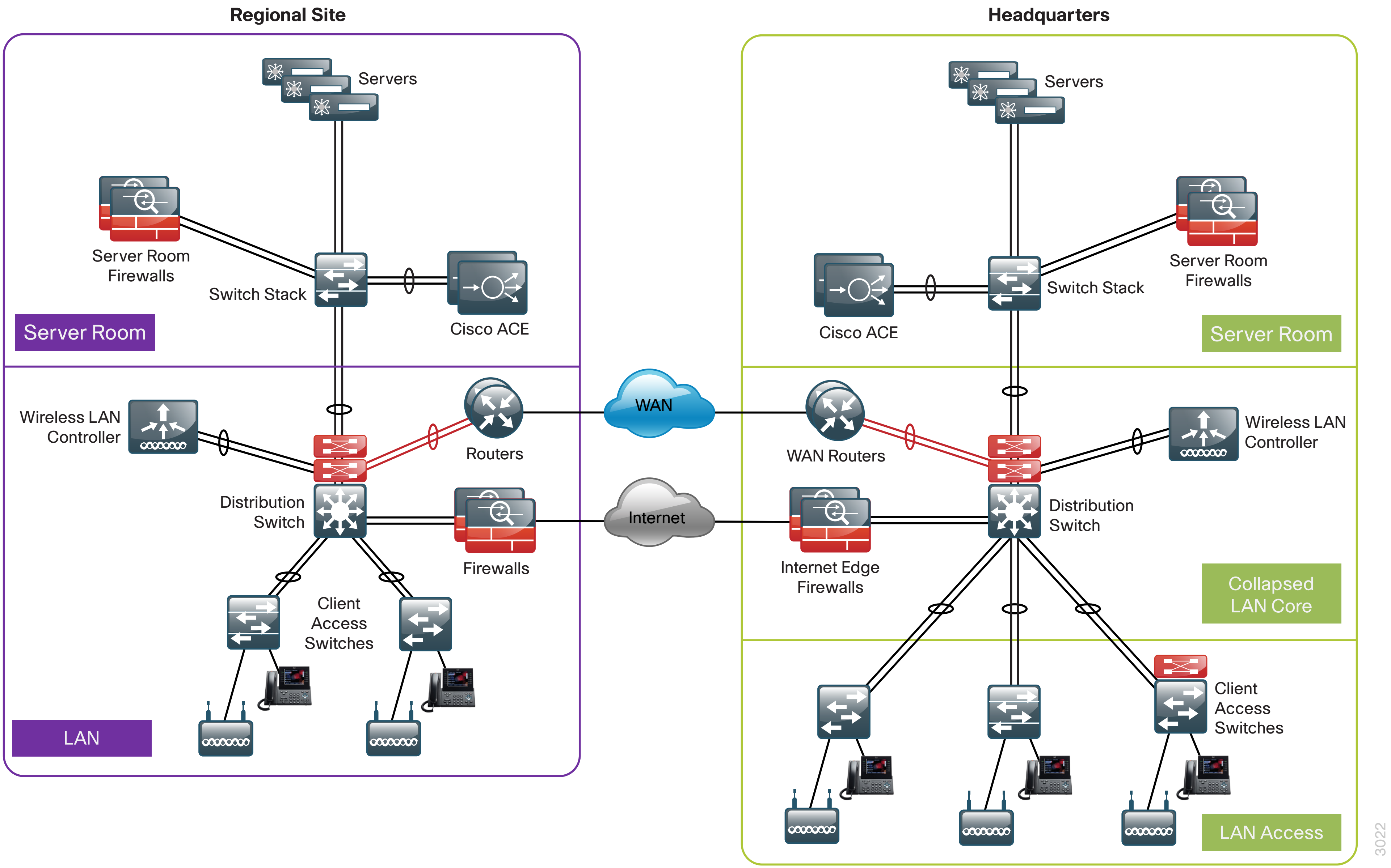
- "Server Room Ethernet LAN" includes guidance for the configuration of server ports on the switches, VLAN usage and trunking, resiliency, and connectivity to the LAN distribution layer or collapsed LAN core.
- "Server Room Security" focuses on the deployment of firewalls and intrusion prevention systems (IPS) to protect the information assets of your organization.
- The Appendix 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.

Server load balancing is a component of many server room deployments to enhance application resilience, balance the traffic and computing load handled by any one server, and offload server processing onto dedicated hardware. The *Cisco SBA Data Center—Advanced Server-Load Balancing Deployment Guide* is a standalone guide that is easily adapted to connect to the server room deployed in this guide.

As organizations scale beyond the server room to data centers with many application servers and larger storage environments, the *Cisco SBA—Data Center Deployment Guide* provides a methodology for a smooth transition.

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

Figure 1 - Typical Cisco SBA server room deployment scenarios



Business Overview

The *Cisco SBA—Data Center Server Room Deployment Guide* is designed to address five primary needs of organizations:

- Provide reliable access to organization resources
- Provide a smaller organization with a primary server room
- Provide a larger organization with a remote-site server room design to serve a large office or regional facility
- Secure the organizations' critical data
- Reduce operational costs

Reliable Access to Organization Resources

Data networks are critical to an organization's ability to operate and compete. Online workforce-enablement tools only offer benefit if the data network provides reliable access to information resources. Collaboration tools and content distribution rely on high-speed, low-latency network infrastructure to provide an effective user experience. Email, payroll systems, resource planning systems, and even print services must be available for the organization to operate. However, as networks become more complex, the risk increases that they will -lose availability or suffer poor performance due to inadequate design, configuration errors, maintenance and upgrade outages, or hardware and software faults. The design and methods used in this deployment guide were created to minimize these risks.

Primary Server Room for Smaller Organizations

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.

Remote-Site Server Room for Regional Locations

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 to focus on geographic and business requirements. These remote-site locations often require an IT environment for their local servers to provide high availability and security for the applications being used. The *Server Room Deployment Guide* provides a foundation for housing those applications and servers in a secure and resilient manner.

Securing the Organization's Critical Data

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

Reduced Operational Costs

Organizations constantly pursue opportunities to reduce network operational costs, while maintaining the network's effectiveness for end users. Operational costs include not only the cost of the physical operation (power, cooling, etc.), but also the labor cost required to staff an IT department that monitors and maintains the network. Additionally, network outages and performance issues impose costs that are more difficult to quantify, in the form of loss of productivity and interruption of business continuity. Centralizing the IT servers in a controlled environment with a reliable network can lower the risk of unplanned and lengthy outages that prevent users from accessing their applications.

The network provided by this deployment guide offers network resilience in its ability to tolerate failure or outage of portions of the network, along with a sufficiently robust—yet simple—design that staff should be able to operate, troubleshoot, and return to service in the event of a network outage.

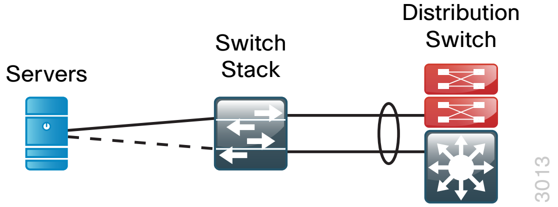
Technical Overview

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 3750-X Series and Cisco Catalyst 3560-X Series switches. Cisco Catalyst 3750-X offers flexible port density and server port connection speeds from 10 Mb Ethernet to 1 Gigabit Ethernet. With a Cisco 3750-X 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 3750-X provides platform resilience when stacked through Cisco StackWise Plus, which allows the control plane for the server room Ethernet switches to reside on either of the 3750-X switches and fail over in the event of a failure. Cisco StackPower on the 3750-X switch provides the ability to spread the power load over multiple power supplies in each chassis for diversity and resilience. The Cisco Catalyst 3560-X 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



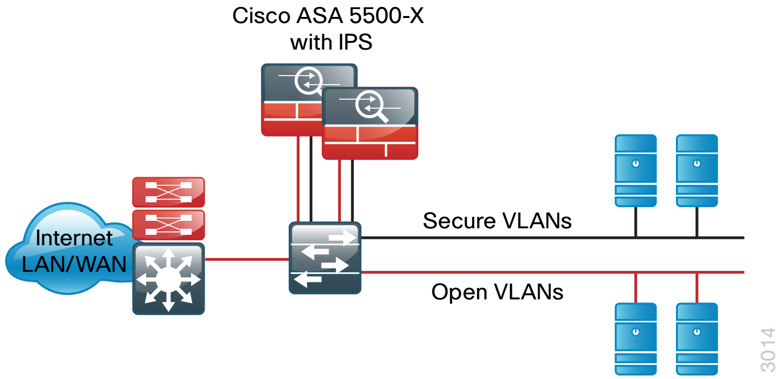
Both the server room and the client LAN access methods connect devices to the network; the difference between the two methods that changes the switch model is the requirement in the LAN access for Power over Ethernet (PoE). Although PoE-capable devices are not typical in the server room, using PoE-capable 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 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 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 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 is highly configurable to allow the maximum flexibility in meeting a specific security policy.

Server Load Balancing

Application performance and availability directly affect employee productivity and the bottom line of an organization. As organizations do business on a global level, it becomes even more important to address application availability and performance issues to ensure achievement of business processes and objectives.

Server load balancers (SLBs) spread the load across servers to improve their response to client requests, improve application response and availability, and increase the productivity of organizations that rely on network-based applications to conduct business.

Cisco Application Control Engine (ACE) is the latest SLB offering from Cisco for Layer 4 through Layer 7 switching, TCP processing offload, Secure Sockets Layer (SSL) offload, compression, and various other acceleration technologies. When server load balancing is required in your server room, we recommend the Cisco ACE 4710 appliance for use with the Cisco SBA design. Please refer to the *Cisco SBA—Data Center Advanced Server-Load Balancing Deployment Guide* for details on deploying server load balancing for your server room.

Notes

Server Room Ethernet LAN

Business Overview

Employee productivity depends on the ability to access applications and services necessary to do their job quickly and efficiently. Consistent and reliable access to the servers that support the applications that drive the organization is critical to ensure customer satisfaction and the success of the overall organization. Whether the servers that support your business applications are located at a headquarters building or a remote site, when critical applications are riding on those servers you require a resilient network to ensure access to the information and services.

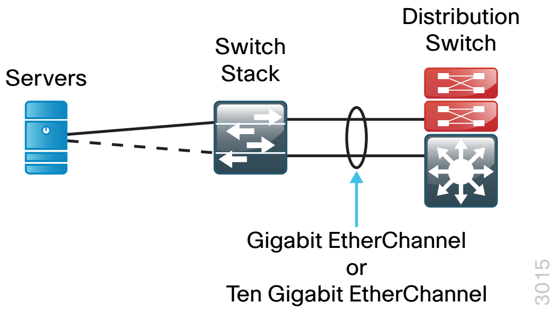
Cisco SBA recognizes the importance of the server room facility and its importance in the function of the overall organization. The design provides a small, yet resilient and scalable, Ethernet LAN foundation to connect the application servers to the users located throughout the rest of the organization's network. As organizations scale beyond the server room to data centers with many application servers and larger storage environments, the *Cisco SBA—Data Center Deployment Guide* provides a methodology for a smooth transition.

Technical Overview

In Cisco SBA, 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 3560-X standalone switch and Cisco Catalyst 3750-X Series stackable Ethernet LAN switches, with 10/100/1000 support to accommodate a wide range of server Ethernet interface speeds.

The Cisco StackWise Plus feature of Cisco Catalyst 3750-X 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 3750-X switches in a stack provide automated control plane failover in the event that the master switch experiences an issue. The option of dual power supplies and Cisco StackPower with the Catalyst 3750-X Series switches provides more resilience to the server room design. Cisco Catalyst 3560-X does not provide the same level of resilience as Cisco Catalyst 3750-X, but is suitable for single connected servers and less-critical systems.

Figure 4 - Cisco Catalyst 3750-X server room switch with EtherChannel uplinks



In the Cisco SBA design, the server room switches are connected to the core with an EtherChannel so that two 1-Gigabit Ethernet ports combine to make a single 2-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; or, if you require very high bandwidth, you can use 10-Gigabit Ethernet links to connect the appropriate core switch ports to 10-Gigabit ports on uplink modules installed in the server room switches.

Deployment Details

This section includes the procedures you need to perform to configure your server room Ethernet LAN connectivity. As you review the *Server Room Deployment Guide*, you may find it useful to understand Table 1, which lists the IP addressing and VLAN assignments used in this deployment. Your design requirements for IP addressing and VLAN numbering may differ.

Table 1 - Deployment guide addressing

VLAN	IP address range	Usage
148	10.8.48.x /24	Server VLAN #1
149	10.8.49.x /24	Server VLAN #2
115	10.8.15.x /25	Management VLAN from LAN core

Process

Configuring the Server Room Ethernet LAN

1. Configure global QoS settings
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 3560-X server room switch or a stack of two Catalyst 3750-X switches used for the server room Ethernet LAN.

Procedure 1 Configure global QoS settings

Step 1: Because AutoQoS may not be configured on this device, manually configure the global quality of service (QoS) sttings by entering the following commands. To make consistent deployment of QoS easier, the procedure defines a macro that you will use in later procedures to apply the platform-specific QoS configuration.

```
mls qos map policed-dscp 0 10 18 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 
51 52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58 
59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 
41 42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40
41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18
19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28
29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38
39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50
51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58
59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 
4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 
13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 3200
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
```

```
macro name EgressQoS
mls qos trust dscp
queue-set 1
srr-queue bandwidth share 1 30 35 5
priority-queue out
@
```

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 2 - 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	10.8.48.10
Cisco Access Control System (ACS) server	10.8.48.15
Network Time Protocol (NTP) server	10.8.48.17

Step 1: Configure the device host name to make it easy to identify the device.

```
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: 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 6: 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 10.8.48.10
```

Step 7: Configure device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) Protocol are secure replacements for the HTTP and Telnet protocols. They use 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 unsecure protocols—Telnet and HTTP—are turned off.

Specify the **transport preferred none** command on vty lines 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.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
  transport preferred none
```

Step 8: Enable Simple Network Management Protocol (SNMP) in order to allow the network infrastructure devices to be managed by a network management system (NMS),and then configure SNMPv2c both for a read-only and a read/write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Step 9: 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 10.8.48.0/24 network will be able to access the device via SSH or SNMP.

```
access-list 55 permit 10.8.48.0 0.0.0.255
line vty 0 15
  access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 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 10: Configure the local login and password

The local login account and password provide basic device access authentication 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 c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

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

Step 11: 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 10 on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
tacacs server TACACS-SERVER-1
address ipv4 10.8.48.15
key SecretKey
```

```
!
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
```

Reader Tip

The AAA server used in this architecture is Cisco ACS. For details about Cisco ACS configuration, see the *Cisco SBA—Borderless Networks Device Management Using ACS Deployment Guide.*

Step 12: 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 10.8.48.17
!
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 Cisco SBA 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 assign an IP default gateway.

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

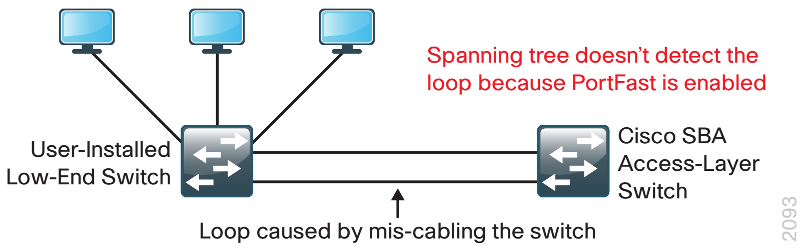
Step 3: Configure bridge protocol data unit (BPDU) Guard globally. This protects PortFast-enabled interfaces by disabling the port if another switch is plugged into the port.

```
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


Spanning tree doesn't detect the loop because PortFast is enabled
User-Installed Low-End Switch
Cisco SBA Access-Layer Switch
Loop caused by mis-cabling the switch
2093

Example

```
vlan 148
name Server_VLAN_1
vlan 149
name Server_VLAN_2
vlan 115
name Management
!
interface vlan 115
ip address 10.8.15.61 255.255.255.128
no shutdown
ip default-gateway 10.8.15.1
```

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 global QoS settings," 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 7 mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

Step 2: Configure the 802.1Q trunk.

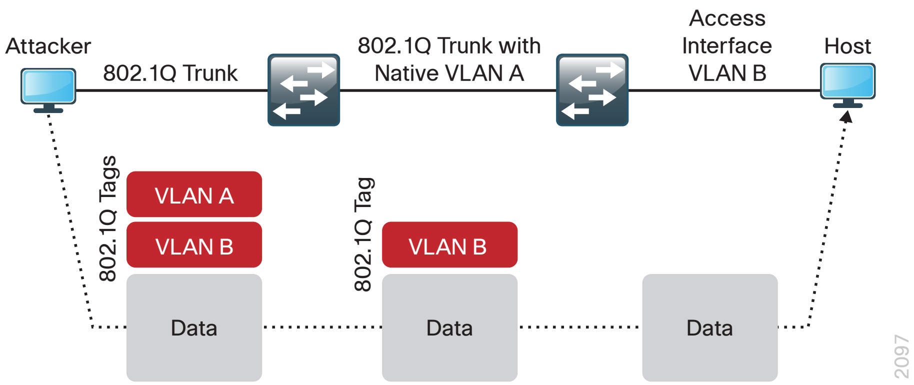
An 802.1Q trunk is used for the connection to this upstream device, which allows the uplink to provide Layer 3 services to all the VLANs defined on the server room switch. Prune the VLANs allowed on the trunk to only the VLANs that are active on the server room switch. When using EtherChannel, the interface 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 GigabitEthernet1/1/1
  description Link to LAN Core 1
interface GigabitEthernet2/1/1
  description Link to LAN Core 2
interface range GigabitEthernet 1/1/1, Gi 2/1/1
  channel-protocol lacp
  channel-group 7 mode active
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
!
interface Port-channel 7
  description EtherChannel Link to LAN Core
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 148-149,115
  switchport mode trunk
  logging event link-status
  no shutdown
!
vlan 999
!
interface Port-channel 7
 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: 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.

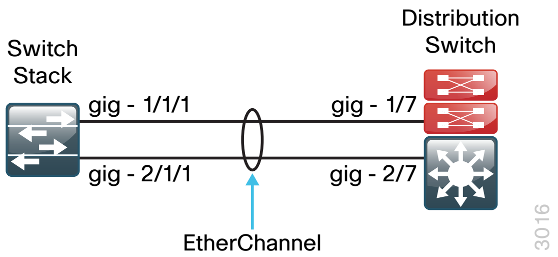
Step 4: Save the running configuration that you have entered so it will be used as the startup configuration file when your switch is rebooted or power-cycled.

```
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 Cisco SBA LAN distribution layer 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
```

Tech Tip

Cisco Catalyst 3750-X requires the **switchport trunk encapsulation dot1q** command.

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]
  ip pim sparse-mode
  no shutdown
```

Example

```
vlan 148
name Server_VLAN_1
vlan 149
name Server_VLAN_2
!
interface GigabitEthernet1/7
  description Link to Server Room port 1
interface GigabitEthernet2/7
  description Link to Server Room port 2
interface range GigabitEthernet 1/7, Gi 2/7
  channel-protocol lacp
  channel-group 7 mode active
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
!
interface Port-channel 7
  description EtherChannel Link to Server Room
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 148-149,115
  switchport mode trunk
  logging event link-status
  no shutdown
!
interface Port-channel 7
 switchport trunk native vlan 999
!
interface vlan 148
  ip address 10.8.48.1 255.255.255.0
  ip pim sparse-mode
  no shutdown
interface vlan 149
  ip address 10.8.49.1 255.255.255.0
  ip pim sparse-mode
  no shutdown
```

Server Room Security

Business Overview

When a formal data center is not yet required, 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 assure confidentiality and availability. Additionally, portions of networks in specific business sectors may be subject to industry or government regulations that mandate specific security controls 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.

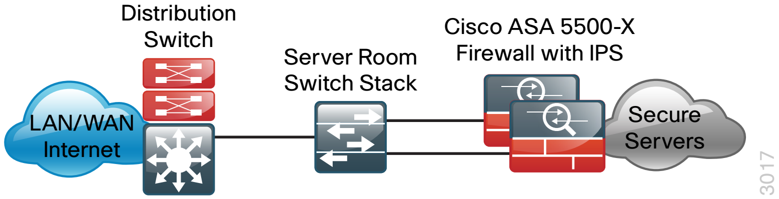
To protect the valuable electronic assets located in the server room, network security helps ensure the facility is protected from automated or human-operated snooping and tampering, and it helps prevent compromise of hosts by resource-consuming worms, viruses, or botnets.

While worms, viruses, and botnets pose a substantial threat to centralized data, particularly from the perspective of host performance and availability, servers must also be protected from employee snooping and unauthorized access. Statistics have consistently shown that the majority of data loss and network disruptions have occurred as the result of human-initiated activity (intentional or accidental) carried out within the boundaries of the business's network.

Technical 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 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/branch networks
- Business partner connections
- Campus networks
- Unprotected data center networks
- Other protected data center 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 leverages the Cisco SecureX Framework for 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.

The Cisco ASA firewalls are dual-homed to 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 Cisco SBA 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 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 primary device must be sized to 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 Cisco ASA itself has an issue or the IPS module becomes unavailable.

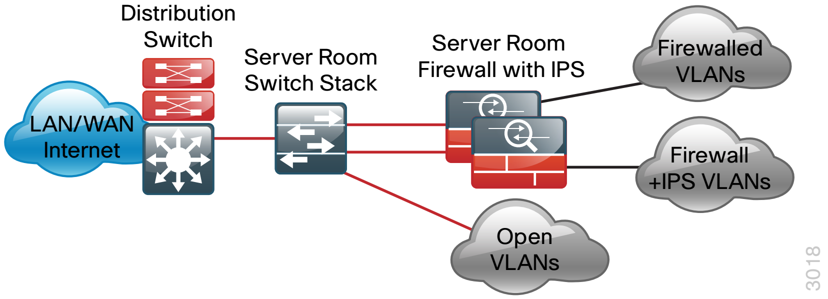
The Cisco ASAs are configured in routing mode; as a result, the secure network must be in a separate subnet from the client subnets. IP subnet allocation would be simplified if the Cisco ASA were deployed in transparent mode; however, hosts might inadvertently be connected to the wrong VLAN, where they 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 IDS mode so that they only monitor and alert for abnormal traffic. The IPS sensors can be deployed inline in IPS mode 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 like compliance requirements for IPS. The ability to run in IDS mode or IPS is highly configurable to allow the maximum flexibility in meeting a specific security policy.

Security Topology Design

The Cisco SBA 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

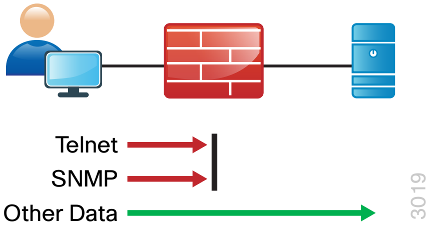
An organization should have an IT security policy as a starting point in defining its firewall policy. If there is no organization-wide security policy, it will be very difficult to define an effective policy for the organization while maintaining a secure computing environment.

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.

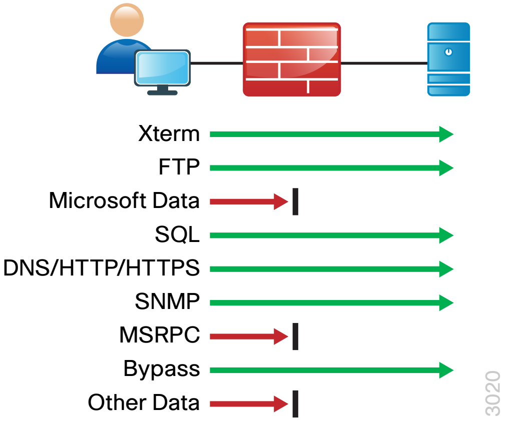
Network security policies can be broken down into two basic categories: whitelist policies and blacklist policies. A *blacklist policy* denies traffic that specifically poses the greatest risk to network resources.

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 assure 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 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 + 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).

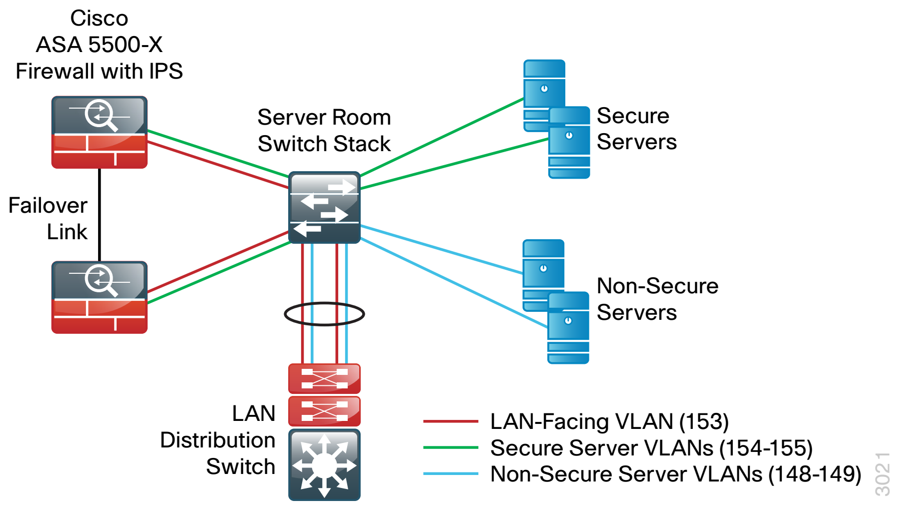
The performance needs in this design do not surpass the performance of a single Cisco ASA.

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

Cisco ASA is statically routed to the Cisco SBA LAN distribution on the outside interface 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 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

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

Table 3 - Server room firewall VLANs

VLAN	IP address	Trust state	Use
153	10.8.53.1 /25	Untrusted	Firewall to core LAN routing
154	10.8.54.X /24	Trusted	Firewall protected VLAN
155	10.8.55.X /24	Trusted	Firewall + IPS protected VLAN

Table 4 - Common network services used in the deployment examples

Service	Address
Domain name	cisco.local
Active Directory, DNS, DHCP server	10.8.48.10
Cisco ACS	10.8.48.15
NTP server:	10.8.48.17

Procedure 1 Configure the LAN distribution layer

Configure the LAN distribution layer or collapsed core switch providing Layer 3 routing for the server room Cisco ASAs' LAN-side (untrusted) interfaces and to forward traffic 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 10.8.53.1 255.255.255.128
  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 LAN distribution layer-switch to server-room switch EtherChannel link configured in Procedure 6, "Configure LAN distribution layer downlinks."

```
interface Port-channel 7
  switchport trunk allowed vlan add 153
```

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

```
ip route 10.8.54.0 255.255.255.0 Vlan 153 10.8.53.126
ip route 10.8.55.0 255.255.255.0 Vlan 153 10.8.53.126
```

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

```
ip access-list standard trusted_subnets
  permit 10.8.54.0 0.0.0.255
  permit 10.8.55.0 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 100
   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.

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

Step 1: Configure the untrusted and trusted VLANs.

```
vlan 153
name Firewall_Outside_VLAN
vlan 154
name Firewall_Secure_VLAN
vlan 155
name Firewall_IPS_Secure_VLAN
```

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 server room-switch to LAN distribution layer-switch EtherChannel link configured in Procedure 4, "Configure server room uplink ports."

```
interface Port-channel 7
  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 ASA will be on switch 1, and the second ASA will be on switch 2 of the Catalyst 3750-X stack.

```
interface GigabitEthernet1/0/23
 description SR-ASA5500a outside gi 0/3
!
interface GigabitEthernet2/0/23
 description SR-ASA5500b outside gi 0/3
!
interface range GigabitEthernet1/0/23,GigabitEthernet2/0/23
 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 GigabitEthernet1/0/24
 description SR-ASA5500a inside gi 0/0
!
interface GigabitEthernet2/0/24
 description SR-ASA5500b inside gi 0/0
!
interface range GigabitEthernet1/0/24,GigabitEthernet2/0/24
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 154-155
 switchport mode trunk
 spanning-tree portfast trunk
 macro apply EgressQoS
```

Process

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

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 5 - Cisco ASA 5500X firewall and IPS module addressing

ASA firewall failover status	ASA firewall IP address	IPS module IP address
Primary	10.8.53.126 /25	10.8.15.21 /24
Secondary	10.8.53.125 /25	10.8.15.22 /24

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 will appear 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: Select your anonymous monitoring preference.

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 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, **0**, will be applied automatically.

```
interface GigabitEthernet0/3
  nameif outside
  ip address 10.8.53.126 255.255.255.128 standby 10.8.53.125
  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 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, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

Reader Tip

The AAA server used in this architecture is Cisco Secure ACS. Configuration of Cisco Secure ACS is discussed in the *Cisco SBA—Borderless Networks Device Management Using ACS Deployment Guide*.

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 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 10.8.48.15 SecretKey
```

Step 2: Configure the appliance’s management authentication to use the TACACS+ server first and then 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
```

Caution

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 do not add sufficient value to justify the number of messages logged.

Step 1: Configure the NTP server IP address.

```
ntp server 10.8.48.17
```

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, 10.8.48.0/24).

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 unsecure protocols (Telnet and HTTP) are turned off.

SNMP is enabled to allow the network infrastructure devices to be managed by an 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 10.8.48.0 255.255.255.0 outside
ssh 10.8.48.0 255.255.255.0 outside
ssh version 2
```

Step 2: Configure the appliance to allow SNMP polling from the NMS.

```
snmp-server host outside 10.8.48.35 community [cisco]
snmp-server community [cisco]
```

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 10.8.54.1 255.255.255.0 standby 10.8.54.2
!
interface GigabitEthernet0/0.155
  vlan 155
  nameif SRVLAN155
  security-level 100
  ip address 10.8.55.1 255.255.255.0 standby 10.8.55.2
```

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: Configure a static route on the Cisco ASA pair pointing to the LAN distribution layer. The static route will point to the VLAN 153 SVI address configured in Step 2 of Procedure 1, "Configure the LAN distribution layer."

```
route outside 0.0.0.0 0.0.0.0 10.8.53.1 1
```

Process

Configuring Firewall High Availability

1. Configure HA on the primary Cisco ASA
2. Configure HA on the secondary Cisco ASA

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 (if the software module is installed). For failover to be enabled, the secondary 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 is replicated from the active to the standby unit though 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, 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 Cisco ASA

Step 1: Enable failover on the primary Cisco ASA, 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, you can 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.

On an appliance with low to average load, the poll times can be tuned down without performance impact.

```
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 10.8.53.130 255.255.255.252 
standby 10.8.53.129
```

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 Cisco ASA

Step 1: On the secondary Cisco ASA, enable failover and 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 10.8.53.130 255.255.255.252 
standby 10.8.53.129
```

Step 4: Enable the failover interface.

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

This step causes the Cisco ASA units to synchronize their configuration from the primary unit to the secondary.

Step 5: Verify standby synchronization between the Cisco ASA devices. On the command-line interface of the primary appliance, 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: Save your Cisco ASA firewall configuration on the primary Cisco ASA. 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. 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 provides the procedures necessary to 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 VLAN that requires firewall needs either a permissive (blacklist) or restrictive (whitelist) security policy.

Procedure 2 Deploy the appropriate security policy

Network security policy configuration is fairly arbitrary to suit the policy and management requirements of an organization. Thus, examples here should be used as a basis for security policy configuration.

Option 1. Deploy a whitelist security policy

A basic whitelist data-service policy can be applied to allow common business services such as HTTP, HTTPS, DNS, and other services typically seen in Microsoft-based networks.

Step 1: Control access so only specific hosts may be accessed.

```
object network BladeWeb1Secure
 host 10.8.54.100
 object network BladeWeb2Secure
 host 10.8.55.100
!
object network Secure-Subnets
 subnet 10.8.54.0 255.255.255.0
object network SecureIPS-Subnets
 subnet 10.8.55.0 255.255.255.0
!
object-group network Application-Servers
 description HTTP, HTTPS, DNS, MSExchange
 network-object object BladeWeb1Secure
 network-object object BladeWeb2Secure
!
object-group service MS-App-Services
 service-object tcp destination eq domain
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq netbios-ssn
 service-object udp destination eq domain
 service-object udp destination eq nameserver
 service-object udp destination eq netbios-dgm
 service-object udp destination eq netbios-ns
!
 access-list global_access extended permit object-group MS-
App-Services any object-group Application-Servers
```

Step 2: 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 10.8.48.224–255 are allowed SSH and SNMP access to server room subnets.

```
object network Mgmt-host-range
 range 10.8.48.224 10.8.48.254
object-group network SR_Secure_Subnet_List
 network-object object Secure-Subnets
 network-object object SecureIPS-Subnets
object-group service Mgmt-Traffic
 service-object tcp destination eq ssh
 service-object udp destination eq snmp
access-list global_access extended permit object-group Mgmt-Traffic object Mgmt-host-range object-group SR_Secure_Subnet_List
```

Step 3: If you want to allow access to an application for firewall policy troubleshooting, configure a bypass rule. A bypass rule allows wide-open access to hosts that are added to the appropriate network object group. The bypass rule must be carefully defined to avoid opening access to hosts or services that must otherwise be blocked. In a whitelist policy, the bypass rule is typically disabled, and it is only called into use whenever firewall policy troubleshooting is required to allow access to an application.

The following policy defines two hosts and applies them to the bypass rule.

```
object-group network Bypass-Rule
 description Open Policy for Server Access
 network-object object BladeWeb1Secure
 network-object object BladeWeb2Secure
access-list global_access extended permit ip any object-group Bypass-Rule
```

This disables the bypass rule:

```
access-list global_access extended permit ip any object-group Bypass-Rule  inactive
```

Tech Tip

The bypass rule group is useful for troubleshooting or providing temporary access to services on the host that must be opened for maintenance or service migration. It is typically disabled unless being used for troubleshooting.

Step 4: Save your Cisco ASA firewall configuration.

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

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.

Step 1: Allow SNMP queries and SSH requests for a specific address range that will be 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.

```
object network Secure-Subnets
 subnet 10.8.54.0 255.255.255.0
object network SecureIPS-Subnets
 subnet 10.8.55.0 255.255.255.0
!
object network Mgmt-host-range
 range 10.8.48.224 10.8.48.254
object-group network SR_Secure_Subnet_List
 network-object object Secure-Subnets
 network-object object SecureIPS-Subnets
object-group service Mgmt-Traffic
 service-object tcp destination eq ssh
 service-object udp destination eq snmp
access-list global_access extended permit object-group Mgmt-Traffic object Mgmt-host-range object-group SR_Secure_Subnet_List
```

Step 2: Block Telnet, SSH, and SNMP to all other hosts.

```
access-list global_access extended deny object-group Mgmt-
Traffic any any
```

Step 3: Configure a rule to permit application traffic through to the servers in the secure server subnets, that was not specifically denied by the blacklist rule in Step 2. Note that logging is disabled on this policy to prevent the firewall from having to log all accesses to the server network.

```
access-list global_access extended permit ip any object-group
DC_Secure_Subnet_List log disable
```

Step 4: Save your Cisco ASA firewall configuration.

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

Process

Deploying Firewall Intrusion Prevention System (IPS)

1. Configure the LAN switch access port
2. Initialize the IPS module
3. Apply initial configuration
4. Complete basic configuration

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 data center design using a Cisco ASA 5500-X 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 GigabitEthernet1/0/20
 description SR-5500X-IPSa
!
interface GigabitEthernet2/0/20
 description SR-5500X-IPSb
!
Interface range GigabitEthernet1/0/20, Gigabit Ethernet 2/0/20
 switchport
 switchport access vlan 115
 switchport mode access
 switchport host
```

Procedure 2 Initialize the IPS module

When a Cisco ASA 5500-X with IPS is initially deployed, the software IPS module may not be initialized, resulting in the 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 and you can skip to Procedure 3.

```
SR-ASA5500X# show module ips detail
Getting details from the Service Module, please wait...

Card Type:          ASA 5545-X IPS Security Services Processor
Model:              ASA5545-IPS
Hardware version:   N/A
Serial Number:      FCH161170MA
Firmware version:   N/A
Software version:   7.1(4)E4
MAC Address Range:  c464.1339.a354 to c464.1339.a354
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.1(4)E4
Data Plane Status:  Up
Status:             Up
```

Step 3: 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:      FCH16097J3F
Firmware version:   N/A
Software version:
MAC Address Range:  c464.1339.2cf1 to c464.1339.2cf1
Data Plane Status:  Not Applicable
Status:             Unresponsive   No Image Present
...
```

Step 4: Verify that you have the correct IPS image on the Cisco ASA firewall disk0:.

```
SR-ASA5500X# dir
Directory of disk0:/
2      drwx  4096        17:06:58 Apr 15 2012  log
5      drwx  4096        17:07:12 Apr 15 2012  crypto_archive
14     drwx  4096        17:07:14 Apr 15 2012  coredumpinfo
115    -rwx  34523136    17:08:56 Apr 15 2012  asa861-smp-k8.
bin
116    -rwx  42637312    17:11:28 Apr 15 2012  IPS-SSP_5525-
K9-sys-1.1-a-7.1-4-E4.aip
```

Reader Tip

Software installation and upgrade information for Cisco ASA-5500X Series can be found at:
http://www.cisco.com/en/US/partner/docs/security/asa/asa84/release/notes/asarn86.html

Step 5: Configure the IPS module to load the software on disk0: and boot with that software.

```
SR-ASA5500X# sw-module module ips recover configure image 
disk0:/IPS-SSP_5525-K9-sys-1.1-a-7.1-4-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 6: 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.

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 will be 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: Mon May 21 06:08:50 2012
```

```
Setup Configuration last modified: Mon May 21 05:48:45 2012
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]:
10.8.15.21/25,10.8.15.1
```

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: 10.8.48.0/24
```

Step 7: Accept the default answer (no) for the next three questions.

```
Use DNS server for Global Correlation? [no]:
Use HTTP proxy server for Global Correlation? [no]:
Modify system clock settings?[no]:
```

Note the following:

- Global correlation is disabled until later in the configuration process.
- 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: Accept the default answer (off) for the option to participate in the SensorBase Network.

```
Participation in the SensorBase Network allows Cisco to
collect aggregated statistics about traffic sent to your IPS.
SensorBase Network Participation level? [off]:
```

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 10.8.15.21/25,10.8.15.1
host-name SR-IPS-A
telnet-option disabled
access-list 10.8.0.0/16
ftp-timeout 300
no login-banner-text
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
http-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 off
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 this procedure, Step 1 through Step 10, for the IPS sensor installed in the other Cisco ASA chassis. In Step 4, assign a unique host name (SR-IPS-B), and in Step 5 be sure to use a different IP address (10.8.15.22) on the other sensor's management interface.

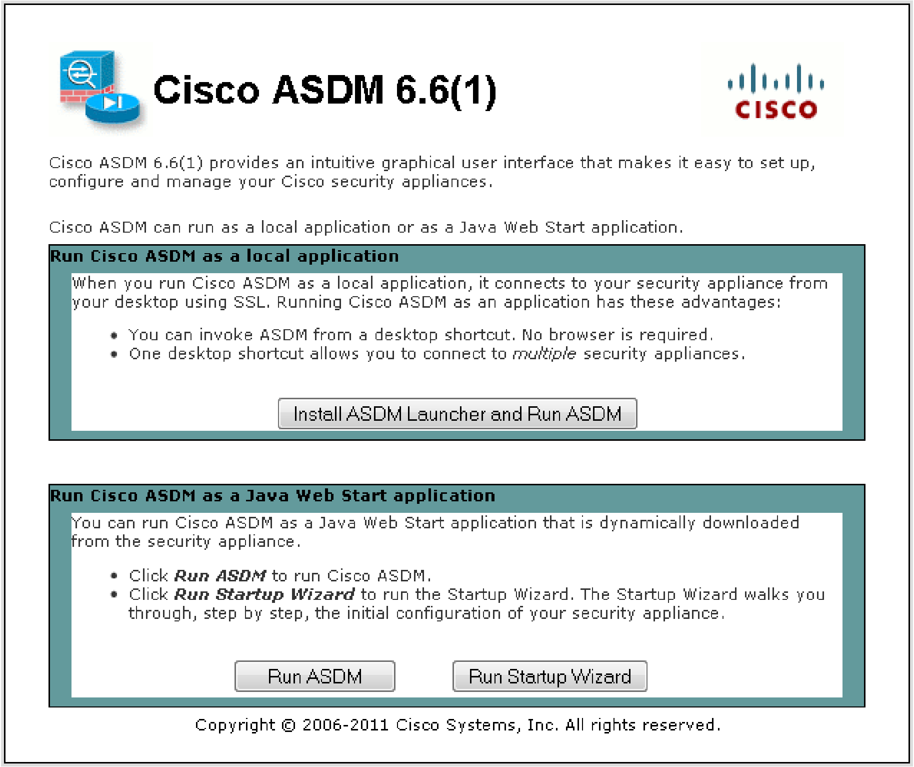
Procedure 4 Complete basic configuration

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 remaining tasks in order to configure 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 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: Connect to the sensor by navigating to the Cisco ASA firewall outside interface programmed in Procedure 2, "Configure the firewall outside port," using a secure HTTP session (https://10.8.53.126), and then click **Run ASDM**, which will run ASDM from a Java Web Start application; alternatively, you can choose **Install ASDM Launcher and Run ASDM** which will allow you to connect to multiple security appliances.



Cisco ASDM 6.6(1)

Cisco ASDM 6.6(1) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.

Cisco ASDM can run as a local application or as a Java Web Start application.

Run Cisco ASDM as a local application

When you run Cisco ASDM as a local application, it connects to your security appliance from your desktop using SSL. Running Cisco ASDM as an application has these advantages:

- You can invoke ASDM from a desktop shortcut. No browser is required.
- One desktop shortcut allows you to connect to *multiple* security appliances.

Run Cisco ASDM as a Java Web Start application

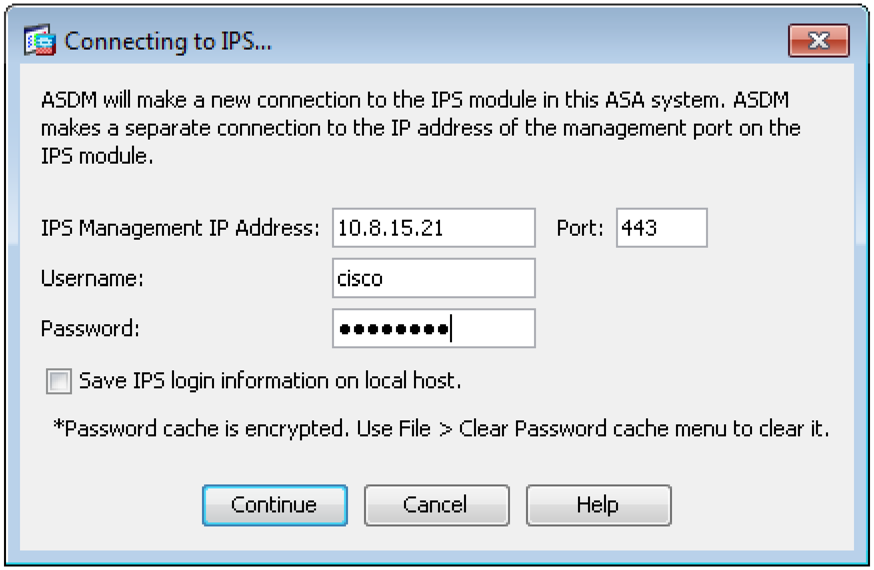
You can run Cisco ASDM as a Java Web Start application that is dynamically downloaded from the security appliance.

- Click ***Run ASDM*** to run Cisco ASDM.
- Click ***Run Startup Wizard*** to run the Startup Wizard. The Startup Wizard walks you through, step by step, the initial configuration of your security appliance.

Copyright © 2006-2011 Cisco Systems, Inc. All rights reserved.

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 required connection information for IPS-A access, and then click **Continue**.



Connecting to IPS...

ASDM will make a new connection to the IPS module in this ASA system. ASDM makes a separate connection to the IP address of the management port on the IPS module.

IPS Management IP Address: 10.8.15.21 Port: 443

Username: cisco

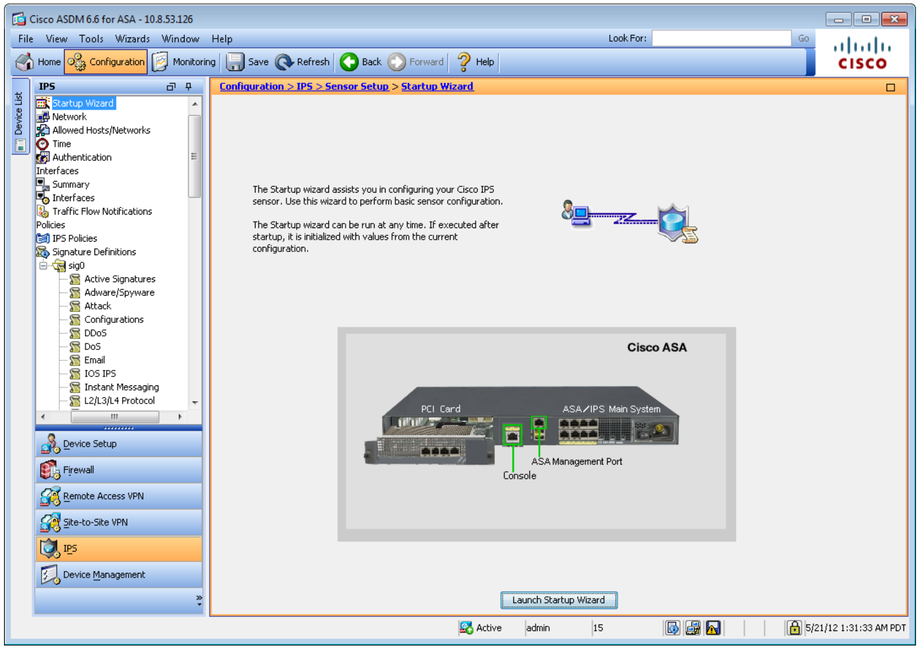
Password: ●●●●●●●●●

□ Save IPS login information on local host.

*Password cache is encrypted. Use File > Clear Password cache menu to clear it.

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**.



Cisco ASDM 6.6 for ASA - 10.8.53.126

Configuration > IPS > Sensor Setup > Startup Wizard

The Startup wizard assists you in configuring your Cisco IPS sensor. Use this wizard to perform basic sensor configuration.

The Startup wizard can be run at any time. If executed after startup, it is initialized with values from the current configuration.

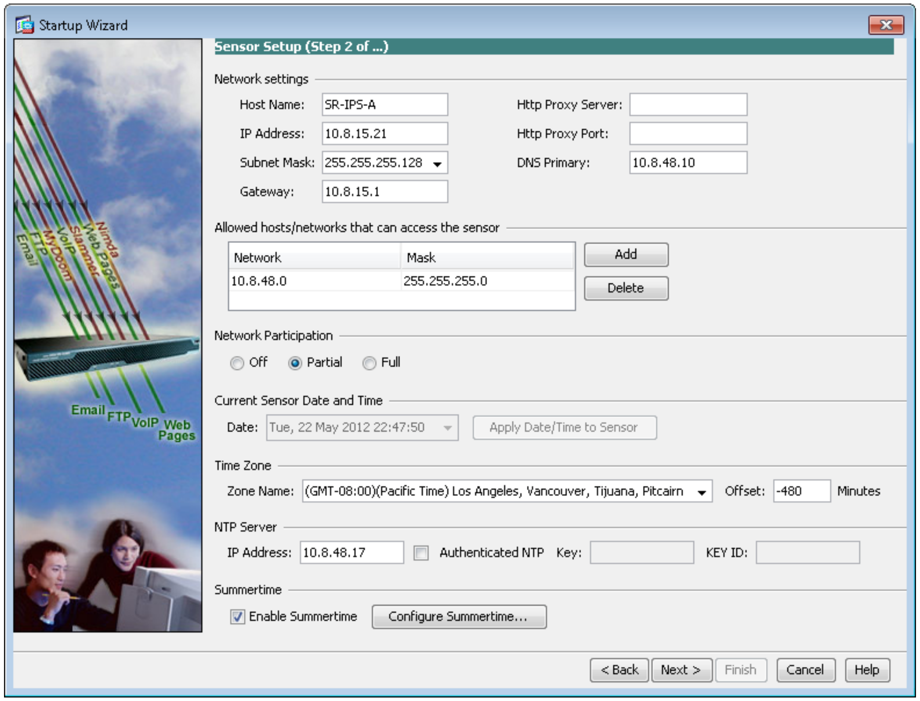
Step 5: Review the Startup Wizard Introduction, and then click **Next**.

Step 6: On the Sensor Setup page, configure the DNS server address, time zone, and NTP server address, and under Network Participation, select **Partial**.

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.

Step 7: If necessary for your time zone, select **Enable Summertime**, ensure that **Authenticated NTP** is not selected, and then click **Next**.



Startup Wizard

Sensor Setup (Step 2 of ...)

Network settings

Host Name:	SR-IPS-A	Http Proxy Server:	
IP Address:	10.8.15.21	Http Proxy Port:	
Subnet Mask:	255.255.255.128	DNS Primary:	10.8.48.10
Gateway:	10.8.15.1		

Allowed hosts/networks that can access the sensor

Network	Mask
10.8.48.0	255.255.255.0

Network Participation

○ Off ● Partial ○ Full

Current Sensor Date and Time

Date: Tue, 22 May 2012 22:47:50

Time Zone

Zone Name: (GMT-08:00)(Pacific Time) Los Angeles, Vancouver, Tijuana, Pitcairn Offset: -480 Minutes

NTP Server

IP Address: 10.8.48.17 □ Authenticated NTP Key: KEY ID:

Summertime

☑ Enable Summertime

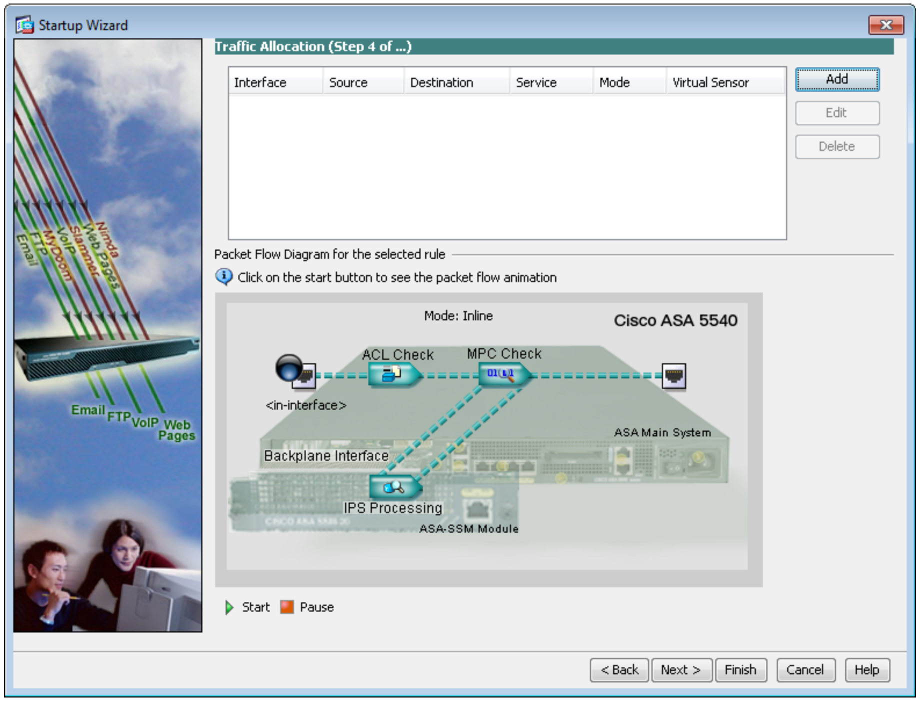
Step 8: Review Network Participation Disclaimer, and then click **Agree**.

You must now decide the sensor mode. "For more information about IPS versus IDS mode, see the introduction to this process."

This procedure assigns IPS mode.

Step 9: On the Startup Wizard: Virtual Sensors page, click **Next**.

Step 10: On the Startup Wizard: Traffic Allocation page, click **Add**.



Startup Wizard

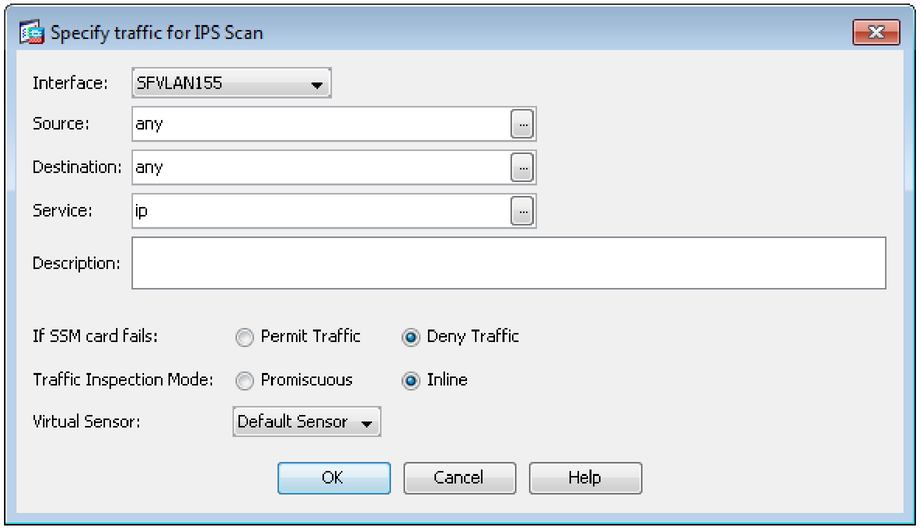
Traffic Allocation (Step 4 of ...)

Interface	Source	Destination	Service	Mode	Virtual Sensor

Packet Flow Diagram for the selected rule

Click on the start button to see the packet flow animation

Step 11: In the Specify traffic for IPS Scan window, in the Interface list, choose **SRVLAN155** for IPS inspection, and next to Traffic Inspection Mode, select **Inline**, and then click **OK.**



Specify traffic for IPS Scan

Interface: SFVLAN155

Source: any

Destination: any

Service: ip

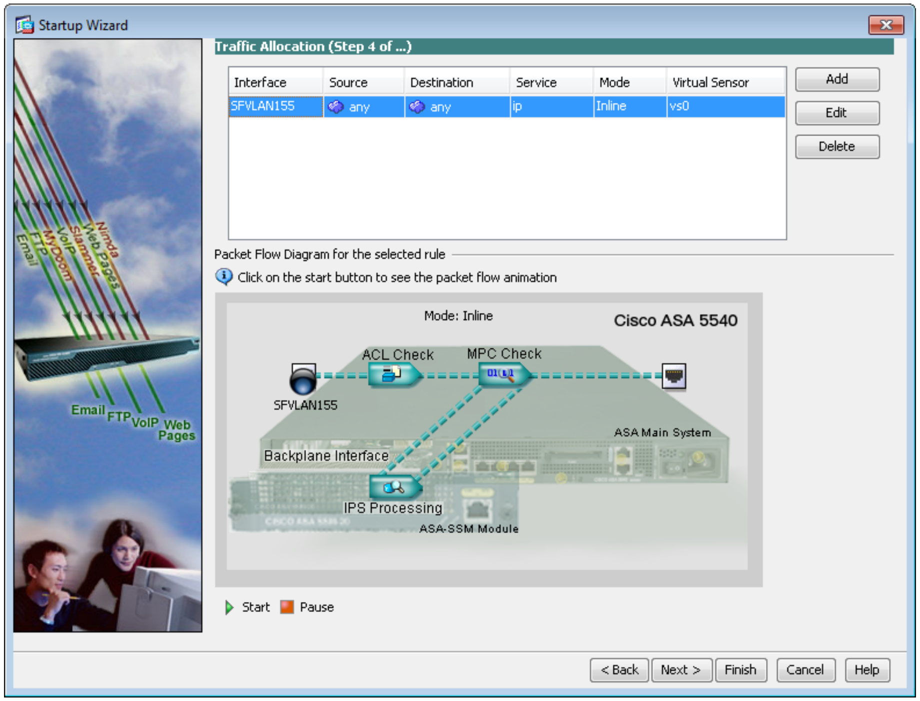
Description:

If SSM card fails: ○ Permit Traffic ● Deny Traffic

Traffic Inspection Mode: ○ Promiscuous ● Inline

Virtual Sensor: Default Sensor

Step 12: On the Traffic Allocation page, in the Packet Flow Diagram for the selected Rule panel, click **Start** to verify traffic allocation path. The animation will illustrate a packet being copied to the IPS module and the egress interface. The animation may display an incorrect platform compared to the one you are configuring, however this will not cause any issue with operation.



Startup Wizard

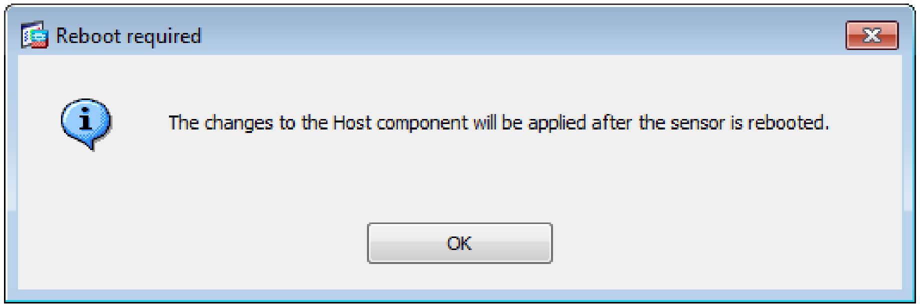
Traffic Allocation (Step 4 of ...)

Interface	Source	Destination	Service	Mode	Virtual Sensor
SFVLAN155	any	any	ip	Inline	vs0

Packet Flow Diagram for the selected rule

Click on the start button to see the packet flow animation

Step 13: On the Startup Wizard page, click **Finish**, and then click **Yes** when you are prompted to commit your changes to the sensor.



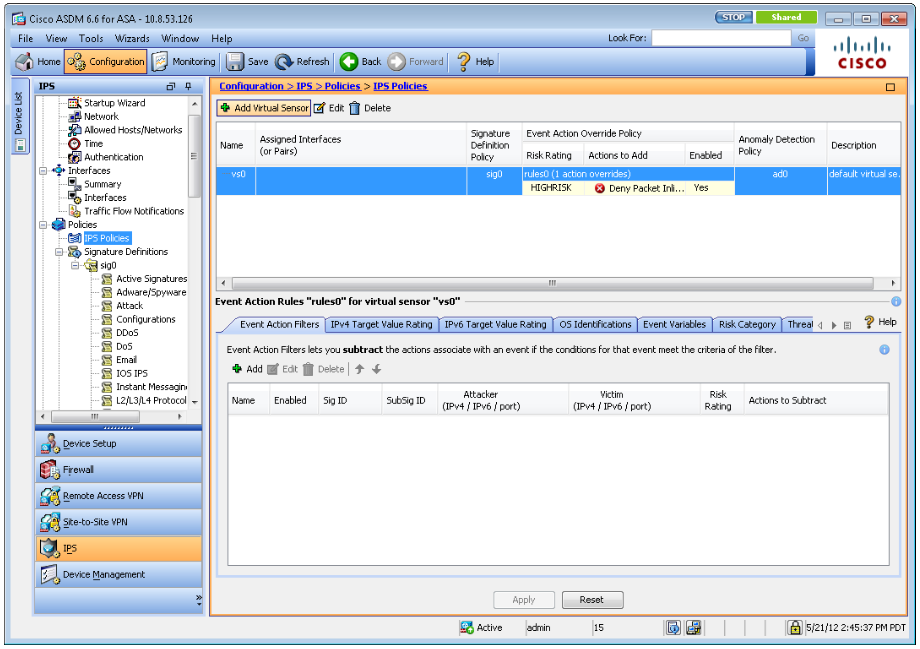
Reboot required

The changes to the Host component will be applied after the sensor is rebooted.

The system notifies you that the IPS sensor requires a reboot to apply the new configuration. Click **OK**, and proceed to the next step, and delay the reboot until the end of this procedure.

Step 14: Navigate to **Policies > IPS Policies.**

Step 15: In the top work pane next to Add Virtual Sensor, click **Edit**.



Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Event Action Override Policy			Anomaly Detection Policy	Description
			Risk Rating	Actions to Add	Enabled		
vs0		sig0	rules0 (1 action overrides)			ad0	default virtual se...
			HIGHRISK	☒ Deny Packet Inli...	Yes		

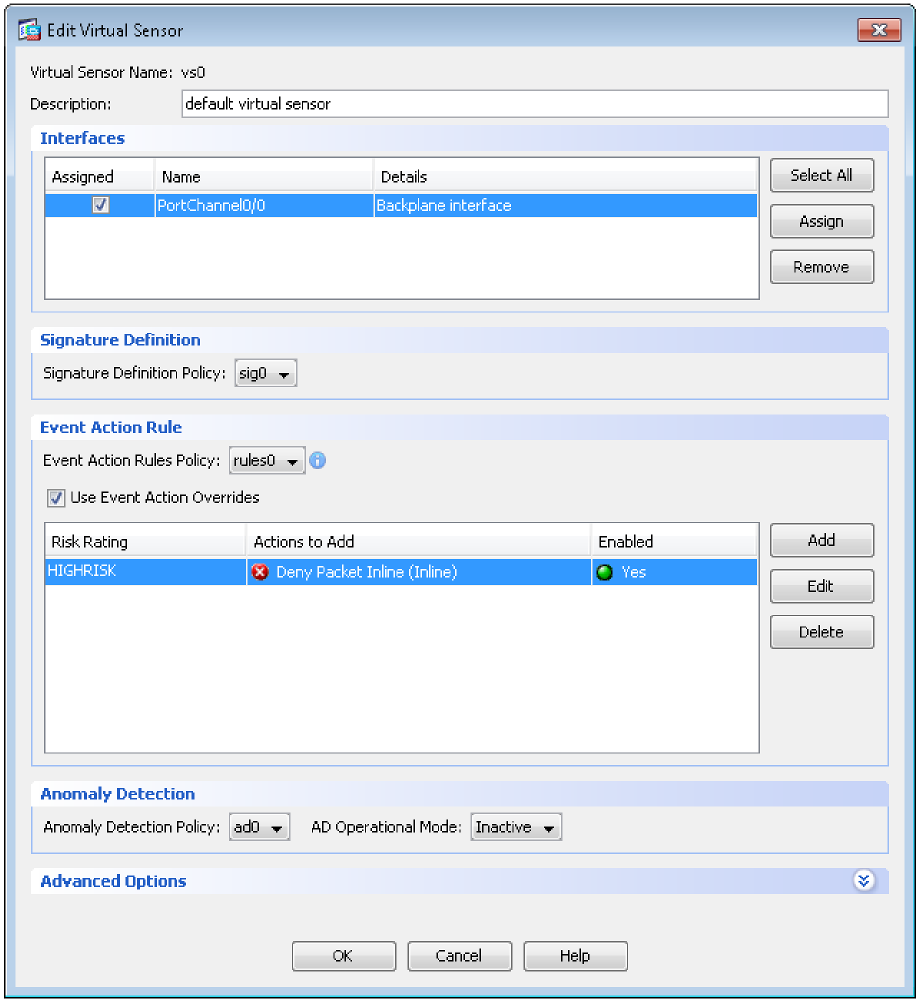
Event Action Rules "rules0" for virtual sensor "vs0"

Event Action Filters lets you **subtract** the actions associate with an event if the conditions for that event meet the criteria of the filter.

Name	Enabled	Sig ID	SubSig ID	Attacker (IPv4 / IPv6 / port)	Victim (IPv4 / IPv6 / port)	Risk Rating	Actions to Subtract

Active admin 15 5/21/12 2:45:37 PM PDT

Step 16: In the Edit Virtual Sensor window, in the Interfaces panel, select **Assigned,** and then click **OK**.



Virtual Sensor Name: vs0

Description: default virtual sensor

Interfaces

Assigned	Name	Details
☑	PortChannel0/0	Backplane interface

Signature Definition

Signature Definition Policy: sig0

Event Action Rule

Event Action Rules Policy: rules0

☑ Use Event Action Overrides

Risk Rating	Actions to Add	Enabled
HIGHRISK	☒ Deny Packet Inline (Inline)	● Yes

Anomaly Detection

Anomaly Detection Policy: ad0 AD Operational Mode: Inactive

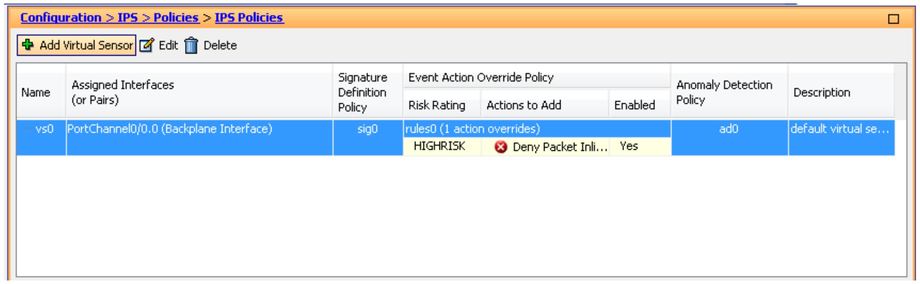
Step 17: Click **Apply** in the work pane. This saves your changes.

On the main panel, note that there is an Event Action Override to Deny Packet Inline for all High Risk events.

Step 18: In the main panel Event Action Rules work pane, click the **Risk Category** tab for information about what High Risk means and the current risk categories and ranges.

In the default case, High Risk means events that have a Risk Rating from 90 to 100. In this deployment, you reduce the risk of dropping non-malicious traffic by editing the Deny Packet action such that it triggers only when the Risk Rating is 100. This means that the sensor will now use the Deny Packet action only on events with a Risk Rating equal to 100, which only occurs when the most accurate, highest-risk signatures fire.

Step 19: In the Virtual Sensor panel, right-click the **vs0** entry, and then click **Edit**.



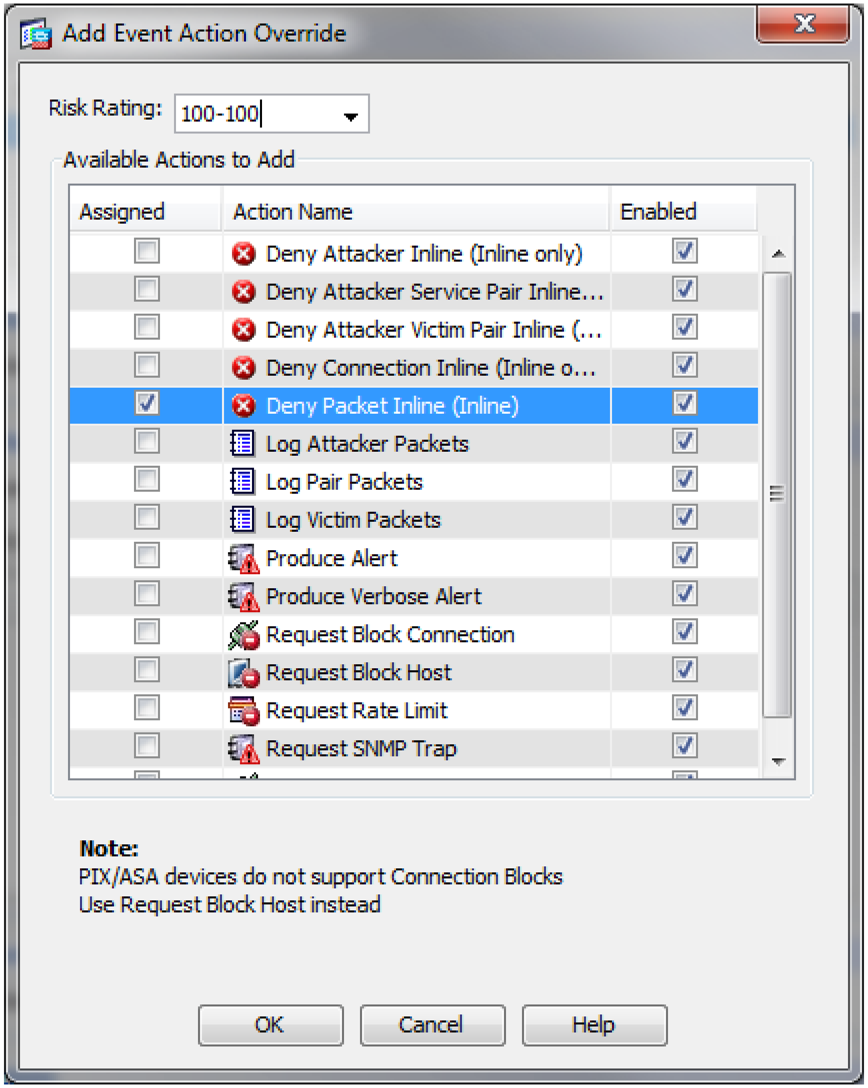
Configuration > IPS > Policies > IPS Policies

Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Event Action Override Policy			Anomaly Detection Policy	Description
			Risk Rating	Actions to Add	Enabled		
vs0	PortChannel0/0.0 (Backplane Interface)	sig0	rules0 (1 action overrides)			ad0	default virtual se…
			HIGHRISK	Deny Packet Inli…	Yes		

Step 20: In the Event Action Rule work pane, click **Deny Packet Inline Override**, and then click **Delete**.

Step 21: Click **Add**. This adds a new override.

Step 22: In the Risk Rating field, enter a value of **100-100**, select **Deny Packet Inline**, and then click **OK.**



Add Event Action Override

Risk Rating: 100-100

Available Actions to Add

Assigned	Action Name	Enabled
□	Deny Attacker Inline (Inline only)	☑
□	Deny Attacker Service Pair Inline…	☑
□	Deny Attacker Victim Pair Inline (…	☑
□	Deny Connection Inline (Inline o…	☑
☑	Deny Packet Inline (Inline)	☑
□	Log Attacker Packets	☑
□	Log Pair Packets	☑
□	Log Victim Packets	☑
□	Produce Alert	☑
□	Produce Verbose Alert	☑
□	Request Block Connection	☑
□	Request Block Host	☑
□	Request Rate Limit	☑
□	Request SNMP Trap	☑

Note:
PIX/ASA devices do not support Connection Blocks
Use Request Block Host instead

Step 23: Click **OK** in the **Edit Virtual Sensor** workpane, and then click **Apply.**

Step 24: Navigate to **IPS > Reboot Sensor**, click **Reboot Sensor**, and then click **OK** again.

The GUI console will disconnect from the IPS session and request that you log in to the Cisco ASDM session on the Cisco ASA firewall again. The primary ASA firewall will now switch to a standby state because it has lost connectivity to the IPS module in the primary ASA.

Step 25: Log in to the Cisco ASDM session on the firewall using the same IP address and credentials you used in Step 1 of this procedure. You are now logging in to the secondary, active ASA firewall.

Step 26: Repeat Step 3 through Step 24, using the SR-IPS-B IP address (10.8.15.22).

There is no configuration synchronization between the two sensors.

Notes

Appendix A: Product List

Server Room

Functional Area	Product Description	Part Numbers	Software
Stackable Ethernet Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 ports	WS-C3750X-48T-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Ethernet Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 ports	WS-C3560X-48T-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 ports	WS-C3560X-24T-S	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 8.6(1)1 IPS 7.1(4)E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	

Appendix B: Configuration Examples

Cisco Catalyst 3750-X Switch Stack

The server room Cisco Catalyst 3750-X 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
!
hostname SR3750Xy
!
boot-start-marker
boot-end-marker
!
enable secret 5 *****
!
username admin privilege 15 password 7 *****
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-c3750x-24p
switch 2 provision ws-c3750x-24p
system mtu routing 1500
authentication mac-move permit
!
!
ip domain-name cisco.local
ip name-server 10.8.48.10
vtp mode transparent
udld enable

!
mls qos map policed-dscp  0 10 18 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51 
52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58 59 
60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41 
42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19
20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29
30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 3200
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
crypto pki trustpoint TP-self-signed-251756672
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-251756672
 revocation-check none
 rsakeypair TP-self-signed-251756672
!
!
crypto pki certificate chain TP-self-signed-251756672
 certificate self-signed 01
  3082024A 308201B3 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 32353137 35363637 32301E17 0D393330 33303130
30303134
  305A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403
1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3235
31373536
  36373230 819F300D 06092A86 4886F70D 01010105 0003818D 00308189
02818100
  CA14A219 7FA6622E F990AD57 DF6A6519 780FBAA9 94125F0B 4E7B5372
A25B8563
  2E47DA39 EB1196A3 7AA22F9D D57285A4 26AB9B08 D206A82B 46E8CB5D
F2E879A7
  B69D3FE4 D13F02E9 A88E7FE3 45633919 2F18FAD2 702110FE C15D66FB
1F8C607C
  868634F1 0ED135D0 3DD13542 EB55BB54 9A29035B 04A890FE 7D549125
7AC0CD1F
  02030100 01A37430 72300F06 03551D13 0101FF04 05300301 01FF301F
0603551D
  11041830 16821453 52333735 3058792E 63697363 6F2E6C6F 63616C30
1F060355
  1D230418 30168014 D41E475F 147873CA 89672DE8 3EDF7158 E28C0520
301D0603
  551D0E04 160414D4 1E475F14 7873CA89 672DE83E DF7158E2 8C052030
0D06092A
  864886F7 0D010104 05000381 810055FA 40B53155 FDCE6DE8 4EE26E23
CE73AAC7
  18989520 B81E4F76 C7FA39EC 383EACBC F6ABA9E9 9127073C B6BA9E99
C998576C
  2A293FB3 423B8BD8 31F9672D 4E588567 5B72DE62 D82F8FF4 BB6E2976
2A5BB9CB
  3FE4C6FC 8D89C53D EDC97BA9 B9B74629 227BD399 7F010E4F 2ADDBB04
4145A292
  CE13AD61 3F98E889 0BE22F49 D071
```

```
        quit
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 154-155 priority 24576
auto qos srnd4
!
!
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
vlan 115
 name ManagementVLAN
!
vlan 148
 name Server_VLAN_1
!
vlan 149
 name ACE
!
vlan 153
 name Firewall_Outside_VLAN
!
vlan 154
 name Firewall_Secure_VLAN
!
vlan 155
 name Firewall_with_IPS_Secure_VLAN
!
vlan 999
 name NATIVE
```

```
!
ip ssh version 2
!
!
!
macro name AccessEdgeQoS
auto qos voip cisco-phone
@
macro name EgressQoS
mls qos trust dscp
queue-set 1
srr-queue bandwidth share 1 30 35 5
priority-queue out
@
!
!
interface Port-channel7
 description EtherChannel Link to LAN Core
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 115,148,149,153
 switchport mode trunk
 logging event link-status
!
interface Port-channel21
 description ACE
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 148
 switchport mode trunk
!
interface Port-channel22
 description P2-WAAS-HE
 switchport access vlan 148
!
interface Port-channel33
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 149,912
 switchport mode trunk
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 spanning-tree portfast
!
interface GigabitEthernet1/0/3
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 spanning-tree portfast
!
interface GigabitEthernet1/0/4
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 auto qos trust dscp
 spanning-tree portfast
!
interface GigabitEthernet1/0/5
 description Connection to C210y
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 auto qos trust dscp
 spanning-tree portfast
!
interface GigabitEthernet1/0/6
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 auto qos trust dscp
 spanning-tree portfast
!
interface GigabitEthernet1/0/7
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 auto qos trust dscp
 spanning-tree portfast
!
```

```
interface GigabitEthernet1/0/8
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 auto qos trust dscp
 spanning-tree portfast
!
interface GigabitEthernet1/0/9
 description IE-SSP45a
 switchport access vlan 115
 switchport mode access
 spanning-tree portfast
!
!*************************************************************
! Interfaces GigabitEthernet 1/0/10 to 1/0/19 are
! configured the same way and have been removed for brevity
!*************************************************************
!
interface GigabitEthernet1/0/20
 description SR-5500X-IPSa
 switchport access vlan 115
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/21
 description ace4710 g1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 149,912
 switchport mode trunk
 channel-group 33 mode on
!
interface GigabitEthernet1/0/22
 description ace4710 g1/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 149,912
 switchport mode trunk
 channel-group 33 mode on
!
interface GigabitEthernet1/0/23
 description SR-ASA5540a outside gig 0/3
 switchport access vlan 153
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS | EgressQoS
 auto qos trust dscp
 spanning-tree portfast
!
interface GigabitEthernet1/0/24
 description SR-ASA5540a inside gig 0/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 154,155
 switchport mode trunk
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS | EgressQoS
 auto qos trust dscp
 spanning-tree portfast trunk
!
interface GigabitEthernet1/1/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 115,148,149,153
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS | EgressQoS | EgressQoS
 channel-protocol lacp
 channel-group 7 mode active
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface TenGigabitEthernet1/1/1
!
interface TenGigabitEthernet1/1/2
!
interface GigabitEthernet2/0/1
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 spanning-tree portfast
!
interface GigabitEthernet2/0/2
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 spanning-tree portfast
!
interface GigabitEthernet2/0/3
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 spanning-tree portfast
!
interface GigabitEthernet2/0/4
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 auto qos trust dscp
 spanning-tree portfast
!
interface GigabitEthernet2/0/5
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 spanning-tree portfast
!
interface GigabitEthernet2/0/6
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 auto qos trust dscp
 spanning-tree portfast
!
interface GigabitEthernet2/0/7
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 auto qos trust dscp
 spanning-tree portfast
!
interface GigabitEthernet2/0/8
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 auto qos trust dscp
 spanning-tree portfast
!
interface GigabitEthernet2/0/9
 description IE-SSP45b
 switchport access vlan 115
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 auto qos trust dscp
 spanning-tree portfast
!
!*************************************************************
! Interfaces GigabitEthernet 2/0/10 to 2/0/19 are
! configured the same way and have been removed for brevity
!*************************************************************
!
interface GigabitEthernet2/0/20
 description SR-5500X-IPSb
 switchport access vlan 115
 switchport mode access
```

```
 spanning-tree portfast
!
interface GigabitEthernet2/0/21
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 spanning-tree portfast
!
interface GigabitEthernet2/0/22
 description waas-he G2/0
 switchport access vlan 148
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS | EgressQoS
 spanning-tree portfast
!
interface GigabitEthernet2/0/23
 description SR-ASA5540b outside gig 0/3
 switchport access vlan 153
 switchport mode access
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS | EgressQoS
 auto qos trust dscp
 spanning-tree portfast
!
interface GigabitEthernet2/0/24
 description SR-ASA5540b inside gig 0/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 154,155
 switchport mode trunk
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS | EgressQoS
 auto qos trust dscp
 spanning-tree portfast trunk
!
interface GigabitEthernet2/1/1
 description Link to LAN Core 2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 115,148,149,153
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS | EgressQoS | EgressQoS
 channel-protocol lacp
 channel-group 7 mode active
!
interface GigabitEthernet2/1/2
!
interface GigabitEthernet2/1/3
!
interface GigabitEthernet2/1/4
!
interface TenGigabitEthernet2/1/1
!
interface TenGigabitEthernet2/1/2
!
interface Vlan1
 no ip address
!
interface Vlan115
 ip address 10.8.15.61 255.255.255.128
!
interface Vlan148
 no ip address
!
ip default-gateway 10.8.15.1
no ip http server
ip http authentication aaa
ip http secure-server
!
!
ip sla enable reaction-alerts
logging esm config
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
tacacs server TACACS-SERVER-1
 address ipv4 10.8.48.15
 key 7 *****
!
!
!
!
line con 0
 exec-timeout 360 0
 logging synchronous
line vty 0 4
 length 0
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp server 10.8.48.17
end
```

Cisco ASA 5500-X Firewall-Primary

The server room Cisco ASA 5500-X primary firewall operates as an active/standby pair with the second Cisco ASA 5500-X firewall to provide a resilient firewall pair.

```
ASA Version 8.6(1)
!
hostname SR-ASA5500X
domain-name cisco.local
enable password ***** encrypted
passwd 2***** 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 10.8.54.1 255.255.255.0 standby 10.8.54.2
!
interface GigabitEthernet0/0.155
 vlan 155
 nameif SRVLAN155
 security-level 100
 ip address 10.8.55.1 255.255.255.0 standby 10.8.55.2
!
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 10.8.53.126 255.255.255.128 standby 10.8.53.125
!
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
 nameif IPS-mgmt
 security-level 0
 no ip address
 management-only
!
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns server-group DefaultDNS
 domain-name cisco.local
object network Secure-Subnets
 subnet 10.8.54.0 255.255.255.0
object network SecureIPS-Subnets
 subnet 10.8.55.0 255.255.255.0
object network Mgmt-host-range
 range 10.8.48.224 10.8.48.254
object-group network SF_Secure_Subnet_List
 network-object object Secure-Subnets
 network-object object SecureIPS-Subnets
```

```
object-group service Mgmt-Traffic
 service-object tcp destination eq ssh
 service-object udp destination eq snmp
access-list global_access extended permit object-group Mgmt-Traffic object Mgmt-host-range object-group SF_Secure_Subnet_List
access-list global_access extended deny object-group Mgmt-Traffic any any
access-list SFVLAN155_mpc extended permit ip any any
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 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 10.8.53.130 255.255.255.252 standby 10.8.53.129
monitor-interface SRVLAN154
monitor-interface SRVLAN155
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 10.8.53.1 1
timeout xlate 3:00:00
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 10.8.48.15 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 10.8.0.0 255.254.0.0 outside
http 10.8.48.0 255.255.255.0 outside
snmp-server host outside 10.8.48.35 community *****
no snmp-server location
no snmp-server contact
snmp-server community *****
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
telnet timeout 5
ssh 10.8.0.0 255.254.0.0 outside
ssh 10.8.48.0 255.255.255.0 outside
ssh timeout 5
ssh version 2
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 10.8.48.17
webvpn
username admin password ***** encrypted privilege 15
!
class-map inspection_default
 match default-inspection-traffic
class-map SFVLAN155-class
```

```
 match access-list SFVLAN155_mpc
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
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
policy-map SFVLAN155-policy
 class SFVLAN155-class
  ips inline fail-close
!
service-policy global_policy global
service-policy SFVLAN155-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 1
  subscribe-to-alert-group configuration periodic monthly 1
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:318cebd83061e26e99fda1d79bd3ad77
: 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 7.1(4)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S615.0   2012-01-03
! ------------------------------
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 10.8.15.21/25,10.8.15.1
host-name SF-IPS-A
telnet-option disabled
```

```
access-list 10.8.48.0/24
dns-primary-server enabled
address 10.8.48.10
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 10.8.48.17
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
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 Firewall-Secondary

The server room Cisco ASA 5500-X secondary firewall operates as an active/standby pair with the primary Cisco ASA 5500-X firewall to provide a resilient firewall pair.

```
ASA Version 8.6(1)
!
hostname SR-ASA5500X
domain-name cisco.local
enable password ***** encrypted
passwd ***** 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 10.8.54.1 255.255.255.0 standby 10.8.54.2
!
interface GigabitEthernet0/0.155
 vlan 155
 nameif SRVLAN155
 security-level 100
 ip address 10.8.55.1 255.255.255.0 standby 10.8.55.2
!
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 10.8.53.126 255.255.255.128 standby 10.8.53.125
!
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
 nameif IPS-mgmt
 security-level 0
 no ip address
 management-only
!
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns server-group DefaultDNS
 domain-name cisco.local
object network Secure-Subnets
 subnet 10.8.54.0 255.255.255.0
object network SecureIPS-Subnets
 subnet 10.8.55.0 255.255.255.0
object network Mgmt-host-range
 range 10.8.48.224 10.8.48.254
object-group network SF_Secure_Subnet_List
 network-object object Secure-Subnets
 network-object object SecureIPS-Subnets
object-group service Mgmt-Traffic
 service-object tcp destination eq ssh
 service-object udp destination eq snmp
access-list global_access extended permit object-group Mgmt-
Traffic object Mgmt-host-range object-group SF_Secure_Subnet_List
access-list global_access extended deny object-group Mgmt-Traffic
any any
access-list SFVLAN155_mpc extended permit ip any any
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 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 10.8.53.130 255.255.255.252 standby 10.8.53.129
monitor-interface SRVLAN154
monitor-interface SRVLAN155
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 10.8.53.1 1
timeout xlate 3:00:00
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 10.8.48.15 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 10.8.0.0 255.254.0.0 outside
http 10.8.48.0 255.255.255.0 outside
snmp-server host outside 10.8.48.35 community *****
no snmp-server location
no snmp-server contact
snmp-server community *****
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
telnet timeout 5
ssh 10.8.0.0 255.254.0.0 outside
ssh 10.8.48.0 255.255.255.0 outside
ssh timeout 5
ssh version 2
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 10.8.48.17
webvpn
username admin password ***** encrypted privilege 15
!
class-map inspection_default
 match default-inspection-traffic
class-map SFVLAN155-class
 match access-list SFVLAN155_mpc
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
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
policy-map SFVLAN155-policy
 class SFVLAN155-class
  ips inline fail-close
!
service-policy global_policy global
service-policy SFVLAN155-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 1
  subscribe-to-alert-group configuration periodic monthly 1
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:f76a9df4fdee4e279e0bcf1d486a7b3b
: end
```

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 7.1(4)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S615.0   2012-01-03
! ------------------------------
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 10.8.15.22/25,10.8.15.1
host-name SF-IPS-B
telnet-option disabled
access-list 10.8.48.0/24
dns-primary-server enabled
address 10.8.48.10
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 10.8.48.17
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
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 to this guide since the previous Cisco SBA series.

- This is a new deployment guide focused solely on server room deployment. The previous server room deployment details were included in the *Cisco SBA for Midsize Organizations—Borderless Networks Foundation Deployment Guide.*
- The "Server Room Ethernet LAN" deployment section is now a complete standalone chapter which includes all requirements for configuring the server room Cisco Catalyst LAN switches. The "Server Room Security" chapter has been changed to focus solely on the firewall and IPS configuration for the server room deployment.
- The Server Load Balancing chapter has been moved from the *Cisco SBA for Midsize Organizations—Borderless Networks Foundation Deployment Guide* to a standalone deployment guide, *Cisco SBA—Data Center Advanced Server-Load Balancing Deployment Guide*.

Notes

Feedback

Click here to provide feedback to Cisco SBA.

SMART BUSINESS ARCHITECTURE

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.

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.