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/Aug13-170

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

SBA

Email Security Using Cisco ESA 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 Borderless Networks

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 Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

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

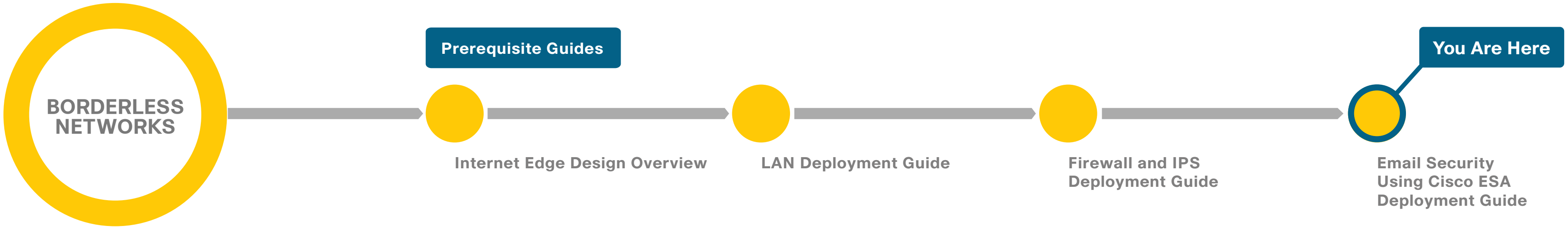
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- 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


BORDERLESS NETWORKS
Prerequisite Guides
Internet Edge Design Overview
LAN Deployment Guide
Firewall and IPS Deployment Guide
You Are Here
Email Security Using Cisco ESA Deployment Guide

Introduction

Business Overview

Email is a critical business service in most organizations. Failing to protect that service can result in a loss of data and employee productivity.

The two major threats to your organization's email system are:

- A flood of unsolicited and unwanted email, called *spam*, that wastes employee time through sheer volume and uses valuable resources like bandwidth and storage.
- Malicious email, which comes in two basic forms: *embedded attacks*, which include viruses and malware that perform actions on the end device when clicked, and *targeted or directed attacks*, such as phishing attacks, which try to mislead employees into releasing sensitive information like credit card numbers, social security numbers, or intellectual property. Phishing attacks might direct employees to inadvertently browse malicious websites that distribute additional malware to computer endpoints.

Technology Overview

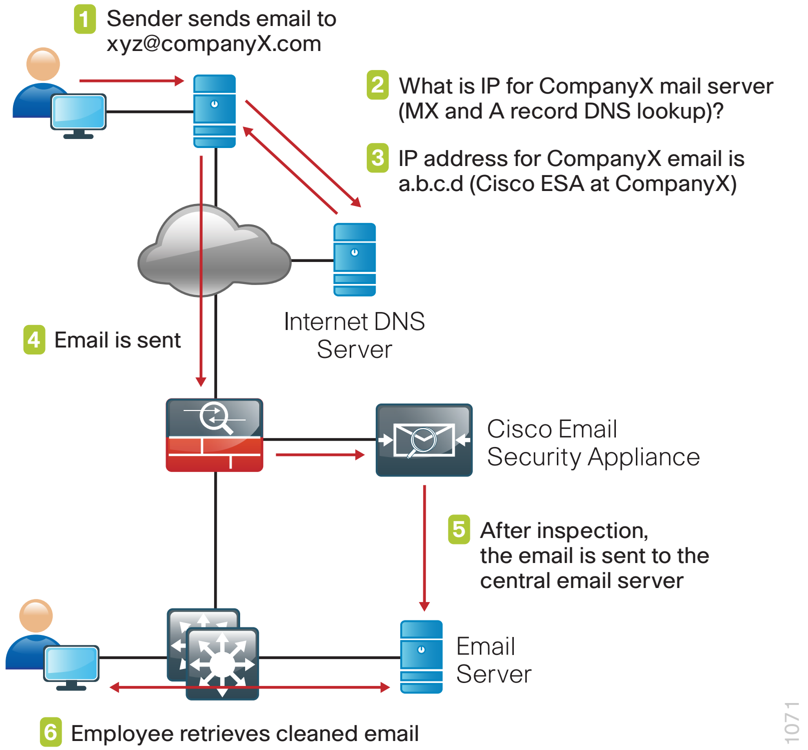
An email solution becomes unusable if junk email is not filtered properly. The sheer volume of junk messages can crowd out legitimate mail and cause employees to waste time manually filtering through messages. A side effect of some junk email-filtering solutions are false positives, or email that is incorrectly identified as spam, causing legitimate messages to be discarded.

When this occurs, the organization must sift through the junk email looking for legitimate messages or lower the level of filtering, allowing more potential junk messages to go to users and making the user responsible for determining whether email is spam. Unsolicited email is also more likely to be malicious and include embedded attacks. Criminal organizations are using attacks in email as an effective and cheap way to attack user machines. An example of an attack contained within email is malware that attempts to infect the host machine or that offers users counterfeit URLs (phishing) to trick them into going to a website where criminals can steal bank login credentials or infect the host machine.

The objective of these types of attacks is to gather social security numbers and credit card numbers or to compromise the host in order to use it as a launch point to send spam and other attacks.

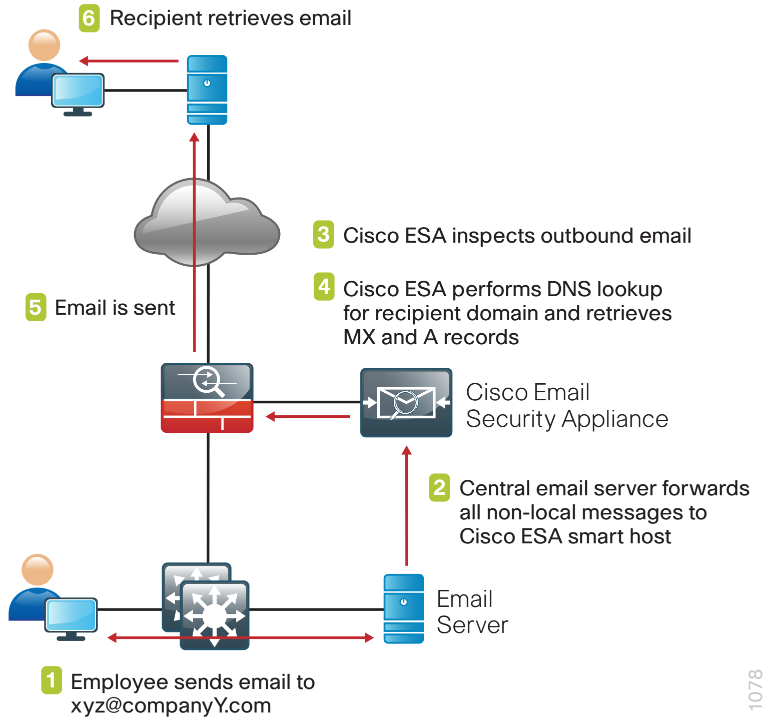
Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay. A normal email exchange in which an organization is using an MTA might look like the message flow shown below.

Figure 1 - Inbound email message flow


1 Sender sends email to xyz@companyX.com
2 What is IP for CompanyX mail server (MX and A record DNS lookup)?
3 IP address for CompanyX email is a.b.c.d (Cisco ESA at CompanyX)
Internet DNS Server
4 Email is sent
Cisco Email Security Appliance
5 After inspection, the email is sent to the central email server
Email Server
6 Employee retrieves cleaned email
1071

In addition to all of the email security capabilities provided by Cisco ESA for inbound email, Cisco ESA also provides anti-virus protection for outbound email.

Figure 2 - Outbound email message flow


6 Recipient retrieves email
3 Cisco ESA inspects outbound email
4 Cisco ESA performs DNS lookup for recipient domain and retrieves MX and A records
5 Email is sent
Cisco Email Security Appliance
2 Central email server forwards all non-local messages to Cisco ESA smart host
Email Server
1 Employee sends email to xyz@companyY.com
1078

Cisco ESA can be deployed with a single physical interface in order to filter email to and from an organization's mail server. The second deployment option is a two-interface configuration, one interface for email transfers to and from the Internet and the other for email transfers to and from the internal servers. This design guide uses the single-interface model for simplicity.

Cisco ESA uses a variety of mechanisms to filter spam and fight malicious attacks. The goal of the solution is to filter out positively identified spam and quarantine or discard email sent from untrusted or potentially hostile locations. Antivirus scanning is applied to emails and attachments from all servers to remove known malware.

Filtering Spam

There are two ways to filter spam and combat phishing attacks: reputation-based filtering and context-based filtering.

Reputation-Based Filtering

This type of filtering relies on the likelihood that if a server is a known spam sender, it is more likely that email coming from that server is spam compared to a host that does not have a reputation for distributing spam. Similar filters can be applied to emails carrying viruses and other threats.

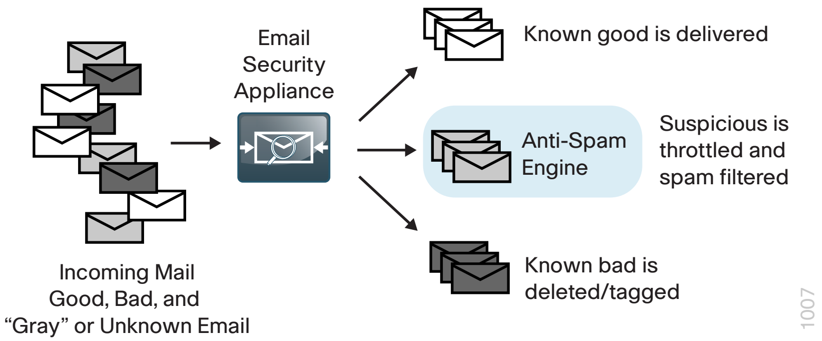
Reputation filters provide the first layer of defense by looking at the source IP address of the email server and comparing it to the reputation data downloaded from Cisco SenderBase. Cisco SenderBase is the world's largest repository for security data, including sources of spam, botnets, and other malicious hosts. When hosts on the Internet engage in malicious activity, SenderBase lowers the reputation of that host. The composite score for reputation from Cisco SenderBase can range from -10 to +10. Devices that use reputation filtering, like Cisco ESA, receive updates from SenderBase several times a day. When the appliance receives an email, it compares the source IP to the SenderBase database and performs the following checks (as illustrated in Figure 3):

- If the sender's reputation is between -1 and +10, the email is accepted.
- If the sender's reputation is between -1 and -3, the email is accepted and additional emails from the sender are throttled.
- If the sender's reputation is between -10 and -3, the email is blocked.

Context-Based Filtering

These anti-spam filters in the appliance inspect the entire mail message, including attachments, analyzing details such as sender identity, message contents, embedded URLs, and email formatting. Using these algorithms, the appliance can identify spam messages without blocking legitimate email.

Figure 3 - Email filtering overview



Fighting Viruses and Malware

Cisco ESA uses a multilayer approach to fight viruses and malware:

- The first layer of defense consists of outbreak filters, which the appliance downloads from Cisco SenderBase. They contain a list of known bad mail servers. These filters are generated by watching global email traffic patterns and looking for anomalies associated with an outbreak. When an email is received from a server on this list, it is kept in quarantine until the antivirus signatures are updated to counter the current threat.
- The second layer of defense is using antivirus signatures to scan quarantined emails, to ensure that they do not carry viruses into the network.
- Cisco ESA also scans outbound emails to provide antivirus protection.

High Availability

Cisco ESA functions as part of the mail transfer chain, and there is a reasonable amount of resiliency built into the system because a mail server in the chain stores a message for some period of time if the destination server is unresponsive.

This design configures Cisco ESA to use resilient Internet connections. You can achieve additional resiliency by adding a second Cisco ESA. You should configure the second Cisco ESA the same as the first Cisco ESA, and then add additional records to the Domain Name System (DNS).

For any additional devices, you need to add access lists and static Network Address Translation (NAT) rules to the firewall appliance.

Monitoring

You can monitor the behavior of Cisco ESA by viewing a variety of reports available under the Monitor tab. These reports allow an administrator to track activity and statistics for spam, virus types, incoming mail domains, outbound destinations, system capacity, and system status.

Troubleshooting

If you need to determine why Cisco ESA applied specific actions for a given email, you can run the Trace tool under System Administration.

By defining a search using details of a given email in question, it is possible to test a specific email to determine how and why Cisco ESA handled the message. This search capability is especially useful if some of the more advanced features of ESA are used, such as data loss prevention (DLP).

Reader Tip

For more information about Cisco ESA products, see the customer support page:
http://www.cisco.com/web/ironport/index.html

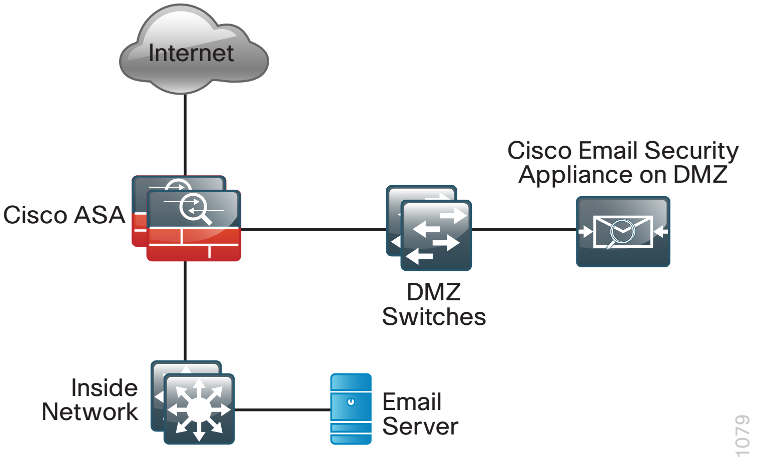
Notes

Deployment Details

Cisco ESA deployment is designed to be as easy as possible. It is deployed into the existing mail delivery chain as a Mail Transfer Agent (MTA). The appliance will be the destination of email for the organization; as such, the public MX records (the DNS record that defines where to send mail) must eventually point to the public IP address of Cisco ESA.

In this deployment guide, the appliance is physically deployed on the demilitarized zone (DMZ) of the Internet Edge firewall, and uses a single interface for simplicity. This interface handles all incoming and outgoing email and carries management traffic. The port on the appliance is the M1 management interface.

Figure 4 - Deployment overview



It is important that Cisco ESA be accessible through the public Internet and that it is the first hop in the email infrastructure. Several of the Cisco ESA processes use the sender IP address, which is one of the primary identifiers Cisco SenderBase uses to determine the reputation of the sender. If another device receives mail before forwarding it to the appliance, the appliance is not able to determine the sender IP address and filtering cannot be applied properly.

The internal email server needs to configure Cisco ESA as a smart host or mail relay. The configuration of the internal email server is not included in this guide.

Process

Configuring Email DMZ

1. Configure the DMZ switch
2. Configure the firewall's mail DMZ interface
3. Configure Network Address Translation
4. Configure security policy

The firewall's 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 in a DMZ for exposure to the Internet. These servers are typically not allowed to initiate connections to the inside network, except for specific circumstances.

Reader Tip

This procedure assumes that the Internet-edge firewall and DMZ switch have already been configured following the guidance in the *Cisco SBA—Borderless Networks Firewall and IPS Deployment Guide*.

In this process, you configure a DMZ for Cisco ESA so it can serve as the organization's MTA for email sent and received using the Internet.

Procedure 1 Configure the DMZ switch

Step 1: Configure the mail DMZ VLAN and set the DMZ switch to be the spanning tree root for the VLAN that contains the email security appliance.

```
vlan 1117
 name dmz-email
```

Step 2: Add the mail DMZ VLAN to the trunks that connect to the Internet-edge firewall.

```
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport trunk allowed vlan add 1117
```

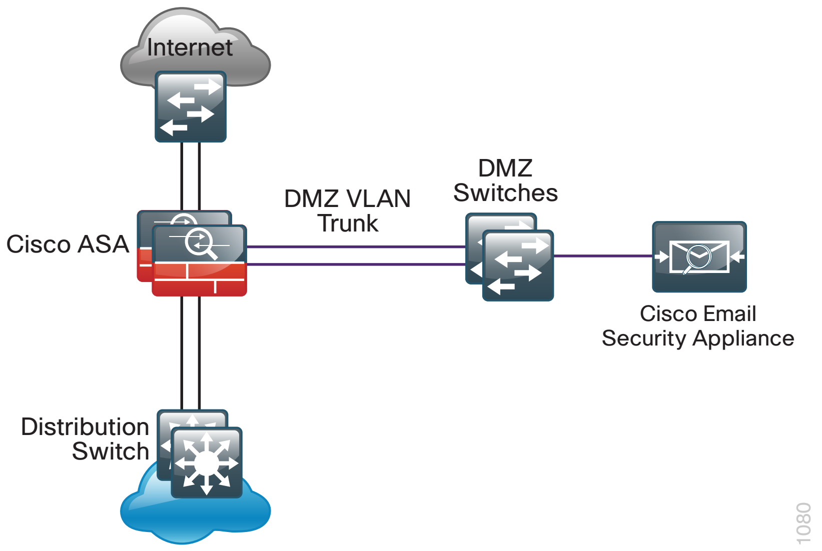
Step 3: Configure the interface that connects to the email security appliance.

```
interface GigabitEthernet1/0/22
 description Cisco ESA M1 management interface
 switchport access vlan 1117
 switchport host
 macro apply EgressQoS
 logging event link-status
 no shutdown
```

Procedure 2 Configure the firewall's mail DMZ interface

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 to connect additional DMZs. The trunk connects the appliances to a 3750X access-switch stack in order to provide resiliency. The DMZ VLAN interfaces on Cisco Adaptive Security Appliance (ASA) 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 5 - DMZ VLAN topology and services



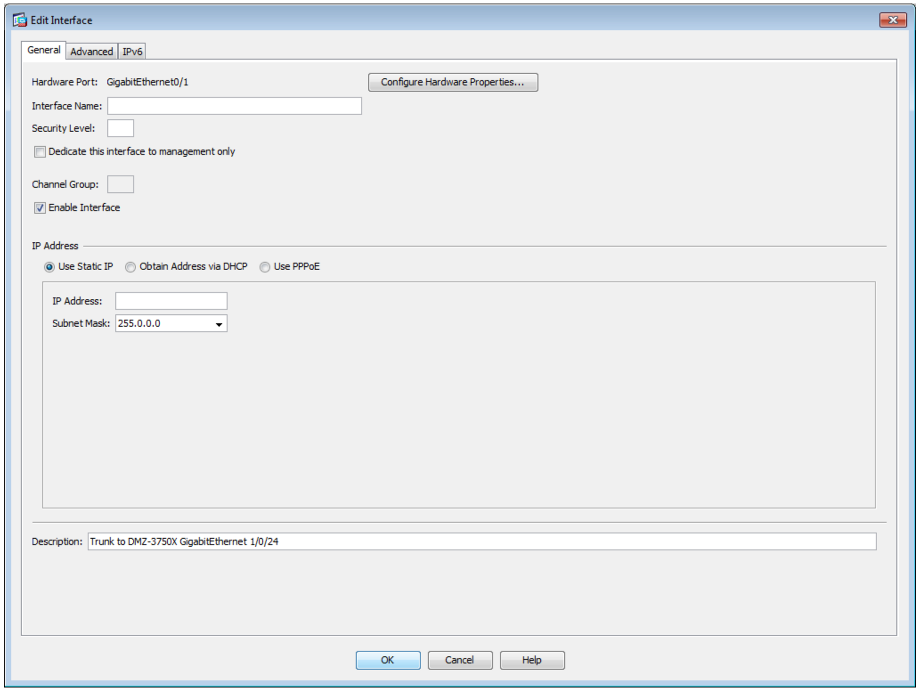
Tech Tip

Setting the DMZ connectivity as a VLAN trunk offers the greatest flexibility.

Step 1: Using a browser, access the ASA's GUI. (Example: https://10.4.24.30)

Step 2: In **Configuration > Device Setup > Interfaces**, click the interface that is connected to the DMZ switch (Example: GigabitEthernet0/1), and then click **Edit**.

Step 3: In the Edit Interface dialog box, if the interface has not already been enabled, select **Enable Interface**, and then click **OK**. Otherwise, click **Cancel**.



Hardware Port: GigabitEthernet0/1
Interface Name:
Security Level:
☐ Dedicate this interface to management only
Channel Group:
☑ Enable Interface
● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE
IP Address:
Subnet Mask: 255.0.0.0
Description: Trunk to DMZ-3750X GigabitEthernet 1/0/24

Step 4: On the Interface pane, click **Add > Interface**.

Step 5: In the Add Interface dialog box, in the **Hardware Port** list, select the interface referenced in Step 2. (Example: GigabitEthernet0/1)

Step 6: In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1117)

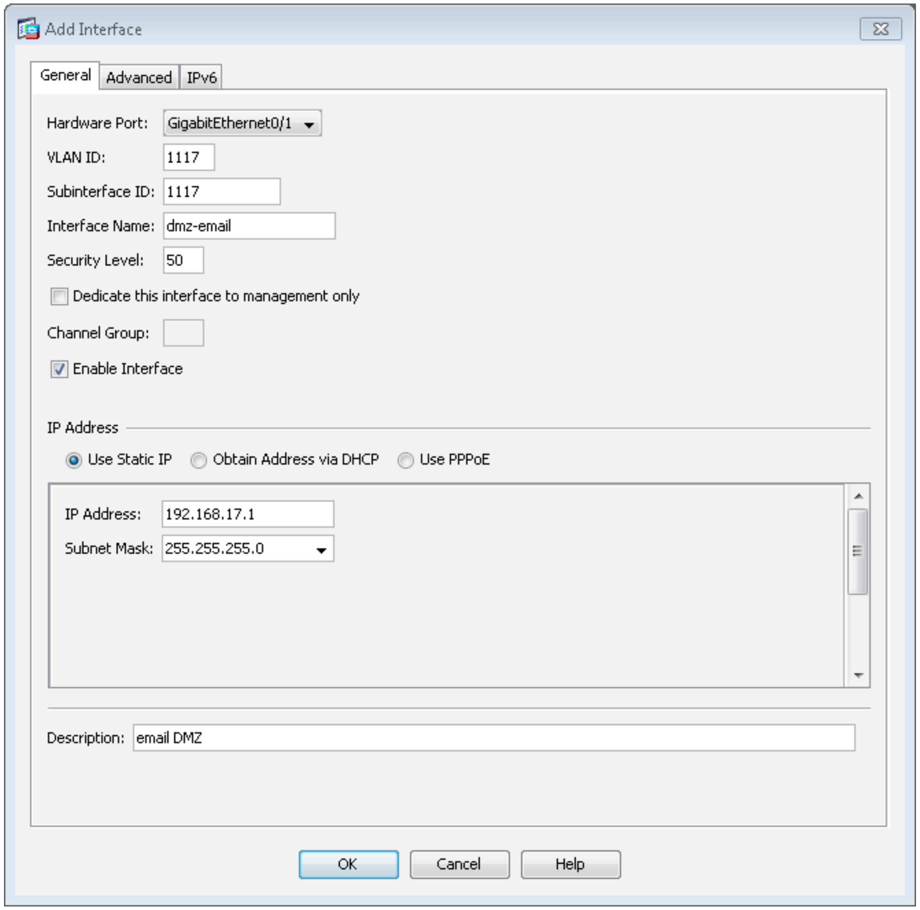
Step 7: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1117)

Step 8: In the **Interface Name** box, enter an interface name. (Example: dmz-email)

Step 9: In the **Security Level** box, enter a value of **50**.

Step 10: In the **IP Address** box, enter an interface IP address. (Example: 192.168.17.1)

Step 11: In the **Subnet Mask** box, enter the interface subnet mask (Example: 255.255.255.0), and then click **OK**.



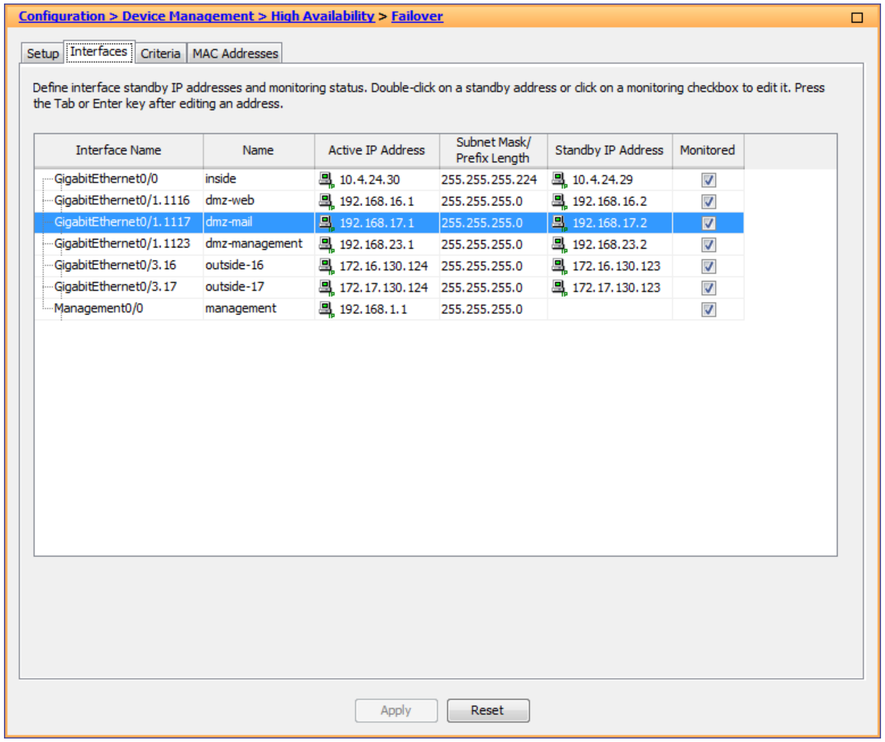
Hardware Port: GigabitEthernet0/1
VLAN ID: 1117
Subinterface ID: 1117
Interface Name: dmz-email
Security Level: 50
☐ Dedicate this interface to management only
Channel Group:
☑ Enable Interface
● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE
IP Address: 192.168.17.1
Subnet Mask: 255.255.255.0
Description: email DMZ

Step 12: On the Interface pane, click **Apply**.

Step 13: Navigate to **Configuration > Device Management > High Availability > Failover.**

Step 14: On the Interfaces tab, in the Standby IP address column, enter the IP address of the standby unit for the interface you just created. (Example: 192.168.17.2)

Step 15: Select **Monitored**, and then click **Apply**.



Configuration > Device Management > High Availability > Failover

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	inside	10.4.24.30	255.255.255.224	10.4.24.29	☑
GigabitEthernet0/1.1116	dmz-web	192.168.16.1	255.255.255.0	192.168.16.2	☑
GigabitEthernet0/1.1117	dmz-mail	192.168.17.1	255.255.255.0	192.168.17.2	☑
GigabitEthernet0/1.1123	dmz-management	192.168.23.1	255.255.255.0	192.168.23.2	☑
GigabitEthernet0/3.16	outside-16	172.16.130.124	255.255.255.0	172.16.130.123	☑
GigabitEthernet0/3.17	outside-17	172.17.130.124	255.255.255.0	172.17.130.123	☑
Management0/0	management	192.168.1.1	255.255.255.0		☑

Procedure 3 Configure Network Address Translation

The DMZ network uses private network (RFC 1918) addressing that is not Internet routable, so the firewall must translate the DMZ address of Cisco ESA to an outside public address. If there is a resilient Internet connection, the appliance can have an address translation for each ISP. This resilient configuration, shown here for completeness, relies on the modification of DNS records to point incoming requests to the resilient Cisco ESA when the primary Internet connection is unavailable.

The example DMZ address to public IP address mapping is shown in the following table.

Table 1 - Cisco ESA address mapping

Cisco ESA DMZ address	Cisco ESA public address (externally routable after NAT)
192.168.17.25	172.16.130.25 (ISP-A)
	172.17.130.25 (ISP-B)

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

First, you add a network object for the public address of the Cisco ESA server on the primary Internet connection.

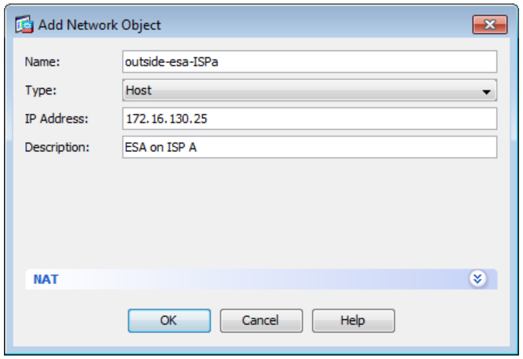
Step 2: Click **Add > Network Object**.

Step 3: On the Add Network Object dialog box, in the **Name** box, enter a description for the Cisco ESA's public IP address. (Example: outside-esa-ISPa)

Step 4: In the **Type** list, choose **Host**.

Step 5: In the **IP Address** box, enter the Cisco ESA's public IP address, and then click **OK**. (Example: 172.16.130.25)

Step 6: On the Network Objects/Groups pane, click **Apply**.



Name: outside-esa-ISPa

Type: Host

IP Address: 172.16.130.25

Description: ESA on ISP A

Next, you add a network object for the private DMZ address of Cisco ESA.

Step 7: Click **Add > Network Object**.

Step 8: On the Add Network Object dialog box, in the **Name** box, enter a description for the Cisco ESA's private DMZ IP address. (Example: dmz-esa370-ISPa)

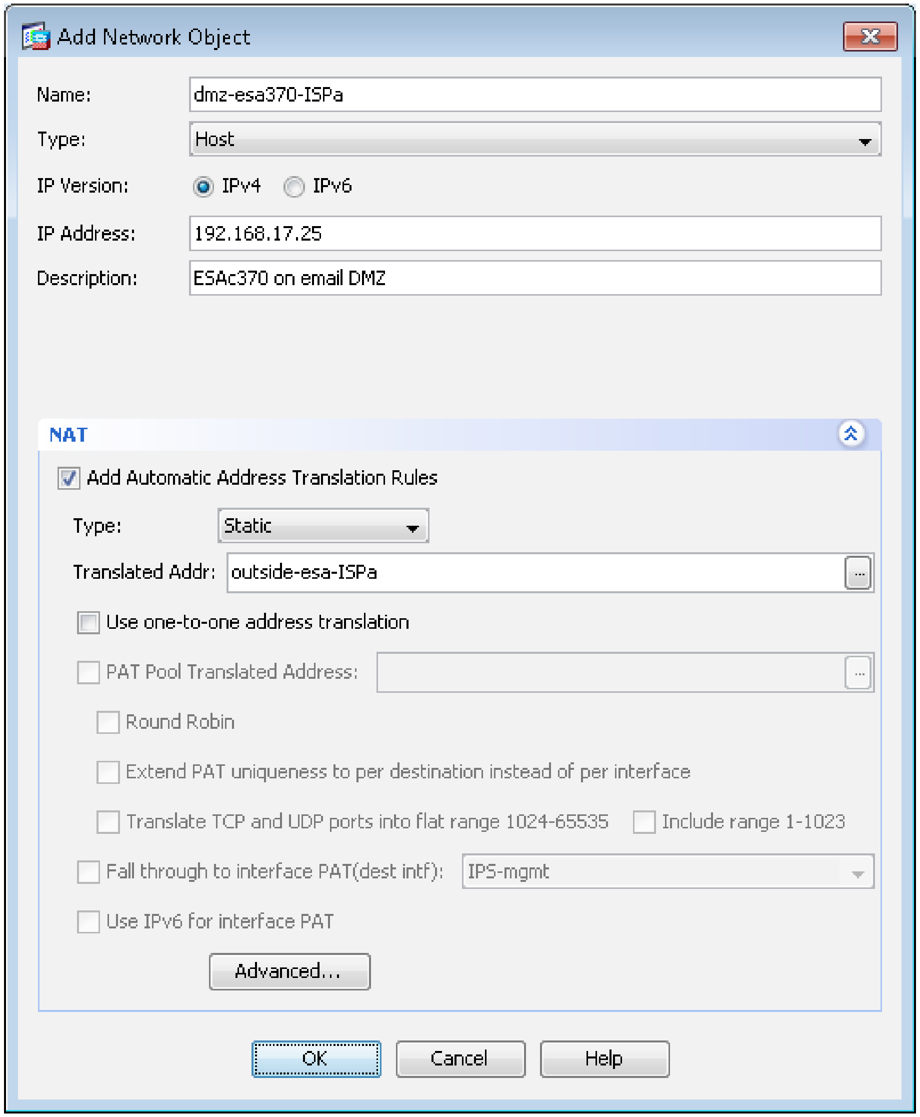
Step 9: In the **Type** list, choose **Host**.

Step 10: In the **IP Address** box, enter the Cisco ESA's private DMZ IP address. (Example: 192.168.17.25)

Step 11: Click the two down arrows. The NAT pane expands.

Step 12: Select **Add Automatic Address Translation Rules**.

Step 13: In the **Translated Addr** list, choose the network object created in Step 2.



Name: dmz-esa370-ISPa

Type: Host

IP Version: ● IPv4 ○ IPv6

IP Address: 192.168.17.25

Description: ESAc370 on email DMZ

☑ Add Automatic Address Translation Rules

Type: Static

Translated Addr: outside-esa-ISPa

□ Use one-to-one address translation

□ PAT Pool Translated Address:

□ Round Robin

□ Extend PAT uniqueness to per destination instead of per interface

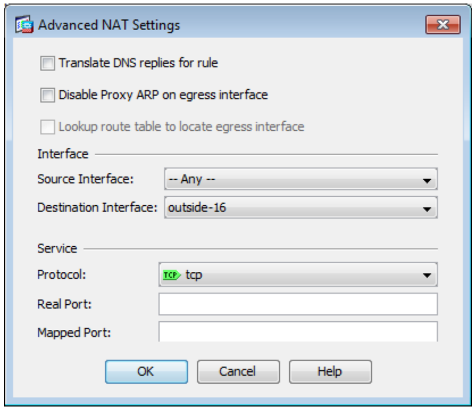
□ Translate TCP and UDP ports into flat range 1024-65535 □ Include range 1-1023

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

□ Use IPv6 for interface PAT

Step 14: Click **Advanced**.

Step 15: In the Advanced NAT Settings dialog box, in the **Destination Interface** list, choose the interface name for the primary Internet connection, and then click **OK**. (Example: outside-16)



Advanced NAT Settings

☐ Translate DNS replies for rule

☐ Disable Proxy ARP on egress interface

☐ Lookup route table to locate egress interface

Interface

Source Interface: -- Any --

Destination Interface: outside-16

Service

Protocol: tcp

Real Port:

Mapped Port:

Step 16: In the Add Network Object dialog box, click **OK**.

Step 17: On the Network Objects/Groups pane, click **Apply**.

Step 18: If you are using a design which has a resilient Internet connection, repeat this procedure for the resilient Internet connection.

Procedure 4 Configure security policy

The Email DMZ provides an additional layer of protection to lower the likelihood of certain types of misconfiguration or a compromise of a host in the DMZ, exposing other devices or networks to an attacker on the Internet. The security policy allows only mail traffic to Cisco ESA. The appliance is allowed to send SMTP traffic as well as make HTTP and HTTPS connections (needed for reputation updates) to any host on the Internet. Cisco ESA is allowed to make inbound SMTP connections to the corporate exchange server as well as DNS requests to the organization's DNS server.

First, you ease the configuration of the security policy by creating the network objects that are used in the firewall policies.

Table 2 - Firewall network objects

Network object name	Object type	IP address
internal-dns	Host	10.4.48.10
internal-exchange	Host	10.4.48.25
internal-ntp	Host	10.4.48.17
internal-network	Network	10.4.0.0/15

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

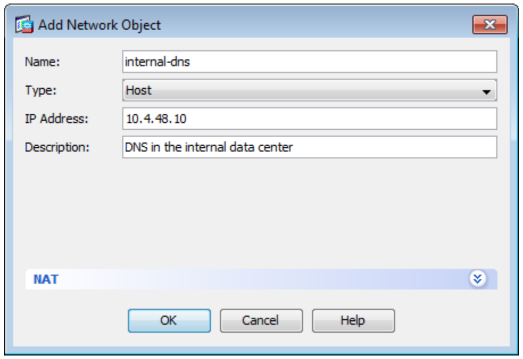
Step 2: Repeat Step 2 through Step 6 for all objects listed in Table 2. If the object already exists, then skip to the next object listed in the table.

Step 3: Click **Add > Network Object**.

Step 4: On the Add Network Object dialog box, in the **Name** box, enter a description. (Example: internal-dns)

Step 5: In the **Type** list, choose **Host** or **Network**, as indicated by Table 2.

Step 6: In the **IP Address** box, enter the address of the internal DNS, and then click **OK**. (Example: 10.4.48.10)



Add Network Object

Name: internal-dns

Type: Host

IP Address: 10.4.48.10

Description: DNS in the internal data center

Step 7: After adding all of the objects listed in Table 2, on the Network Objects/Groups pane, click **Apply**.

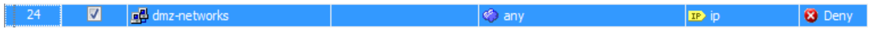
Step 8: Navigate to **Configuration > Firewall > Access Rules**.

Table 3 - Firewall policy rules for ESA

Action	Source object	Destination object	Service	Description
permit	internal-exchange	dmz-email-network	tcp/smtp	Exchange to ESA out-bound SMTP
deny	internal-network	any4	tcp/smtp	Block other outbound SMTP
permit	any4	dmz-email-network	tcp/smtp	Internet to ESA inbound SMTP
permit	dmz-email-network	internal-exchange	tcp/smtp	ESA to Exchange inbound SMTP
permit	dmz-email-network	internal-dns	udp/domain	DNS
permit	dmz-email-network	internal-ntp	udp/ntp	NTP
deny	dmz-email-network	internal-network	ip	Block other to internal networks
permit	dmz-email-network	any4	tcp/smtp	ESA to Internet outbound SMTP
permit	dmz-email-network	any4	tcp/http	HTTP to Internet
permit	dmz-email-network	any4	tcp/https	HTTPS to Internet

Step 9: Repeat Step 10 through Step 17 for all rules listed in Table 3.

Step 10: Click the rule that denies traffic from the DMZ toward the internal network.



24	☑	dmz-networks		any	ip	Deny

Step 11: Click **Add > Insert**.

Step 12: In the Add Access Rule dialog box, in the **Interface** list, choose **—Any—**.

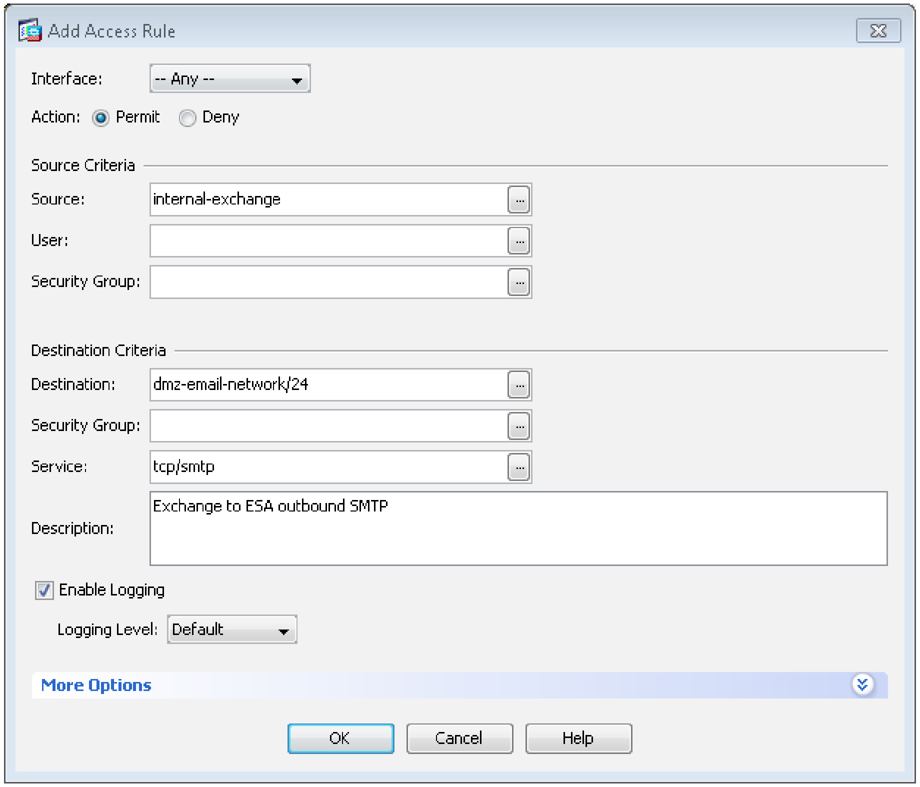
Step 13: For Action, select the action listed in Table 3.

Step 14: For Source, select the source object listed in Table 3.

Step 15: For Destination, select the destination object listed in Table 3.

Step 16: For Service, enter the service listed in Table 3.

Step 17: Enter a description, and then click **OK**.



Add Access Rule

Interface: -- Any --

Action: ● Permit ○ Deny

Source Criteria

Source: internal-exchange

User:

Security Group:

Destination Criteria

Destination: dmz-email-network/24

Security Group:

Service: tcp/smtp

Description: Exchange to ESA outbound SMTP

☑ Enable Logging

Logging Level: Default

Step 18: After adding all of the rules listed in Table 3, on the Access Rules pane, click **Apply**.

Process

Configuring Cisco Email Security Appliance

1. Configure DNS entries
2. Deploy Cisco ESA
3. Complete the GUI-based system setup
4. Install system updates and feature keys

Before you begin the Cisco ESA deployment, you need to configure the DNS.

Procedure 1 Configure DNS entries

Prepare for the following configuration procedures by creating the DNS records that are required for email communication. The DNS address (A) record provides a Fully Qualified Domain Name (FQDN) to IP addressing mapping and the DNS pointer record (PTR) provides an IP to FQDN mapping, also known as a reverse lookup.

Configure your internal DNS server to advertise the records listed in Table 4.

Table 4 - Example DNS A and PTR records (Internal DNS)

FQDN	Outside IP address
internal-exchange.cisco.local	10.4.48.25
mail.cisco.local	192.168.17.25

If you are using a resilient ISP design, then each outside IP address requires its FQDN as shown in Table 5.

The domain (Example: cisco.local) requires one or more mail exchange records (MX), which are used to determine the MTA for an organization. In a resilient design, multiple MX records with differing mail server priorities are used. The mail server with the lowest mail server priority is the primary MTA. Example values are shown in Table 6.

Configure your external DNS server to advertise the records listed in Table 5 and Table 6.

Table 5 - Example DNS A and PTR records (External DNS)

ISP	FQDN	Outside IP address
Primary	mail-a.cisco.local	172.16.130.25
Secondary	mail-b.cisco.local	172.17.130.25

Table 6 - Example MX records (External DNS)

ISP	FQDN	Mail server	Mail server priority
Primary	cisco.local	mail-a.cisco.local	10
Secondary	cisco.local	mail-b.cisco.local	20

Procedure 2 Deploy Cisco ESA

First, configure management access.

Step 1: Connect to the appliance's serial console port by using a standard null modem cable with the terminal emulator settings of 8-1-none-9600 baud, and then log in.

Tech Tip

The default username is **admin**, and the default password is **ironport**.

Step 2: Run **interfaceconfig** and **setgateway**, which change the basic network settings, and then issue the **commit** command, which saves the changes to the running configuration.

Tech Tip

Depending on the code version the appliance has installed, the CLI or GUI interfaces might display slightly different options.

```
ironport.example.com> interfaceconfig

Currently configured interfaces:
1. Management (192.168.42.42/24 on Management: ironport.
example.com)

Choose the operation you want to perform:
[]> EDIT

Enter the number of the interface you wish to edit.
[]> 1

IP interface name (Ex: "InternalNet"):
[Management]> dmz-email

Would you like to configure an IPv4 address for this interface
(y/n)? [Y]> y

IP Address (Ex: 192.168.1.2):
[192.168.42.42]> 192.168.17.25

Netmask (Ex: "24", "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> 255.255.255.0

Would you like to configure an IPv6 address for this interface
(y/n)? [N]> n
```

```
Ethernet interface:
1. Data 1
2. Data 2
3. Data 3
4. Management
[4]> 4

Hostname:
[ironport.example.com]> DMZ-ESAc370.cisco.local

Do you want to enable Telnet on this interface? [Y]> n
Do you want to enable SSH on this interface? [Y]> y
Which port do you want to use for SSH? [22]> 22
Do you want to enable FTP on this interface? [N]> n
Do you want to enable Cluster Communication Service on this
interface? [N]> n
Do you want to enable HTTP on this interface? [Y]> y
Which port do you want to use for HTTP? [80]> 80
Do you want to enable HTTPS on this interface? [Y]> y
Which port do you want to use for HTTPS? [443]> 443

Do you want to enable Spam Quarantine HTTP on this interface?
[N]> Y

Which port do you want to use for Spam Quarantine HTTP? [82]>
82

Do you want to enable Spam Quarantine HTTPS on this interface?
[N]> Y
Which port do you want to use for Spam Quarantine HTTPS?[83]>
83

The “Demo” certificate is currently configured. You may use
“Demo”, but this will not be secure. To assure privacy, run
“certconfig” first.
Both HTTP and HTTPS are enabled for this interface, should
HTTP requests redirect to the secure service? [Y]> Y

Both Spam Quarantine HTTP and Spam Quarantine HTTPS are
enabled for this interface, should Spam Quarantine HTTP
requests redirect to the secure service? [Y]> Y

Do you want dmz-email as the default interface for Spam
Quarantine? [N]> Y

Do you want to use a custom base URL in your Spam Quarantine
email notifications? [N]> N

The interface you edited might be the one you are currently
logged into. Are you sure you want to change it? [Y]> Y
Updating SNMP agent interface referencing the old interface
name “Management” to the new interface name “dmz-email”.
Currently configured interfaces:
1. dmz-email (192.168.17.25/24 on Management: DMZ-ESAc370.
cisco.local)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> <Return>

ironport.example.com> setgateway

Warning: setting an incorrect default gateway may cause the
current
connection to be interrupted when the changes are committed.
Set gateway for:

1. IPv4
2. IPv6
[1]> 1
```

```
Enter new default gateway:[]> 192.168.17.1

ironport.example.com> commit

Please enter some comments describing your changes:
[]> initial setup

Changes committed
```

Cisco ESA is now configured. You can verify connectivity by pinging the default gateway.

```
ironport.example.com> ping 192.168.17.1
Press Ctrl-C to stop.
PING 192.168.17.1 (192.168.17.1): 56 data bytes
64 bytes from 192.168.17.1: icmp_seq=0 ttl=255 time=0.481 ms
64 bytes from 192.168.17.1: icmp_seq=1 ttl=255 time=0.271 ms
64 bytes from 192.168.17.1: icmp_seq=2 ttl=255 time=0.195 ms
^C
```

Procedure 3 Complete the GUI-based system setup

Step 1: From a client on the internal network, navigate and log in to the appliance. (Example: https://192.168.17.25)

Tech Tip

The default username is **admin**, and the default password is **ironport**.

Step 2: Navigate to **System Administration** > **System Setup Wizard**.

Step 3: At the Start screen, read the license, click **I accept**, and then click **Begin Setup**.

Step 4: On the System tab, in the **Default System Hostname** box, enter the appliance hostname. (Example: DMZ-ESAc370.cisco.local)

Step 5: In the **Email System Alerts** box, enter the administrators email address. (Example: admin@cisco.local)

Step 6: Set the appropriate time zone for the appliance.

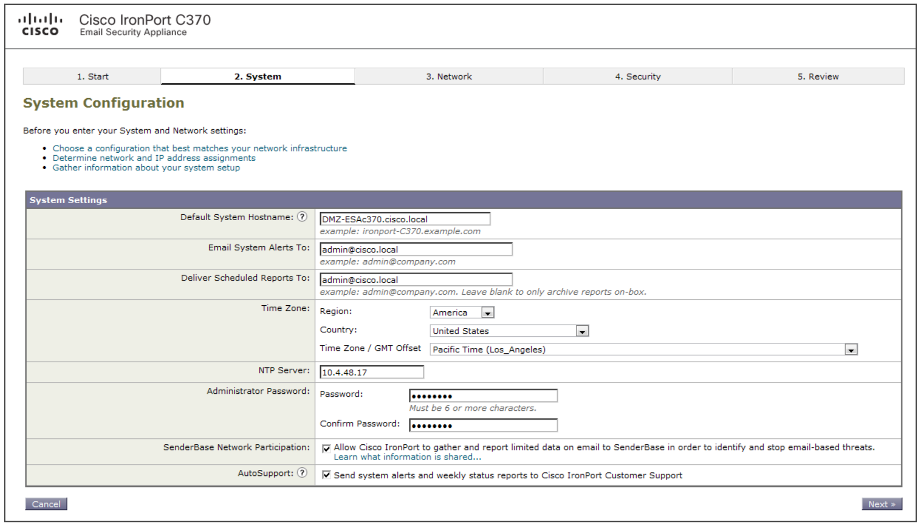
- Region—**America**
- Country—**United States**
- Time Zone / GMT Offset—**Pacific Time (Los_Angeles)**

Step 7: In the **NTP Server** box, enter the internal NTP server. (Example: 10.4.48.17)

Step 8: Set and confirm the administrator password, and then click **Next**.

Tech Tip

The last two checkboxes determine whether Cisco ESA participates in the Cisco SenderBase network. This allows Cisco ESA to send anonymized reputation details about email traffic to Cisco in order to improve SenderBase and the product in general.



System Configuration

Before you enter your System and Network settings:

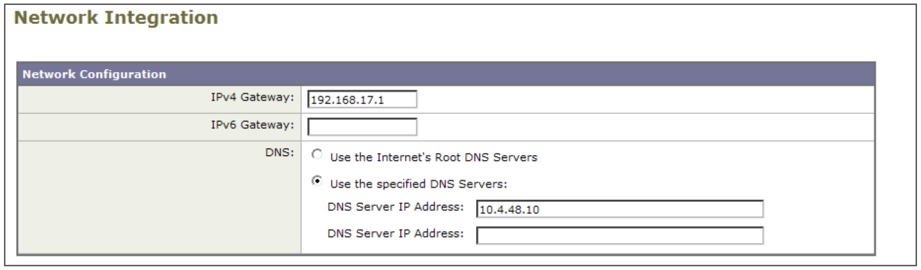
- Choose a configuration that best matches your network infrastructure
- Determine network and IP address assignments
- Gather information about your system setup

System Settings

Default System Hostname: ?	DMZ-ESAc370.cisco.local example: ironport-C370.example.com
Email System Alerts To:	admin@cisco.local example: admin@company.com
Deliver Scheduled Reports To:	admin@cisco.local example: admin@company.com. Leave blank to only archive reports on-box.
Time Zone:	Region: America Country: United States Time Zone / GMT Offset Pacific Time (Los_Angeles)
NTP Server:	10.4.48.17
Administrator Password:	Password: •••••••• Must be 6 or more characters. Confirm Password: ••••••••
SenderBase Network Participation:	☑ Allow Cisco IronPort to gather and report limited data on email to SenderBase in order to identify and stop email-based threats. Learn what information is shared...
AutoSupport: ?	☑ Send system alerts and weekly status reports to Cisco IronPort Customer Support

Step 9: On the Network tab, choose **Use the specified DNS Servers.**

Step 10: In the **DNS Server IP Address** box, enter the internal DNS. (Example: 10.4.48.10)



Network Integration

Network Configuration

IPv4 Gateway:	192.168.17.1
IPv6 Gateway:	
DNS:	○ Use the Internet's Root DNS Servers ● Use the specified DNS Servers: DNS Server IP Address: 10.4.48.10 DNS Server IP Address:

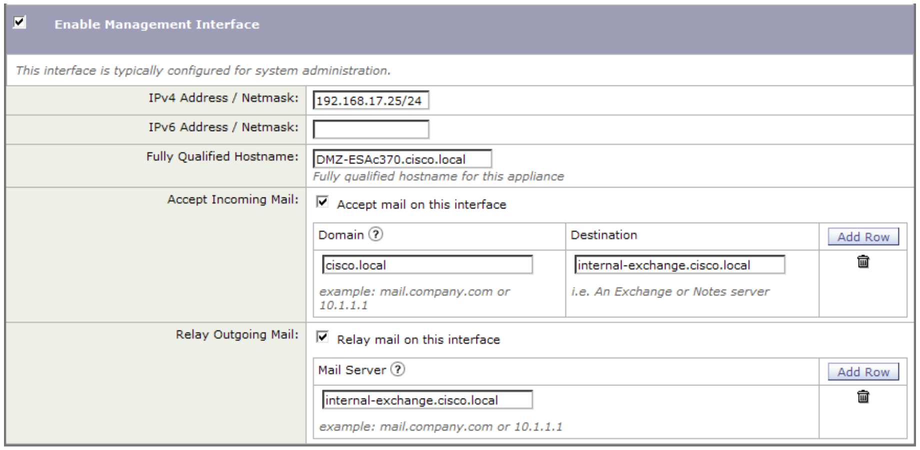
Step 11: For Accept Incoming Mail, select **Accept mail on this interface**.

Step 12: In the **Domain** box, enter the organization's email domain. (Example: cisco.local)

Step 13: In the **Destination** box, enter the internal email server. (Example internal-exchange.cisco.local)

Step 14: For Relay Outgoing Mail, select **Relay mail on this interface**.

Step 15: In the **Mail Server** box, enter the internal email server, and then click **Next**. (Example internal-exchange.cisco.local)

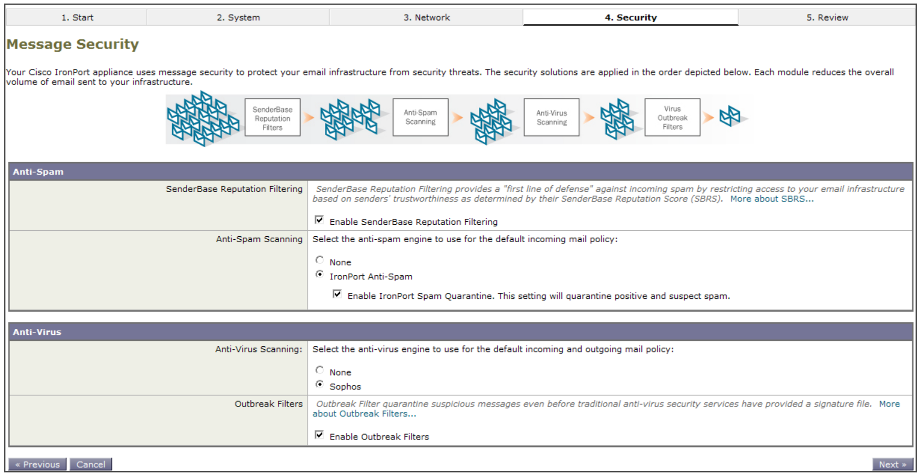


☑ **Enable Management Interface**

This interface is typically configured for system administration.

IPv4 Address / Netmask:	192.168.17.25/24
IPv6 Address / Netmask:	
Fully Qualified Hostname:	DMZ-ESAc370.cisco.local *Fully qualified hostname for this appliance*
Accept Incoming Mail:	☑ Accept mail on this interface Domain: cisco.local (*example: mail.company.com or 10.1.1.1*) Destination: internal-exchange.cisco.local (*i.e. An Exchange or Notes server*)
Relay Outgoing Mail:	☑ Relay mail on this interface Mail Server: internal-exchange.cisco.local (*example: mail.company.com or 10.1.1.1*)

Step 16: On the Security tab, ensure anti-spam and anti-virus filtering are enabled, and then click **Next**.



Message Security

Your Cisco IronPort appliance uses message security to protect your email infrastructure from security threats. The security solutions are applied in the order depicted below. Each module reduces the overall volume of email sent to your infrastructure.

Anti-Spam

SenderBase Reputation Filtering	*SenderBase Reputation Filtering provides a "first line of defense" against incoming spam by restricting access to your email infrastructure based on senders' trustworthiness as determined by their SenderBase Reputation Score (SBRS).* More about SBRS... ☑ Enable SenderBase Reputation Filtering
Anti-Spam Scanning	Select the anti-spam engine to use for the default incoming mail policy: ○ None ● IronPort Anti-Spam ☑ Enable IronPort Spam Quarantine. This setting will quarantine positive and suspect spam.

Anti-Virus

Anti-Virus Scanning:	Select the anti-virus engine to use for the default incoming and outgoing mail policy: ○ None ● Sophos
Outbreak Filters	*Outbreak Filter quarantine suspicious messages even before traditional anti-virus security services have provided a signature file.* More about Outbreak Filters... ☑ Enable Outbreak Filters

Step 17: On the Review tab, review the configuration, and then click **Install this Configuration**.

Step 18: On the Confirm Install window, accept the warning by clicking **Install**. Cisco ESA installs the configuration.

Step 19: When the Active Directory wizard appears, click **Cancel**. In this example, you do not configure an Active Directory server.

Procedure 4 Install system updates and feature keys

Step 1: In the web configuration tool, browse to **System Administration > Feature Keys**. This is where the license keys for the different features on the box are displayed.

Step 2: Check whether your appliance has any licenses that are not currently enabled by clicking **Check for New Keys**. This enables the appliance to connect to Cisco.com and determine if all purchased licenses are installed and enabled.

Next, upgrade the system software on the appliance.

Tech Tip

It is not possible to downgrade software versions, so be certain that you want to upgrade before proceeding. It is possible that an appliance can receive different upgrade options if it is on an early release list.

Step 3: Select the **System Administration >System Upgrade** button. The current software version appears.

Step 4: Click **Available Upgrades**. This determines if updates are available.

Step 5: If newer versions are available, you may select and install them now.

Tech Tip

While it is not necessary to load all updates sequentially, it is possible that a more recent update will require interim updates before it can be loaded. If interim updates are required, the appliance will alert the operator.

If the latest version isn't available in the list of software upgrade versions, then upgrade to the latest version listed and check the list again after rebooting as there may not be an immediate upgrade path from the version the appliance is running to the latest available version.

Process

Enabling Mail Policies

1. Configure outbound email
2. Set up Bounce Verification
3. Review incoming mail policies
4. Enable message tracking (optional)

Now that system setup is complete, you are ready to enable mail policies.

Procedure 1 Configure outbound email

Cisco ESA uses a Recipient Access Table (RAT) to control whether to accept or reject email messages to a recipient address. The System Setup Wizard configures Cisco ESA to accept email to your organization (Example: cisco.local), but rejects email to all other recipients.

You must configure Cisco ESA to accept email for other recipients so that your internal email server can use Cisco ESA as an email relay (sometimes referred to as a smart host).

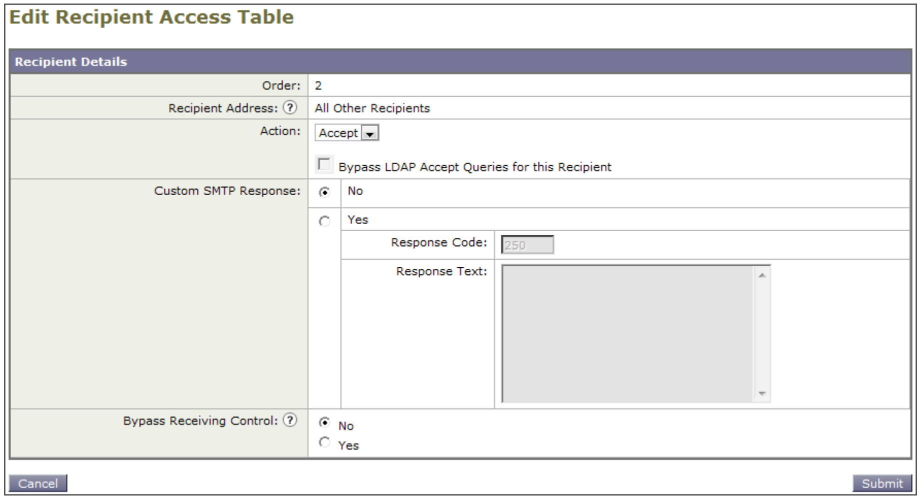
Tech Tip

Cisco ESA restricts the hosts that can use it as a relay through Host Access Table (HAT). Only your internal mail server(s) should be listed in the HAT as a relay.

This was automatically configured through the System Setup Wizard.

Step 1: Navigate to **Mail Policies > Recipient Access Table (RAT)**, and then click **All Other Recipients**.

Step 2: In the **Action** list, choose **Accept**, and then click **Submit**.

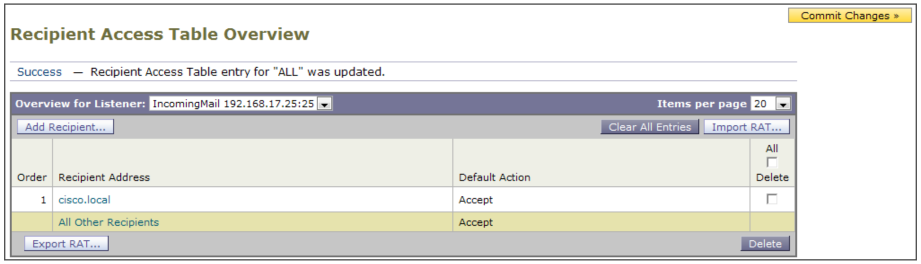


Edit Recipient Access Table

Recipient Details

Order:	2
Recipient Address:	All Other Recipients
Action:	Accept □ Bypass LDAP Accept Queries for this Recipient
Custom SMTP Response:	● No ○ Yes Response Code: 250 Response Text:
Bypass Receiving Control:	● No ○ Yes

Step 3: Click **Commit Changes**.



Recipient Access Table Overview

Success — Recipient Access Table entry for "ALL" was updated.

Overview for Listener: IncomingMail 192.168.17.25:25   Items per page 20

Order	Recipient Address	Default Action	All □ Delete
1	cisco.local	Accept	□
	All Other Recipients	Accept	

Step 4: In the Uncommitted Changes pane, enter a comment to describe the change and click **Commit Changes**.

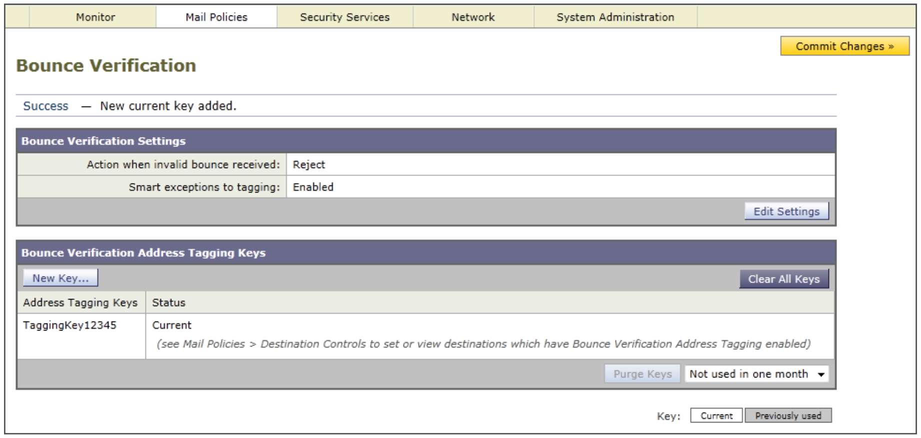
Procedure 2 Set up Bounce Verification

One of the last steps of setting up a standard configuration for Cisco ESA is setting up Bounce Verifications. Bounce Verification is a process that allows Cisco ESA to tag outgoing messages so that when bounced email comes back to the appliance, it can verify that the email was actually sent out originally by Cisco ESA. Spammers and hackers use fake bounced messages for many malicious purposes.

Step 1: Navigate to **Mail Policies > Bounce Verification**, and then click **New Key.**

Step 2: In the **Address Tagging Key** box, enter an arbitrary text string that Cisco ESA will apply in the Bounce Verification process, and then click **Submit**.

Step 3: Click **Commit Changes**.



Bounce Verification

Success — New current key added.

Bounce Verification Settings

Action when invalid bounce received:	Reject
Smart exceptions to tagging:	Enabled

Bounce Verification Address Tagging Keys

Address Tagging Keys	Status
TaggingKey12345	Current *(see Mail Policies > Destination Controls to set or view destinations which have Bounce Verification Address Tagging enabled)*

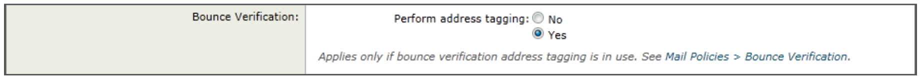
Step 4: In the Uncommitted Changes pane, enter a comment to describe the change, and then click **Commit Changes**.

Step 5: Navigate to **Mail Policies > Destination Controls.**

Step 6: Under Domain, in the first table, click **Default**.

Step 7: Under IP Address Preference, select **IPv4 Preferred**.

Step 8: Under Bounce Verification, change **Perform Address Tagging** to **Yes,** and then click **Submit.**



Bounce Verification:	Perform address tagging: ○ No ● Yes *Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.*

Step 9: Click **Commit Changes**.

Step 10: In the Uncommitted Changes pane, enter a comment to describe the change, and then click **Commit Changes**.

Procedure 3 Review incoming mail policies

The last stage in appliance setup is reviewing the incoming mail policies. Currently there is one default mail policy. It marks a positive anti-spam result for quarantine. You change this to instead take a Drop action.

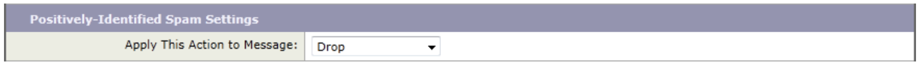
Step 1: Navigate to **Mail Policies > Incoming Mail Policies**.

Step 2: Under the Anti-Spam column header, select the policy definition.

Step 3: Change the Positively-Identified Spam Settings from **Spam Quarantine** to **Drop**, and then click **Submit**.

Step 4: Click **Commit Changes**.

Step 5: In the Uncommitted Changes pane, enter a comment to describe the change, and then click **Commit Changes**.



Positively-Identified Spam Settings

Apply This Action to Message: Drop

Procedure 4 Enable message tracking (optional)

Troubleshooting inbound and outbound email on Cisco ESA requires that you enable the Message Tracking Service. Once this service is enabled, you can search the message logs and view detailed tracking information for all email messages.

Tech Tip

This is an optional procedure, and may impact the performance of your Cisco ESA if left on permanently.

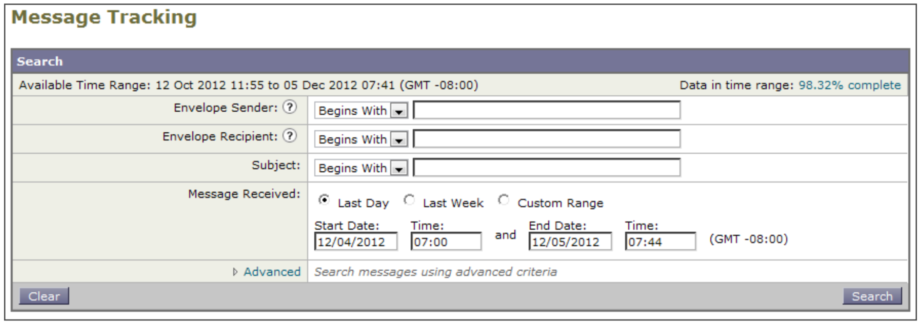
Step 1: Navigate to **Security Services > Message Tracking** , and then click **Edit Settings**.

Step 2: Select **Enable Message Tracking Service**, and then click **Submit**.

Step 3: Click **Commit Changes**.

Step 4: In the Uncommitted Changes pane, enter a comment to describe the change, and then click **Commit Changes**.

Step 5: Navigate to **Monitor > Message Tracking**. You can search for messages using any of the available fields. After enabling the Message Tracking Service, it may take a few minutes before logs are available for searching.



Message Tracking

Search

Available Time Range: 12 Oct 2012 11:55 to 05 Dec 2012 07:41 (GMT -08:00) Data in time range: 98.32% complete

Envelope Sender: Begins With

Envelope Recipient: Begins With

Subject: Begins With

Message Received: ● Last Day ○ Last Week ○ Custom Range

Start Date: 12/04/2012 Time: 07:00 and End Date: 12/05/2012 Time: 07:44 (GMT -08:00)

Advanced Search messages using advanced criteria

Summary

Cisco ESA has been configured for basic network access, and an anti-spam and anti-virus policy has been built and applied. DNS has been modified to support Cisco ESA, the appliance software was updated, and the feature keys for the appliance were installed. Some slight policy changes have been made, but a detailed policy discussion, troubleshooting, and ongoing monitoring are topics that can be pursued with a trusted Cisco partner or account team.

Appendix A: Product List

Email Security

Functional Area	Product Description	Part Numbers	Software
Email Security Appliance	Cisco Email Security Appliance C370	C370-BUN-R-NA	Async OS 7.6.1-022

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.0(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 ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)

Internet Edge LAN

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

Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We upgraded the Cisco ESA software to version 7.6.1.
- We updated configuration procedures to support outbound email.
- We modified the firewall policies and revised the procedures for creating network objects and access rules.
- We included an optional procedure to enable message tracking.

Notes

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.