Newer Design Guide Available

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program.

For up-to-date guidance on the designs described in this guide, see http://cvddocs.com/fw/Aug13-169

For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd

SBA

SOLUTIONS

MANUFACTURING

Discrete Manufacturing Security Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2013 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 February 2013 is the "February 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 Solutions

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 Solutions are designs for specific problems found within the most common technology trends. Often, Cisco SBA addresses more than one use case per solution because customers adopt new trends differently and deploy new technology based upon their needs.

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

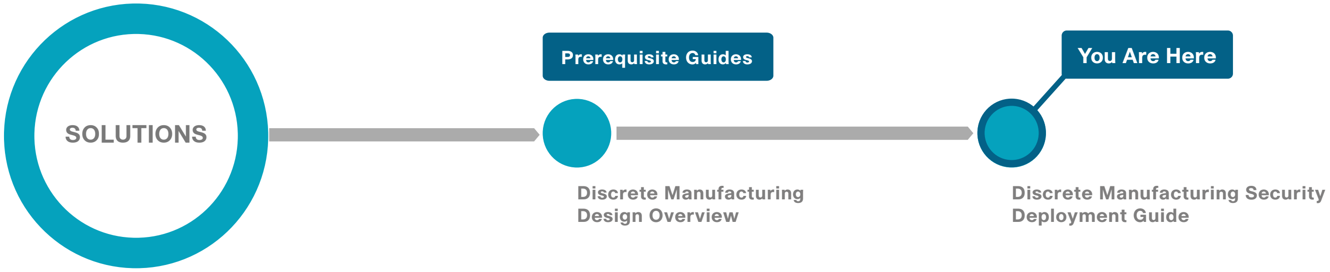
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- 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


SOLUTIONS
Prerequisite Guides
Discrete Manufacturing Design Overview
You Are Here
Discrete Manufacturing Security Deployment Guide

Introduction

As global manufacturing increasingly bases its Industrial Automation and Control System (IACS) applications on standard Ethernet and IP networking, creating a converged industrial Ethernet network, manufacturers have been able to operate more efficiently and effectively. *Converged industrial Ethernet* network is a comprehensive network design that targets industrial Ethernet networks that support hundreds to thousands of IACS devices. This new ability to integrate IACS and enterprise data enables real-time information sharing across the value chain, which increases data visibility, makes systems more available, assists rapid resolution of problems, and reduces operational and support costs.

IP networking facilitates interconnection of the industrial Ethernet network with the enterprise network. *Enterprise* refers to the organization's networks and systems for typical IT uses. Many industries have implemented enterprise applications for more efficient manufacturing, as well as Internet business applications, in order to communicate more efficiently with their suppliers, customers, and business partners. Internet-based enterprise resource planning and supply-chain management systems simplify connections both to other organizations and to internal business processes. These connections can enable greater efficiencies in processes and manufacturing. In manufacturing a small percentage increase in efficiency can translate into significant cost savings.

Such powerful connectivity throughout the organization and to outside partners has become indispensable for success. At the same time, it creates an environment where network security threats are a far greater concern. Because of the critical nature of IACS applications and the risks associated with them, it is more important than ever for manufacturers to implement a comprehensive network security strategy that protects while it enables access and integration, in order to achieve efficiencies and complete visibility.

Connecting the industrial Ethernet network to the enterprise network exposes the IACS applications to the security risks of the Internet and enterprise network. Mitigating these risks is critical because of the high availability requirements in IACS environments and the sensitivity of these systems to disruption. Many of the applications that industrial Ethernet networks support cannot be stopped or interrupted without serious physical damage or loss of productivity with measurable financial damage.

Business Overview

Decisions impacting industrial Ethernet networks are typically driven by plant managers and control engineers, rather than by an organization's IT department. The IACS vendor and support supply chain is different than those typically used by the IT department. This is driven by the different requirements of an IACS environment and the fact that, in the past, many makers of manufacturing equipment had specified the networking components. Today, IT departments in manufacturing organizations are increasingly engaging with plant managers and control engineers in order to leverage the knowledge and expertise in standard networking technologies for the benefit of plant operations. Plant-to-business integration at the application layer, convergence of the industrial Ethernet and enterprise networks, and the deployment and operation of common network technologies within plants are bringing these groups together.

The integrity and confidentiality of the information contained in IACS applications and devices is important. In the past, this meant building a separate plant network not connected to the enterprise network or even building a disparate set of networks based on different technologies. The need to drive down costs and improve efficiencies for services organization-wide has led to the desire to standardize and integrate plant and enterprise networks.

Security, which helps to preserve the availability of the network, is critical to avoiding outages caused by intentional or unintentional actions. Controlling access to resources on integrated industrial Ethernet and enterprise networks is challenging, and care must be taken to make sure the right people have access to the right services.

Quick and effective responses to issues on the plant floor often require real-time access to information and status from IACS applications as well as the skills and knowledge to take corrective action or optimize the manufac turing process. However, many manufacturers do not have key skilled and experienced personnel available at their global manufacturing facilities, and remote access is required. The standard remote-access VPN technologies that have been available for many years in traditional enterprise networks have been difficult to successfully apply to IACS environments for the following reasons:

- IACS applications are often managed by plant personnel, while enterprise-level remote-access solutions such as VPNs are the responsibility of the IT organization
- Remote access can expose critical IACS applications to viruses and malware that may be present on a remote or partner machine, potentially impacting manufacturing
- It is challenging to ensure that the end-device being used for remote access is secure and has the appropriate versions of the applications needed
- Manufacturers are often unable to limit a partner or remote employee's access to only specific machines, applications, or parts of the network for which they are responsible and have authorization

As a result, remote-access solutions, while widely deployed in the enterprise network, are just beginning to be adopted in industrial Ethernet networks.

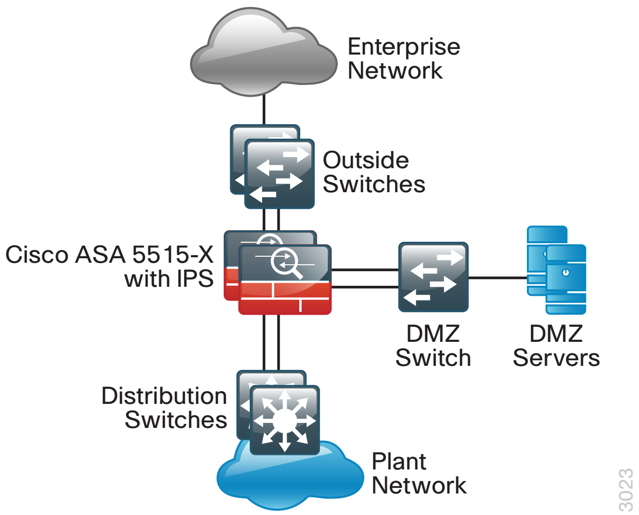
Technical Overview

The Cisco Smart Business Architecture for Discrete Manufacturing design provides for a converged Industrial Ethernet architecture that provides the performance, cost, and efficiency benefits of merged industrial and enterprise networks while helping to protect the IACS applications and industrial Ethernet network from the security risks associated with Internet access.

The *Discrete Manufacturing Security Deployment Guide:*

- Raises awareness of the particular security challenges and requirements of IACS environments.
- Outlines a solution and relevant design and implementation guidance.
- Develops a reference architecture standard on which to quickly and assuredly deploy converged industrial Ethernet networks.
- Provides considerations for the use and deployment of common technology and tools.
- Addresses plant-to-enterprise network and application convergence, making it easier to support wider business demands.
- Delivers standard Ethernet and IP networking technologies.

Figure 1 - Overview Diagram



The necessary components of helping to secure a converged industrial Ethernet network are creating a demilitarized zone (DMZ) and plant firewalls that separate the enterprise network from the industrial Ethernet network, using Cisco Intrusion Prevention System (IPS) modes to monitor traffic flow through the industrial Ethernet network, configuring secure remote access through VPN, and setting up authorization, authentication, and accounting services that track events, changes, and access.

Understanding the architecture of a converged industrial Ethernet network and the provisions upon which the framework is designed is key to addressing the security challenges posed by industrial Ethernet networks and the solutions for overcoming those challenges.

Relevant Standards and Frameworks

The International Society of Automation (ISA-99) Committee for Manufacturing and Control Systems Security establishes standards, recommended practices, and technical reports, and it defines procedures for implementing electronically secure IACS applications and for assessing electronic security performance. Guidance is directed towards those responsible for designing, implementing, or managing IACS applications and also applies to manufacturers, system integrators, machine builders, security practitioners, and IACS vendors.

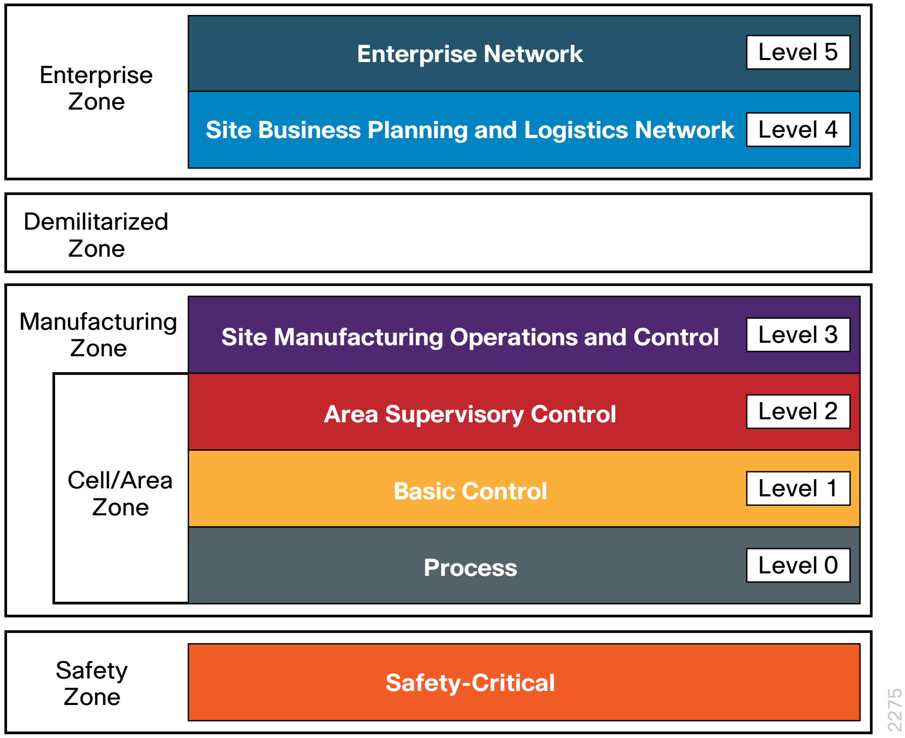
Standards bodies such as ISA-99 and National Institute of Standards and Technology (NIST) are continually developing security design axioms, and there is an emerging consensus on what a secure IACS architecture should provide. This includes an industrial Ethernet network that is highly available and redundant, is secure against both outside and inside threats, and has fast convergence, thus being more deterministic and therefore more suitable for real-time control. The specific security principles of the architecture are as follows:

- Control data flows between different levels of the industrial Ethernet network
- Prevent direct communication between IACS and enterprise applications
- Restrict access to real-time manufacturing data to within the industrial Ethernet network
- Allow enterprise access to copies of IACS data only through the demilitarized zone (DMZ)
- Authenticate and authorize user access based on the level within the industrial Ethernet network and role.
- Control rogue access to switches inside the industrial Ethernet network.
- Control which IACS devices can be plugged into the industrial Ethernet network.
- Detect and mitigate malicious traffic originating from the enterprise network or from infected devices that are plugged into the industrial Ethernet network.
- Secure connectivity for remote access to IACS devices.
- Use DMZ design options based on costs and levels of security and redundancy required.
- Limit rogue network communication activity from impacting networking devices.
- Document and define policy and risk appropriate for the environment.

The above are provided as principles on the understanding that you may make modifications for your network. A security risk assessment is recommended in order to determine the appropriate level of risk mitigation required for a specific situation.

The Purdue Model for Control Hierarchy (reference ISBN 1-55617-265-6) is a common and well-understood model in the manufacturing industry, and it segments IACS devices and equipment into hierarchical functions. ISA-99 has identified the levels and logical framework, as shown in Figure 2.

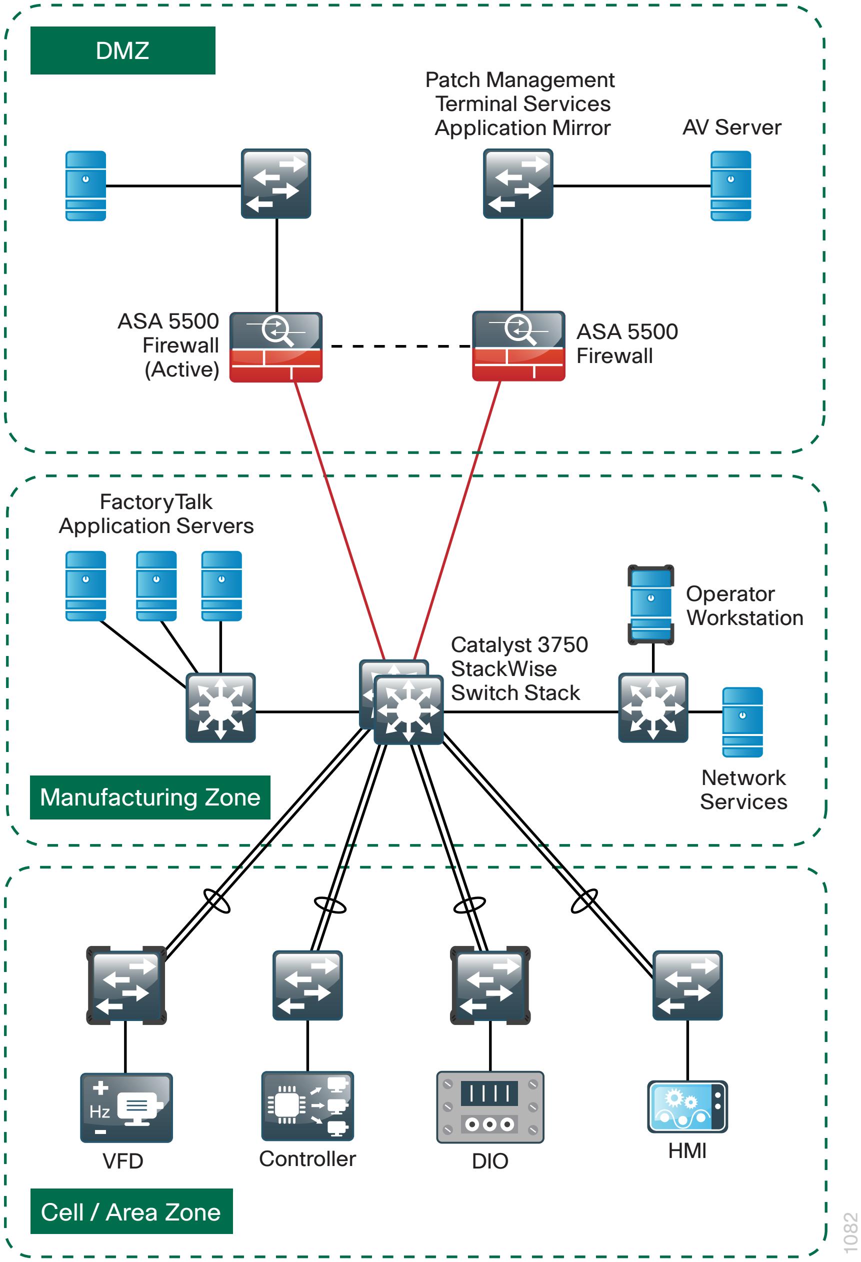
Figure 2 - Converged industrial Ethernet architecture



This model identifies the operational zones of the converged industrial Ethernet architecture, and each zone has its own security requirements:

- Safety zone—This zone consists of the safety systems that, upon the occurrence of a safety event, provide predictable, fail-safe shutdown of the IACS application in order to protect personnel, the environment, and the IACS application itself.
- Cell/Area zone—Most plants have multiple Cell/Area zones, and they are all contained within the Manufacturing zone. Each Cell/Area zone consists of a set of IACS devices, such as controllers, that are in real-time communication with each other and are responsible for a functional aspect of the manufacturing process.
- Manufacturing zone—All of the IACS applications, devices, and controllers critical to monitoring and controlling the plant-floor IACS operations are in this zone. To preserve smooth, plant-wide operations and functioning of the IACS application and industrial Ethernet network, this zone requires clear isolation and protection from the Enterprise zone via security devices within the Demilitarized zone (DMZ). This approach permits the Manufacturing zone to function entirely on its own, irrespective of the connectivity status to the higher levels.
- Demilitarized zone—The DMZ and plant firewalls separate the Enterprise and Manufacturing zones, but they also provide a securely managed connection for data and services to be shared between the enterprise and industrial Ethernet networks. With the deployment of a DMZ and plant firewall, attacks and issues that arise in one zone cannot easily affect the other zone. This zone is essential to the security of the converged industrial Ethernet network and is covered in-depth in this guide.
- Enterprise zone—This zone relies on standard IT services and is where basic business administration tasks are performed, such as email, Internet connections, and non-critical plant systems such as inventory. Remote access for IACS management occurs at this level and is managed through the DMZ.

Figure 3 - Industrial Ethernet Zone Mapping



For more information about the levels and zones of the Purdue Model for Control Hierarchy, see the *Discrete Manufacturing Design Guide*.

DMZ and Firewall

The DMZ and plant firewalls are an essential aspect of protecting the industrial Ethernet network and IACS applications and are key to the defense-in-depth approach for industrial Ethernet network security.

This design uses Cisco ASA 5500-X Series midrange security appliances for IACS security. They are configured in an active/standby pair for high availability in order to ensure that Internet access is minimally impacted by firewall software maintenance or hardware failure. The Cisco ASA 5500-X Series appliances are configured in routing mode. They apply Network Address Translation (NAT) and firewall policy, and they host Cisco Intrusion Prevention System (IPS) software modules in order to detect and mitigate malicious or harmful traffic.

Deploy plant firewalls that manage traffic between the Enterprise and Manufacturing zones. A plant firewall supplies the following:

- Established traffic patterns between the network zones via assigned security levels, for example, establishing the DMZ
- Stateful packet inspection of all traffic between the various zones
- Enforced authentication of users from one zone that try to access resources in another, for example, a user from the Enterprise zone attempts to access DMZ services

Table 1 - Cisco ASA 5500-X Series device performance

Cisco ASA family product	Firewall throughput
Cisco ASA 5512-X	1 Gbps
Cisco ASA 5515-X	1.2 Gbps
Cisco ASA 5525-X	2 Gbps
Cisco ASA 5545-X	3 Gbps
Cisco ASA 5555-X	4 Gbps

Cisco IPS

Cisco IPS on the Cisco ASA firewall supports both inline and promiscuous modes. Using *inline mode* means that network traffic flows through an IPS device. The advantage inline mode offers is that when the sensor detects malicious behavior, the IPS can drop malicious packets, generate alarms, or reset a connection, allowing the Cisco ASA appliance in the DMZ to respond immediately to security threats and protect the network. This allows the IPS device a much greater capacity to actually prevent attacks, but the drawback is that if the IPS device fails or misbehaves, it impacts production traffic.

Using *promiscuous mode* means that the IPS device must use another inline enforcement device in order to stop malicious traffic. This means that for activity such as single-packet attacks (slammer worm over User Datagram Protocol), a Cisco Intrusion Detection System (IDS) sensor could not prevent the attack from occurring. However, an IDS sensor can offer great value when identifying and cleaning up infected hosts.

Table 2 - Cisco ASA 5500-X Series IPS Solution performance levels

Cisco ASA 5500-X Series IPS Solution module	IPS performance
Cisco ASA 5512-X	250 Mbps
Cisco ASA 5515-X	400 Mbps
Cisco ASA 5525-X	600 Mbps
Cisco ASA 5545-X	900 Mbps
Cisco ASA 5555-X	1.3 Gbps

Remote-Access VPN

Given the critical nature of IACS applications and the unique security considerations associated with them, it is important to ensure that remote access is implemented in a highly secure manner. This is achieved through a multilayer security approach that addresses the different potential security threats that could occur in a remote-access scenario. Although there is no single technology or methodology that fully secures industrial Ethernet networks, combining technologies forms a strong deterrent to most known types of threats and security breaches, while limiting the impact of any compromise.

The Cisco VPN solution on the Cisco ASA 5500-X Series midrange security appliance supports IP Security (IPsec), web portal, full-tunnel Secure Sockets Layer (SSL) VPNs for client-based remote access, and IPsec for site-to-site VPN. The Cisco AnyConnect Secure Mobility Client is recommended for remote users who require full network connectivity. The Cisco AnyConnect client uses SSL and is designed for automated download and installation. SSL access can be more flexible and is likely to be accessible from more locations than IPsec.

Table 3 - Maximum number of SSL VPN sessions

Cisco ASA 5500-X Series product	Maximum SSL VPN sessions
Cisco ASA 5515-X	250
Cisco ASA 5525-X	750
Cisco ASA 5545-X	2500
Cisco ASA 5555-X	5000

AAA

Authentication, authorization, and accounting (AAA) is designed to enable you to dynamically configure the type of access you want on a per-user or per-service basis. Through AAA, the converged industrial Ethernet network solution provides the ability to implement security services that provide the necessary control mechanisms in order to limit access to systems, applications, and network devices, and it also provides auditing mechanisms in order to track access, changes, and events.

Notes

Firewall

Process

Configuring the Firewall

1. Configure the LAN distribution switch
2. Apply Cisco ASA initial configuration
3. Configure internal routing
4. Configure user authentication
5. Configure NTP and logging
6. Configure device-management protocols

Cisco ASA can be configured from the command line or from the graphical user interface, Cisco Adaptive Security Device Manager (ASDM). Cisco ASDM is the primary method of configuration illustrated in this deployment guide. This process uses the command line to initially configure the appliance and then uses Cisco ASDM to manage the configuration.

Only the primary Cisco ASA appliance in the high availability pair needs to be configured. The "Configuring Firewall High Availability" process sets up high availability and synchronizes the configuration from the primary to the secondary device.

Procedure 1 Configure the LAN distribution switch

The LAN distribution switch is the path to the industrial Ethernet network. A unique VLAN supports the industrial Ethernet network devices, and the routing protocol peers with Cisco ASAs across this network. To support future use, the connections from ASAs to the inside LAN distribution switches are configured as trunks.

Reader Tip

This procedure assumes that the distribution switch has already been configured following the guidance in the *Discrete Manufacturing LAN Deployment Guide*. Only the procedures required to support the integration of the firewall into the deployment are included in this guide.

Devices located in the industrial Ethernet network are referred to as the Plant Edge in the deployment.

Step 1: Configure the plant edge VLAN on the LAN distribution switch.

```
vlan 300
 name PlantEdge
```

Step 2: Configure a Layer 3 switched virtual interface (SVI). This allows devices in the VLAN to communicate with the rest of the network.

```
interface vlan 300
 description Plant Edge SVI
 ip address 10.13.24.1 255.255.255.224
 no shutdown
```

Step 3: Configure the interfaces that are connected to the plant edge firewall.

An 802.1Q trunk is used for the connection to the plant edge firewall, which allows the distribution switch to provide the Layer 3 services to all the VLANs defined on the firewall. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the firewall.

```
interface GigabitEthernet1/0/24
 description PE-ASA5515Xa Gig0/0
!
interface GigabitEthernet2/0/24
 description PE-ASA5515Xb Gig0/0
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport
switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 300
 switchport mode trunk
 spanning-tree portfast trunk
 macro apply CiscoIEEgress
logging event link-status
logging event trunk-status
no shutdown
```

Cisco Catalyst 4500 Series switches do not require the **switchport trunk encapsulation dot1q** command.

For Cisco Catalyst 4500 Series switches, use the **CiscoIEEgress-GE** macro, per guidelines from *Discrete Manufacturing LAN Deployment Guide.*

Step 4: Configure the routing protocol to form neighbor relationships on the plant edge VLAN.

```
router eigrp 101
  no passive-interface Vlan300
```

Procedure 2 Apply Cisco ASA initial configuration

This procedure configures connectivity to the appliance from the internal network in order to enable management access.

Step 1: Configure the appliance host name.

```
hostname PE-ASA5515X
```

Step 2: Configure the Cisco ASA interface that is connected to the internal distribution switch to be a subinterface on VLAN 300. The interface is configured as a VLAN trunk port in order to allow flexibility to add additional connectivity.

```
interface GigabitEthernet0/0
no shutdown
!
interface GigabitEthernet0/0.300
 vlan 300
 nameif inside
 ip address 10.13.24.30 255.255.255.224
```

Step 3: Enable the dedicated management interface and remove any IP address that might be applied. This interface is used only for IPS management.

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

Step 4: 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 organization's policy, or if no policy exists, create a password using a minimum of 8 characters with a combination of uppercase letters, lowercase letters, and numbers.

Procedure 3 Configure internal routing

A dynamic routing protocol is used to configure reachability between networks connected to the appliance and those that are internal to the organization.

Step 1: Enable Enhanced Interior Gateway Routing Protocol (EIGRP) on the appliance.

```
router eigrp 101
```

Step 2: Configure the appliance to advertise its statically defined routes and connected networks that are inside the plant edge network range.

```
 no auto-summary
 network 10.13.24.0 255.255.252.0
 redistribute static
```

Step 3: Configure EIGRP to peer with neighbors across the inside interface only.

```
 passive-interface default
 no passive-interface inside
```

Step 4: Configure a network object for the summary address of the internal network. The network object is used later during security policy configuration.

```
object network internal-network
 subnet 10.13.0.0 255.255.0.0
 description The plant's internal network range
```

Procedure 4 Configure user authentication

(Optional)

As networks scale in the number of devices to maintain, it poses an operational burden to maintain local user accounts on every device. A centralized authentication, authorization, and accounting (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 Authentication Control Server (ACS). Please refer to the "Configuring Cisco Secure ACS" section of this guide for configuration details.

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 (inside) host 10.13.48.15 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
```

Tech Tip

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

Procedure 5 Configure NTP and logging

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

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.

```
ntp server 10.13.48.17
```

Step 2: Configure the time zone.

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

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

```
logging enable
logging buffered informational
```

Procedure 6 Configure device-management protocols

Cisco ASDM requires that the appliance's HTTPS server be available. Be sure that the configuration includes networks from which administrative staff has access to the Cisco ASA through Cisco ASDM; the appliance can offer controlled Cisco ASDM access for a single address or management subnet (in this case, 10.13.48.0/24).

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

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

Simple Network Management Protocol (SNMP) is enabled to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured for a read-only community string.

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

```
domain-name cisco.local
http server enable
http 10.13.48.0 255.255.255.0 inside
ssh 10.13.48.0 255.255.255.0 inside
ssh version 2
```

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

```
snmp-server host inside 10.13.48.35 community cisco
snmp-server community cisco
```

Process

Configuring Firewall High Availability

1. Configure resilience on primary appliance
2. Configure resilience on standby appliance

The Cisco ASA appliances are set up as a highly available active/standby pair. 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, IPS, and VPN functions. In an active/standby configuration, only one device is passing traffic at a time; thus, the appliances must be sized so that the entire traffic load can be handled by either appliance in the pair.

Both appliances in the failover pair must be the same model, with identical feature licenses and IPSs (if the software module is installed). For failover to be enabled, the secondary appliance needs to be powered up and cabled to the same networks as the primary appliance.

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 appliance 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 appliance, the poll times can be tuned down without performance impact to the appliance, which minimizes the downtime users experience during failover. Reducing the failover timer intervals below the values in this guide is not recommended.

Procedure 1 Configure resilience on primary appliance

This procedure describes how to configure active/standby failover. The failover key value must match on both devices in an active/standby pair. This key is used for two purposes: to authenticate the two devices to each other, and to secure state-synchronization messages between the devices, which enables the Cisco ASA pair to maintain service for existing connections, in the event of a failover.

Step 1: On the primary appliance, enable failover.

```
failover
```

Step 2: Configure the appliance as the primary appliance of the high availability pair.

```
failover lan unit primary
```

Step 3: Configure the failover interface.

```
failover lan interface failover GigabitEthernet0/2
failover key FailoverKey
failover replication http
failover link failover GigabitEthernet0/2
```

Step 4: Tune the failover poll timers. This minimizes the downtime experienced during failover.

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

Step 5: Configure the failover interface IP address.

```
failover interface ip failover 10.13.24.33 255.255.255.248
standby 10.13.24.34
```

Step 6: Enable the failover interface.

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

Step 7: Configure the standby IP address and monitoring of the inside interface.

```
interface GigabitEthernet0/0.300
 ip address 10.13.24.30 255.255.255.224 standby 10.13.24.29
monitor-interface inside
```

Procedure 2 Configure resilience on standby appliance

Step 1: On the secondary appliance, enable failover.

```
failover
```

Step 2: Configure the appliance as the secondary appliance of the high availability pair.

```
failover lan unit secondary
```

Step 3: Configure the failover interface.

```
failover lan interface failover GigabitEthernet0/2
failover key FailoverKey
failover replication http
failover link failover GigabitEthernet0/2
```

Step 4: Tune the failover poll timers. This minimizes the downtime experienced during failover.

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

Step 5: Configure the failover interface IP address.

```
failover interface ip failover 10.13.24.33 255.255.255.248
standby 10.13.24.34
```

Step 6: Enable the failover interface.

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

Step 7: On the command-line interface of the primary appliance, issue the **show failover state** command. This verifies the standby synchronization between the appliances.

```
PE-ASA5515X# 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
```

Process

Configuring the Management DMZ

1. Configure the DMZ switch
2. Configure the DMZ interface
3. Configure the DMZ routing
4. Permit DMZ management traffic

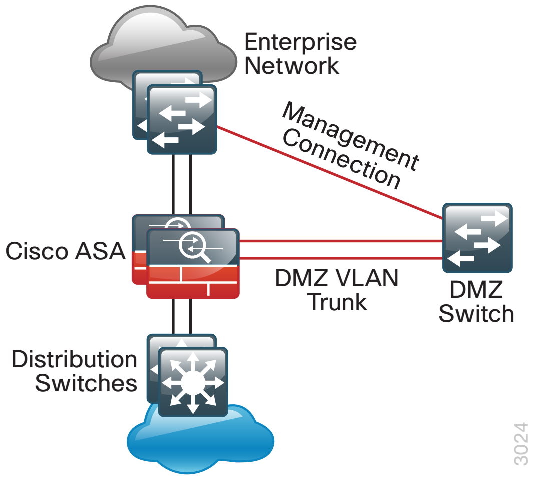
The firewall's *demilitarized zone* (DMZ) is a portion of the network where, typically, traffic to and from other parts of the network is tightly restricted. Organizations place network services and servers in a DMZ in order to make them accessible from the enterprise network. These servers are allowed to initiate connections to the industrial Ethernet network for certain services, allowing users on the enterprise network to access the plant from a controlled device.

To ease the management of the network devices on the DMZ, you configure a dedicated management VLAN.

The DMZ network is connected to the appliances on the appliances' Gigabit Ethernet interface via a VLAN trunk in order to allow the greatest flexibility if new VLANs must be added in order to connect additional DMZs. In this architecture, the trunk connects the appliances to a Cisco Catalyst 3750-X Series switch stack that provides resiliency.

The DMZ interface on the appliance is assigned an IP address, which is the default gateway for each DMZ network. The DMZ switch is configured to offer Layer-2 switching capability only; the DMZ switch does not have a switched virtual interface (SVI) for any VLAN, except for the management DMZ VLAN. This SVI is used for the management of the switch.

Figure 4 - DMZ VLAN topology and services



Procedure 1 Configure the DMZ switch

The DMZ switch in this deployment is a pair of Cisco Catalyst 3750-X Series switches in a stacked configuration. The configuration below is complete for the features required for the DMZ switch. This configuration is taken from the *Discrete Manufacturing LAN Deployment Guide*.

To make consistent deployment of quality of service (QoS) easier, each platform defines a macro that you use in later procedures in order to apply the platform-specific QoS configuration.

As networks scale in the number of devices to maintain, it poses an operational burden to maintain local user accounts on every device. A centralized authentication, authorization, and accounting (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, AAA controls all management access to the network infrastructure devices (SSH and HTTPS). This procedure provides optional guidance for configuring the device to use AAA services in order to authenticate users.

Reader Tip

The AAA server used in this architecture is Cisco Secure Authentication Control Server. Please refer to the “Configuring Cisco Secure ACS” section of this guide for configuration details.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. In Step 12, you define a local AAA user database on each network infrastructure device in order to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

Step 1: Set the stack master switch.

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

Step 2: Ensure that the original master MAC address remains the stack MAC address after a failure.

```
stack-mac persistent timer 0
```

Step 3: Because AutoQoS might not be configured on this device, manually configure the global QoS settings:

```
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
@
!
```

Step 4: Configure the device host name.

```
hostname DMZ-3750X
```

Step 5: Configure VLAN Trunking Protocol (VTP) transparent mode.

```
vtp mode transparent
```

Step 6: Enable Rapid Per-VLAN Spanning-Tree (PVST+).

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

Step 7: Enable Unidirectional Link Detection (UDLD).

```
udld enable
```

Step 8: Set EtherChannels to use the traffic source and destination IP address.

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

Step 9: Configure device management protocols.

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

Step 10: If your network operational support is centralized and you would like to increase network security, use an access list in order to limit the networks that can access the device. In this example, only devices on the 10.13.48.0/24 network are able to access the device via SSH or SNMP.

```
access-list 55 permit 10.13.48.0 0.0.0.255
line vty 0 15
  access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```

Step 11: Configure DNS for host lookup.

```
ip name-server 10.13.48.10
```

Step 12: Configure local login and password.

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

Step 13: If you are using AAA services, configure centralized user authentication.

```
tacacs server TACACS-SERVER-1
address ipv4 10.13.48.15
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
```

Step 14: Configure a synchronized clock.

```
ntp server 10.13.48.17
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Step 15: Configure the management VLAN and set the DMZ switch to be the spanning tree root for the management VLAN.

```
vlan 1229
 name dmz-mgmt
spanning-tree vlan 1-4094 root primary
```

Step 16: Configure the interfaces that connect to the Cisco ASA firewalls.

```
interface GigabitEthernet1/0/24
 description PE-ASA5515Xa Gig0/1
!
interface GigabitEthernet2/0/24
 description PE-ASA5515Xb Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1229
 switchport mode trunk
 spanning-tree portfast trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 no shutdown
```

Step 17: Configure the switch with an IP address. This allows the switch to be managed via in-band connectivity.

```
interface Vlan1229
 description In-band management
 ip address 10.13.129.5 255.255.255.0
 no shutdown
```

Step 18: Configure the appliance as the DMZ switch's default route.

```
ip default-gateway 10.13.129.1
```

Step 19: Configure bridge protocol data unit (BPDU) Guard globally to protect portfast-enabled interfaces.

```
spanning-tree portfast bpduguard default
```

Procedure 2 Configure the DMZ interface

Step 1: Connect to Cisco Adaptive Security Device Manager (ASDM) by navigating to https://pe-asa5515x.cisco.local/admin and then logging in with your username and password.

Step 2: Navigate to **Configuration > Device Setup > Interfaces**.

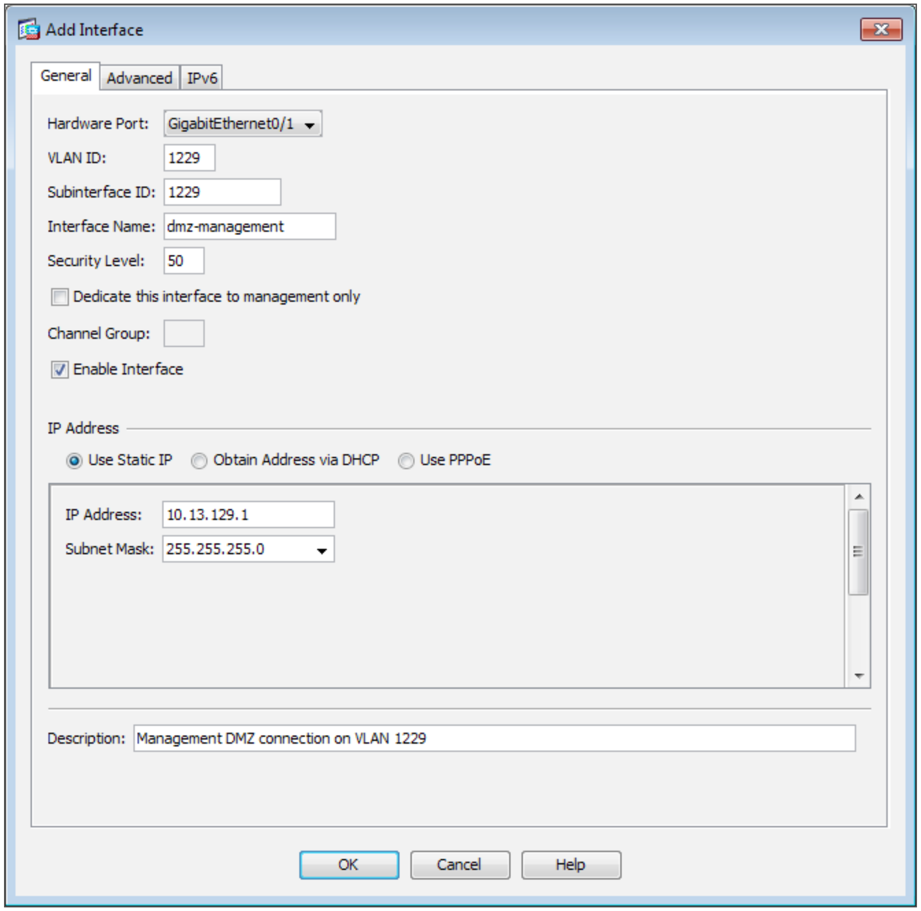
Step 3: Select the interface that is connected to the DMZ switch, and then click **Edit** (Example: GigabitEthernet0/1). The Edit Interface dialog box appears.

Step 4: Select **Enable Interface**, and then click **OK**.

Step 5: In the Interface pane, click **Add**, and then choose **Interface**. The Add Interface dialog box appears.

Step 6: On the Add Interface dialog box, enter the following, and then click **OK**:

- Hardware Port—**GigabitEthernet0/1**
- VLAN ID—**1229**
- Subinterface ID—**1229**
- Interface Name—**dmz-management**
- Security Level—**50**
- Enable Interface—**Selected**
- IP Address—**10.13.129.1**
- Subnet Mask—**255.255.255.0**



Hardware Port: GigabitEthernet0/1

VLAN ID: 1229

Subinterface ID: 1229

Interface Name: dmz-management

Security Level: 50

□ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address: 10.13.129.1

Subnet Mask: 255.255.255.0

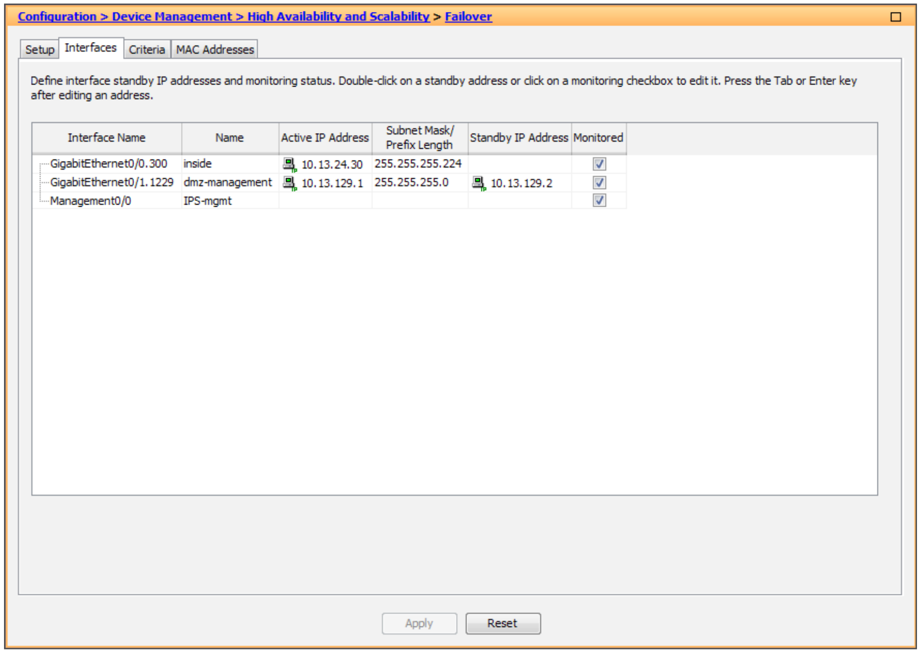
Description: Management DMZ connection on VLAN 1229

Step 7: At the bottom of the window, click **Apply**. This saves the configuration.

Step 8: Navigate to **Configuration > Device Management > High Availability and Scalability > Failover > Interfaces**. On the Interfaces tab, the interfaces you configured are displayed.

Step 9: Select the management interface (Example: dmz-management), click the empty **Standby IP Address** field, enter the failover IP address (Example: 10.13.129.2), and then press **Enter**.

Step 10: Select **Monitored**, and then click **Apply**.


Configuration > Device Management > High Availability and Scalability > Failover
Setup
Interfaces
Criteria
MAC Addresses
Apply
Reset

Define interface standby IP addresses and monitoring status. Double-click on a standby address or click on a monitoring checkbox to edit it. Press the Tab or Enter key after editing an address.

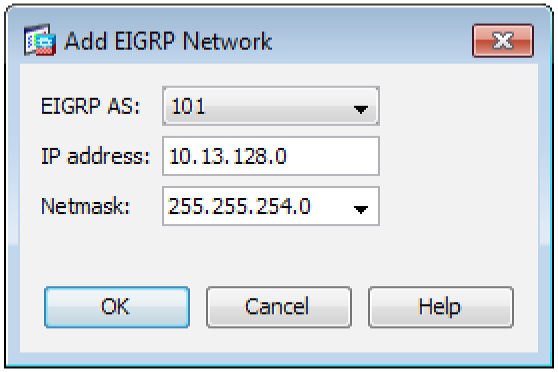
Interface Name	Name	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/0.300	inside	10.13.24.30	255.255.255.224		☑
GigabitEthernet0/1.1229	dmz-management	10.13.129.1	255.255.255.0	10.13.129.2	☑
Management0/0	IPS-mgmt				☑

Procedure 3 Configure the DMZ routing

Step 1: Navigate to **Configuration > Device Setup > Routing > EIGRP > Setup > Networks**, and then click **Add**.

Step 2: On the Add EIGRP Network dialog box, enter the following, and then click **OK**:

- IP Address—**10.13.128.0**
- Netmask—**255.255.254.0**



EIGRP AS: 101

IP address: 10.13.128.0

Netmask: 255.255.254.0

Step 3: At the bottom of the window, click **Apply**. This saves the configuration.

Procedure 4 Permit DMZ management traffic

Tech Tip

Each security policy is unique to the policy and management requirements of an organization. Examples in this document are intended to illustrate policy configuration concepts.

The management DMZ provides connectivity to the internal industrial Ethernet network for devices in the DMZ and outside the firewall. This connectivity is limited to the protocols required to maintain and operate the devices. You enable devices in the management DMZ to communicate with the internal industrial Ethernet network, for management and user authentication.

Step 1: Navigate to **Configuration > Firewall > Access Rule**, and then click **Add**. The Add Access Rule dialog box appears.

Step 2: On the Add Access Rule dialog box, in the **Interface** list, ensure that **Any** is selected.

Step 3: In the **Source** box, click the ellipsis button (**...**). The Browse Source dialog box appears.

Step 4: On the Browse Source dialog box, locate the object (Example: dmz-management-network), double-click the object, and then click **OK**.

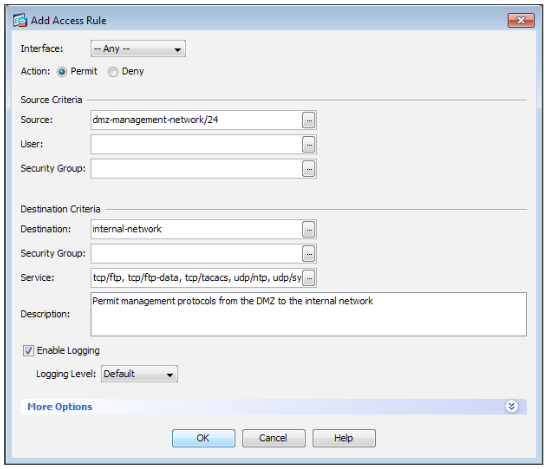
Step 5: In the **Destination** box, click the ellipsis button (**...**). The Browse Destination dialog box appears.

Step 6: On the Browse Destination dialog box, locate the object (Example: internal-network), double-click the object, and then click **OK**.

Step 7: In the **Service** box, click the ellipsis button (**...**). The Browse Service dialog box appears.

Step 8: On the Browse Service dialog box, locate the following objects (Example: tcp/ftp, tcp/ftp-data, tcp/tacacs, udp/ntp, udp/syslog), double-click the objects, and then click **OK**.

Step 9: Verify that the Add Access Rule dialog box resembles the following figure, and then click **OK**.



Add Access Rule

Interface: -- Any --

Action: ● Permit ○ Deny

Source Criteria

Source: dmz-management-network/24

User:

Security Group:

Destination Criteria

Destination: internal-network

Security Group:

Service: tcp/ftp, tcp/ftp-data, tcp/tacacs, udp/ntp, udp/sy

Description: Permit management protocols from the DMZ to the internal network

☑ Enable Logging

Logging Level: Default

Step 10: At the bottom of the window, click **Apply**. This saves the configuration.

Process

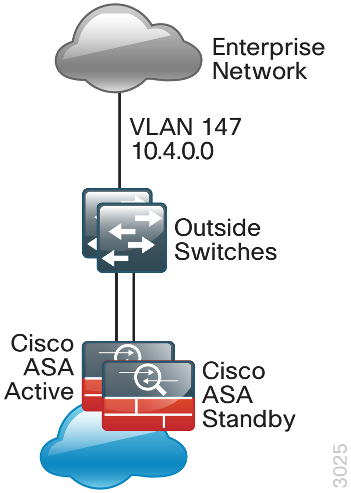
Configuring the Firewall Enterprise Edge

1. Configure the outside switch
2. Configure Cisco ASA outside connectivity
3. Create a default route out of the plant

Procedure 1 Configure the outside switch

The enterprise distribution switch is the path to the enterprise network and the outside or untrusted side of the Cisco ASA firewall, from the plant perspective. This procedure shows only the configuration needed to connect the appliance to the enterprise network. The configuration for the enterprise network LAN is covered in the *LAN Deployment Guide*.

Figure 5 - Single ISP connectivity



Step 1: Configure the enterprise edge VLAN on the enterprise WAN distribution switch.

```
vlan 147
 name Manufacturing
```

Step 2: Configure a Layer 3 switched virtual interface (SVI). This enables devices in the VLAN to communicate with the rest of the network.

```
interface vlan 147
 ip address 10.4.47.1 255.255.255.0
 ip pim sparse-mode
```

Step 3: Configure the interfaces that are connected to the plant edge firewall.

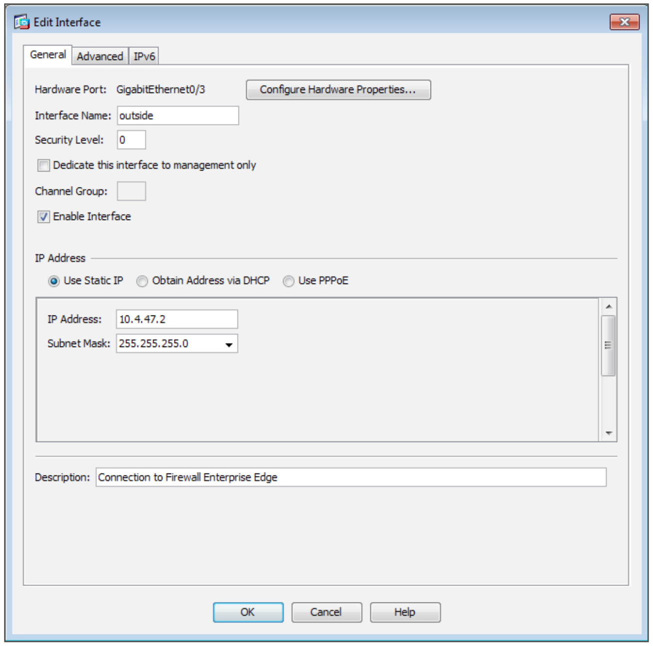
```
interface GigabitEthernet1/0/23
 description FE-ASA5515Xa Gig0/3
!
interface GigabitEthernet2/0/23
 description FE-ASA5515Xb Gig0/3
!
interface range GigabitEthernet1/0/23, GigabitEthernet2/0/23
 switchport host
 switchport access vlan 147
 macro apply EgressQoS
```

Procedure 2 Configure Cisco ASA outside connectivity

Step 1: Navigate to **Configuration > Device Setup > Interfaces**, click the interface that is connected to the outside switch (Example: GigabitEthernet0/3), and then click **Edit**.

Step 2: On the Edit Interface dialog box, enter the following, and then click **OK**:

- Interface Name—**outside**
- Security Level—**0**
- Enable Interface—**Selected**
- IP Address—**10.4.47.2**
- Netmask—**255.255.255.0**



Hardware Port: GigabitEthernet0/3

Interface Name: outside

Security Level: 0

☐ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address: 10.4.47.2

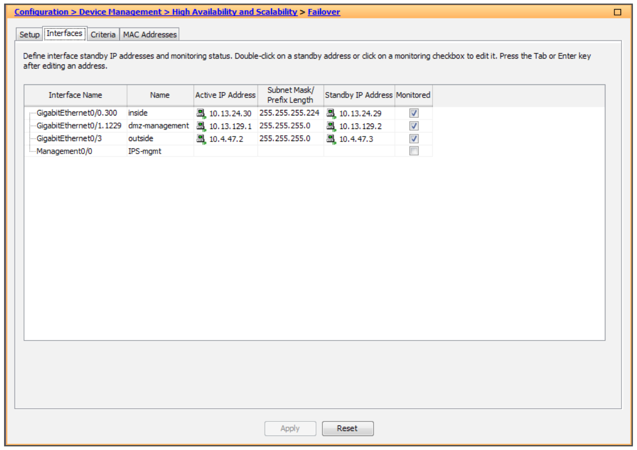
Subnet Mask: 255.255.255.0

Description: Connection to Firewall Enterprise Edge

Step 3: Navigate to **Configuration > Device Management > High Availability and Scalability > Failover > Interfaces**.

Step 4: Select the outside interface (Example: outside), click the empty **Standby IP Address** field, enter the failover address (Example: 10.4.47.3), and then press **Enter**.

Step 5: Select **Monitored**, and then click **Apply**.


Configuration > Device Management > High Availability and Scalability > Failover
Setup
Interfaces
Criteria
MAC Addresses
Apply
Reset

Define interface standby IP addresses and monitoring status. Double-click on a standby address or click on a monitoring checkbox to edit it. Press the Tab or Enter key after editing an address.

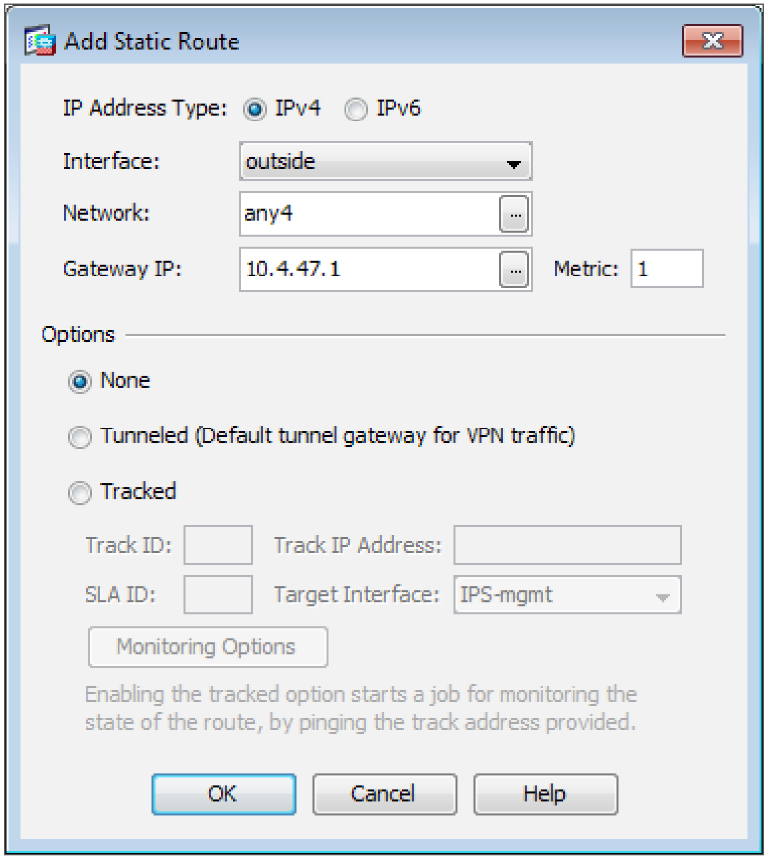
Interface Name	Name	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/0.300	inside	10.13.24.30	255.255.255.224	10.13.24.29	☑
GigabitEthernet0/1.1229	dmz-management	10.13.129.1	255.255.255.0	10.13.129.2	☑
GigabitEthernet0/3	outside	10.4.47.2	255.255.255.0	10.4.47.3	☑
Management0/0	IPS-mgmt				☐

Procedure 3 Create a default route out of the plant

Step 1: Navigate to **Configuration** > **Device Setup** > **Routing** > **Static Routes**, and then click **Add**.

Step 2: On the Add Static Route dialog box, enter the following, and then click **OK**:

- Interface—**outside**
- Network—**any4**
- Gateway IP—**10.4.47.1**



IP Address Type: ● IPv4 ○ IPv6

Interface: outside

Network: any4

Gateway IP: 10.4.47.1 Metric: 1

● None

○ Tunneled (Default tunnel gateway for VPN traffic)

○ Tracked

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

Step 3: At the bottom of the window, click **Apply**. This saves the configuration.

Process

Configuring Industrial Ethernet Network Access to the Enterprise Network

1. Configure network address translation
2. Configure security policy to allow voice

Procedure 1 Configure network address translation

Prior to completing this procedure, access to the outside enterprise network from within the inside industrial Ethernet network is not functional. The 10.13.0.0/16 network in the plant is not routed in the enterprise network. For this configuration, all inside industrial Ethernet network addresses are translated to the address on the outside interface of the appliance. It is also possible to allow the industrial Ethernet networks to access the enterprise network without translation by routing the 10.13.0.0/16 network in the enterprise.

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**, click **Add**, and then choose **Network Object**.

Step 2: On the Add Network Object dialog box, enter the following:

- Name—**inside-plant-network**
- Type—**Network**
- IP Address—**10.13.0.0**
- Netmask—**255.255.0.0**

Step 3: Next to **NAT**, click the two down arrows. The NAT section expands.

Step 4: Select **Add Automatic Address Translation Rules**.

Step 5: In the **Type** list, choose **Dynamic PAT (Hide)**.

Step 6: In the **Translated Addr** list, click the ellipsis button (**…**). The Browse Translated Address dialog box appears.

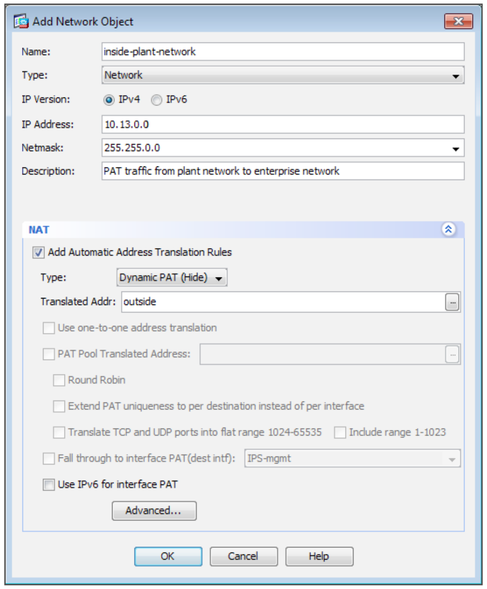
Step 7: On the Browse Translated Address dialog box, locate the object (Example: outside), double-click the object, and then click **OK**.

Step 8: On the Add Network Object dialog box, click **Advanced**. The Advanced NAT Settings dialog box appears.

Step 9: On the Advanced NAT Settings dialog box, in the **Source Interface** list, choose **inside**.

Step 10: On the Advanced NAT Settings dialog box, in the **Destination Interface** list, choose **outside**, and then click **OK**.

Step 11: On the Add Network Object dialog box, click **OK**.



Add Network Object

Name: inside-plant-network
Type: Network
IP Version: ● IPv4 ○ IPv6
IP Address: 10.13.0.0
Netmask: 255.255.0.0
Description: PAT traffic from plant network to enterprise network

NAT
☑ Add Automatic Address Translation Rules
Type: Dynamic PAT (Hide)
Translated Addr: outside
□ Use one-to-one address translation
□ PAT Pool Translated Address:
□ Round Robin
□ Extend PAT uniqueness to per destination instead of per interface
□ Translate TCP and UDP ports into flat range 1024-65535 □ Include range 1-1023
□ Fall through to interface PAT(dest intf): IPS-mgmt
□ Use IPv6 for interface PAT

Step 12: At the bottom of the window, click **Apply**. This saves the configuration.

Procedure 2 Configure security policy to allow voice

(Optional)

This procedure shows how to configure the appliance so that you can permit a configured voice VLAN in the industrial Ethernet network to access the enterprise network. This allows phones in the plant to access call processing resources in the enterprise network and permits voice calls between plant and enterprise phones.

Reader Tip

This procedure assumes that the distribution switch has already been configured with a voice VLAN following the guidance in the *Discrete Manufacturing LAN Deployment Guide*. Only the procedures required to allow the voice traffic through the appliance in order to access the enterprise are included in this guide.

Step 1: Navigate to **Configuration > Firewall > Access Rules**, and then click **Add**.

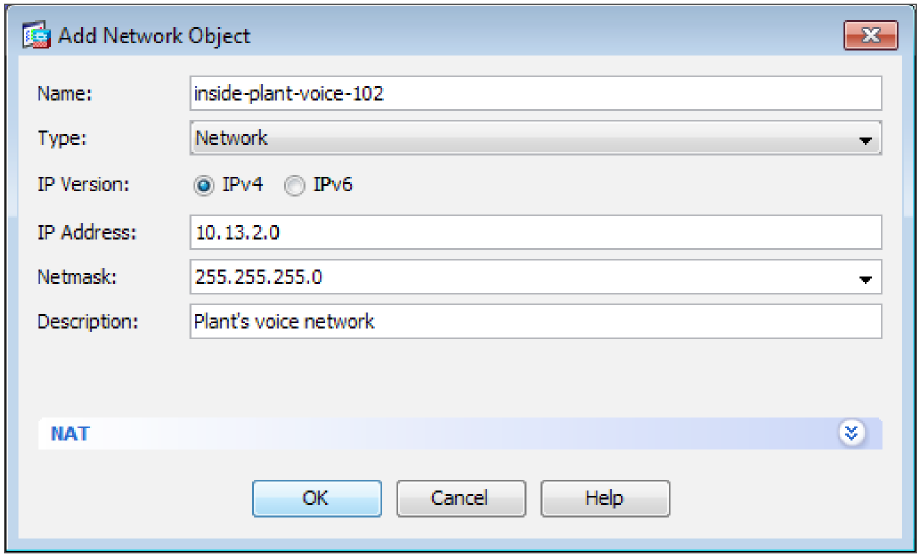
Step 2: On the Add Access Rule dialog box, in the **Interface** list, ensure that **Any** is selected.

Step 3: In the **Source** box, click the ellipsis button (**...**). The Browse Source dialog box appears.

Step 4: On the Browse Source dialog box, in the **Add** list, choose **Network Object**.

Step 5: On the Add Network Object dialog box, enter the following, and then click **OK**:

- Name—**inside-plant-voice-102**
- Type—**Network**
- IP Address—**10.13.2.0**
- Netmask—**255.255.255.0**


Add Network Object

Name: inside-plant-voice-102

Type: Network

IP Version: ● IPv4 ○ IPv6

IP Address: 10.13.2.0

Netmask: 255.255.255.0

Description: Plant's voice network

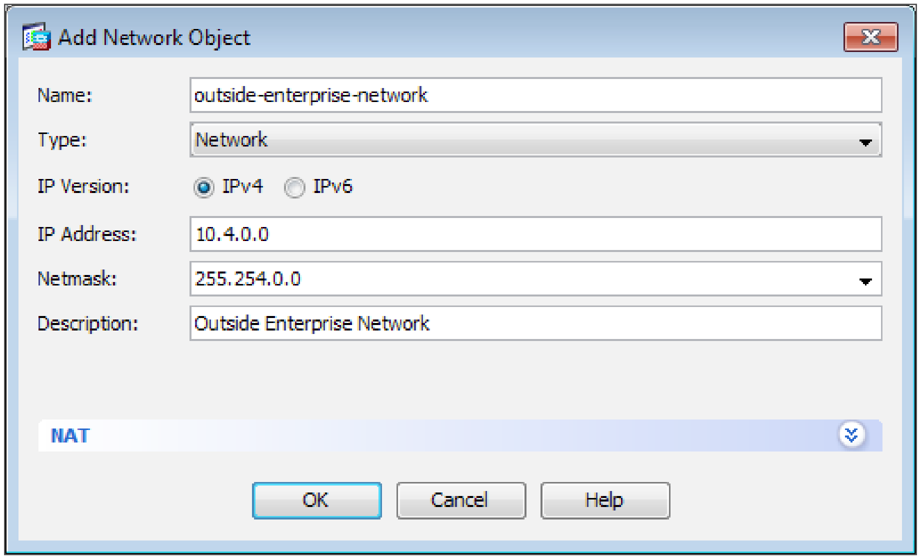
Step 6: On the Browse Source dialog box, locate the object (Example: inside-plant-voice-102), double-click the object, and then click **OK**.

Step 7: In the **Destination** box, click the ellipsis button (**...**). The Browse Destination dialog box appears.

Step 8: On the Browse Destination dialog box, in the **Add** list, choose **Network Object**.

Step 9: On the Add Network Object dialog box, enter the following, and then click **OK**:

- Name—**outside-enterprise-network**
- Type—**Network**
- IP Address—**10.4.0.0**
- Netmask—**255.254.0.0**


Add Network Object

Name: outside-enterprise-network

Type: Network

IP Version: ● IPv4 ○ IPv6

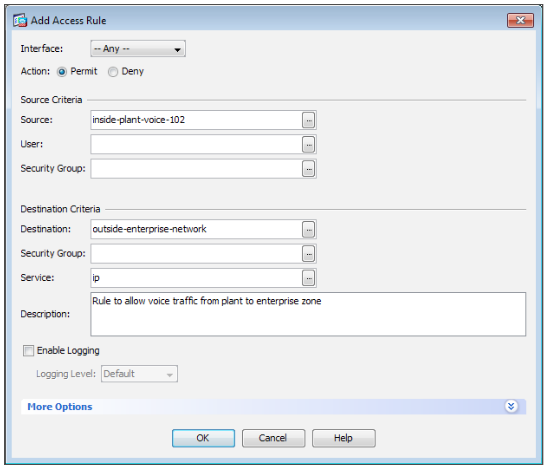
IP Address: 10.4.0.0

Netmask: 255.254.0.0

Description: Outside Enterprise Network

Step 10: On the Browse Destination dialog box, locate the object (Example: outside-enterprise-network), double-click the object, and then click **OK**.

Step 11: On the Add Access Rule dialog box, click **OK**.


Add Access Rule

Interface: -- Any --

Action: ● Permit ○ Deny

Source Criteria

Source: inside-plant-voice-102

User:

Security Group:

Destination Criteria

Destination: outside-enterprise-network

Security Group:

Service: ip

Description: Rule to allow voice traffic from plant to enterprise zone

□ Enable Logging

Logging Level: Default

Step 12: At the bottom of the window, click **Apply**. This saves the configuration.

Process

Configuring the Server DMZ

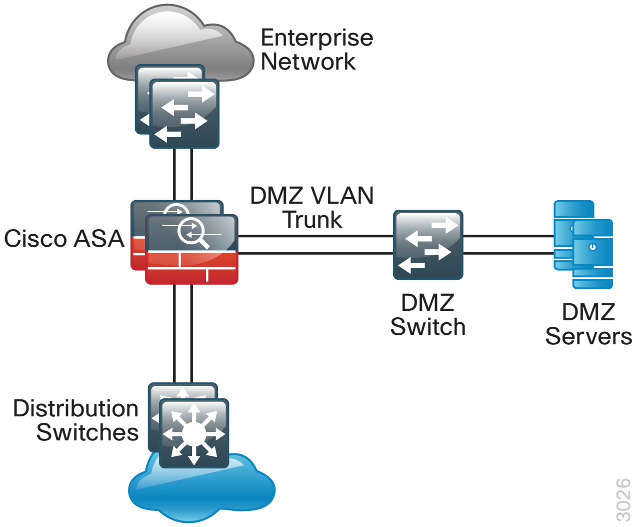
1. Configure server interface on DMZ switch
2. Configure DMZ interface on Cisco ASA
3. Configure static NAT for DMZ server
4. Permit RDP access to DMZ server

The firewall's demilitarized zone (DMZ) is a portion of the network where, typically, traffic to and from other parts of the network is tightly restricted. Organizations place network services and servers in a DMZ in order to make them accessible from the enterprise network. These servers are typically not allowed to initiate connections to the industrial Ethernet network, except for specific circumstances.

In this process, you configure a DMZ in order to enable you to host enterprise-accessible servers in the DMZ of the industrial Ethernet network.

The DMZ is connected to the appliances on the appliances' GigabitEthernet interface via a VLAN trunk. This allows the greatest flexibility to connect additional DMZs, in event that new VLANs must be added. The trunk connects the appliances to a Cisco Catalyst 3750-X Series access-switch stack in order to provide resiliency. The DMZ VLAN interfaces on the Cisco ASA appliances are each assigned an IP address that is the default gateway for each of the VLAN subnets. The DMZ switch only offers Layer-2 switching capability; the DMZ switch's VLAN interfaces do not have an IP address assigned, except for one VLAN interface with an IP address for management of the switch.

Figure 6 - Server DMZ VLAN topology



The number of secure VLANs is arbitrary. The following deployment illustrates an example of one secured network. If multiple types of hosts are to be connected in an enterprise-network-facing DMZ, segmenting the DMZ along functional boundaries may be necessary, particularly because hosts that are exposed to the enterprise network are vulnerable and could offer a springboard to other hosts. Traffic between DMZ VLANs should be kept to a minimum. Placing servers that must share data on a single VLAN improves performance and reduces load on network devices.

Procedure 1 Configure server interface on DMZ switch

This procedure assumes that the DMZ switch has already been configured following the guidance in Procedure 1, "Configure the DMZ switch."

Step 1: Configure the DMZ server VLAN on the DMZ switch.

```
vlan 1228
 name dmz-server
```

Step 2: Configure the interfaces that connect to the appliances.

```
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport trunk allowed vlan add 1228
```

Step 3: Configure the interfaces that are connected to the servers.

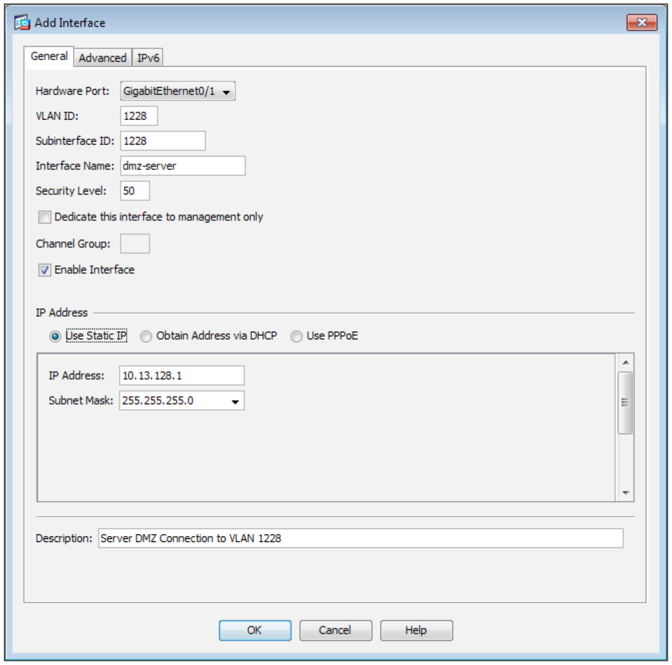
```
interface GigabitEthernet1/0/2
 description dmz-server
 switchport access vlan 1228
 switchport host
 macro apply EgressQoS
 logging event link-status
 no shutdown
```

Procedure 2 Configure DMZ interface on Cisco ASA

Step 1: Navigate to **Configuration > Device Setup > Interfaces**, and then in the **Add** list, choose **Interface**. The Add Interface dialog box appears.

Step 2: On the Add Interface dialog box, enter the following, and then click **OK**:

- Hardware Port—**GigabitEthernet0/1**
- VLAN ID—**1228**
- Subinterface ID—**1228**
- Interface Name—**dmz-server**
- Security Level—**50**
- Enable Interface—**Selected**
- IP Address—**10.13.128.1**
- Subnet Mask—**255.255.255.0**



Hardware Port: GigabitEthernet0/1

VLAN ID: 1228

Subinterface ID: 1228

Interface Name: dmz-server

Security Level: 50

□ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address: 10.13.128.1

Subnet Mask: 255.255.255.0

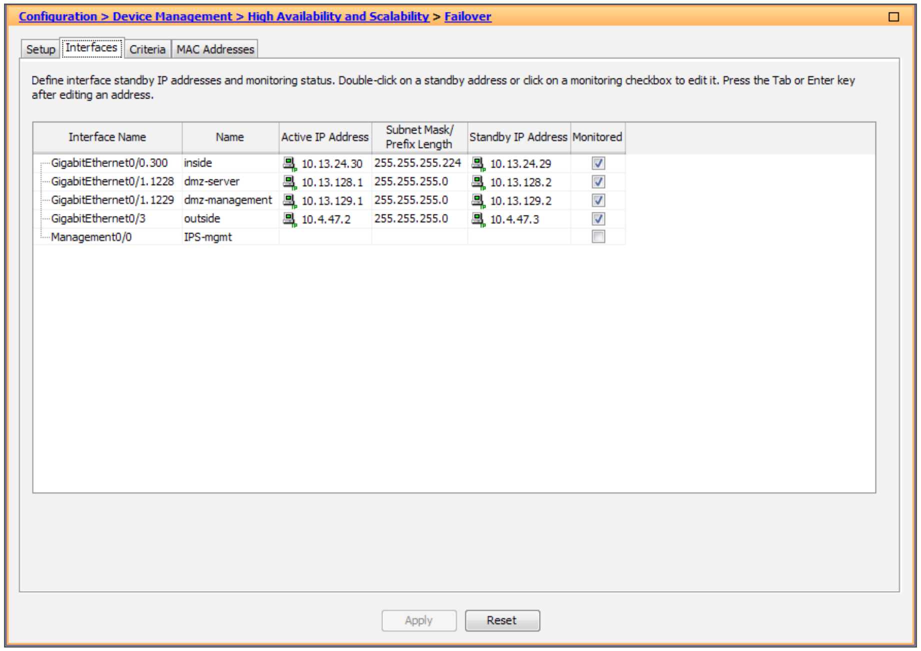
Description: Server DMZ Connection to VLAN 1228

Step 3: At the bottom of the window, click **Apply**. This saves the configuration.

Step 4: Navigate to **Configuration > Device Management > High Availability and Scalability > Failover > Interfaces**. On the Interfaces tab, the interfaces you configured are displayed.

Step 5: Select the management interface (Example: dmz-server), click the empty **Standby IP Address** field, enter the failover address (Example: 10.13.128.2), and then press **Enter**.

Step 6: Select **Monitored**, and then click **Apply**.


Configuration > Device Management > High Availability and Scalability > Failover
Setup
Interfaces
Criteria
MAC Addresses

Define interface standby IP addresses and monitoring status. Double-click on a standby address or click on a monitoring checkbox to edit it. Press the Tab or Enter key after editing an address.

Interface Name	Name	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/0.300	inside	10.13.24.30	255.255.255.224	10.13.24.29	☑
GigabitEthernet0/1.1228	dmz-server	10.13.128.1	255.255.255.0	10.13.128.2	☑
GigabitEthernet0/1.1229	dmz-management	10.13.129.1	255.255.255.0	10.13.129.2	☑
GigabitEthernet0/3	outside	10.4.47.2	255.255.255.0	10.4.47.3	☑
Management0/0	IPS-mgmt				□

Procedure 3 Configure static NAT for DMZ server

For access to services in the DMZ from the enterprise network, two options are available. The industrial Ethernet network, 10.13.0.0/16, can be routed in the enterprise network, or NAT can be configured to translate an existing enterprise network address to a server in the DMZ. In this example, the latter option was chosen.

Tech Tip

This procedure provides guidance on configuring NAT for a Remote Desktop Protocol (RDP) server that is located in the DMZ. If other services need to be configured within the DMZ, repeat the following process for additional services.

The example address mapping from the DMZ to the enterprise network is shown in Table 4.

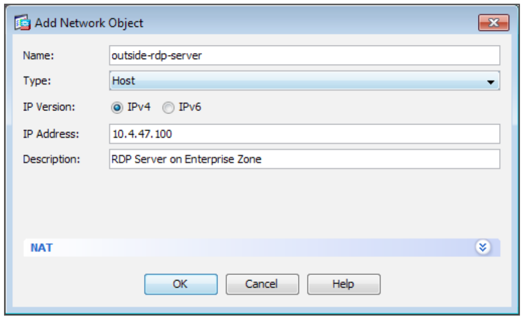
Table 4 - DMZ address mapping

RDP server DMZ address	RDP server public address (externally routable after NAT)
10.13.128.100	10.4.47.100

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**, and then in the **Add** list, choose **Network Object**.

Step 2: On the Add Network Object dialog box, enter the following, and then click **OK**:

- Name—**outside-rdp-server**
- Type—**Host**
- IP Version—**IPv4**
- IP Address—**10.4.47.100**


Add Network Object

Name: outside-rdp-server
Type: Host
IP Version: ● IPv4 ○ IPv6
IP Address: 10.4.47.100
Description: RDP Server on Enterprise Zone

Step 3: At the bottom of the window, click **Apply**. This saves the configuration.

Next, you add a network object for the private DMZ address of the RDP server.

Step 4: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**, and then in the **Add** list, choose **Network Object**.

Step 5: On the Add Network Object dialog box, enter the following:

- Name—**dmz-rdp-server**
- Type—**Host**
- IP Version—**IPv4**
- IP Address—**10.13.128.100**

Step 6: Next to **NAT**, click the two down arrows. The NAT section expands.

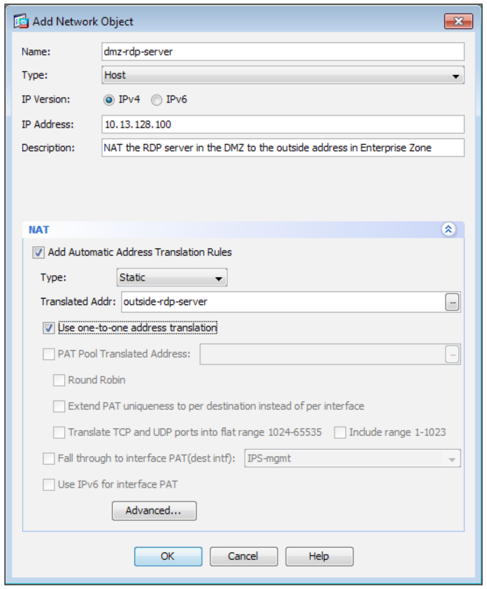
Step 7: Select **Add Automatic Address Translation Rules**.

Step 8: In the **Type** list, choose **Static**.

Step 9: In the **Translated Addr** list, click the ellipsis button (**...**). The Browse Translated Address dialog box appears.

Step 10: On the Browse Translated Address dialog box, locate the object (Example: outside-rdp-server), double-click the object, and then click **OK**.

Step 11: Select **Use one-to-one address translation**.



Add Network Object

Name: dmz-rdp-server

Type: Host

IP Version: ● IPv4 ○ IPv6

IP Address: 10.13.128.100

Description: NAT the RDP server in the DMZ to the outside address in Enterprise Zone

NAT

☑ Add Automatic Address Translation Rules

Type: Static

Translated Addr: outside-rdp-server

☑ Use one-to-one address translation

□ PAT Pool Translated Address:

□ Round Robin

□ Extend PAT uniqueness to per destination instead of per interface

□ Translate TCP and UDP ports into flat range 1024-65535 □ Include range 1-1023

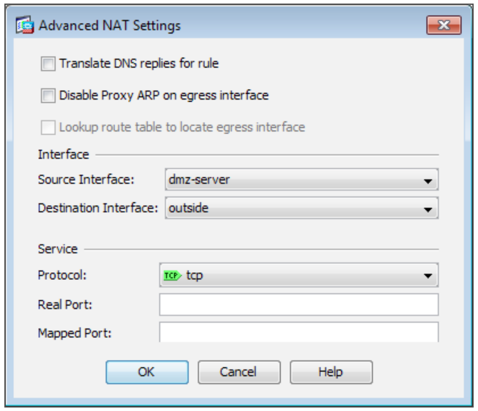
□ Fall through to interface PAT(dest intf): IPS-mgmt

□ Use IPv6 for interface PAT

Step 12: On the Add Network Object dialog box, click **Advanced**. The Advanced NAT Settings dialog box appears.

Step 13: On the Advanced NAT Settings dialog box, in the **Source Interface** list, choose **dmz-server**.

Step 14: On the Advanced NAT Settings dialog box, in the **Destination Interface** list, choose **outside**, and then **click OK**.



Advanced NAT Settings

□ Translate DNS replies for rule

□ Disable Proxy ARP on egress interface

□ Lookup route table to locate egress interface

Interface

Source Interface: dmz-server

Destination Interface: outside

Service

Protocol: tcp

Real Port:

Mapped Port:

Step 15: On the Add Network Object dialog box, click **OK**.

Step 16: At the bottom of the window, click **Apply**. This saves the configuration.

Procedure 4 Permit RDP access to DMZ server

The server DMZ in this example allows users on the enterprise network to connect to it via RDP. Then access can be permitted to resources in the industrial Ethernet network from the DMZ server without allowing direct access from the enterprise network.

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

Step 2: Click **Add** to create a new access rule.

Step 3: In the **Source** box, click the ellipsis button (**...**). The Browse Source dialog box appears.

Step 4: On the Browse Source dialog box, locate the object (Example: outside-enterprise-network), double-click the object, and then click **OK**.

Step 5: In the **Destination** box, click the ellipsis button (**...**). The Browse Destination dialog box appears.

Step 6: On the Browse Destination dialog box, locate the object (Example: dmz-server-network/24), double-click the object, and then click **OK**.

Step 7: On the Add Access Rule dialog box click **OK**.

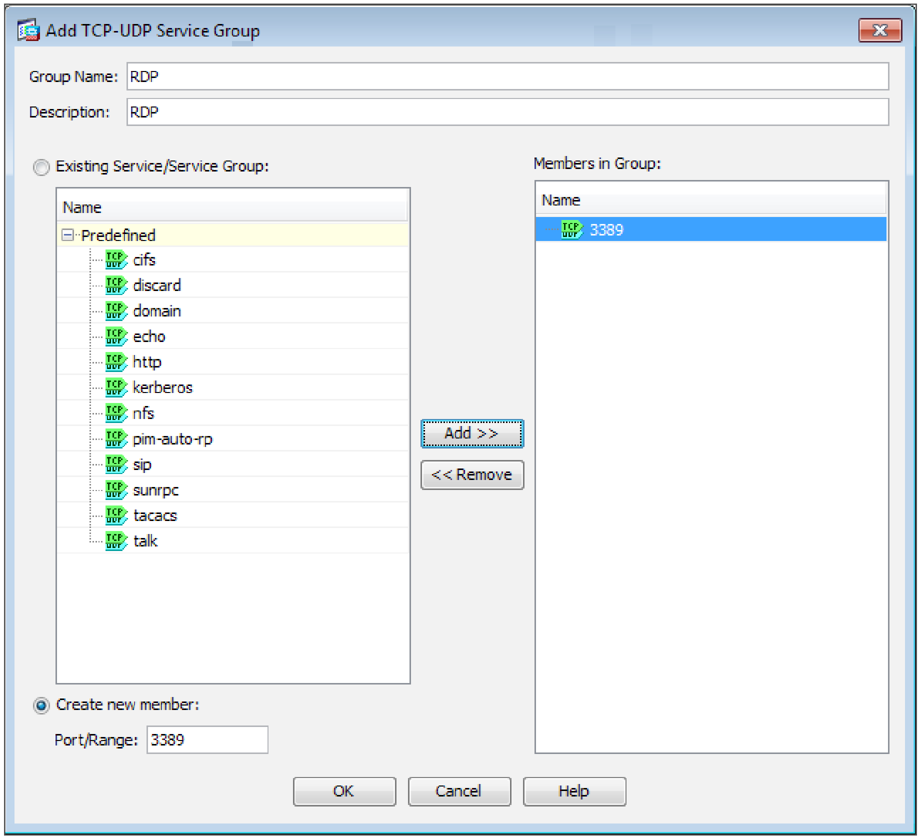
Step 8: In the **Service** box, click the ellipsis button (**...**). The Browse Service dialog box appears.

Step 9: On the **Browse Service** dialog box, click **Add**, and then click **TCP-UDP Service Group**.

Next, you create a new service group for RDP.

Step 10: On the Add TCP-UDP Service Group dialog box, in the **Group Name** box, enter a name for the protocol. (Example: RDP)

Step 11: Select **Create new member**, enter the port number for the protocol (Example: 3389), click **Add**, and then click **OK**.



Add TCP-UDP Service Group

Group Name: RDP

Description: RDP

○ Existing Service/Service Group:

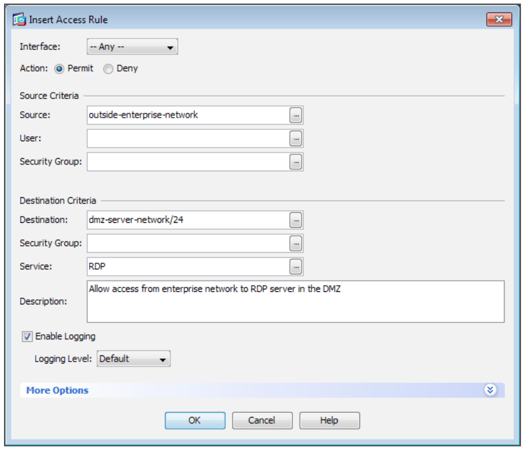
● Create new member:

Port/Range: 3389

Members in Group: 3389

Step 12: On the Browse Service dialog box, locate the following objects (Example: rdp), double-click the objects, and then click **OK**.

Step 13: Verify that the Add Access Rule dialog box resembles the following figure, and then click **OK**.



Interface: -- Any --

Action: ● Permit ○ Deny

Source Criteria

Source: outside-enterprise-network

User:

Security Group:

Destination Criteria

Destination: dmz-server-network/24

Security Group:

Service: RDP

Description: Allow access from enterprise network to RDP server in the DMZ

☑ Enable Logging

Logging Level: Default

Step 14: At the bottom of the window, click **Apply**. This saves the configuration.

Intrusion Prevention System

Process

Deploying Cisco IPS

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

Procedure 1 Configure the LAN switch access port

A LAN switch near the Cisco IPS sensor provides connectivity for the sensor's management interface. On the Cisco ASA 5500-X Series firewalls, the firewall and IPS software modules share a single management interface. This deployment uses the management interface for IPS software module access only, and the management interface is not used for the firewall.

Step 1: Configure the LAN distribution switch interfaces that are connected to the Cisco ASA management interfaces. This allows management access to the Cisco IPS software modules.

```
interface GigabitEthernet1/0/19
 description IPS-5515Xa
!
interface GigabitEthernet2/0/19
 description IPS-5515Xb
!
interface range GigabitEthernet1/0/19, GigabitEthernet2/0/19
 switchport access vlan 300
 switchport mode access
 spanning-tree portfast
```

Tech Tip

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

Procedure 2 Initialize the Cisco IPS software module

When a Cisco ASA 5500-X Series IPS Solution module is initially deployed, the software Cisco IPS software module may not be initialized, resulting in the Cisco ASA firewall being unaware of what code version to boot for the Cisco IPS software module. This procedure verifies the Cisco IPS software module status and prepares for configuration completion.

Step 1: From the Cisco ASA command-line interface, run the following command.

```
PE-ASA5515X# show module ips detail
```

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

```
PE-ASA5515X# show module ips detail
Getting details from the Service Module, please wait...

Card Type:          ASA 5515-X IPS Security Services Processor
Model:              ASA5515-IPS
Hardware version:   N/A
Serial Number:      FCH16257ATU
Firmware version:   N/A
Software version:   7.1(6)E4
MAC Address Range:  d48c.b54d.ab68 to d48c.b54d.ab68
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.1(6)E4
Data Plane Status:  Up
Status:             Up
```

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

```
PE-ASA5515X# 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:      FCH16257ATU
Firmware version:   N/A
Software version:
MAC Address Range:  d48c.b54d.ab68 to d48c.b54d.ab68
Data Plane Status:  Not Applicable
Status:             Unresponsive   No Image Present
...
```

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

Tech Tip

Cisco IPS recovery requires an image with file extension .aip

Cisco IPS upgrades require an image with file extension .pkg

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

```
PE-ASA5515X# dir
Directory of disk0:/
128    -rwx  37416960     14:53:34 Dec 03 2012  asa901-smp-k8.
bin
140    -rwx  17738924     11:12:33 Dec 03 2012  asdm-702.bin
139    -rwx  45854720     11:30:16 Sep 19 2012  IPS-SSP_5515-
K9-sys-1.1-a-7.1-6-E4.aip
```

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

```
PE-ASA5515X# sw-module module ips recover configure image 
disk0:/IPS-SSP_5515-K9-sys-1.1-a-7.1-6-E4.aip
PE-ASA5515X# 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.
```

Step 5: After a few minutes the recovery will complete, run the following command, and then verify that the module status is **Up**.

```
PE-ASA5515X# show module ips detail
```

Procedure 3 Complete the initial setup

The initial setup involves configuring each Cisco IPS device (module or appliance) with the initial networking information in order to allow the use of the GUI to complete the configuration. This procedure shows the configuration of Cisco IPS software modules in a pair of Cisco ASA 5515-X appliances. Adjust this example in order to meet your organization's requirements.

Table 5 - Cisco IPS device configuration

	Plant edge Cisco IPS A	Plant edge Cisco IPS B
Device type	Software module	Software module
Host name	IPS-5515Xa	IPS-5515Xb
IP address	10.13.24.27	10.13.24.28
Network mask	255.255.255.224	255.255.255.224
Default gateway	10.13.24.1	10.13.24.1
Location	Plant edge	Plant edge

Step 1: If you are using Cisco ASA , log into the appliance, and then access the Cisco IPS software module.

```
PE-ASA5515X# session ips
Opening command session with module ips.
Connected to module ips. Escape character sequence is 'CTRL-
^X'.
```

Tech Tip

The default username and password for the Cisco IPS software module is cisco/cisco. If this is the first time the sensor has been logged into, there will be a prompt 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 the organization.

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

Step 2: Run the **setup** command. The module starts the System Configuration Dialog.

```
sensor# setup
Enter host name[sensor]: IPS-5515Xa
Enter IP interface[]: 10.13.24.27/27,10.13.24.1
Modify current access list?[no]: yes
Current access list entries:
   No entries
Permit: 10.13.48.0/24
Permit:
Use DNS server for Global Correlation?[no]: yes
   DNS server IP address[]: 10.13.48.10
Use HTTP proxy server for Global Correlation?[no]: no
Modify system clock settings?[no]: no
Participation in the SensorBase Network allows Cisco to
collect aggregated statistics about traffic sent to your IPS.
SensorBase Network Participation level?[off]: partial
...
Do you agree to participate in the SensorBase Network?[no]:yes
...
[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
...
--- Configuration Saved ---

Complete the advanced setup using CLI or IDM.
To use IDM, point your web browser at https://<sensor-ip-
address>.
```

Step 3: Enter **exit**. The Cisco ASA command-line interface returns.

Step 4: Repeat Step 1 through Step 3Step 2 for the Cisco IPS software module in the standby Cisco ASA appliance.

Tech Tip

A different host name and IP address must be used on each Cisco IPS device so that monitoring systems do not get confused. In this example, IPS-5515Xb and 10.13.24.28 were used on the standby Cisco ASA 5500-X Series IPS Solution module.

Procedure 4 Finish the basic configuration

Once the basic setup in the System Configuration Dialog is complete, you use the startup wizard in the integrated management tool, Cisco Adaptive Security Device Manager, for Cisco ASAs in order to complete the remaining Cisco IPS configuration tasks:

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

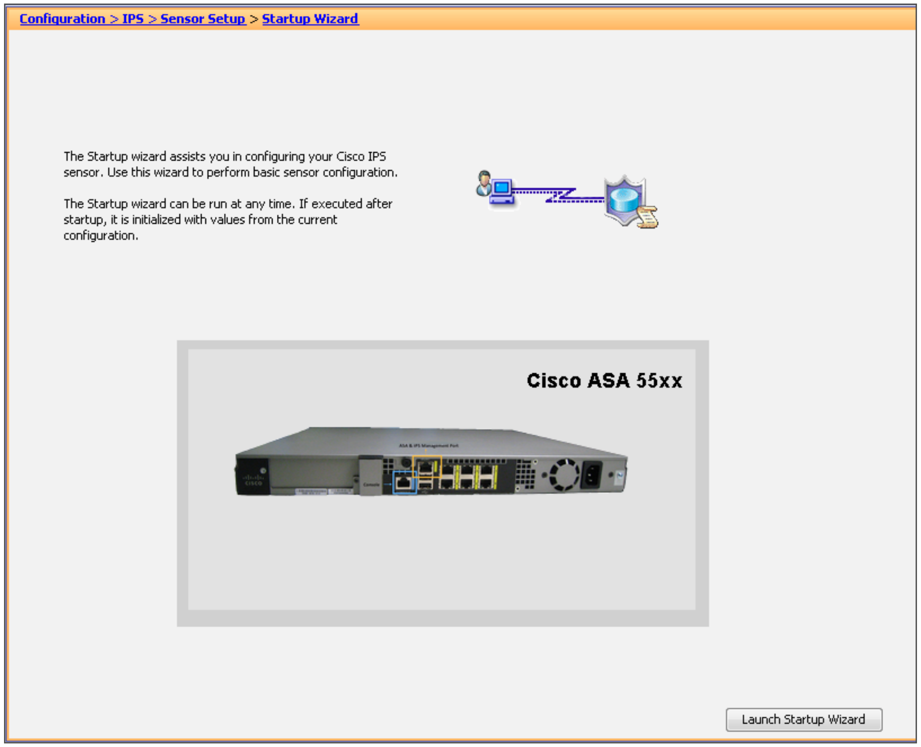
Step 1: From a client on the internal industrial Ethernet network, navigate to the primary firewall's inside IP address, and then launch Cisco ASDM. (Example: https://10.13.24.30)

Step 2: Click the **Configuration** tab, and then click **IPS**.

Step 3: On the Connecting to IPS dialog box, enter the IP address, username, and password you specified on the Cisco IPS sensor, and then click **Continue**.

Cisco ASDM imports the current configuration from the Cisco IPS sensor, and the startup wizard launcher is displayed in the main window.

Step 4: Click **Launch Startup Wizard**.



Configuration > IPS > Sensor Setup > Startup Wizard

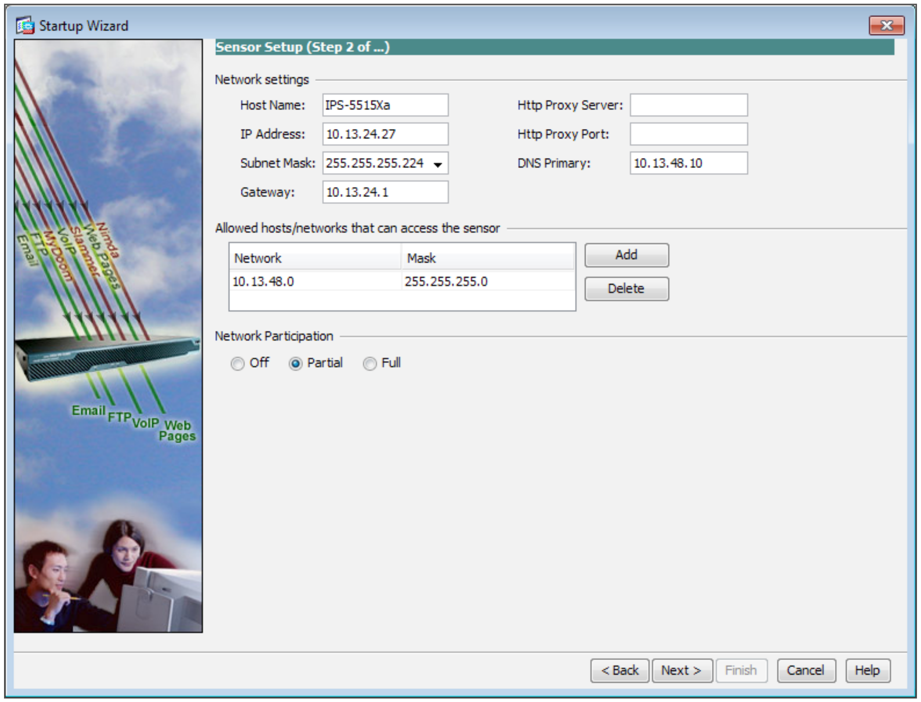
The Startup wizard assists you in configuring your Cisco IPS sensor. Use this wizard to perform basic sensor configuration.

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

Cisco ASA 55xx

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

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



Startup Wizard

Sensor Setup (Step 2 of ...)

Network settings

Host Name: IPS-5515Xa

IP Address: 10.13.24.27

Subnet Mask: 255.255.255.224

Gateway: 10.13.24.1

Http Proxy Server:

Http Proxy Port:

DNS Primary: 10.13.48.10

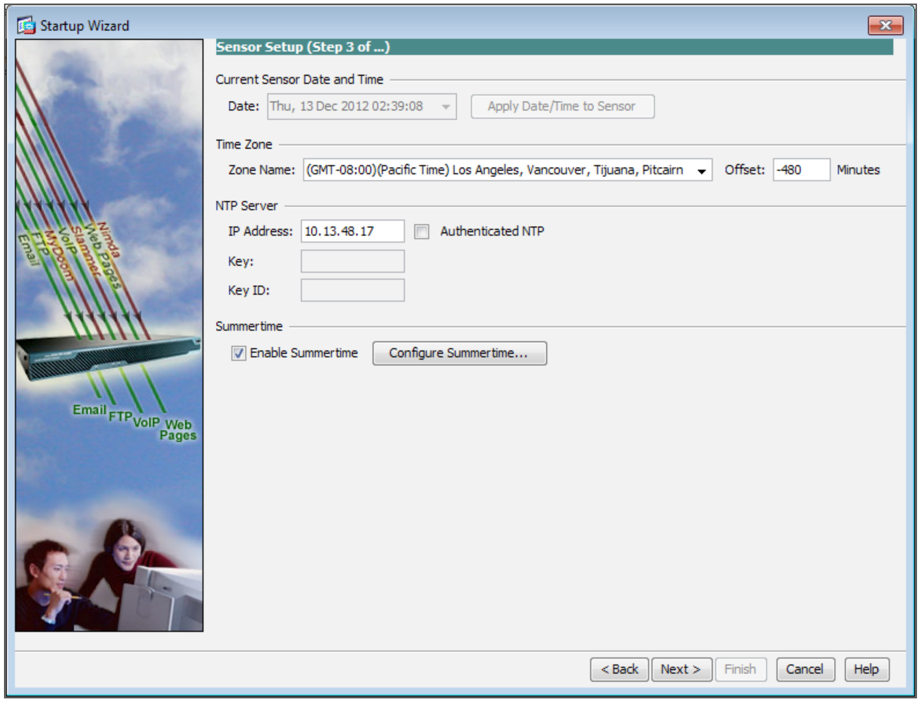
Allowed hosts/networks that can access the sensor

Network	Mask
10.13.48.0	255.255.255.0

Network Participation

○ Off ● Partial ○ Full

- On the next Sensor Setup page, in the **Zone Name** list, choose the appropriate time zone. Enter the NTP Server IP address (Ex: 10.13.48.17), ensure that **Authenticated NTP** is clear, set the summertime settings, and then click **Next**.



Sensor Setup (Step 3 of ...)

Current Sensor Date and Time

Date: Thu, 13 Dec 2012 02:39:08 Apply Date/Time to Sensor

Time Zone

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

NTP Server

IP Address: 10.13.48.17 □ Authenticated NTP

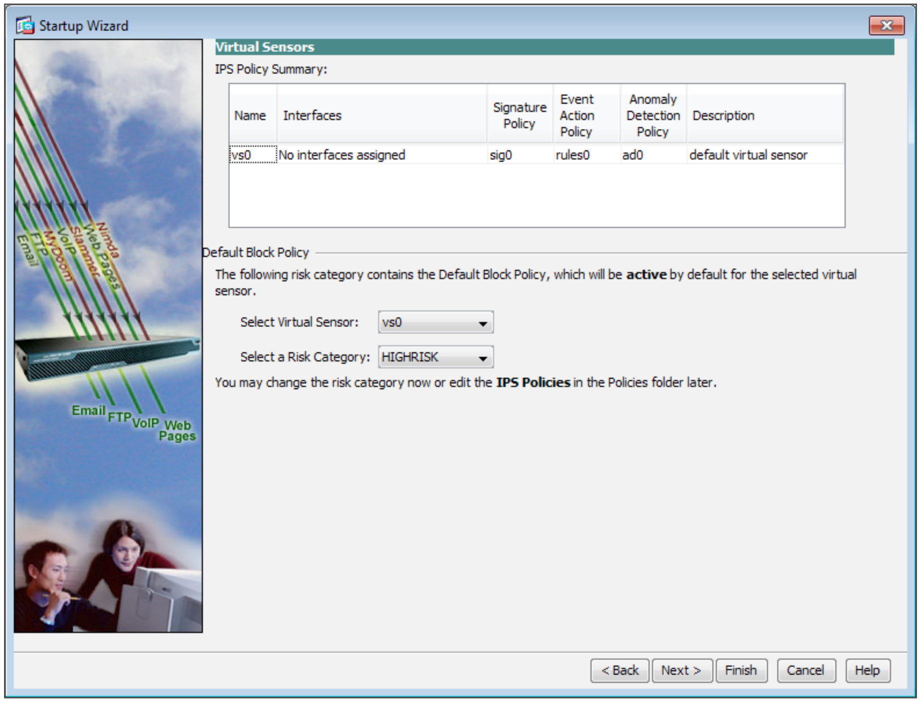
Key:

Key ID:

Summertime

☑ Enable Summertime Configure Summertime...

- On the Virtual Sensors page, click **Next**.



Virtual Sensors

IPS Policy Summary:

Name	Interfaces	Signature Policy	Event Action Policy	Anomaly Detection Policy	Description
vs0	No interfaces assigned	sig0	rules0	ad0	default virtual sensor

Default Block Policy

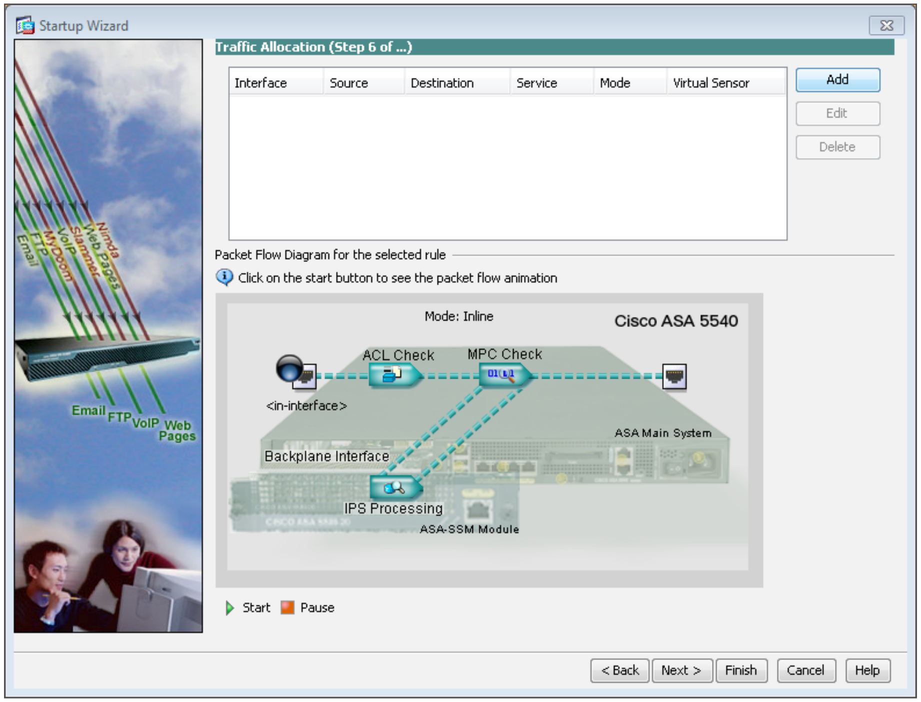
The following risk category contains the Default Block Policy, which will be **active** by default for the selected virtual sensor.

Select Virtual Sensor: vs0

Select a Risk Category: HIGHRISK

You may change the risk category now or edit the **IPS Policies** in the Policies folder later.

- On the Traffic Allocation page, click **Add**.



Startup Wizard

Traffic Allocation (Step 6 of ...)

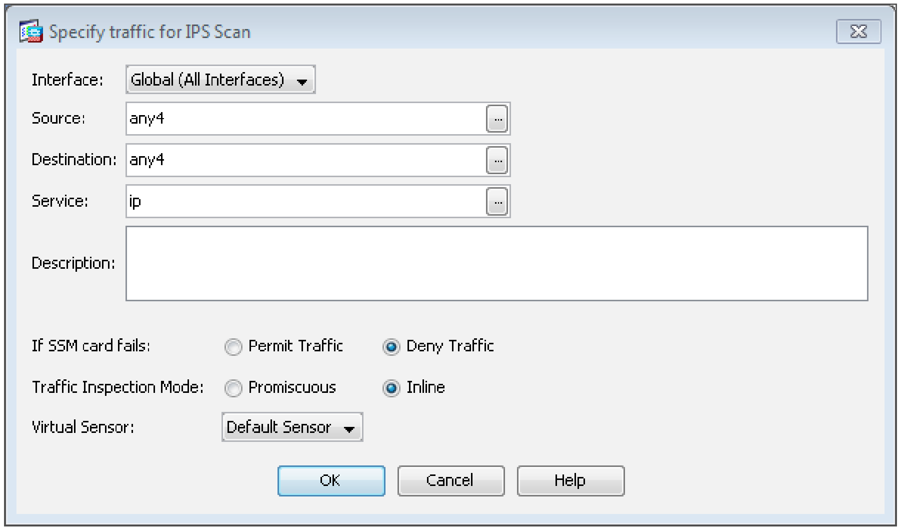
Interface	Source	Destination	Service	Mode	Virtual Sensor

Packet Flow Diagram for the selected rule

Click on the start button to see the packet flow animation

If Cisco ASA already has a default traffic allocation policy, a "The Service Rule Policy you are trying to create already exists" message appears. If you receive this message, click **Cancel**, and then on the Traffic Allocation page, click **Next**.

If the Specify traffic for IPS Scan dialog box appears, for **Traffic Inspection Mode**, select **Inline**, and then click **OK**. On the Traffic Allocation page, click **Next**.



Specify traffic for IPS Scan

Interface: Global (All Interfaces)

Source: any4

Destination: any4

Service: ip

Description:

If SSM card fails: ○ Permit Traffic ● Deny Traffic

Traffic Inspection Mode: ○ Promiscuous ● Inline

Virtual Sensor: Default Sensor

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

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

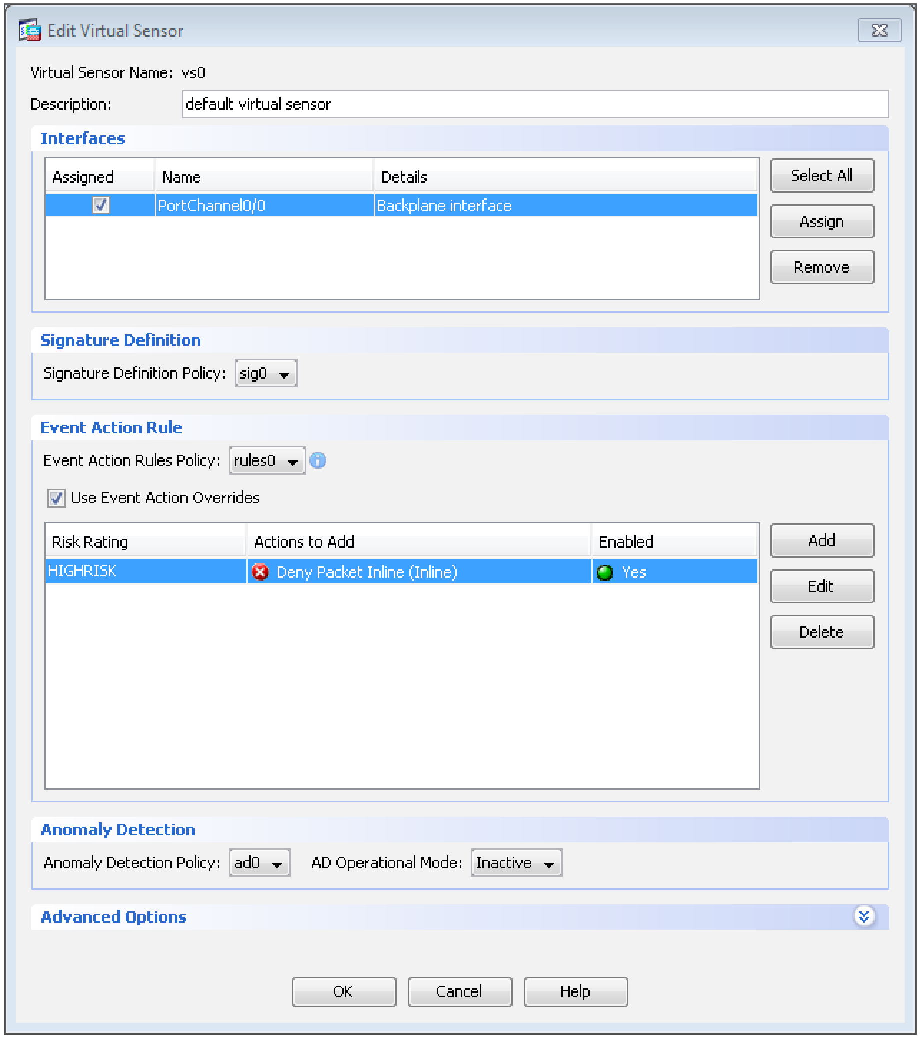
Step 7: Click **OK**. Do not reboot the IPS sensor yet.

Next, you assign interfaces to the virtual sensor.

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

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

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



Edit Virtual Sensor

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

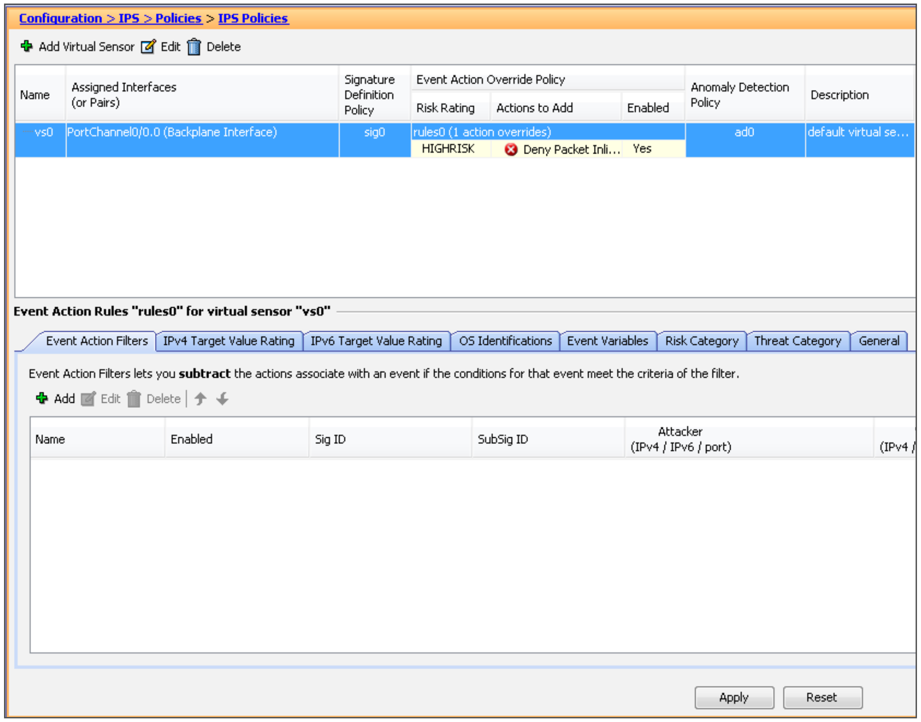
Risk Rating	Actions to Add	Enabled
HIGHRISK	Deny Packet Inline (Inline)	Yes

Anomaly Detection

Anomaly Detection Policy: ad0 AD Operational Mode: Inactive

Advanced Options

Step 11: Click **Apply**.



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		

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)	(IPv4 /

Next, you reboot the sensor.

Step 12: Navigate to **Sensor Management > Reboot Sensor**.

Step 13: Click **Reboot Sensor**, and then on the Reboot Sensor dialog box, click **OK**.

Step 14: Repeat this procedure for the Cisco IPS software module in the resilient Cisco ASA appliance. There is no configuration synchronization between the two Cisco IPS software modules like there is between the Cisco ASA firewalls. Note that in Step 1, from a client on the internal industrial Ethernet network, navigate to the resilient appliance's inside IP address, and then launch Cisco ASDM. (Example: https://10.13.24.29)

Tech Tip

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

Procedure 5 Modify the inline security policy

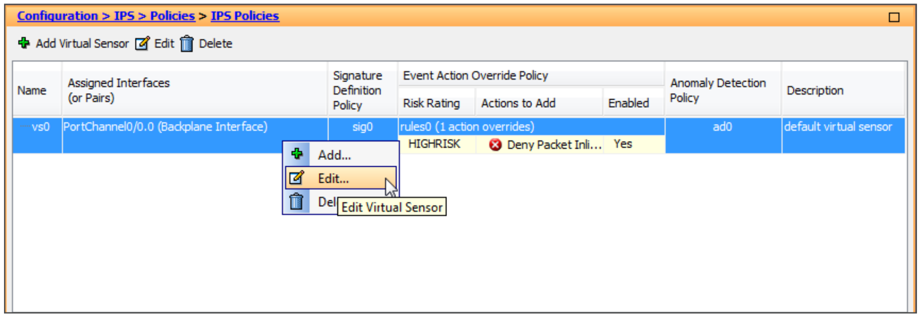
(Optional)

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

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

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

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

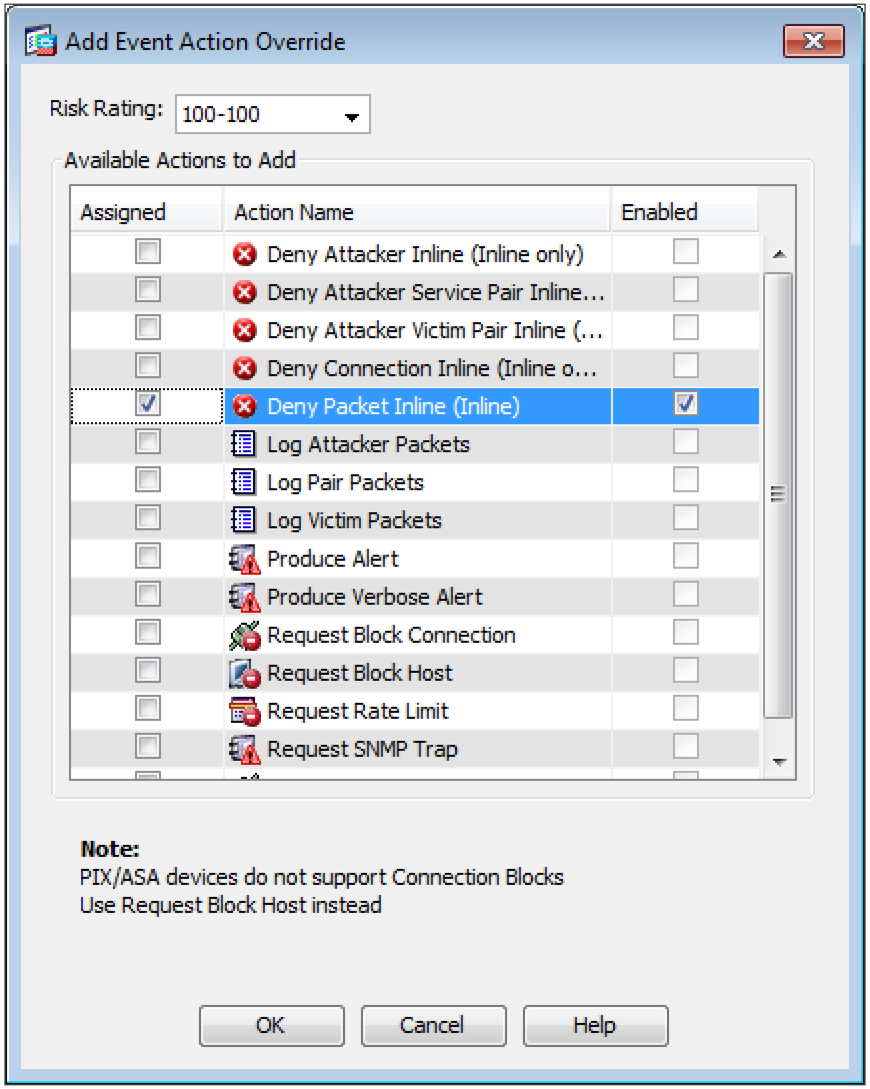


Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Event Action Override Policy			Anomaly Detection Policy	Description
			Risk Rating	Actions to Add	Enabled		
vs0	PortChannel0/0.0 (Backplane Interface)	sig0	rules0 (1 action overrides)			ad0	default virtual sensor
			HIGHRISK	Deny Packet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

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

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

Step 5: On the Add Event Action Override dialog box, in the **Risk Rating** box, type **100-100**, select the Assigned checkbox for **Deny Packet Inline**, and then click **OK**.



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 6: Click **Apply**.

Step 7: Repeat Step 1 through Step 6 for the Cisco IPS software module located on the standby firewall.

Remote-Access VPN

Process

Configuring the Remote-Access VPN

1. Configure remote access
2. Create the AAA server group
3. Define the VPN address pool
4. Configure remote-access routing
5. Configure the group URL
6. Configure the partner policy
7. Configure the admin policy
8. Configure Cisco AnyConnect client profile

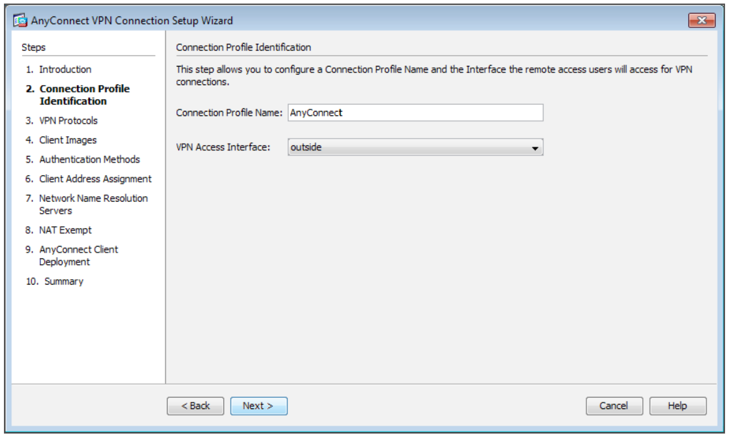
The majority of the VPN configuration tasks are addressed in the Cisco AnyConnect VPN Connection Setup Wizard. Depending on requirements, additional work might need to be completed after the wizard.

Procedure 1 Configure remote access

Step 1: Navigate to **Wizards > VPN Wizards > AnyConnect VPN Wizard**.

Step 2: In the AnyConnect VPN Connection Setup Wizard, on the Introduction page, click **Next**.

Step 3: On the Connection Profile Identification page, in the **Connection Profile Name** box, enter a name (Example: AnyConnect), and in the **VPN Access Interface** list, choose the enterprise edge connection (Example: outside), and then click **Next**.


AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
< Back
Next >
Cancel
Help

Connection Profile Identification

This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections.

Connection Profile Name: AnyConnect

VPN Access Interface: outside

Next, you generate a self-signed identity certificate and install it on the appliance.

Tech Tip

Note that because the certificate in this example is self-signed, clients generate a security warning until they accept the certificate.

Step 4: In the Device Certificate section, click **Manage** for Device Certificate with RSA key**.**

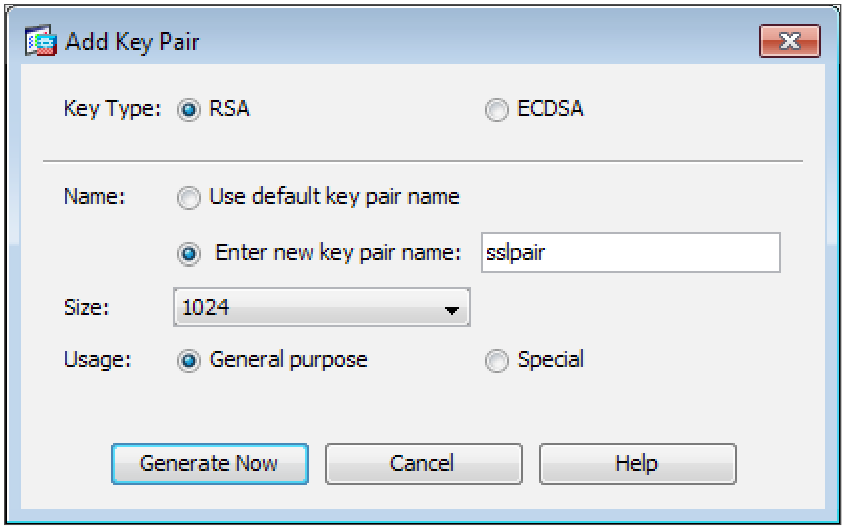
Step 5: On the Manage Identity Certificates dialog box, click **Add**.

Step 6: On the Add Identity Certificate dialog box, select **Add a new identity certificate**, and then for **Key Pair**, click **New**.

Tech Tip

Entering a new key pair name prevents the certificate from becoming invalid if an administrator accidentally regenerates the default RSA key pair.

Step 7: On the Add Key Pair dialog box, select **Enter new key pair name**, and in the box, enter a name (Example: sslpair), and then click **Generate Now**.



Add Key Pair

Key Type: ● RSA ○ ECDSA

Name: ○ Use default key pair name

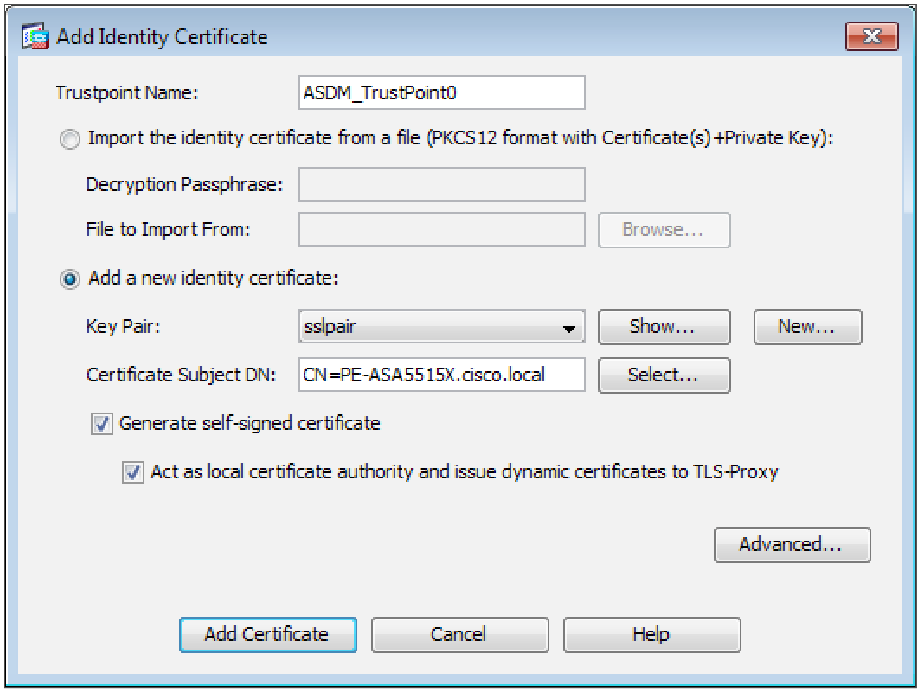
● Enter new key pair name: sslpair

Size: 1024

Usage: ● General purpose ○ Special

Step 8: On the Add Identity Certificate dialog box, in the **Certificate Subject DN** box, enter the fully qualified domain name used to access the appliance on the outside interface. (Example: CN=PE-ASA5515X.cisco.local)

Step 9: Select **Generate self-signed certificate** and **Act as Local certificate authority and issue dynamic certificates to TLS-Proxy**, and then click **Add Certificate**.



Add Identity Certificate

Trustpoint Name: ASDM_TrustPoint0

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: sslpair

Certificate Subject DN: CN=PE-ASA5515X.cisco.local

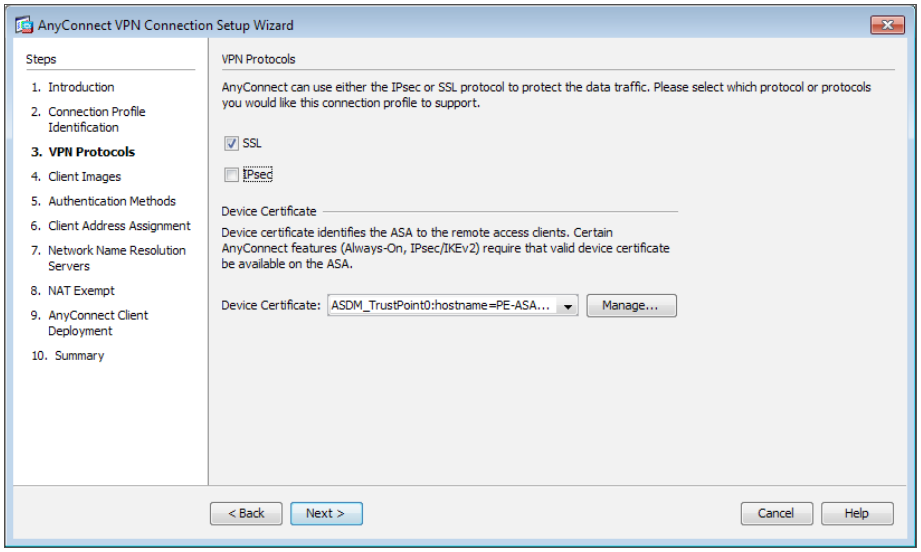
☑ Generate self-signed certificate

☑ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Step 10: On the Enrollment Status message showing that the enrollment succeeded, click **OK**.

Step 11: On the Manage Identity Certificates dialog box, click **OK**.

Step 12: On the VPN Protocols page, clear **IPsec**, verify that the certificate you created is reflected in the **Device Certificate** list, and then click **Next**.


AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
VPN Protocols
< Back
Next >
Cancel
Help
Manage...

AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.

☑ SSL

□ IPsec

Device Certificate

Device certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.

Device Certificate: ASDM_TrustPoint0:hostname=PE-ASA...

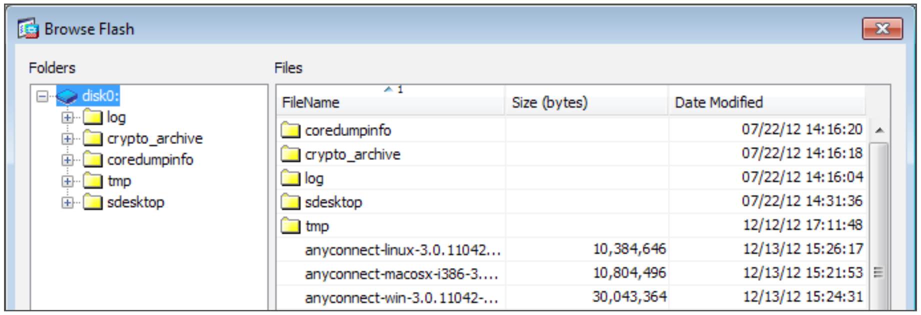
Step 13: On the Client Images page, click **Add**.

Step 14: On the Add AnyConnect Client Image dialog box, click **Browse Flash**.

Tech Tip

If the appliance does not already have Cisco AnyConnect client images loaded in the flash disk, you can use the **Upload** button in order to install new or updated client images into the flash disk of the appliance.

Step 15: On the Browse Flash dialog box, select the appropriate AnyConnect client image to support your user community, and then click **OK**.

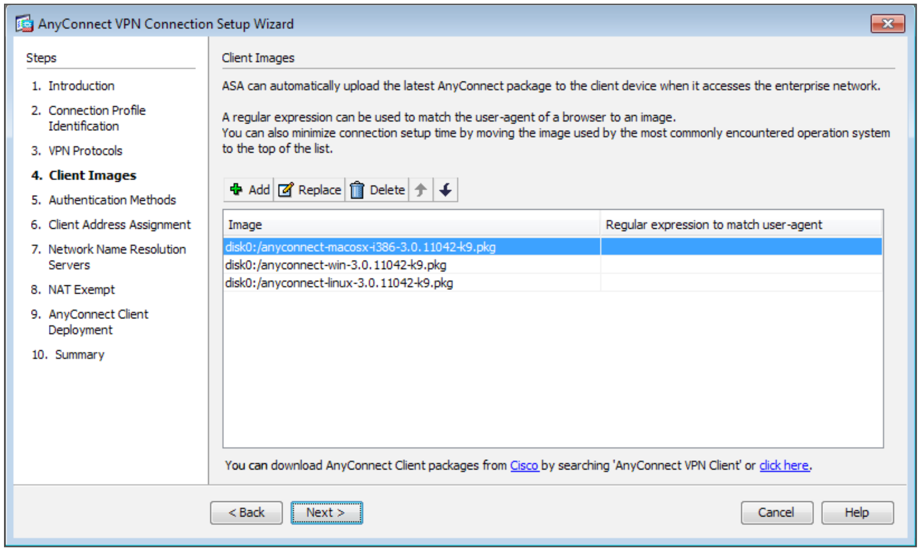


FileName	Size (bytes)	Date Modified
coredumpinfo		07/22/12 14:16:20
crypto_archive		07/22/12 14:16:18
log		07/22/12 14:16:04
sdesktop		07/22/12 14:31:36
tmp		12/12/12 17:11:48
anyconnect-linux-3.0.11042...	10,384,646	12/13/12 15:26:17
anyconnect-macosx-i386-3....	10,804,496	12/13/12 15:21:53
anyconnect-win-3.0.11042-...	30,043,364	12/13/12 15:24:31

Step 16: On the Add AnyConnect Client Image dialog box, click **OK**.

Step 17: Repeat Step 13 through Step 16 for all the required Cisco AnyConnect client images.

Step 18: On the Client Images page, click **Next**.


AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
Client Images
Add
Replace
Delete
< Back
Next >
Cancel
Help

ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network.

A regular expression can be used to match the user-agent of a browser to an image.
You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

Image	Regular expression to match user-agent
disk0:/anyconnect-macosx-i386-3.0.11042-k9.pkg	
disk0:/anyconnect-win-3.0.11042-k9.pkg	
disk0:/anyconnect-linux-3.0.11042-k9.pkg	

You can download AnyConnect Client packages from Cisco by searching 'AnyConnect VPN Client' or click here.

Remaining in the wizard, you now create a new AAA server group in order to authenticate remote-access users. To authenticated users, the server group uses either NT LAN Manager (NTLM) to the Active Directory server or RADIUS to the Cisco Secure ACS server.

Procedure 2 Create the AAA server group

For VPN user authentication, you point Cisco ASA to either the plant Cisco Secure ACS server or to the plant Active Directory server.

Reader Tip

Please refer to the "Configuring Cisco Secure ACS" section of this guide for procedure details on how to configure the Cisco Secure ACS server.

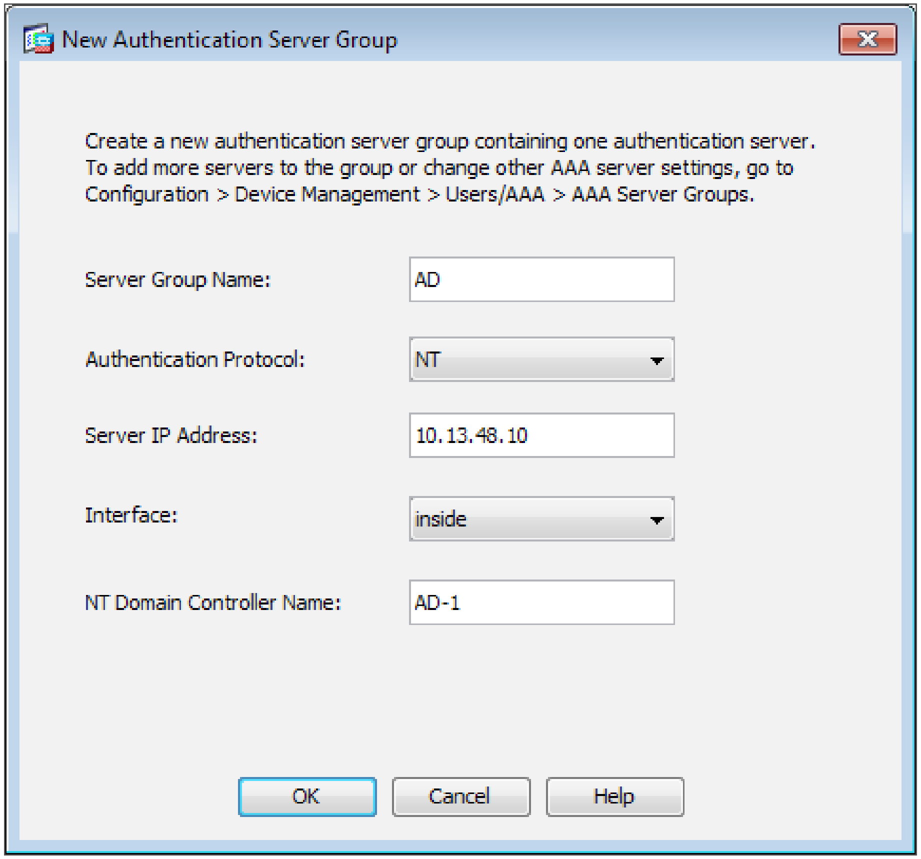
If the authentication process authenticates directly to Active Directory, complete Option 1 of this procedure. If the authentication process uses Cisco Secure ACS, complete Option 2 of this procedure.

Option 1. Use Active Directory for AAA

Step 1: On the Authentication Methods page, next to **AAA Server Group**, click **New**.

Step 2: On the New Authentication Server Group dialog box, enter the following values, and then click **OK**:

- Server Group Name—**AD**
- Authentication Protocol—**NT**
- Server IP Address—**10.13.48.10** (IP address of the Active Directory server)
- Interface—**inside**
- NT Domain Controller Name—**AD-1**



New Authentication Server Group

Create a new authentication server group containing one authentication server.
To add more servers to the group or change other AAA server settings, go to Configuration > Device Management > Users/AAA > AAA Server Groups.

Server Group Name: AD

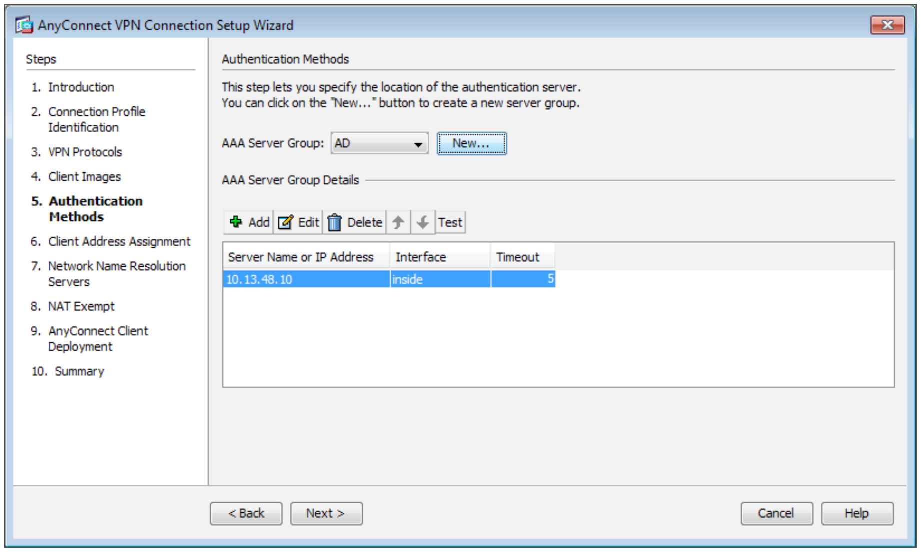
Authentication Protocol: NT

Server IP Address: 10.13.48.10

Interface: inside

NT Domain Controller Name: AD-1

Step 3: On the Authentication Methods page, click **Next**.


AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
Add
Edit
Delete
Test
< Back
Next >
Cancel
Help

Authentication Methods

This step lets you specify the location of the authentication server.
You can click on the "New..." button to create a new server group.

AAA Server Group: AD New...

AAA Server Group Details

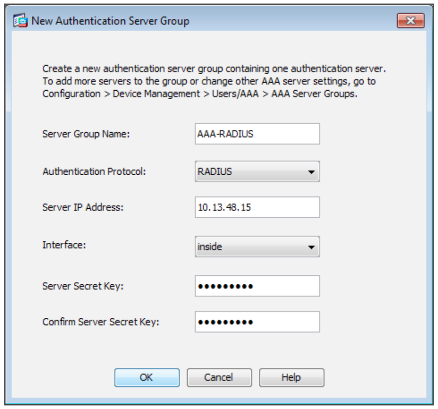
Server Name or IP Address	Interface	Timeout
10.13.48.10	inside	5

Option 2. Use Cisco Secure ACS for AAA

Step 1: On the Authentication Methods page, next to **AAA Server Group**, click **New**.

Step 2: On the New Authentication Server Group dialog box, enter the following values, and then click **OK**:

- Server Group Name—**AAA-RADIUS**
- Authentication Protocol—**RADIUS**
- Server IP Address—**10.13.48.15** (IP address of the Cisco Secure ACS server)
- Interface—**inside**
- Server Secret Key—**SecretKey**
- Confirm Server Secret Key—**SecretKey**



Create a new authentication server group containing one authentication server.
To add more servers to the group or change other AAA server settings, go to
Configuration > Device Management > Users/AAA > AAA Server Groups.

Server Group Name: AAA-RADIUS

Authentication Protocol: RADIUS

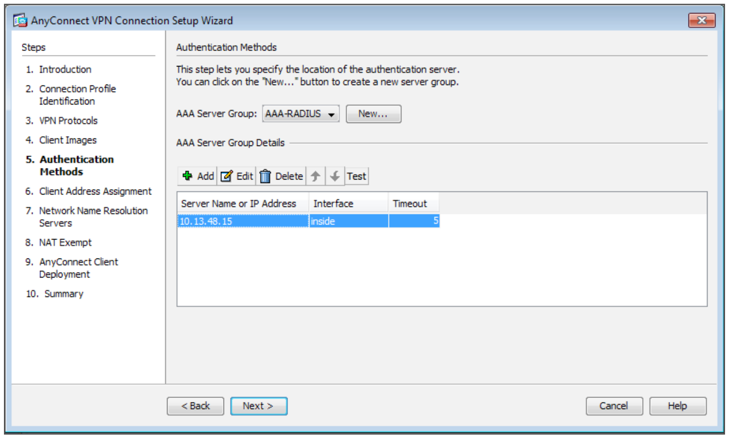
Server IP Address: 10.13.48.15

Interface: inside

Server Secret Key: •••••••••

Confirm Server Secret Key: •••••••••

Step 3: On the Authentication Methods page, click **Next**.


AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
Add
Edit
Delete
Test
< Back
Next >
Cancel
Help

Authentication Methods

This step lets you specify the location of the authentication server.
You can click on the "New..." button to create a new server group.

AAA Server Group: AAA-RADIUS New...

AAA Server Group Details

Server Name or IP Address	Interface	Timeout
10.13.48.15	inside	5

Next, you define the remote-access VPN address pool that will be assigned to users when they connect to the VPN service.

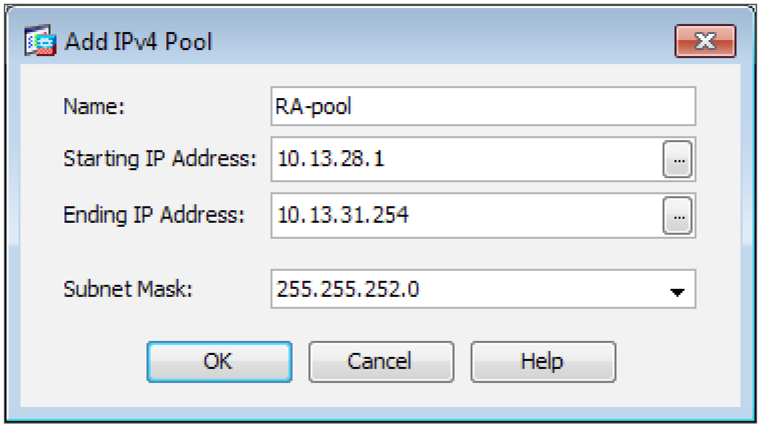
Procedure 3 Define the VPN address pool

You need to decide on an appropriate address space for your remote-access VPN address pool. In this example you use 4 class-C address ranges (~1000 addresses) as the pool.

Step 1: On the Client Address Assignment page, on the IPv4 Address Pool tab, click **New**.

Step 2: On the Add IP Pool dialog box, enter the following values, and then click **OK**:

- Name—RA-pool
- Starting IP Address—10.13.28.1
- Ending IP Address—10.13.31.254
- Subnet Mask—255.255.252.0



Add IPv4 Pool

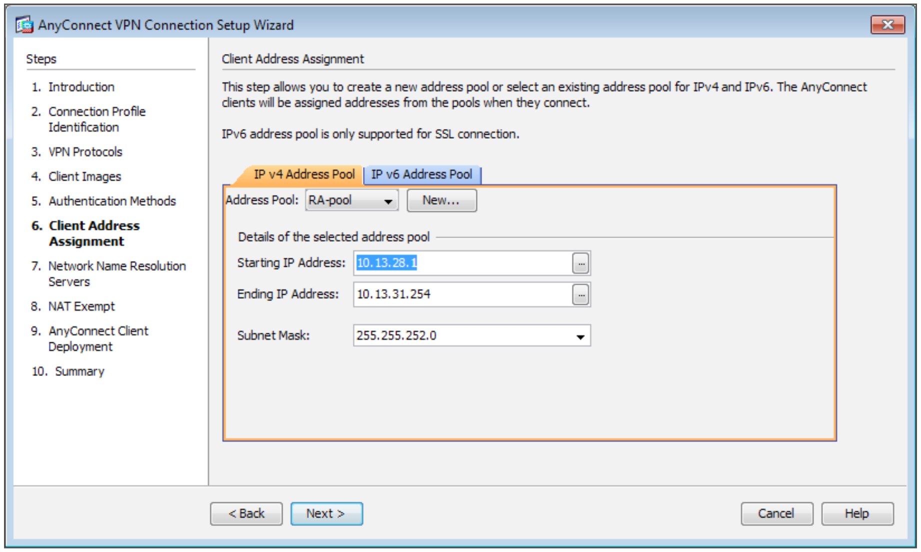
Name: RA-pool

Starting IP Address: 10.13.28.1

Ending IP Address: 10.13.31.254

Subnet Mask: 255.255.252.0

Step 3: On the Client Address Assignment page, in the **Address Pool** list, verify that the pool you just created is selected, and then click **Next**.



AnyConnect VPN Connection Setup Wizard

Client Address Assignment

This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect.

IPv6 address pool is only supported for SSL connection.

Address Pool: RA-pool

Details of the selected address pool

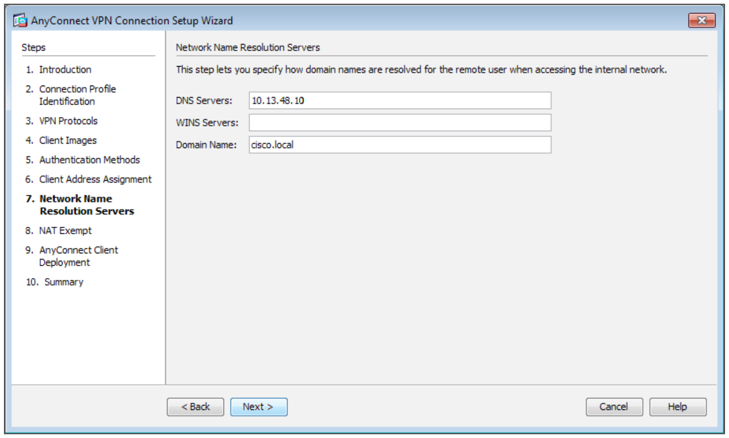
Starting IP Address: 10.13.28.1

Ending IP Address: 10.13.31.254

Subnet Mask: 255.255.252.0

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
IP v4 Address Pool
IP v6 Address Pool
New...
< Back
Next >
Cancel
Help

Step 4: On the Network Name Resolution Servers page, enter the organization's **DNS Servers** (Example: 10.13.48.10) and the organization's **Domain Name** (Example: cisco.local), and then click **Next**.



AnyConnect VPN Connection Setup Wizard

Network Name Resolution Servers

This step lets you specify how domain names are resolved for the remote user when accessing the internal network.

DNS Servers: 10.13.48.10

WINS Servers:

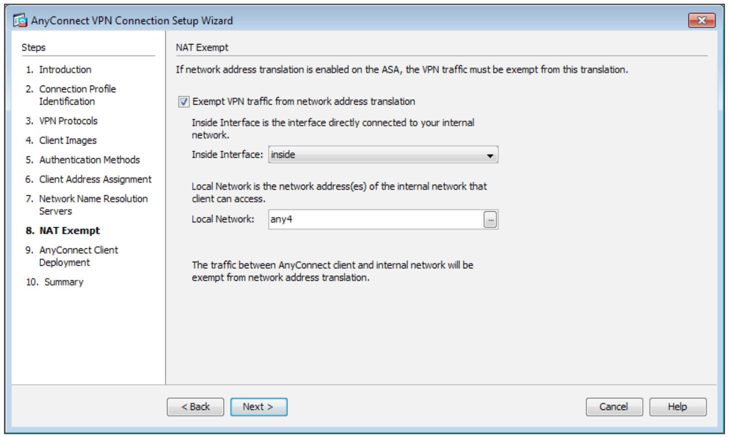
Domain Name: cisco.local

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
< Back
Next >
Cancel
Help

Step 5: On the NAT Exempt page, select **Exempt VPN traffic from network address translation**, in the **Insider Interface** list, choose **inside**, and in the **Local Network** box, enter **any4**, and then click **Next**.

Tech Tip

For remote-access VPN integrated with Cisco ASA Series firewalls, NAT exemption must be configured for traffic from the LAN that is going to the remote-access clients. If this were not configured, traffic to clients would be translated, changing the source address of the traffic and making it impossible for clients to receive traffic correctly from servers with which they communicate.


AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
< Back
Next >
Cancel
Help

NAT Exempt

If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.

☑ Exempt VPN traffic from network address translation

Inside Interface is the interface directly connected to your internal network.

Inside Interface: inside

Local Network is the network address(es) of the internal network that client can access.

Local Network: any4

The traffic between AnyConnect client and internal network will be exempt from network address translation.

Step 6: On the AnyConnect Client Deployment page, click **Next**.

Step 7: On the Summary page, click **Finish**.

Finally, you must upload the Cisco AnyConnect client images to the secondary appliance.

Step 8: On the secondary appliance, copy the following Cisco AnyConnect client images to the local flash disk.

```
ftp://10.13.48.27/anyconnect-win-3.0.11042-k9.pkg disk0:
ftp://10.13.48.27/anyconnect-macosx-i386-3.0.11042-k9.pkg 
disk0:
ftp://10.13.48.27/anyconnect-linux-3.0.11042-k9.pkg disk0:
```

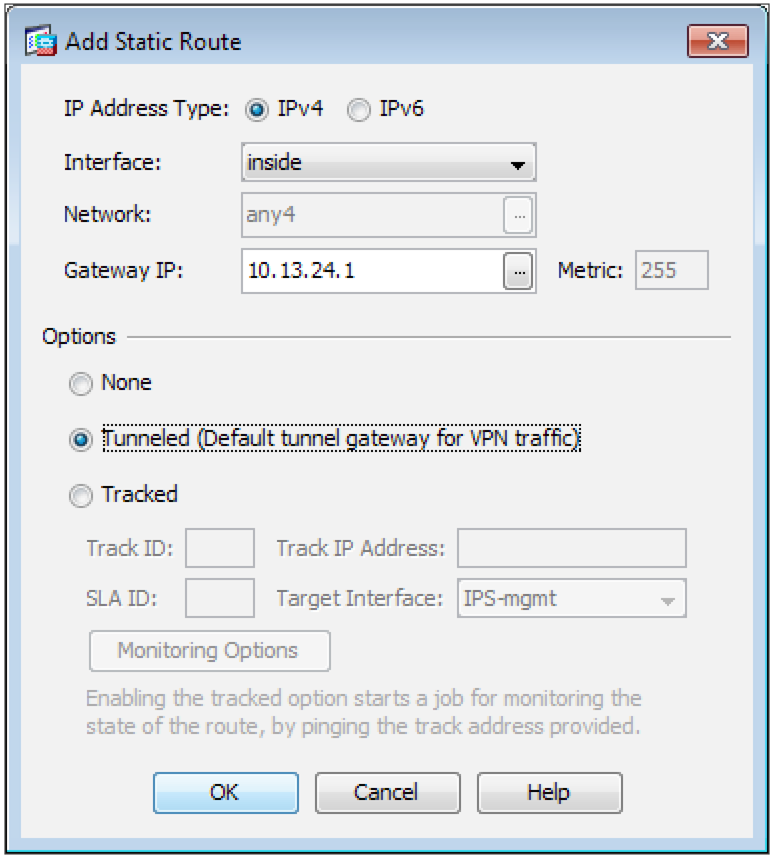
Procedure 4 Configure remote-access routing

Traffic from remote-access VPN clients to and from the enterprise network must be inspected by the plant firewall and IPS. To accomplish this, all traffic to and from the VPN clients must be routed toward the LAN distribution switch, regardless of the traffic's destination, so that the Cisco ASA policy engine has the visibility to handle the traffic correctly.

Step 1: Navigate to **Configuration > Device Setup > Routing > Static Routes**, and then click **Add**.

Step 2: On the Add Static Route dialog box, configure the following values, and then click **OK**:

- IP Address Type—**IPv4**
- Interface—**inside**
- Network—**any4**
- Gateway IP—**10.13.24.1**
- Options—**Tunneled (Default tunnel gateway for VPN traffic)**



Add Static Route

IP Address Type: ● IPv4 ○ IPv6

Interface: inside

Network: any4

Gateway IP: 10.13.24.1 Metric: 255

Options

○ None

● Tunneled (Default tunnel gateway for VPN traffic)

○ Tracked

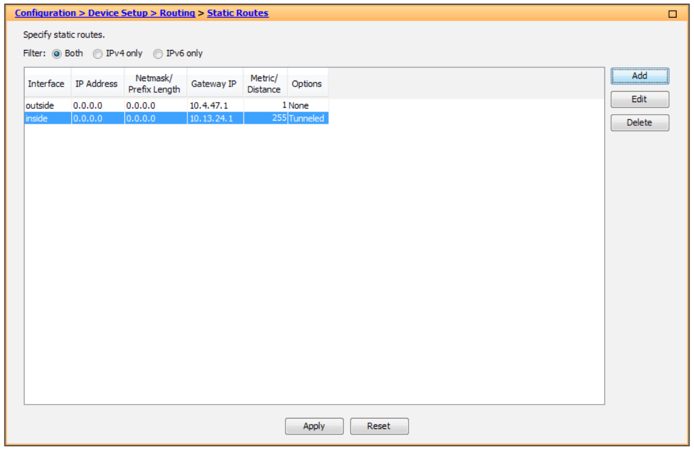
Track ID: Track IP Address:

SLA ID: Target Interface: IPS-mgmt

Monitoring Options

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

Step 3: Verify the configuration, and then click **Apply**.



Configuration > Device Setup > Routing > Static Routes

Specify static routes.

Filter: ● Both ○ IPv4 only ○ IPv6 only

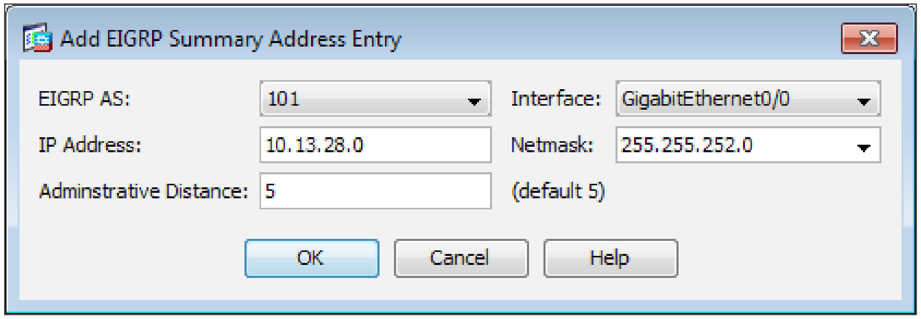
Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options
outside	0.0.0.0	0.0.0.0	10.4.47.1	1	None
inside	0.0.0.0	0.0.0.0	10.13.24.1	255	Tunneled

Cisco ASA advertises each connected user to the rest of the network as individual host routes. Next, you summarize the address pool. This reduces the IP route table size for easier troubleshooting and faster recovery from failures.

Step 4: Navigate to **Configuration > Device Setup > Routing > EIGRP > Summary Address**, and then click **Add**.

Step 5: On the Add EIGRP Summary Address Entry dialog box, configure the following values, and then click **OK**:

- EIGRP AS—**101**
- Interface—**GigabitEthernet0/0**
- IP Address—**10.13.28.0** (Enter the remote-access pool's summary network address.)
- Netmask—**255.255.252.0**
- Administrative Distance—**5**


Add EIGRP Summary Address Entry

EIGRP AS: 101

Interface: GigabitEthernet0/0

IP Address: 10.13.28.0

Netmask: 255.255.252.0

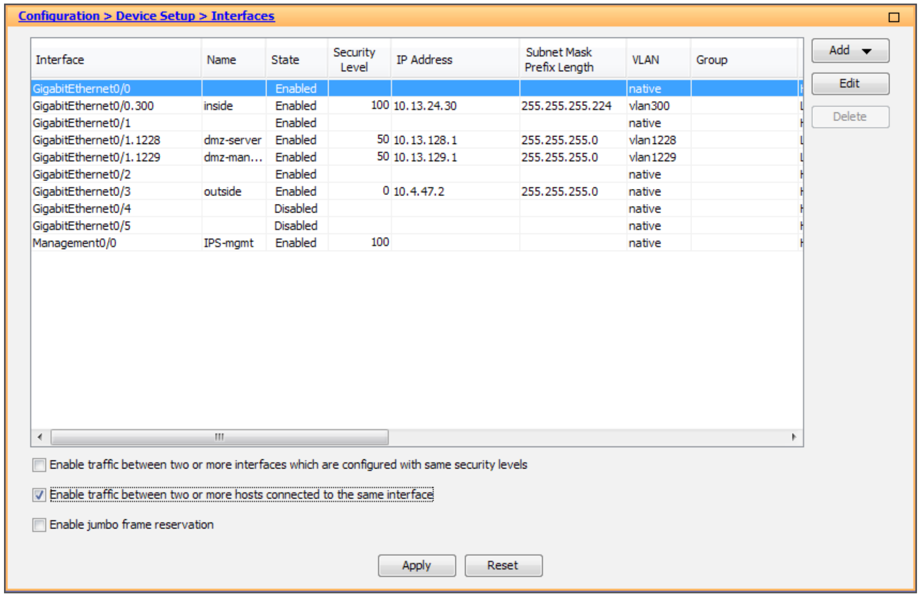
Adminstrative Distance: 5 (default 5)

Step 6: On the Summary Address pane, click **Apply**.

Next, you allow intra-interface traffic. This is critical in allowing VPN users to communicate with each other.

Step 7: Navigate to **Configuration > Device Setup > Interfaces**.

Step 8: Select **Enable traffic between two or more hosts connected to the same interface**, and then click **Apply**.


Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN	Group
GigabitEthernet0/0		Enabled				native	
GigabitEthernet0/0.300	inside	Enabled	100	10.13.24.30	255.255.255.224	vlan300	
GigabitEthernet0/1		Enabled				native	
GigabitEthernet0/1.1228	dmz-server	Enabled	50	10.13.128.1	255.255.255.0	vlan1228	
GigabitEthernet0/1.1229	dmz-man...	Enabled	50	10.13.129.1	255.255.255.0	vlan1229	
GigabitEthernet0/2		Enabled				native	
GigabitEthernet0/3	outside	Enabled	0	10.4.47.2	255.255.255.0	native	
GigabitEthernet0/4		Disabled				native	
GigabitEthernet0/5		Disabled				native	
Management0/0	IPS-mgmt	Enabled	100			native	

☐ Enable traffic between two or more interfaces which are configured with same security levels

☑ Enable traffic between two or more hosts connected to the same interface

☐ Enable jumbo frame reservation

Procedure 5 Configure the group URL

The Cisco AnyConnect client's initial connection is typically launched with a web browser. After the client is installed on a user's computer, subsequent connections can be established through the web browser again or directly through the Cisco AnyConnect client, which is now installed on the user's computer. The user needs the IP address or DNS name of the appliance, a username and password, and the name of the VPN group to which they are assigned. Alternatively, the user can directly access the VPN group with the group URL, after which they need to provide their username and password.

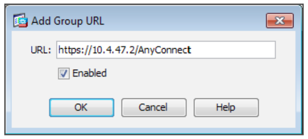
Step 1: Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

Step 2: In the **Connection Profiles** pane, select the profile created in the previous procedure (Example: AnyConnect), and then click **Edit**.

Step 3: On the **Edit AnyConnect Connect Profile** dialog box, navigate to **Advanced > Group Alias/Group URL**.

Step 4: On the **Group URLs** pane, click **Add**.

Step 5: On the Add Group URL dialog box, in the **URL** box, enter the URL containing the firewall's enterprise edge IP address and a user group string, and then click **OK**. (Example: https://10.4.47.2/AnyConnect)


Add Group URL

URL: https://10.4.47.2/AnyConnect

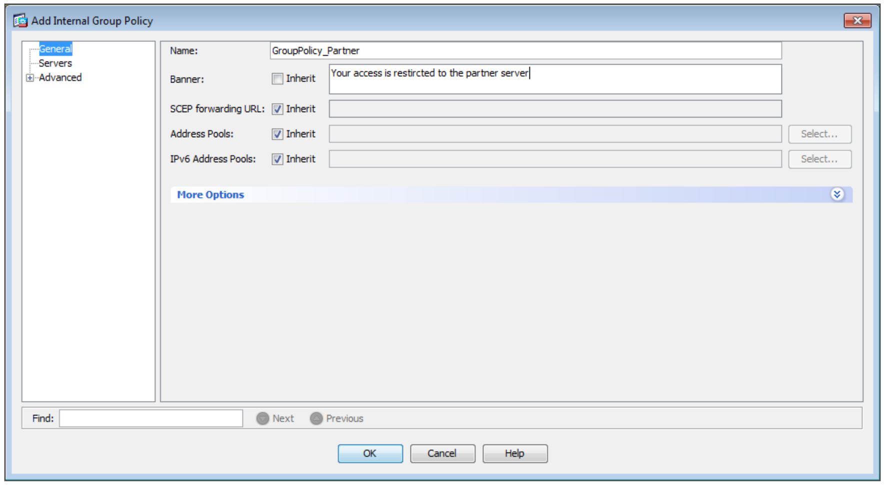
☑ Enabled

Step 6: Click **Apply**.

Procedure 6 Configure the partner policy

Step 1: Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, and then click **Add**.

Step 2: On the Add Internal Group Policy dialog box, enter a **Name**. (Example: GroupPolicy_Partner)


Add Internal Group Policy

Name: GroupPolicy_Partner

Banner: □ Inherit Your access is restircted to the partner server

SCEP forwarding URL: ☑ Inherit

Address Pools: ☑ Inherit

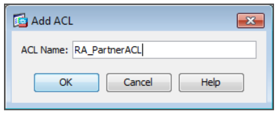
IPv6 Address Pools: ☑ Inherit

Step 3: Click the two down arrows. The **More Options** pane expands.

Step 4: For **Filter**, clear **Inherit**, and then click **Manage**.

Step 5: On the ACL Manager dialog box, select the **Standard ACL** tab, and then click **Add > Add ACL**.

Step 6: On the Add ACL dialog box, enter an **ACL Name**, and then click **OK**. (Example: RA_PartnerACL)

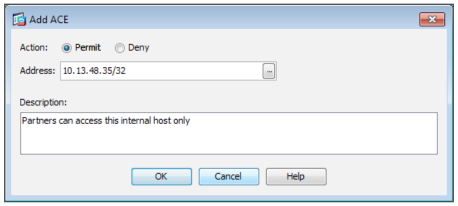

Add ACL

ACL Name: RA_PartnerACL

Step 7: On the ACL Manager dialog box, click **Add**, and then choose **Add ACE**.

Step 8: On the Add ACE dialog box, for **Action**, select **Permit**.

Step 9: In the **Address** box, enter the IP address and netmask that the partner is allowed to access, and then click **OK**. (Example: 10.13.48.35/32)

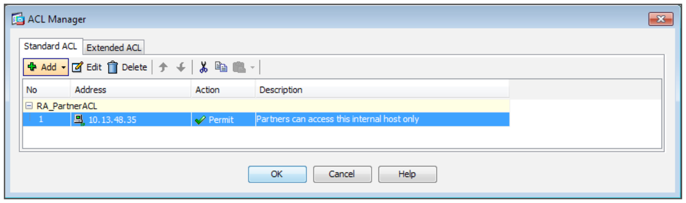

Add ACE

Action: ● Permit ○ Deny

Address: 10.13.48.35/32

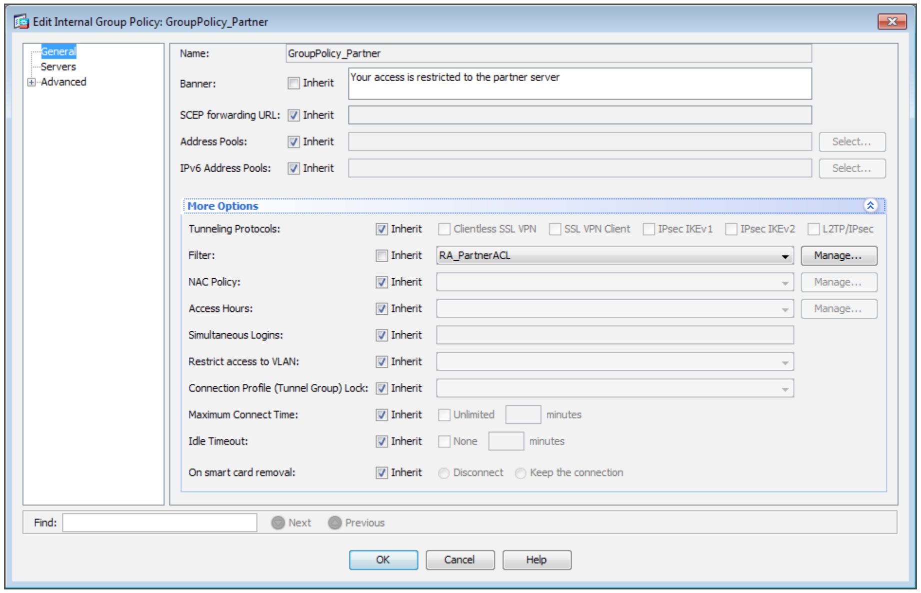
Description:
Partners can access this internal host only

Step 10: On the ACL Manager dialog box, click **OK**.


ACL Manager

No	Address	Action	Description
RA_PartnerACL			
1	10.13.48.35	✓ Permit	Partners can access this internal host only

Step 11: On the Add Internal Group Policy dialog box, click **OK**.



Edit Internal Group Policy: GroupPolicy_Partner

General
Servers
Advanced

Name: GroupPolicy_Partner

Banner: □ Inherit Your access is restricted to the partner server

SCEP forwarding URL: ☑ Inherit

Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

Tunneling Protocols: ☑ Inherit □ Clientless SSL VPN □ SSL VPN Client □ IPsec IKEv1 □ IPsec IKEv2 □ L2TP/IPsec

Filter: □ Inherit RA_PartnerACL

NAC Policy: ☑ Inherit

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

Connection Profile (Tunnel Group) Lock: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ None minutes

On smart card removal: ☑ Inherit ○ Disconnect ○ Keep the connection

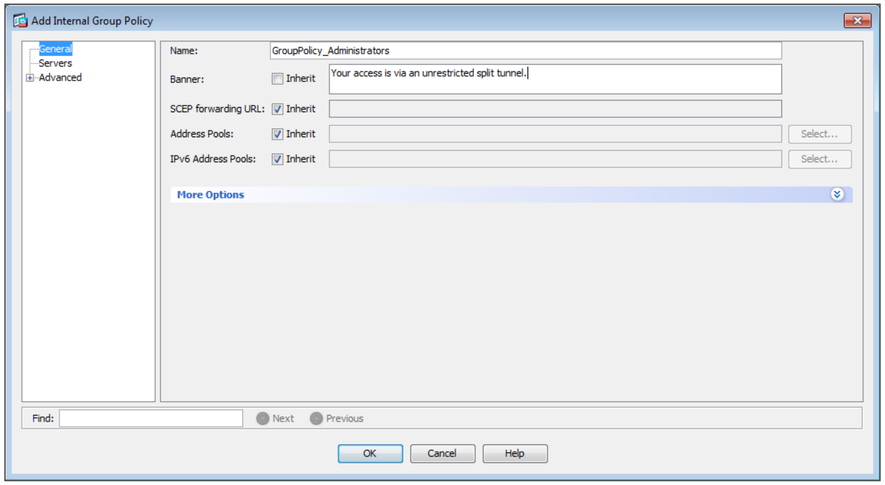
Find:

Step 12: On the Group Policies pane, click **Apply**.

Procedure 7 Configure the admin policy

Step 1: Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, and then click **Add**.

Step 2: On the Add Internal Group Policy dialog box, enter a **Name**. (Example: GroupPolicy_Administrators)



Add Internal Group Policy

General
Servers
Advanced

Name: GroupPolicy_Administrators

Banner: □ Inherit Your access is via an unrestricted split tunnel.

SCEP forwarding URL: ☑ Inherit

Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

Find:

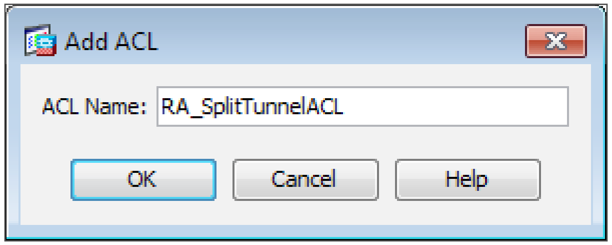
Step 3: In the navigation tree, click **Advanced > Split Tunneling**.

Step 4: For **Policy**, clear **Inherit**, and then select **Tunnel Network List Below**.

Step 5: For **Network List**, clear **Inherit**, and then click **Manage**.

Step 6: On the ACL Manager dialog box, click **Add**, and then choose **Add ACL**.

Step 7: On the Add ACL dialog box, enter an **ACL Name**, and then click **OK**. (Example: RA_SplitTunnelACL)



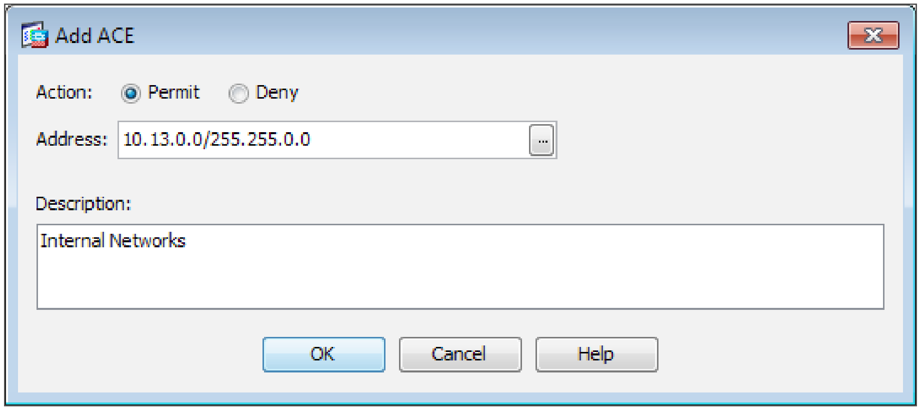
Add ACL

ACL Name: RA_SplitTunnelACL

Step 8: On the ACL Manager dialog box, click **Add**, and then choose **Add ACE**.

Step 9: On the Add ACE dialog box, for **Action**, select **Permit**.

Step 10: In the **Address** box, enter the internal summary IP address and netmask, and then click **OK**. (Example: 10.13.0.0/255.255.0.0)


Add ACE

Action: ● Permit ○ Deny

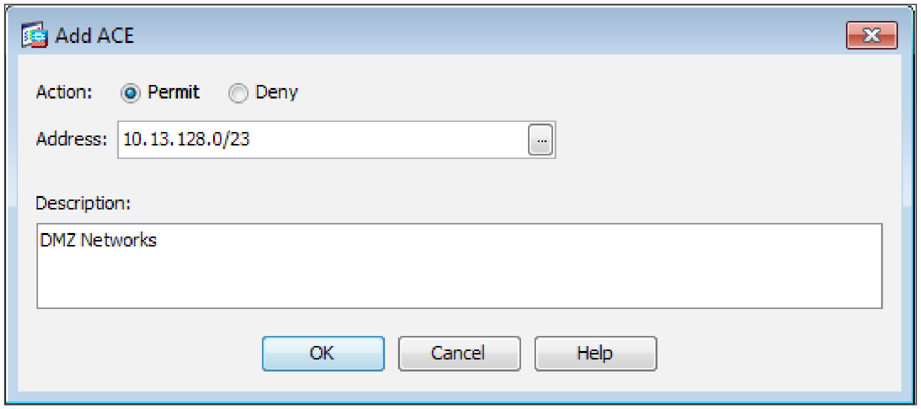
Address: 10.13.0.0/255.255.0.0

Description: Internal Networks

Step 11: On the ACL Manager dialog box, click **Add**, and then choose **Add ACE**.

Step 12: On the Add ACE dialog box, for **Action**, select **Permit**.

Step 13: In the **Address** box, enter the DMZ summary IP address and netmask, and then click **OK**. (Example: 10.13.128.0/23)

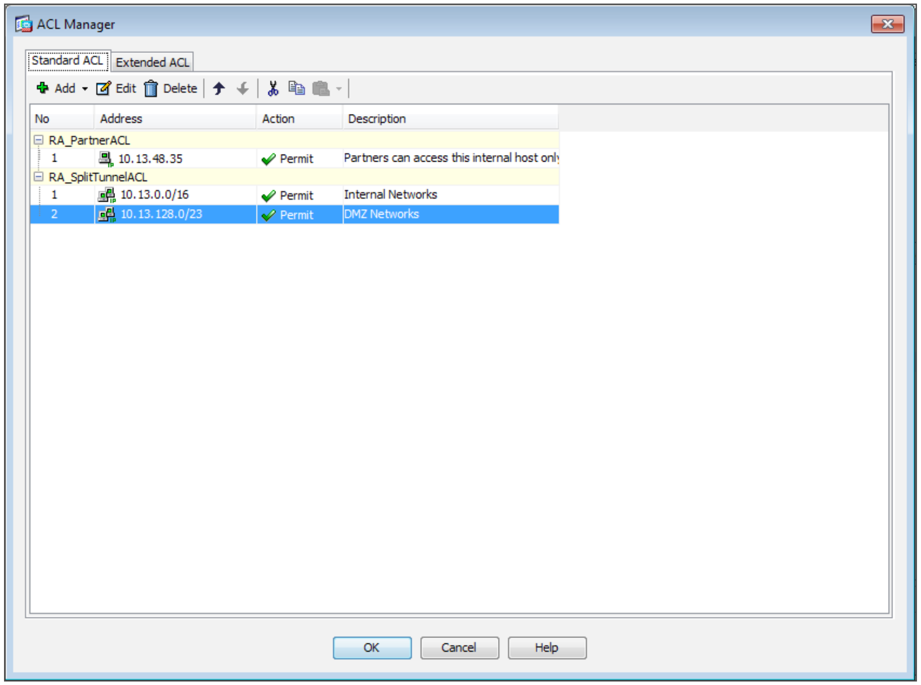

Add ACE

Action: ● Permit ○ Deny

Address: 10.13.128.0/23

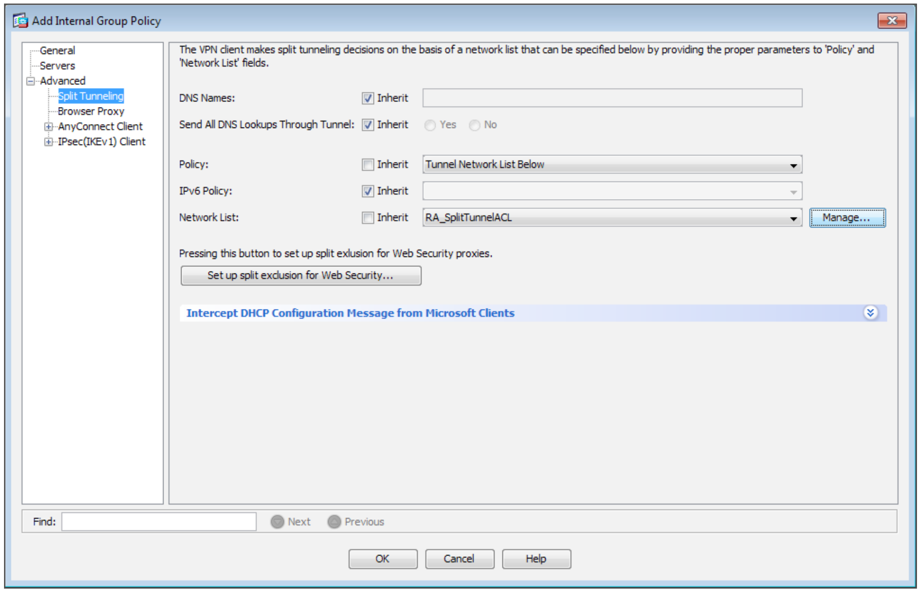
Description: DMZ Networks

Step 14: On the ACL Manager dialog box, click **OK**.


ACL Manager

No	Address	Action	Description
RA_PartnerACL			
1	10.13.48.35	✓ Permit	Partners can access this internal host onl
RA_SplitTunnelACL			
1	10.13.0.0/16	✓ Permit	Internal Networks
2	10.13.128.0/23	✓ Permit	DMZ Networks

Step 15: On the Add Internal Group Policy dialog box, click **OK**.



Add Internal Group Policy

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network List' fields.

DNS Names: ☑ Inherit

Send All DNS Lookups Through Tunnel: ☑ Inherit ○ Yes ○ No

Policy: □ Inherit Tunnel Network List Below

IPv6 Policy: ☑ Inherit

Network List: □ Inherit RA_SplitTunnelACL

Pressing this button to set up split exlusion for Web Security proxies.

Manage...
Set up split exclusion for Web Security...
Intercept DHCP Configuration Message from Microsoft Clients
Find:
Next
Previous
OK
Cancel
Help

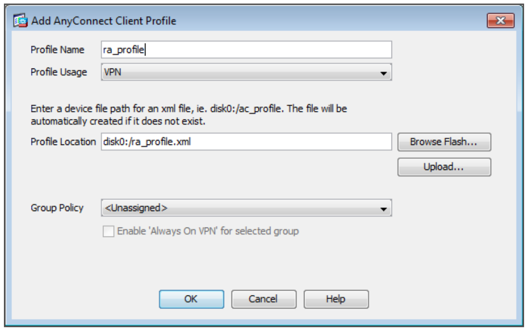
Step 16: On the Group Policies pane, click **Apply**.

Procedure 8 Configure Cisco AnyConnect client profile

The Cisco AnyConnect Client Profile dialog box is the location where some of the newer configuration of the Cisco AnyConnect client is defined. Cisco AnyConnect 2.5 and later use the configuration in this section, including many of the newest features added to the Cisco AnyConnect client.

Step 1: In **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**, click **Add**.

Step 2: On the Add AnyConnect Client Profile dialog box, in the **Profile Name** box, enter **ra_profile**, click **OK**, and then click **Apply**.



Add AnyConnect Client Profile

Profile Name: ra_profile

Profile Usage: VPN

Enter a device file path for an xml file, ie. disk0:/ac_profile. The file will be automatically created if it does not exist.

Profile Location: disk0:/ra_profile.xml

Group Policy: <Unassigned>

□ Enable 'Always On VPN' for selected group

Step 3: On the AnyConnect Client Profile pane, select the profile you just built (Example: ra_profile), and then click **Edit**.

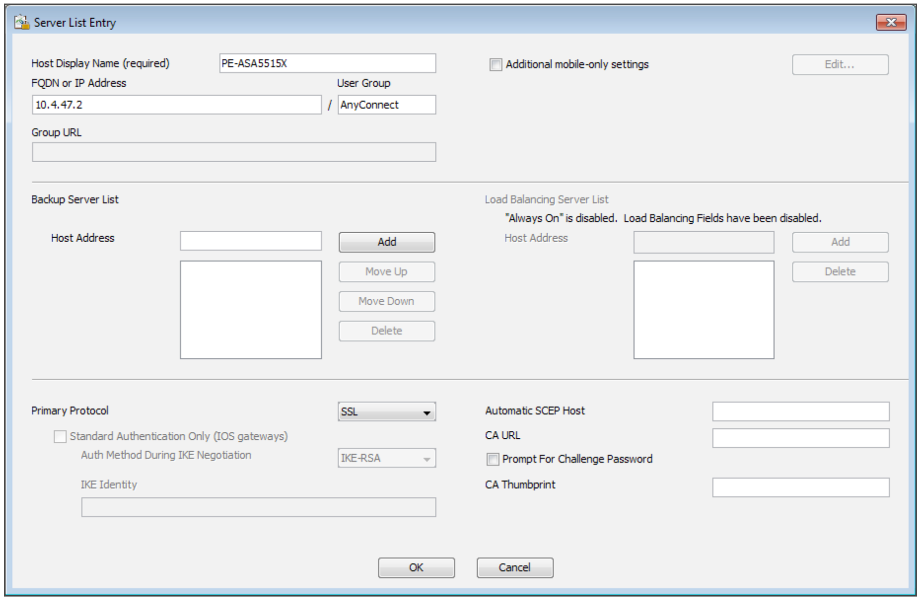
The **Server List Panel** allows you to enter names and addresses for the appliances to which the Cisco AnyConnect Client is allowed to connect.

Step 4: Select **Server List**, then click **Add**.

Step 5: On the Server List Entry dialog box, in the **Hostname** box, enter the name of the remote-access firewall. (Example: PE-ASA5515X)

Step 6: In the **Host Address** box, enter the firewall's enterprise edge connection IP address. (Example: 10.4.47.2)

Step 7: In the **User Group** box, enter the name defined in Step 3 of Procedure 1, “Configure remote access,” and then click **OK**. (Example: AnyConnect)



Server List Entry

Host Display Name (required) PE-ASA5515X

FQDN or IP Address 10.4.47.2 / User Group AnyConnect

Group URL

□ Additional mobile-only settings

Backup Server List

Host Address

Load Balancing Server List

"Always On" is disabled. Load Balancing Fields have been disabled.

Host Address

Primary Protocol SSL

□ Standard Authentication Only (IOS gateways)

Auth Method During IKE Negotiation IKE-RSA

IKE Identity

Automatic SCEP Host

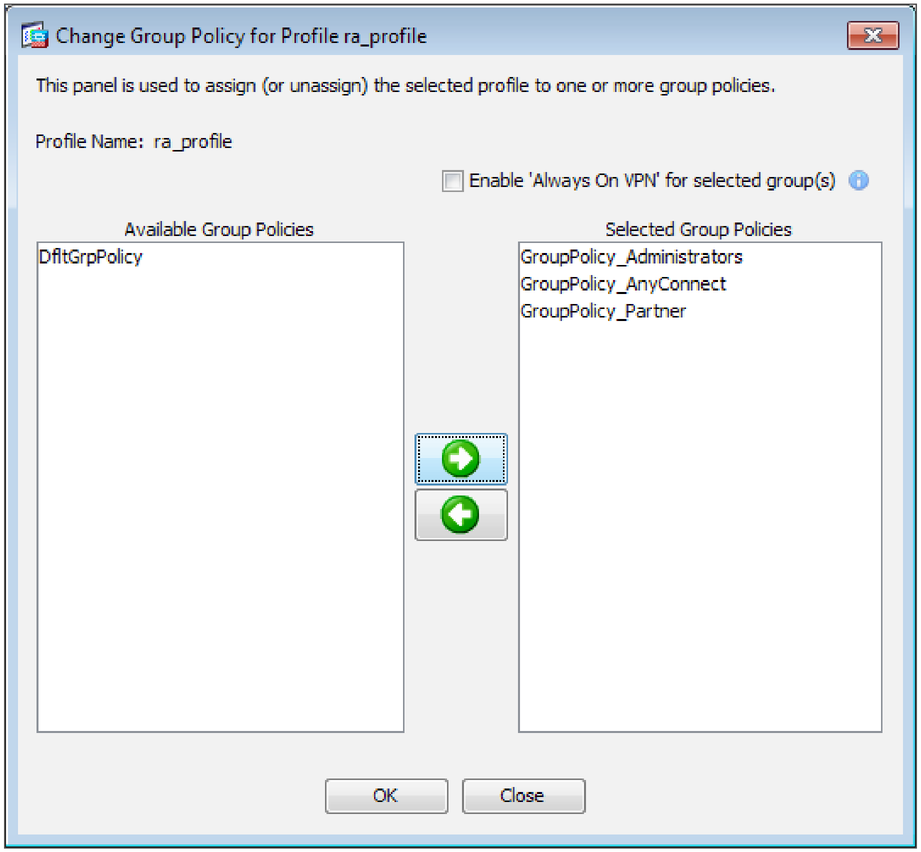
CA URL

□ Prompt For Challenge Password

CA Thumbprint

Step 8: On the AnyConnect Client Profile pane, click **Change Group Policy**.

Step 9: On the Change Group Policy for Profile dialog box, in the Available Group Policies list, select the three group policies you just created, click the right arrow, and then click **OK**.



Change Group Policy for Profile ra_profile

This panel is used to assign (or unassign) the selected profile to one or more group policies.

Profile Name: ra_profile

□ Enable 'Always On VPN' for selected group(s)

Available Group Policies

DfltGrpPolicy

Selected Group Policies

GroupPolicy_Administrators
GroupPolicy_AnyConnect
GroupPolicy_Partner

Step 10: On the AnyConnect Client Profile pane, click **Apply**.

AAA

Process

Configuring Cisco Secure ACS

1. Define external groups
2. Create the device-type group
3. Create the network device
4. Create authorization profiles
5. Configure the access service
6. Create authorization rules

This process is only for organizations that use Cisco Secure ACS for authentication of remote-access VPN users. If your organization uses Microsoft Active Directory by itself, skip this process.

Authentication is the portion of the configuration that verifies that users' credentials (username and password) match those stored within the organization's database of users that are allowed to access electronic resources. Cisco SBA designs use either Cisco Secure ACS or Microsoft Active Directory for authentication of remote-access VPN users. Cisco Secure ACS gives an organization enhanced ability to control the access that VPN users receive.

When the Cisco ASA firewall queries the Cisco Secure ACS server (which then proxies the request to the Active Directory database) in order to determine whether a user's name and password is valid, Cisco Secure ACS also retrieves other Active Directory attributes, such as group membership, that Cisco Secure ACS may use when making an authorization decision. Based on the group membership, Cisco Secure ACS sends back a group policy name to the appliance, along with the success or failure of the login. Cisco ASA uses the group policy name in order to assign the user to the appropriate VPN group policy.

In this process, Active Directory is the primary directory container for user credentials and group membership. Before you begin this process, your Active Directory must have three groups defined: **vpn-administrator**, **vpn-employee**, and **vpn-partner**. These groups map users to the respective VPN access policies.

Procedure 1 Define external groups

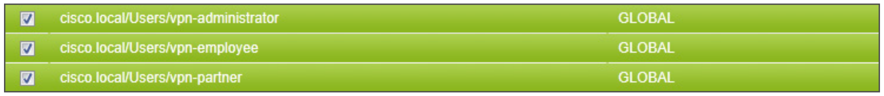
Step 1: In a web browser, navigate to the Cisco Secure ACS Administration Page. (Example: https://acs.cisco.local)

Tech Tip

To reduce compatibility issues with Cisco Secure ACS, use Internet Explorer to configure settings

Step 2: Navigate to **Users and Identity Stores > External Identity Stores > Active Directory**, click the **Directory Groups** tab, and then click **Select**.

Step 3: On the **External User Groups** pane, select the three VPN groups, and then click **OK**.



☑	cisco.local/Users/vpn-administrator	GLOBAL
☑	cisco.local/Users/vpn-employee	GLOBAL
☑	cisco.local/Users/vpn-partner	GLOBAL

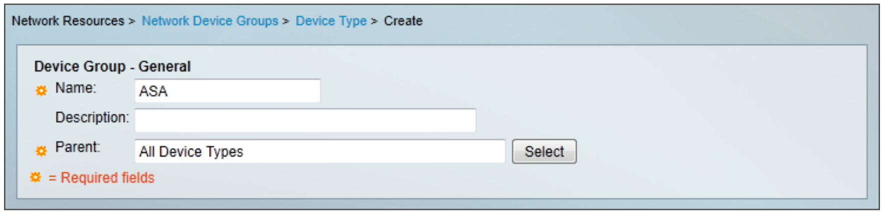
Step 4: On the Active Directory pane, click **Save Changes**.

Procedure 2 Create the device-type group

Step 1: Navigate to **Network Resources > Network Device Groups > Device Type**, and then click **Create**.

Step 2: In the **Name** box, enter a name for the group. (Example: ASA)

Step 3: In the **Parent** box, enter All Device Types, and then click **Submit**.



Network Resources > Network Device Groups > Device Type > Create

Device Group - General

- Name: ASA
- Description:
- Parent: All Device Types [Select]

= Required fields

Procedure 3 Create the network device

For the Cisco ASA firewall, create a network device entry in Cisco Secure ACS.

Step 1: Navigate to **Network Resources > Network Devices and AAA Clients**, and then click **Create**.

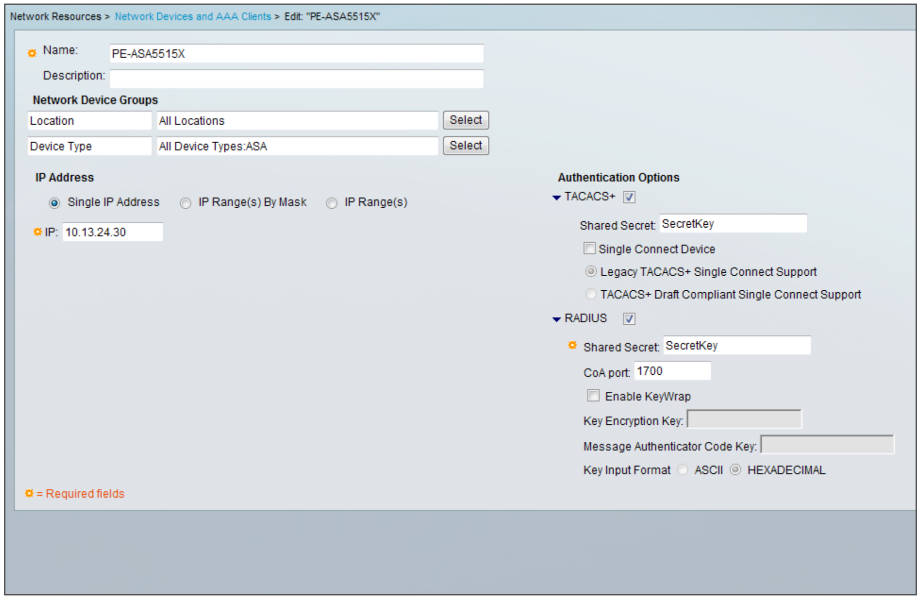
Step 2: In the **Name** box, enter the device host name. (Example: PE-ASA5515X)

Step 3: In the **Device Type** box, enter All Device Types:ASA.

Step 4: In the **IP** box, enter the inside interface IP address of the appliance. (Example: 10.13.24.30)

Step 5: Select **TACACS+**, and then in the **Shared Secret** box, enter the TACACS+ shared secret key. (Example: SecretKey)

Step 6: Select **RADIUS**, and then in the **Shared Secret** box, enter the RADIUS shared secret key. (Example: SecretKey)



Network Resources > Network Devices and AAA Clients > Edit: "PE-ASA5515X"

- Name: PE-ASA5515X
- Description:

Network Device Groups

Location	All Locations	Select
Device Type	All Device Types:ASA	Select

IP Address

● Single IP Address ○ IP Range(s) By Mask ○ IP Range(s)

IP: 10.13.24.30

Authentication Options

TACACS+ ☑

- Shared Secret: SecretKey
- □ Single Connect Device
- ● Legacy TACACS+ Single Connect Support
- ○ TACACS+ Draft Compliant Single Connect Support

RADIUS ☑

- Shared Secret: SecretKey
- CoA port: 1700
- □ Enable KeyWrap
- Key Encryption Key:
- Message Authenticator Code Key:
- Key Input Format ○ ASCII ● HEXADECIMAL

= Required fields

Step 7: Click **Submit** to save changes.

Procedure 4 Create authorization profiles

You create two different authorization profiles in order to identify users that belong to either the vpn-administrator or vpn-partner groups in Active Directory.

Step 1: Navigate to **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, and then click **Create**.

Step 2: In the **Name** box, enter a name for the authorization profile. (Example: RA-Administrator)

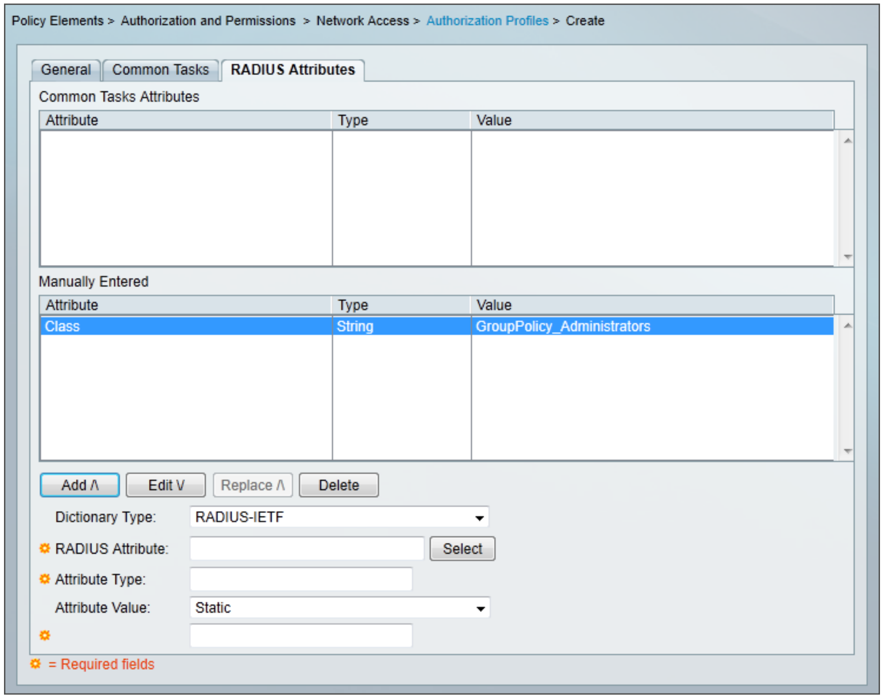
Step 3: Click the **RADIUS Attributes** tab, and below the Manually Entered pane, click **Select** to the right of the RADIUS Attribute box.

Step 4: Select the Class attribute row in the RADIUS Dictionary window and click **OK**.

Next, you must configure the attribute value to match the group policy that you configure on the appliance.

Step 5: Under Attribute Value, select **Static**, enter the group policy name, and then click **Add**. (Example: GroupPolicy_Administrators)

Step 6: Click **Submit** to save the profile.



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
Class	String	GroupPolicy_Administrators

Dictionary Type: RADIUS-IETF

RADIUS Attribute:

Attribute Type:

Attribute Value: Static

= Required fields

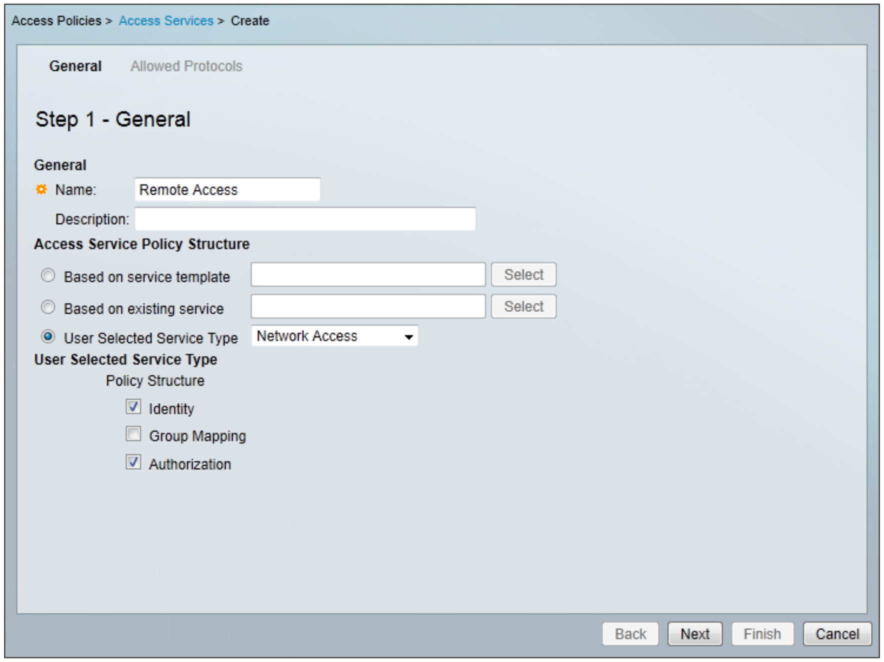
Step 7: Repeat this procedure to build an authorization profile for partners, using the group policy **GroupPolicy_Partner** value.

Procedure 5 Configure the access service

Create a policy that inspects for group membership in the return traffic from the Active Directory server.

Step 1: Navigate to **Access Policies > Access Services**, and then click **Create**.

Step 2: On the General page, in the **Name** box, enter **Remote Access**, select **User Selected Service Type**, and then click **Next**.



Access Policies > Access Services > Create

Step 1 - General

General

Name: Remote Access

Description:

Access Service Policy Structure

○ Based on service template

○ Based on existing service

● User Selected Service Type Network Access

User Selected Service Type

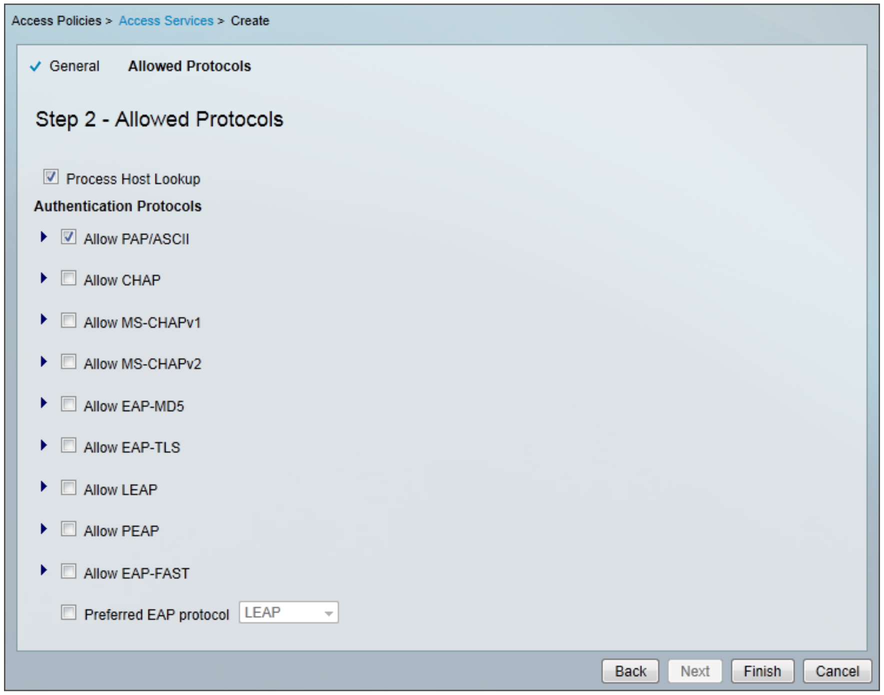
Policy Structure

☑ Identity

□ Group Mapping

☑ Authorization

Step 3: On the Allowed Protocols page, select **Allow PAP/ASCII**, and then click **Finish**.


Access Policies > Access Services > Create

✓ General **Allowed Protocols**

Step 2 - Allowed Protocols

☑ Process Host Lookup

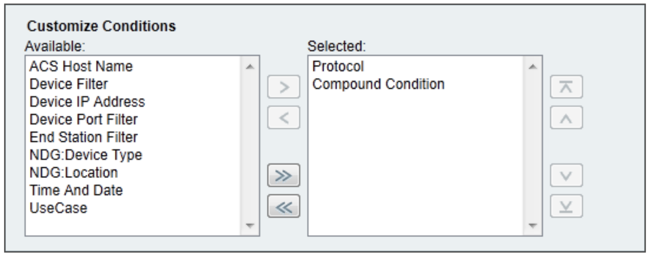
Authentication Protocols

- ☑ Allow PAP/ASCII
- □ Allow CHAP
- □ Allow MS-CHAPv1
- □ Allow MS-CHAPv2
- □ Allow EAP-MD5
- □ Allow EAP-TLS
- □ Allow LEAP
- □ Allow PEAP
- □ Allow EAP-FAST

□ Preferred EAP protocol: LEAP

Step 4: Navigate to **Access Policies > Access Services > Service Selection Rules**, and then click **Customize**.

Step 5: On the Customize Conditions pane, move **Compound Condition** from the **Available** list to the **Selected** list, and then click **OK**.


Customize Conditions

Available:
ACS Host Name
Device Filter
Device IP Address
Device Port Filter
End Station Filter
NDG:Device Type
NDG:Location
Time And Date
UseCase

Selected:
Protocol
Compound Condition

Step 6: On the **Service Selection Rules** pane, click **Create**.

Step 7: On the dialog box, in the Name box, enter Remote Access.

Step 8: Select **Protocol**, and in the list, choose **match**, and then in the box, enter Radius.

Step 9: Select **Compound Condition**, and then in the **Dictionary** list, choose **NDG**.

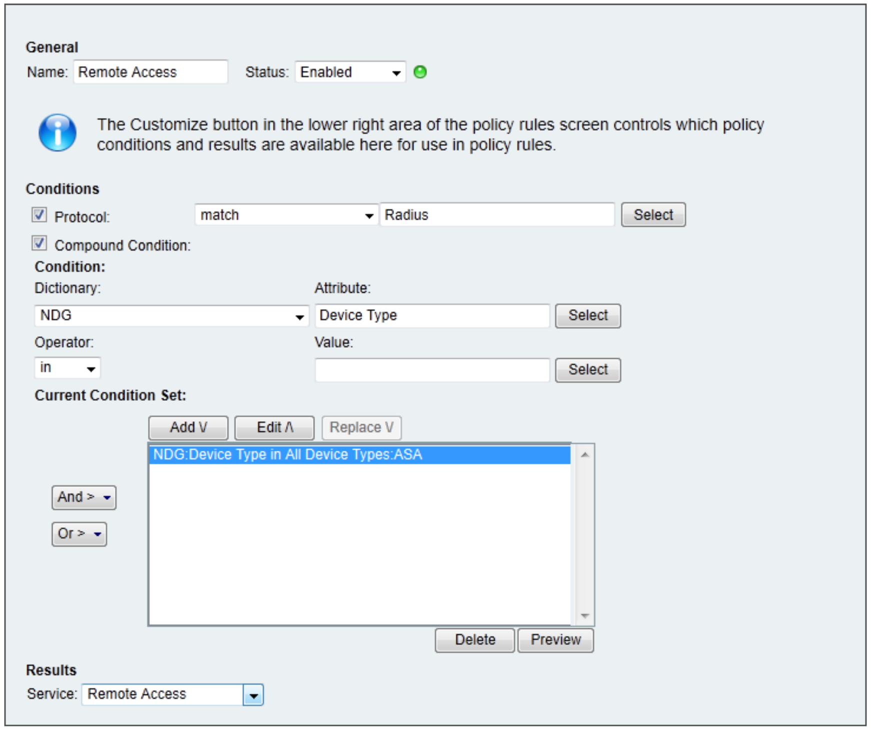
Step 10: In the **Attribute** box, enter Device Type.

Step 11: In the **Value** box, enter All Device Types: ASA.

Step 12: Under Current Condition Set, click **Add**. The information is added to the Current Condition Set list.

Step 13: In the **Service** list, choose **Remote Access**, and then click **OK**.

Step 14: Click **Save Changes**.


General

Name: Remote Access Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☑ Protocol: match Radius

☑ Compound Condition:

Condition:

Dictionary: NDG

Attribute: Device Type

Operator: in

Value:

Current Condition Set:

NDG:Device Type in All Device Types:ASA

Results

Service: Remote Access

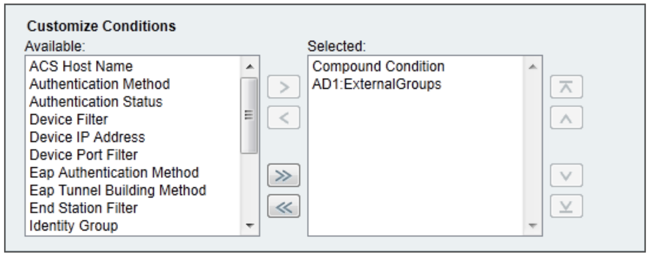
Step 15: Navigate to **Access Policies > Access Services > Remote Access > Identity**.

Step 16: In the **Identity Source** box, enter AD1, and then click **Save Changes**.

Step 17: Navigate to **Access Policies > Access Services > Remote Access > Authorization**, and then click **Customize**.

Step 18: On the Customize Conditions pane, move **AD1:ExternalGroups** from the **Available** list to the **Selected** list, and then click **OK**.

Step 19: Click **Save Changes**.



Customize Conditions

Available:

- ACS Host Name
- Authentication Method
- Authentication Status
- Device Filter
- Device IP Address
- Device Port Filter
- Eap Authentication Method
- Eap Tunnel Building Method
- End Station Filter
- Identity Group

Selected:

- Compound Condition
- AD1:ExternalGroups

Procedure 6 Create authorization rules

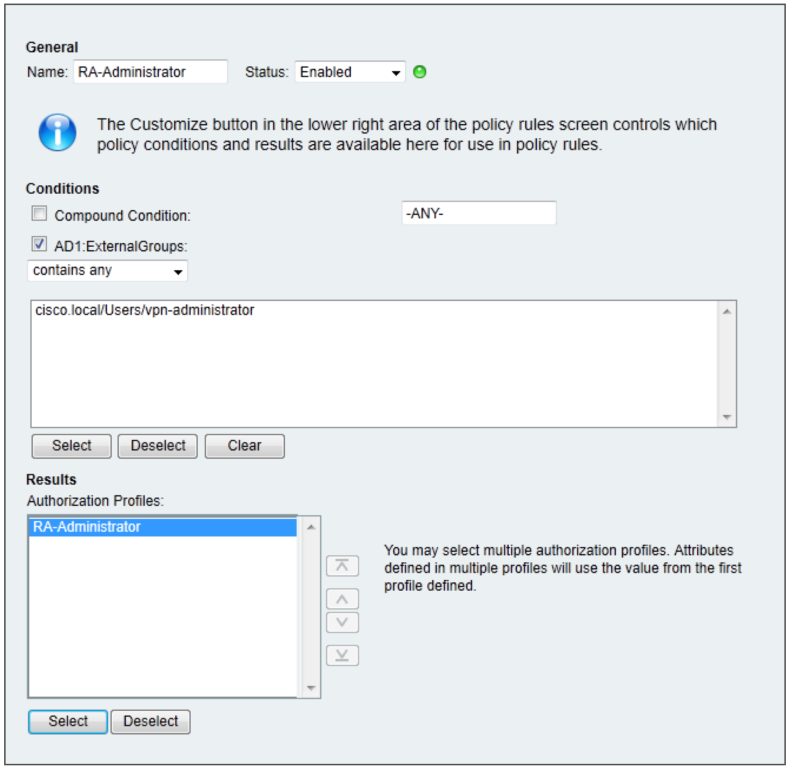
Step 1: Navigate to **Access Policies > Access Services > Remote Access > Authorization**, and then click **Create**.

Step 2: In the **Name** box, enter a rule name.(Example: RA-Administrator)

Step 3: Under **Conditions**, select **AD1:ExternalGroups**.

Step 4: Under Conditions, click **Select**, select the Active Directory administrator group (Example: cisco.local/Users/vpn-administrator), and then click **OK**.

Step 5: Under **Results**, select the authorization profile, and then click **Select**. (Example: RA-Administrator)



General

Name: RA-Administrator Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

□ Compound Condition: -ANY-

☑ AD1:ExternalGroups:

contains any

cisco.local/Users/vpn-administrator

Results

Authorization Profiles:

RA-Administrator

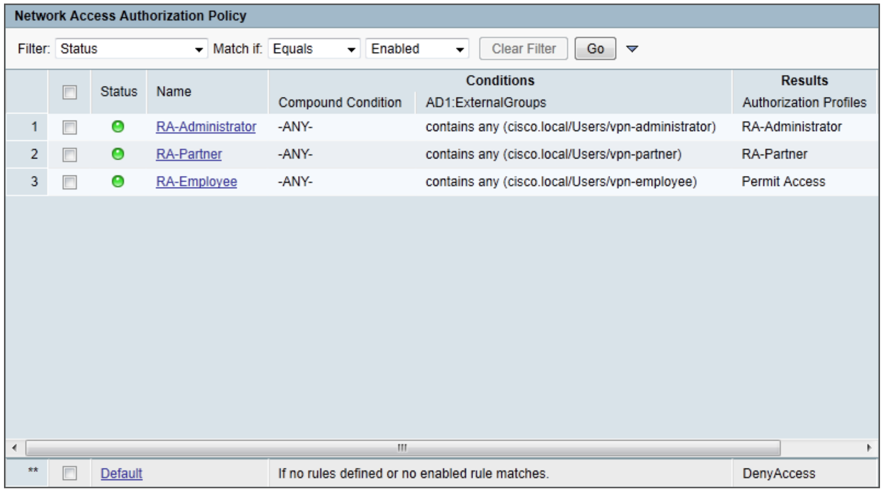
You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

Step 6: Repeat Step 1 through Step 5 for the partner rule.

Step 7: Repeat Step 1 through Step 5 for the employee rule, using **Permit Access** as the authorization profile.

Step 8: On the Authorization pane, click the **Default** rule.

Step 9: Select **Deny Access** as the authorization profile, and then click **OK**.



Network Access Authorization Policy

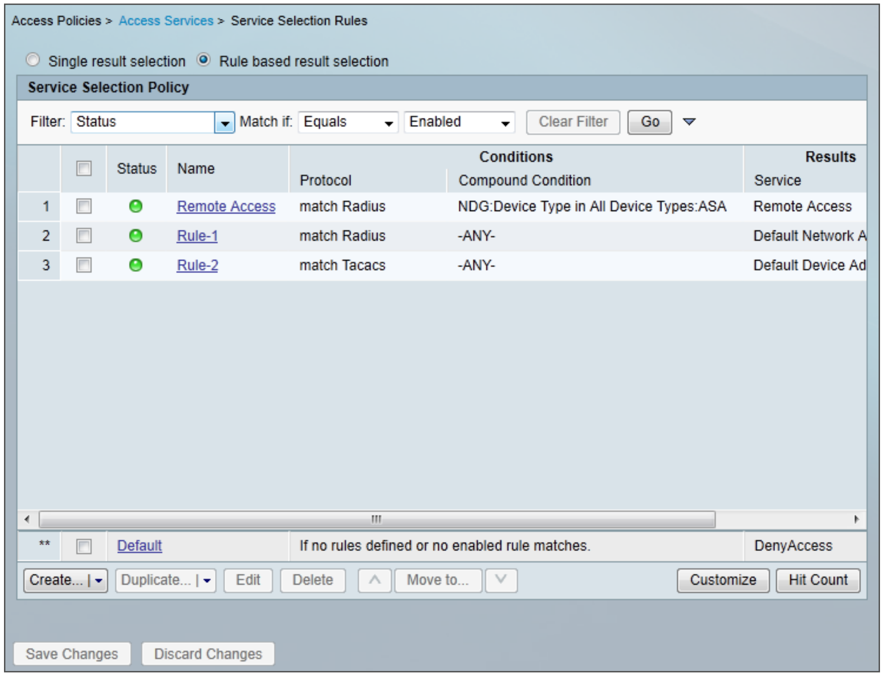
Filter: Status Match if: Equals Enabled

	□	Status	Name	Conditions		Results
				Compound Condition	AD1:ExternalGroups	Authorization Profiles
1	□	●	RA-Administrator	-ANY-	contains any (cisco.local/Users/vpn-administrator)	RA-Administrator
2	□	●	RA-Partner	-ANY-	contains any (cisco.local/Users/vpn-partner)	RA-Partner
3	□	●	RA-Employee	-ANY-	contains any (cisco.local/Users/vpn-employee)	Permit Access
**	□		Default	If no rules defined or no enabled rule matches.		DenyAccess

Step 10: Click **Save Changes**.

The remote access services are created, and next, you change the order of the policies.

Step 11: Navigate to **Access Policies > Access Services > Service Selection Rules**, select the **Remote Access** policy, and then use the up arrow button to move it to the first position.



Access Policies > Access Services > Service Selection Rules

○ Single result selection ● Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals Enabled

	□	Status	Name	Conditions		Results
				Protocol	Compound Condition	Service
1	□	●	Remote Access	match Radius	NDG:Device Type in All Device Types:ASA	Remote Access
2	□	●	Rule-1	match Radius	-ANY-	Default Network A
3	□	●	Rule-2	match Tacacs	-ANY-	Default Device Ad
**	□		Default	If no rules defined or no enabled rule matches.		DenyAccess

Step 12: Click **Save Changes**. The Cisco Secure ACS server has now been configured for remote-access VPN authentication.

Appendix A: Product List

Plant Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.0(1)1 IPS 7.1(6) E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA 5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)

Plant DMZ

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	15.0(2)SE IP Base license

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) Enterprise Services license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(2)SE IP Services license
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

Appendix B: Configuration Files

ASA Firewall 5515-X

```
ASA Version 9.0(1)
!
hostname PE-ASA5515X
domain-name cisco.local
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool RA-pool 10.13.28.1-10.13.31.254 mask 255.255.252.0
!
interface GigabitEthernet0/0
 no nameif
 no security-level
 no ip address
 summary-address eigrp 101 10.13.28.0 255.255.252.0 5
!
interface GigabitEthernet0/0.300
 vlan 300
 nameif inside
 security-level 100
 ip address 10.13.24.30 255.255.255.224 standby 10.13.24.29
!
interface GigabitEthernet0/1
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/1.1228
 description Server DMZ Connection to VLAN 1228
 vlan 1228
 nameif dmz-server
security-level 50
 ip address 10.13.128.1 255.255.255.0 standby 10.13.128.2
!
interface GigabitEthernet0/1.1229
 description Management DMZ connection on VLAN 1229
 vlan 1229
 nameif dmz-management
 security-level 50
 ip address 10.13.129.1 255.255.255.0 standby 10.13.129.2
!
interface GigabitEthernet0/2
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/3
 description Connection to Firewall Enterprise Edge
 nameif outside
 security-level 0
 ip address 10.4.47.2 255.255.255.0 standby 10.4.47.3
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
```

```
interface Management0/0
 management-only
 nameif IPS-mgmt
 security-level 100
 no ip address
!
boot system disk0:/asa901-smp-k8.bin
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns server-group DefaultDNS
 domain-name cisco.local
same-security-traffic permit intra-interface
object network internal-network
 subnet 10.13.0.0 255.255.0.0
 description The plant’s internal network range
object network dmz-networks
 subnet 10.13.128.0 255.255.254.0
 description The plant’s DMZ network range
object network inside-plant-network
 subnet 10.13.0.0 255.255.0.0
 description PAT traffic from plant network to enterprise network
object network inside-plant-voice-102
 subnet 10.13.2.0 255.255.255.0
 description Plant’s voice network
object network outside-enterprise-network
 subnet 10.4.0.0 255.254.0.0
 description Outside Enterprise Network
object network outside-rdp-server
 host 10.4.47.100
 description RDP Server on Enterprise Zone
object network dmz-rdp-server
 host 10.13.128.100
object network NETWORK_OBJ_10.13.28.0_22
 subnet 10.13.28.0 255.255.252.0
```

```
object-group service DM_INLINE_SERVICE_1
 service-object tcp destination eq ftp
 service-object tcp destination eq ftp-data
 service-object tcp destination eq tacacs
 service-object udp destination eq ntp
 service-object udp destination eq syslog
object-group service RDP tcp-udp
 port-object eq 3389
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
access-list global_access extended permit object-group DM_INLINE_
SERVICE_1 10.13.129.0 255.255.255.0 object internal-network
access-list global_access extended permit object-group TCPUDP
object outside-enterprise-network 10.13.128.0 255.255.255.0
object-group RDP
access-list global_access remark Rule to allow voice traffic from
plant to enterprise zone
access-list global_access extended permit ip object inside-plant-
voice-102 object outside-enterprise-network
access-list global_mpc extended permit ip any4 any4
access-list RA_PartnerACL remark Partners can access internal
hosts only
access-list RA_PartnerACL standard permit host 10.13.48.35
access-list RA_SplitTunnelACL remark Internal Networks
access-list RA_SplitTunnelACL standard permit 10.13.0.0
255.255.0.0
access-list RA_SplitTunnelACL remark DMZ Networks
access-list RA_SplitTunnelACL standard permit 10.13.128.0
255.255.254.0
pager lines 24
logging enable
logging buffered informational
logging asdm informational
mtu inside 1500
mtu IPS-mgmt 1500
mtu outside 1500
mtu dmz-management 1500
mtu dmz-server 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 10.13.24.33 255.255.255.248 
standby 10.13.24.34
monitor-interface inside
monitor-interface dmz-management
monitor-interface dmz-server
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-702.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (inside,outside) source static any any destination static 
NETWORK_OBJ_10.13.28.0_22 NETWORK_OBJ_10.13.28.0_22 no-proxy-arp 
route-lookup
!
object network inside-plant-network
 nat (inside,outside) dynamic interface
object network dmz-rdp-server
 nat (dmz-server,outside) static outside-rdp-server net-to-net
access-group global_access global
!
router eigrp 101
 no auto-summary
 network 10.13.24.0 255.255.252.0
 network 10.13.128.0 255.255.254.0
 passive-interface default
 no passive-interface inside
 redistribute static
!
route outside 0.0.0.0 0.0.0.0 10.4.47.1 1
route inside 0.0.0.0 0.0.0.0 10.13.24.1 tunneled
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 
mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (inside) host 10.13.48.15
 key *****
aaa-server AAA-RADIUS protocol radius
aaa-server AAA-RADIUS (inside) host 10.13.48.15
 timeout 5
 key *****
aaa-server AD protocol nt
aaa-server AD (inside) host 10.13.48.10
 timeout 5
 nt-auth-domain-controller AD-1
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 192.168.1.0 255.255.255.0 IPS-mgmt
http 10.13.48.0 255.255.255.0 inside
snmp-server host inside 10.13.48.35 community *****
no snmp-server location
no snmp-server contact
```

```
snmp-server community *****
snmp-server enable traps snmp authentication linkup linkdown 
coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint ASDM_TrustPoint0
 enrollment self
 subject-name CN=PE-ASA5515X
 keypair sslpair
 proxy-ldc-issuer
 crl configure
crypto ca trustpool policy
crypto ca certificate chain ASDM_TrustPoint0
 certificate bc39f750
    30820258 308201c1 a0030201 020204bc 39f75030 0d06092a 
864886f7 0d010105
    0500303e 31143012 06035504 03130b50 452d4153 41353531 
35583126 30240609
    2a864886 f70d0109 02161750 452d4153 41353531 35582e63 
6973636f 2e6c6f63
    616c301e 170d3133 30313239 31383239 31305a17 0d323330 
31323731 38323931
    305a303e 31143012 06035504 03130b50 452d4153 41353531 
35583126 30240609
    2a864886 f70d0109 02161750 452d4153 41353531 35582e63 
6973636f 2e6c6f63
    616c3081 9f300d06 092a8648 86f70d01 01010500 03818d00 
30818902 8181009d
    0413511d 0ce45f14 aea5f241 921fec71 069d057e 79fd1930 
d2348d67 098e0e83
    04a91661 85e53b86 b5b10a0c 0ef1ee50 9dd8d251 24e962eb 
c925f73a aafa4b9f
    e27ebf58 5ef21724 e82c6e73 daf7d581 02be62f1 97d7f405 
7c59fab4 d988ade3
    4d322687 2610fc13 10863ab3 8294b016 b8c54dc7 2ccfc43d 
07c1e0f6 5d0b9302
    03010001 a3633061 300f0603 551d1301 01ff0405 30030101 
ff300e06 03551d0f
    0101ff04 04030201 86301f06 03551d23 04183016 8014c83b 
caebd410 095f285d
    647c9d40 b011e005 2ab0301d 0603551d 0e041604 14c83bca 
ebd41009 5f285d64
    7c9d40b0 11e0052a b0300d06 092a8648 86f70d01 01050500 
03818100 4caacd77
    b161e1d0 cd3dc922 70e75945 73f1287f 450958c9 a6a4438b 
c4f384bf 4832a537
    0a692e41 c6d8f2d7 48d5a509 0969bbef 1f71e74b 02cb94bc 
b07bc4a8 d4c1dbe3
    7975de40 64dec87c 7f0c2058 2b6a642f 1cc2bbe2 65a725f5 
85b24737 e33ffdc3
    4b4f2d54 80b23f93 7e0911f3 d387ebc3 c5cfb6fb 0a803807 
f1226b4e
  quit
telnet timeout 5
ssh 10.13.48.0 255.255.255.0 inside
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 10.13.48.17
ssl encryption aes256-sha1 aes128-sha1 3des-sha1
ssl trust-point ASDM_TrustPoint0 outside
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-macosx-i386-3.0.11042-k9.pkg 
1
 anyconnect image disk0:/anyconnect-win-3.0.11042-k9.pkg 2
 anyconnect image disk0:/anyconnect-linux-3.0.11042-k9.pkg 3
 anyconnect profiles ra_profile disk0:/ra_profile.xml
 anyconnect enable
 tunnel-group-list enable
group-policy GroupPolicy_AnyConnect internal
```

```
group-policy GroupPolicy_AnyConnect attributes
 wins-server none
 dns-server value 10.13.48.10
 vpn-tunnel-protocol ssl-client
 default-domain value cisco.local
 webvpn
  anyconnect profiles value ra_profile type user
group-policy GroupPolicy_Administrators internal
group-policy GroupPolicy_Administrators attributes
 banner value Your access is via an unrestricted split tunnel
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value RA_SplitTunnelACL
 webvpn
  anyconnect profiles value ra_profile type user
group-policy GroupPolicy_Partner internal
group-policy GroupPolicy_Partner attributes
 banner value Your access is restricted to the partner server
 banner value Your access is restricted to the partner server.
 vpn-filter value RA_PartnerACL
 webvpn
  anyconnect profiles value ra_profile type user
username admin password w2Y.6Op4j7clVDk2 encrypted privilege 15
tunnel-group AnyConnect type remote-access
tunnel-group AnyConnect general-attributes
 address-pool RA-pool
 authentication-server-group AAA-RADIUS
 default-group-policy GroupPolicy_AnyConnect
tunnel-group AnyConnect webvpn-attributes
 group-alias AnyConnect enable
 group-url https://10.4.47.2/AnyConnect enable
!
class-map global-class
 match access-list global_mpc
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
 class global-class
  ips inline fail-close
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
```

Feedback

Please use the feedback form to send comments and suggestions about this guide.

SMART BUSINESS ARCHITECTURE

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.

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.