Newer Cisco SBA Guides Available

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

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

SBA

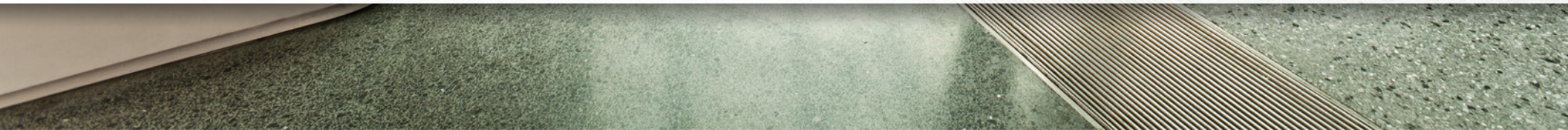
BORDERLESS NETWORKS

DEPLOYMENT GUIDE

Email Security Using ESA Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series



Preface

Who Should Read This Guide

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

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

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

Release Series

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

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

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

month year Series

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

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

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

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

How to Read Commands

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

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

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

```
Router# enable
```

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

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

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

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

Comments and Questions

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

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

Table of Contents

What's In This SBA Guide 1
- Cisco SBA Borderless Networks 1
- Route to Success 1
- About This Guide 1

Introduction 2
- Business Overview 2
- Technology Overview 2

Deployment Details 5
- Configuring DMZ for Email 5
- Configuring IronPort Email Security Appliance 13
- Enabling Mail Policies 17

Appendix A: Product List 19

Appendix B: Changes 20

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

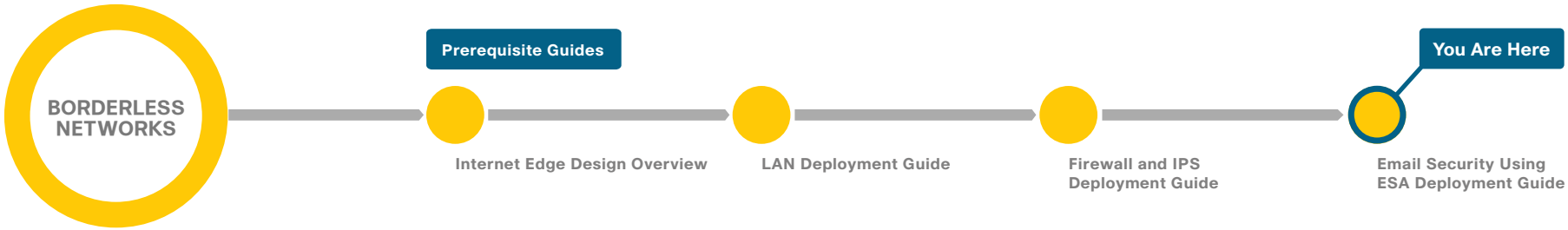
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **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



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 *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

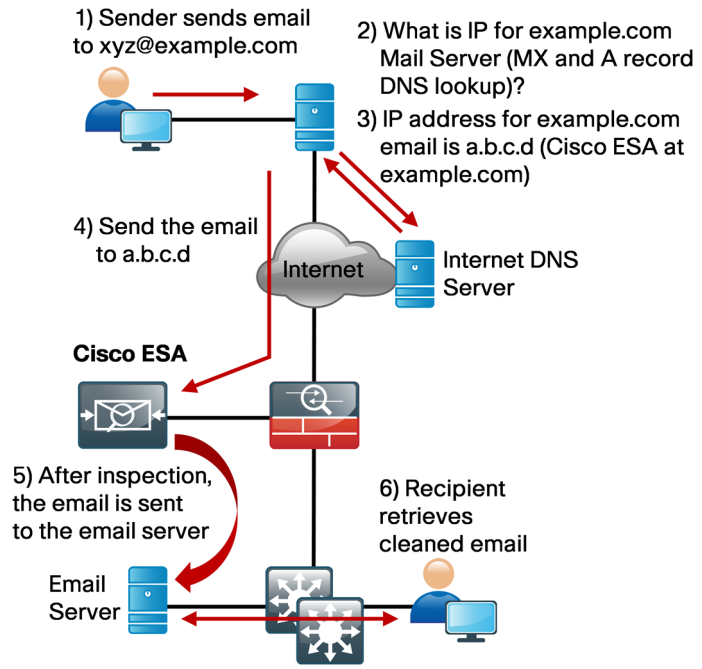
An email solution becomes unusable if junk email is not filtered properly. The sheer volume of junk messages can crowd out legitimate mail and cause employees to waste time manually filtering through messages. A side effect of some junk email-filtering solutions are false positives, or email that is 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 IronPort 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. IronPort 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 - Email message flow



Cisco IronPort 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. The Internet Edge design uses the single-interface model for simplicity.

Cisco IronPort 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.

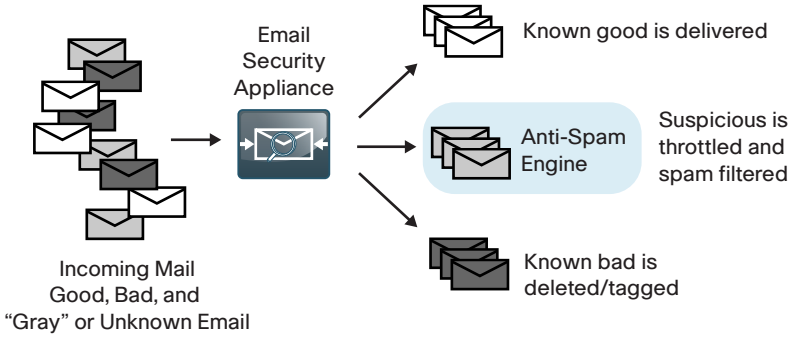
Reputation filters provide the first layer of defense by looking at the source IP address of the email server and comparing it to the reputation data downloaded from Cisco SenderBase. Cisco SenderBase is the world's largest repository for security data, including sources of spam, botnets, and other malicious hosts. When hosts on the Internet engage in malicious activity, SenderBase lowers the reputation of that host. Devices that use reputation filtering, like Cisco IronPort 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 2):

- If the sender's reputation is positive, the email gets forwarded on to the next layer of defense.
- If the sender's reputation is negative, the email is discarded.
- If the sender has neither a positive nor negative reputation, the email is considered suspicious and is quarantined, and must wait for inspection before being delivered.

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 2 - Email filtering overview



Fighting Viruses and Malware

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

- The first layer of defense consists of virus 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.

High Availability

The Cisco IronPort 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. You can achieve additional resiliency by adding a second IronPort ESA. You should configure the second IronPort ESA the same as the first IronPort ESA, and then add an additional MX record 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 appliance.

Monitoring

You can monitor the behavior of the Cisco IronPort 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 the Cisco IronPort 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 the Cisco IronPort ESA handled the message. This search capability is especially useful if some of the more advanced features of the IronPort ESA are used, such as data loss prevention (DLP).

Reader Tip

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

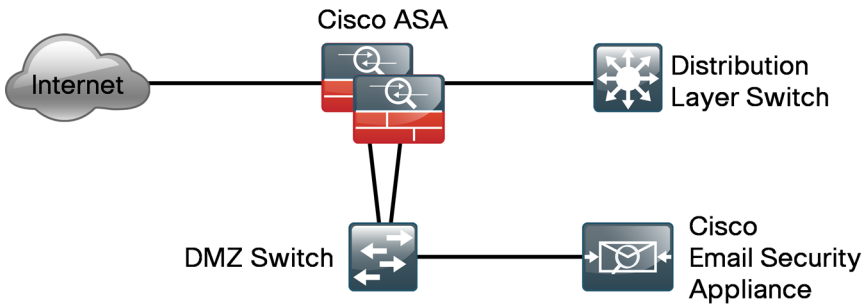
Notes

Deployment Details

Cisco IronPort 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 IronPort 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 3 - Deployment overview



It is important that Cisco IronPort ESA be accessible through the public Internet and that it is the first hop in the email infrastructure. Several of IronPort 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.

Process

Configuring DMZ for Email

1. Configure the DMZ switch
2. Configure the 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 has already been configured following the guidance in the *Firewall and IPS Deployment Guide*.

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

Procedure 1 Configure the DMZ switch

Step 1: Set the DMZ switch to be the spanning tree root for the VLAN that contains the email security appliance.

```
vlan 1117
 name mail-dmz
```

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

```
interface GigabitEthernet1/0/24
 description IE-ASA5540a Gig0/1
!
interface GigabitEthernet2/0/24
 description IE-ASA5540b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan add 1117
 switchport mode trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 no shutdown
```

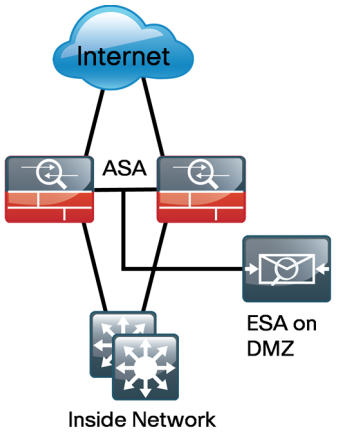
Step 3: Configure the interfaces that connect to the email security appliance.

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

Procedure 2 Configure the 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 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 4 - DMZ VLAN topology and services



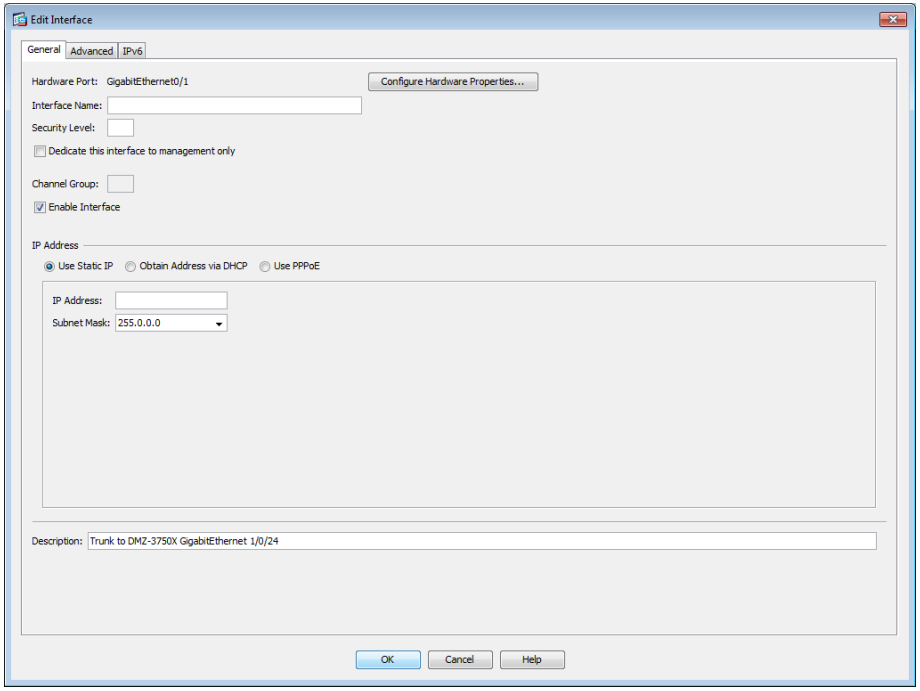
Tech Tip

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

Step 1: Using a browser, access the ASA's GUI. In **Configuration** > **Device Setup** > **Interfaces**, click the interface that is connected to the DMZ switch. (Example: GigabitEthernet0/1)

Step 2: Click **Edit**.

Step 3: In the Edit Interface dialog box, select **Enable Interface**, and then click **OK**.



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 configured in Step 1.(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)

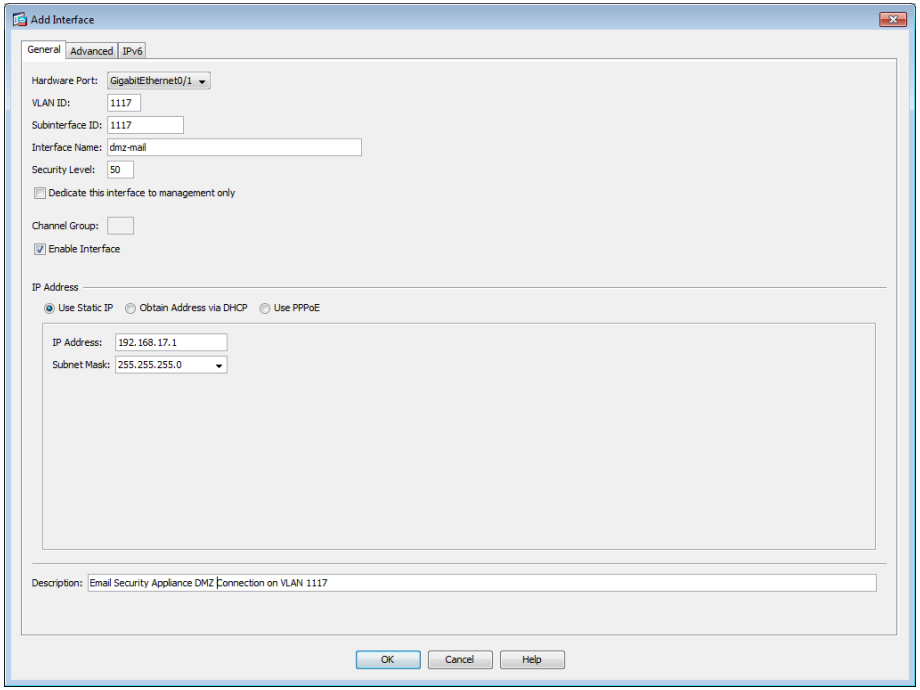
Step 8: Enter an **Interface Name**. (Example: dmz-email)

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

Step 10: Enter the interface **IP Address**. (Example: 192.168.17.1)

Step 11: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

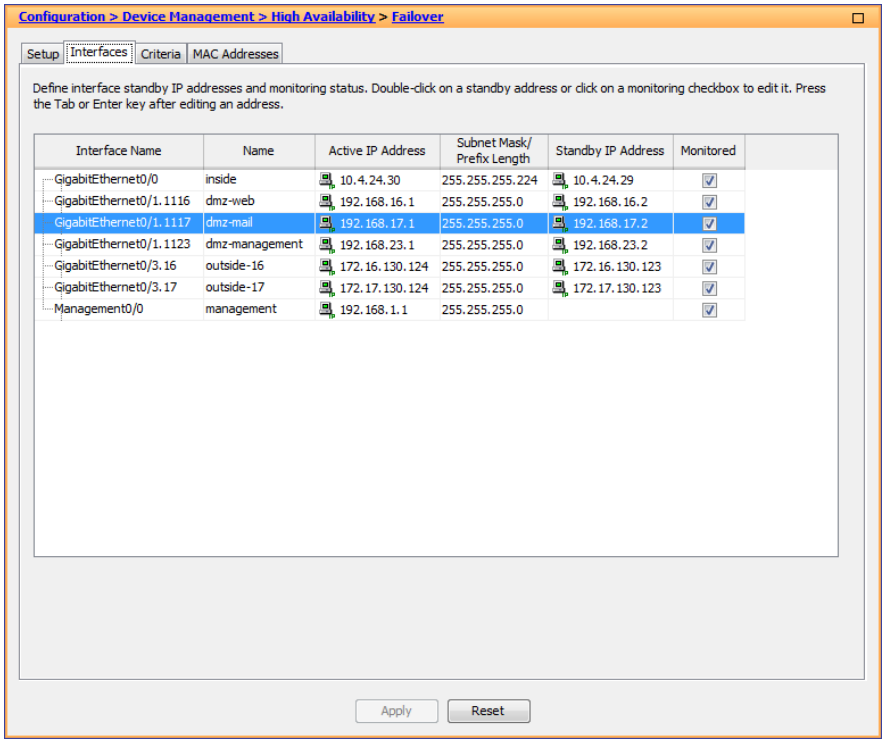
Step 12: On the Interface pane, click **Apply**.



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**.



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 IronPort 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 IronPort 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 IronPort ESA address mapping

IronPort ESA DMZ address	IronPort 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 IronPort ESA server on the primary Internet connection.

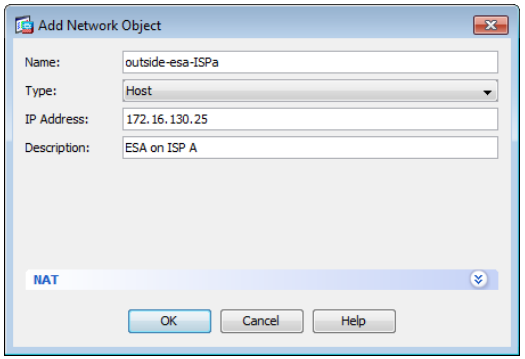
Step 2: Click **Add > Network Object**.

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

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

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

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



Next, you add a network object for the private DMZ address of Cisco IronPort 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 IronPort ESA's private DMZ IP address. (Example: dmz-esa-ISPa)

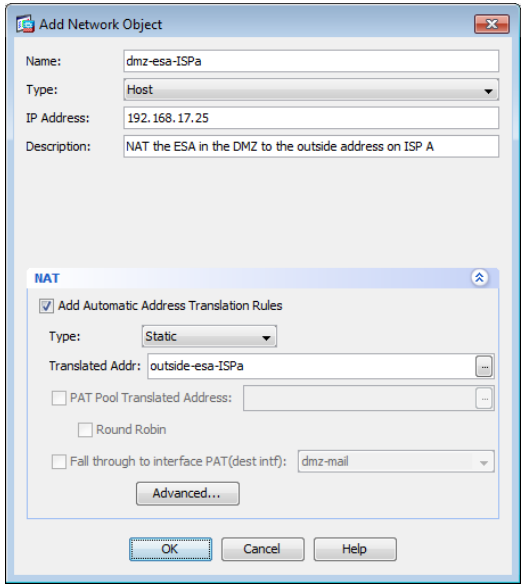
Step 9: In the Type list, select **Host**.

Step 10: In the IP Address box, enter the primary wireless LAN controller's private DMZ IP address. (Example: 192.168.17.25)

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

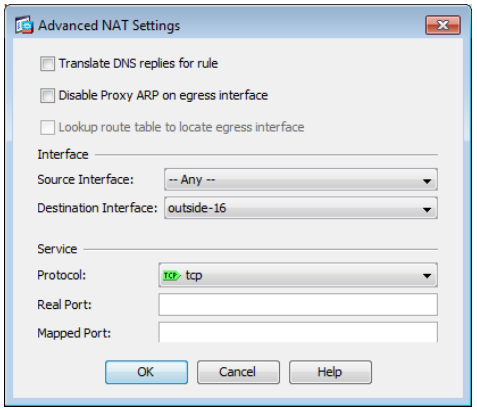
Step 12: Select **Add Automatic Address Translation Rules**.

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



Step 14: Click **Advanced**.

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



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 IronPort 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 IronPort 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 two network objects that summarize all the DMZ networks. All the DMZ networks deployed in Cisco SBA can be summarized as 192.168.16.0/21.

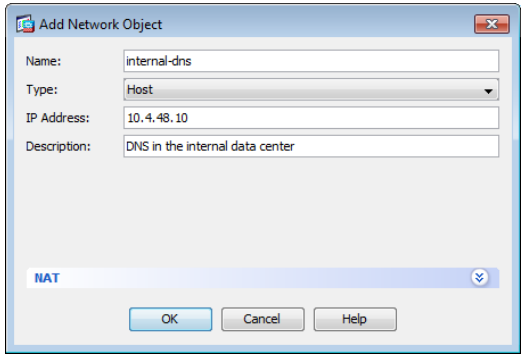
Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

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

Step 3: On the Add Network Object dialog box, in the **Name box**, enter a description. (Example: internal-dns)

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

Step 5: In the IP Address box, enter the address of the internal DNS, and then click **OK**. (Example: 10.4.48.10)

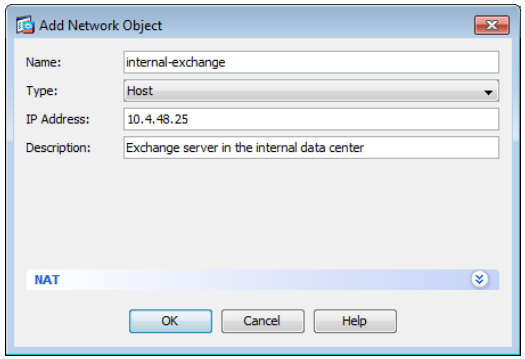


Step 6: Click **Add** > **Network Object**.

Step 7: On the Add Network Object dialog box, in the **Name box**, enter a description. (Example: internal-exchange)

Step 8: In the Type list, select **Host**.

Step 9: In the IP Address box, enter the address of the internal Microsoft Exchange server, and then click **OK**. (Example: 10.4.48.25)

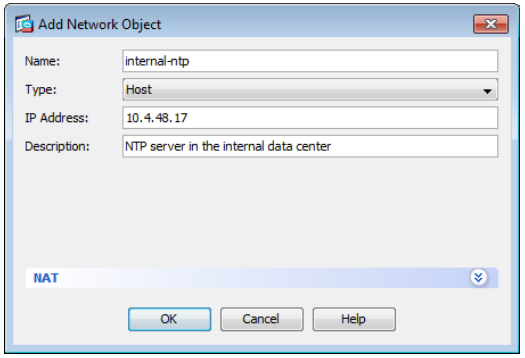


Step 10: Click **Add** > **Network Object**.

Step 11: On the Add Network Object dialog box, in the Name box, enter a description. (Example: internal-ntp)

Step 12: In the Type list, select **Host**.

Step 13: In the IP Address box, enter the address of the internal NTP server, and then click **OK**. (Example: 10.4.48.17)



Step 14: On the Network Objects/Groups pane, click **Apply**.

Step 15: Navigate to **Configuration** > **Firewall** > **Access Rules**.

Step 16: Click the rule that denies traffic from the DMZ toward the internal network.

Next, insert a new rule above the rule you selected that permits Cisco IronPort ESA to receive email.

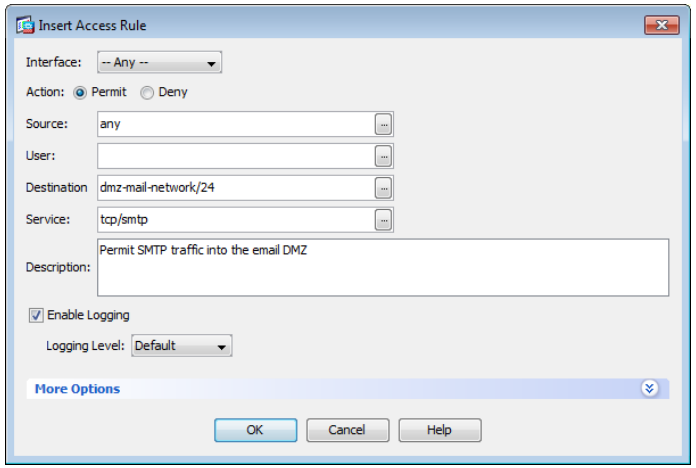
Step 17: Click **Add** > **Insert**.

Step 18: In the Add Access Rule dialog box, in the **Interface** list, select **—Any—**.

Step 19: For Action, select **Permit**.

Step 20: In the Destination list, select the network object automatically created for the email DMZ. (Example: dmz-mail-network/24)

Step 21: In the Service list, enter **tcp/smtp**, and then click **OK**.



Next, insert a new rule above the rule you selected that permits Cisco IronPort ESA to transfer email to the internal email server.

Step 22: Click **Add** > **Insert**.

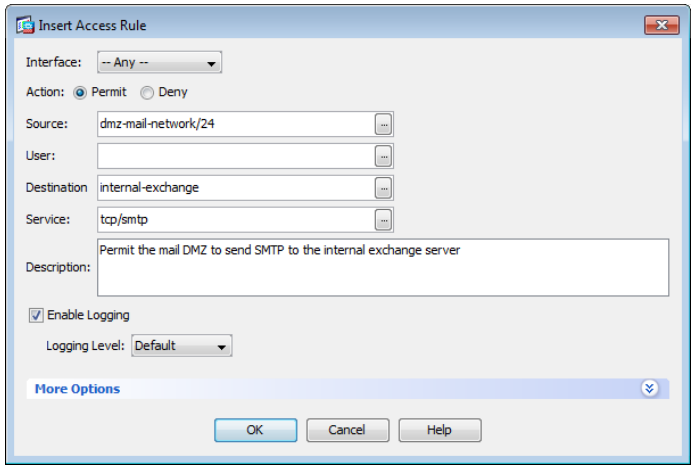
Step 23: In the Insert Access Rule dialog box, in the **Interface** list, select **—Any—**.

Step 24: For Action, select **Permit**.

Step 25: In the Source list, select the network object automatically created for the email DMZ. (Example: dmz-email-network/24)

Step 26: In the Destination list, select the internal Microsoft Exchange server network object. (Example: internal-exchange)

Step 27: In the Service list, enter **tcp/smtp**, and then click **OK**.



Next, insert a new rule above the rule you selected the permits the ESA to perform domain lookups on the internal DNS.

Step 28: Click **Add** > **Insert**.

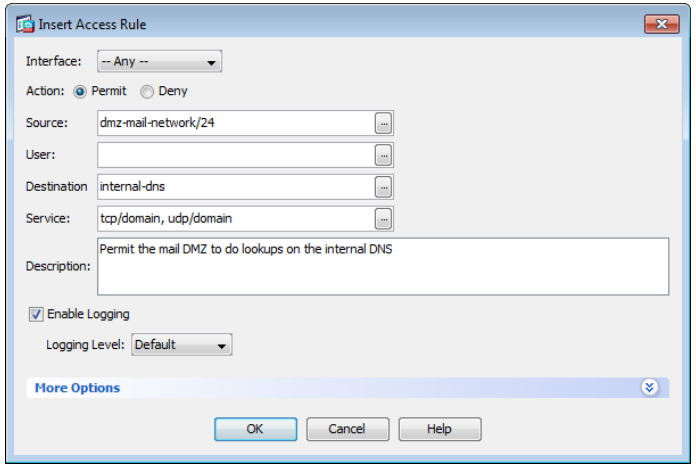
Step 29: In the Insert Access Rule dialog box, in the **Interface** list, select **—Any—**.

Step 30: For Action, select **Permit**.

Step 31: In the Source list, select the network object automatically created for the email DMZ. (Example: dmz-email-network/24)

Step 32: In the Destination list, select the internal DNS server network object. (Example: internal-dns)

Step 33: In the Service list, enter **tcp/domin, udp/domain**, and then click **OK**.



Next, insert a new rule above the rule you selected that permits Cisco IronPort ESA to update its clock using the internal NTP server.

Step 34: Click **Add > Insert**.

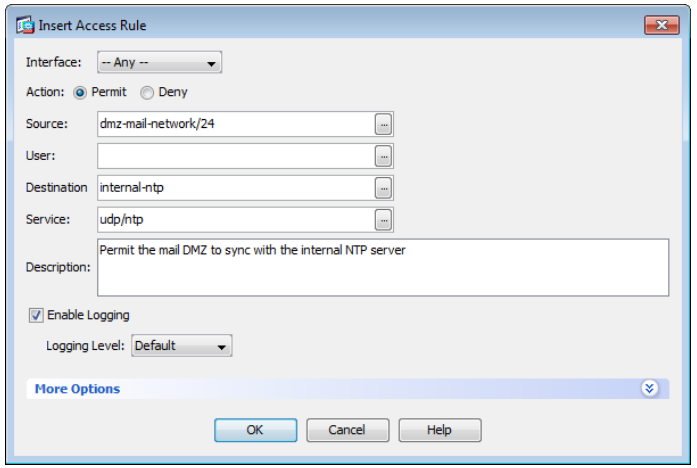
Step 35: In the Insert Access Rule dialog box, in the **Interface** list, select **—Any—**.

Step 36: For Action, select **Permit**.

Step 37: In the Source list, select the network object automatically created for the email DMZ. (Example: dmz-email-network/24)

Step 38: In the Destination list, select the internal NTP server network object. (Example: internal-ntp)

Step 39: In the Service list, enter **udp/ntp**, and then click **OK**.



Next, insert a new rule above the rule you selected that permits Cisco IronPort ESA to update its software and feature keys.

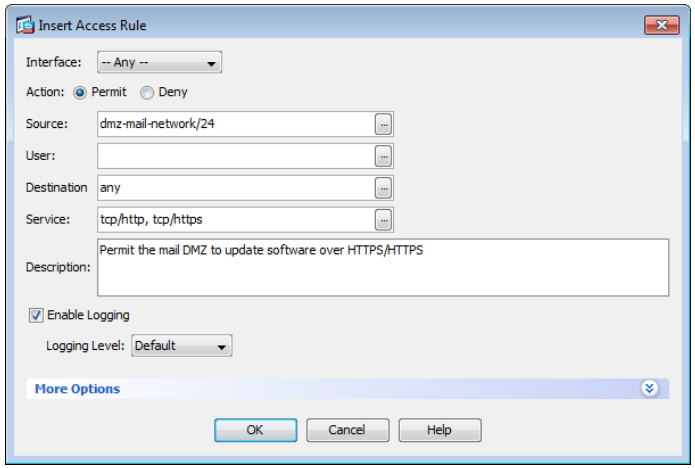
Step 40: Click **Add > Insert**.

Step 41: In the Add Access Rule dialog box, in the **Interface** list, select **—Any—**.

Step 42: For Action, select **Permit**.

Step 43: In the Source list, select the network object automatically created for the email DMZ. (Example: dmz-mail-network/24)

Step 44: In the Service list, enter tcp/http, tcp/https, and then click OK.



Step 45: In the Access Rules window, click Apply.

Process

Configuring IronPort Email Security Appliance

1. Deploy IronPort ESA
2. Complete the GUI-based system setup
3. Install system updates and feature keys

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

The Cisco IronPort ESA host name is the name carried in the DNS MX record and indicates that IronPort ESA is the primary MTA. The DNS A record corresponds to the IP address that Cisco Adaptive Security Appliance (ASA) is statically translating to the appliance's address in the DMZ.

Procedure 1 Deploy IronPort 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-mail

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

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

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

Hostname:
[ironport.example.com]> DMZ-ESA.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 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-mail 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-mail".
Currently configured interfaces:
1. dmz-mail (192.168.17.25/24 on Management: DMZ-ESA.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

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

```
ironport.example.com> commit

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

Changes committed
```

Cisco IronPort ESA is now configured.

Step 3: 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 2 Complete the GUI-based system setup

Step 1: From a client on the internal network, navigate and log in to the appliance. (Example: https://DMZ-ESA.cisco.local/)

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 **D**efault System Hostname box, enter the appliance hostname. (Example: DMZ-ESA.cisco.local)

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

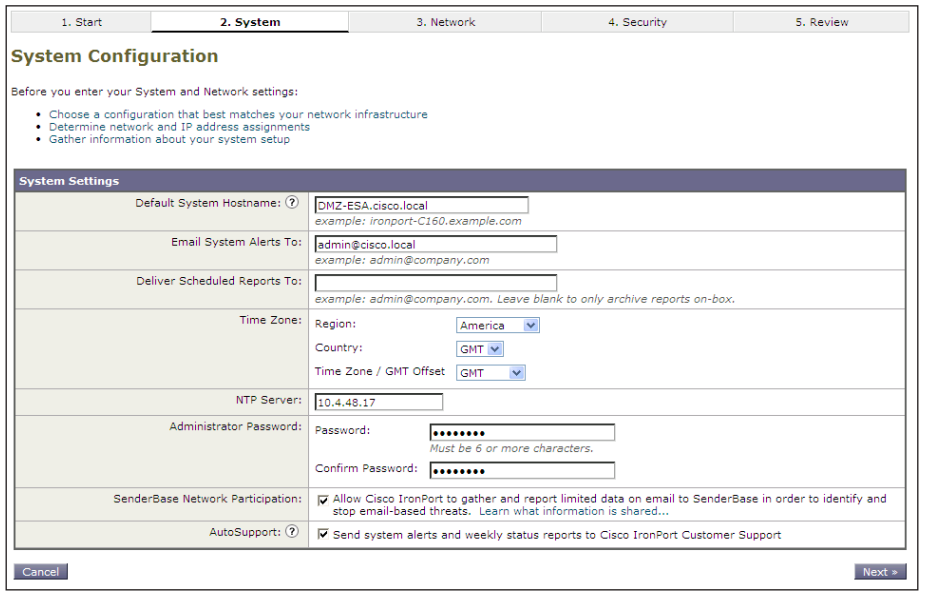
Step 6: Set the appropriate time zone for the appliance.

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 check boxes determine whether Cisco IronPort ESA participates in the Cisco SenderBase network. This allows IronPort ESA to send anonymized reputation details about email traffic to Cisco in order to improve SenderBase and the product in general.



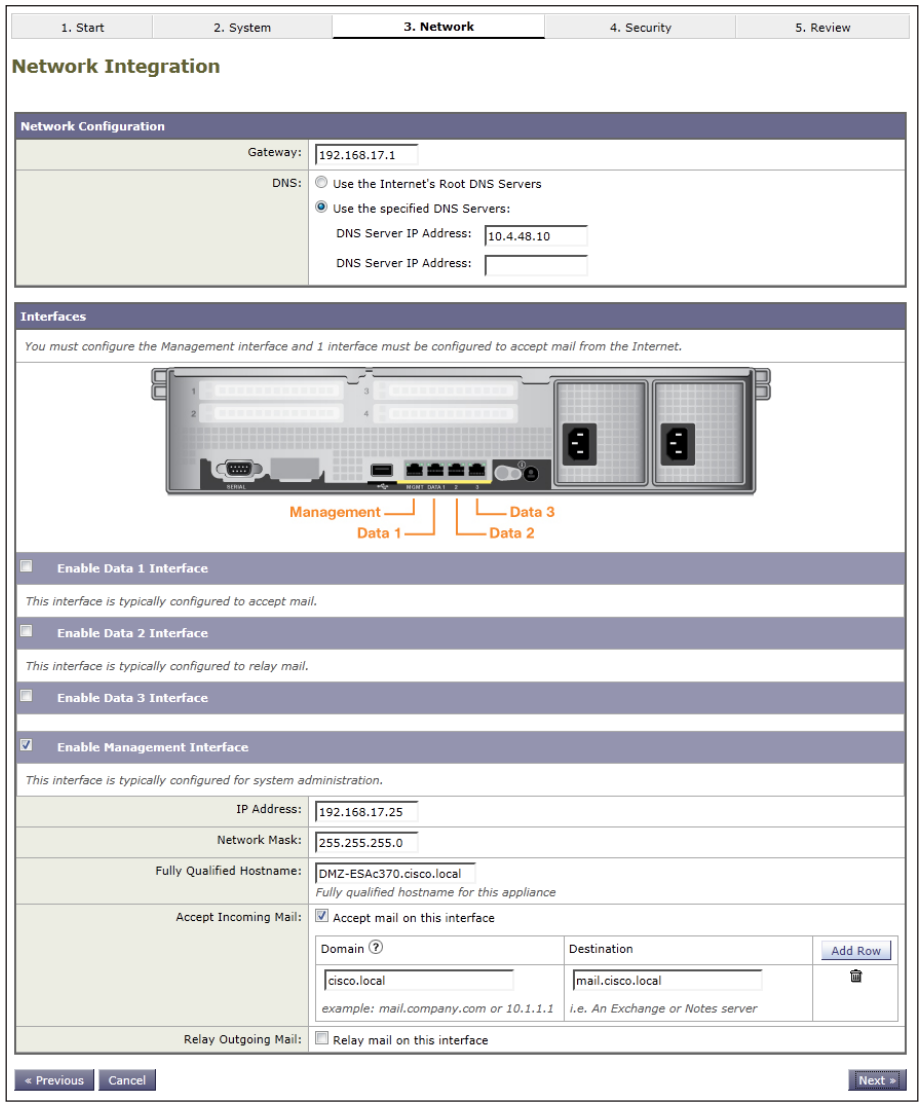
Step 9: On the Network tab, choose **Use the specified DNS Servers.**

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

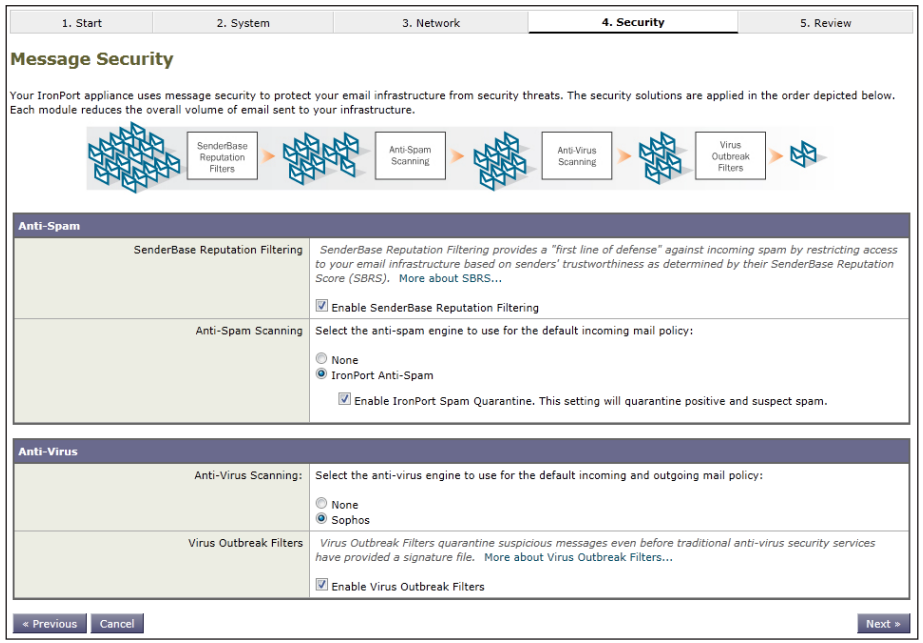
Step 11: Select **Accept mail on this interface**.

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, and then click **Next**. (Example mail.cisco.local)



Step 14: On the Security tab, ensure anti-spam and anti-virus filtering are enabled, and then click **Next**.



Step 15: On the Review tab, review the configuration, and then click **Install this Configuration**. Cisco IronPort ESA installs the configuration.

Step 16: When the Active Directory wizard appears, click **Cancel**. In this example, you do not configure an Active Directory server.

Procedure 3 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 Updates**. 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.

Process

Enabling Mail Policies

1. Set up Bounce Verification
2. Review incoming mail policies

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

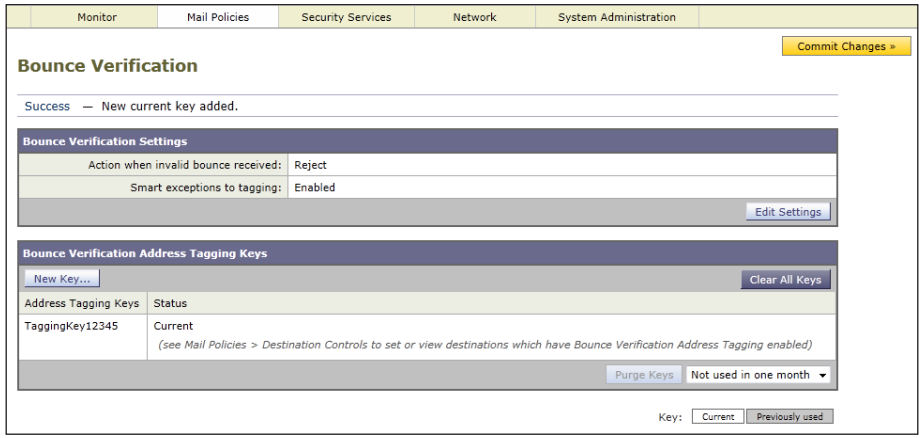
Procedure 1 Set up Bounce Verification

One of the last steps of setting up a standard configuration for Cisco IronPort ESA is setting up Bounce Verifications. Bounce Verification is a process that allows IronPort 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 IronPort ESA. Spammers and hackers use fake bounced messages for many malicious purposes.

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

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

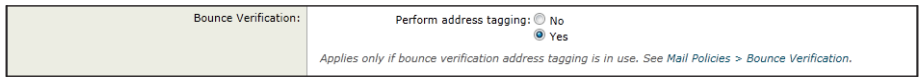
Step 3: Click **Commit Changes**.



Step 4: Navigate to **Mail Policies > Destination Controls.**

Step 5: Under Domain, in the first table, click **Default**.

Step 6: Under Bounce Verification, change **Perform Address Tagging** to **Yes,** and then click **Submit.**



Step 7: Click **Commit Changes**.

Procedure 2 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**.

Summary

Cisco IronPort 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 IronPort 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 IronPort Email Security Appliance C370	C370-BUN-R-NA	Async OS 7.6.0-444

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 8.6(1)1, IPS 7.1(4) E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	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	6.6.114

Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 3750-X Series Stackable 24 10/100/1000 Ethernet ports	WS-C3750X-24T-S	15.0(1)SE2 IP Base

Appendix B: Changes

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

- We upgraded Cisco IronPort ESA software to version 7.6.0.
- We made minor changes to improve the readability of this guide.

Notes

Feedback

Click here to provide feedback to Cisco SBA.

SMART BUSINESS ARCHITECTURE

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

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

© 2012 Cisco Systems, Inc. All rights reserved.

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.

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

B-0000170-1 8/12