# Table of Contents

Preface ................................................................................................................................. 1

CVD Navigator .......................................................................................................................... 2
  Use Cases ............................................................................................................................... 2
  Scope .................................................................................................................................. 2
  Proficiency ......................................................................................................................... 2

Introduction ............................................................................................................................ 3
  Technology Use Case .......................................................................................................... 3
    Use Case: Inbound Mail Filtering ..................................................................................... 3
  Design Overview ................................................................................................................. 3
  Filtering Spam ...................................................................................................................... 5
  Fighting Viruses and Malware ............................................................................................ 6
  High Availability .................................................................................................................. 6
  Monitoring .......................................................................................................................... 6
  Troubleshooting .................................................................................................................. 6

Deployment Details ................................................................................................................. 7
  Configuring Email DMZ ...................................................................................................... 8
  Configuring Cisco Email Security Appliance ................................................................. 19
  Enabling Mail Policies ....................................................................................................... 27
  Summary ............................................................................................................................ 30

Appendix A: Product List ....................................................................................................... 31

Appendix B: Changes ............................................................................................................. 33
Cisco Validated Designs (CVDs) present systems that are based on common use cases or engineering priorities. CVDs incorporate a broad set of technologies, features, and applications that address customer needs. Cisco engineers have comprehensively tested and documented each design in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested design details:

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

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

**CVD Foundation Series**

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

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

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

**Comments and Questions**

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

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

Use Cases

This guide addresses the following technology use cases:

- **Inbound Mail Filtering**—Inbound mail filtering helps prevent spam and malicious email from being delivered to users.

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

Scope

This guide covers the following areas of technology and products:

- Cisco Email Security Appliance
- Internet edge firewalls and demilitarized zone (DMZ) switching

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

Proficiency

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

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

To view the related CVD guides, click the titles or visit the CVD Foundation web site.
Technology Use Case

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 and targeted or directed attacks. Embedded attacks include viruses and malware that perform actions on the end device when clicked. Targeted or directed attacks, such as phishing attacks, 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.

Use Case: Inbound Mail Filtering

Inbound mail filtering helps prevent spam and malicious email from being delivered to users.

This design guide enables the following capabilities:

- Preventing unsolicited email from being delivered to the mail system, thereby reducing the flood of spam.
- Preventing malicious email from being delivered to the mail system (Malicious email is quarantined to allow it to be further evaluated.)
- Tracking and providing reports on email that was filtered.

Design 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.

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)
4. Email is sent
5. After inspection, the email is sent to the central email server
6. Employee retrieves cleaned email

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**

1. Employee sends email to xyz@companyY.com
2. Central email server forwards all non-local messages to Cisco ESA smart host
3. Cisco ESA performs DNS lookup for recipient domain and retrieves MX and A records
4. Cisco ESA inspects outbound email
5. Email is sent
6. Recipient retrieves email
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/services/acquisitions/ironport.html
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 design guide, the appliance is physically deployed on the demilitarized zone (DMZ) of the Internet Edge, and uses a single interface for simplicity. This interface handles all incoming and outgoing email and carries management traffic. The port is the management interface, labeled “M1” on the appliance.

**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.

### Configuring Email DMZ

1. Configure the DMZ switch connection to the firewall
2. Configure the DMZ switch connection to the ESA
3. Configure the firewall’s mail DMZ interface
4. Configure Network Address Translation
5. Configure security policy

The enterprise 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 Firewall and IPS Design Guide and the Campus Wired LAN Technology Design 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 connection to the firewall

**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.

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

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

```bash
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport trunk allowed vlan add 1117
```
**Procedure 2** Configure the DMZ switch connection to the ESA

**Option 1: Virtual ESA on a server in the DMZ**

**Step 1:** Configure the interface(s) that connect to the virtual email security server as follows:

```plaintext
interface GigabitEthernet1/0/21
    description IE-C220M3-1 (vmnic4)
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 1116,1117
    switchport mode trunk
    logging event trunk-status
    srr-queue bandwidth share 1 30 35 5
    priority-queue out
    mls qos trust dscp
    macro description EgressQoS
    spanning-tree portfast trunk
    no shutdown

interface GigabitEthernet1/0/22
    description IE-C220M3-2 (vmnic4)
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 1116,1117
    switchport mode trunk
    logging event trunk-status
    mls qos trust dscp
    macro description EgressQoS
    spanning-tree portfast trunk
    no shutdown
```

**Option 2: Physical ESA as a stand-alone appliance in the DMZ**

**Step 1:** If the interface is connecting to an ESA appliance, the following is the configuration:

```plaintext
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 3** Configure the firewall’s mail DMZ interface

The DMZ network is connected to 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**.

![Edit Interface dialog box](image)

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 Email VLAN. (Example: 1117)

Step 7: In the **Subinterface ID** box, enter the VLAN number for the DMZ Email 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**.

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

Step 13: Navigate to **Configuration > Device Management > High Availability and Scalability > 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 4 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>
<thead>
<tr>
<th>Cisco ESA DMZ address</th>
<th>Cisco ESA public address (externally routable after NAT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.17.25</td>
<td>172.16.130.25 (ISP-A)</td>
</tr>
<tr>
<td></td>
<td>172.17.130.25 (ISP-B)</td>
</tr>
</tbody>
</table>

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**.

![Add Network Object](image)

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-esa-c100v-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.

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)

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 (a connection to each of two different ISPs), repeat this entire procedure for the second Internet connection (ISP B).
Procedure 5  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, to simplify the configuration of the security policy, you create the network objects that are used in the firewall policies.

Table 2 - Firewall network objects

<table>
<thead>
<tr>
<th>Network object name</th>
<th>Object type</th>
<th>IP address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal-dns</td>
<td>Host</td>
<td>10.4.48.10</td>
<td>DNS server</td>
</tr>
<tr>
<td>internal-exchange</td>
<td>Host</td>
<td>10.4.48.25</td>
<td>Exchange server</td>
</tr>
<tr>
<td>internal-ntp</td>
<td>Host</td>
<td>10.4.48.17</td>
<td>NTP server</td>
</tr>
<tr>
<td>internal-network</td>
<td>Network</td>
<td>10.4.0.0/15</td>
<td>Internal network</td>
</tr>
</tbody>
</table>

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

Step 2: Repeat Step 3 through Step 7 for each object 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: In the Name box, enter the object name. (Example: internal-dns)

Step 5: In the Type list, choose Host or Network. Example: Host)

Step 6: In the IP Address box, enter the address. (Example: 10.4.48.10)

Step 7: In the Description box, enter a useful description, and then click OK. (Example: DNS server)

Step 8: After adding all of the objects listed in Table 2, on the Network Objects/Groups pane, click Apply.
Step 9: Navigate to Configuration > Firewall > Access Rules.

Table 3 - Firewall policy rules for ESA

<table>
<thead>
<tr>
<th>Interface</th>
<th>Action</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Description</th>
<th>Logging Enable / Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Permit</td>
<td>internal-exchange</td>
<td>dmz-email-network</td>
<td>tcp/smtp</td>
<td>Exchange to ESA outbound SMTP</td>
<td>Selected / Default</td>
</tr>
<tr>
<td>Any</td>
<td>Deny</td>
<td>internal-network</td>
<td>any4</td>
<td>tcp/smtp</td>
<td>Block other outbound SMTP</td>
<td>Selected / Default</td>
</tr>
<tr>
<td>Any</td>
<td>Permit</td>
<td>any4</td>
<td>dmz-email-network</td>
<td>tcp/smtp</td>
<td>Internet to ESA inbound SMTP</td>
<td>Selected / Default</td>
</tr>
<tr>
<td>Any</td>
<td>Permit</td>
<td>dmz-email-network</td>
<td>internal-exchange</td>
<td>tcp/smtp</td>
<td>ESA to Exchange inbound SMTP</td>
<td>Selected / Default</td>
</tr>
<tr>
<td>Any</td>
<td>Permit</td>
<td>dmz-email-network</td>
<td>internal-dns</td>
<td>udp/domain</td>
<td>DNS</td>
<td>Selected / Default</td>
</tr>
<tr>
<td>Any</td>
<td>Permit</td>
<td>dmz-email-network</td>
<td>internal-ntp</td>
<td>udp/ntp</td>
<td>NTP</td>
<td>Selected / Default</td>
</tr>
<tr>
<td>Any</td>
<td>Deny</td>
<td>dmz-email-network</td>
<td>internal-network</td>
<td>ip</td>
<td>Block other to internal networks</td>
<td>Selected / Default</td>
</tr>
<tr>
<td>Any</td>
<td>Permit</td>
<td>dmz-email-network</td>
<td>any4</td>
<td>tcp/smtp</td>
<td>ESA to Internet outbound SMTP</td>
<td>Selected / Default</td>
</tr>
<tr>
<td>Any</td>
<td>Permit</td>
<td>dmz-email-network</td>
<td>any4</td>
<td>tcp/http</td>
<td>HTTP to Internet</td>
<td>Selected / Default</td>
</tr>
<tr>
<td>Any</td>
<td>Permit</td>
<td>dmz-email-network</td>
<td>any4</td>
<td>tcp/https</td>
<td>HTTPS to Internet</td>
<td>Selected / Default</td>
</tr>
</tbody>
</table>

Step 10: Repeat Step 11 through Step 20 for all rules listed in Table 3.

Step 11: Click the rule that denies traffic from the DMZ toward the internal network.

Tech Tip

Be sure to perform this step for every rule listed in Table 3. Inserting the rules above the DMZ-to-any rule keeps the added rules in the same order as listed, which is essential for the proper execution of the security policy.

Step 12: Click Add > Insert.

The Add Access Rule dialog box appears.

Step 13: In the Interface list, choose the interface. (Example: Any)

Step 14: For the Action option, select the action. (Example: Permit)

Step 15: In the Source box, choose the source. (Example: internal-exchange)

Step 16: In the Destination box, choose the destination. (Example: dmz-email-network)

Step 17: In the Service box, enter the service. (Example: tcp/smtp)
**Step 18:** In the **Description** box, enter a useful description. (Example: Exchange to ESA outbound SMTP)

**Step 19:** Select or clear **Enable Logging**. (Example: Selected)

**Step 20:** In the **Logging Level** list, choose the logging level value, and then click **OK**. (Example: Default)

![Add Access Rule](image)

**Step 21:** After adding all of the rules in Table 3, in the order listed, click **Apply** on the Access Rules pane.
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)**

<table>
<thead>
<tr>
<th>FQDN</th>
<th>Outside IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal-exchange.cisco.local</td>
<td>10.4.48.25</td>
</tr>
<tr>
<td>mail.cisco.local</td>
<td>192.168.17.25</td>
</tr>
</tbody>
</table>

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)**

<table>
<thead>
<tr>
<th>ISP</th>
<th>FQDN</th>
<th>Outside IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>mail-a.cisco.local</td>
<td>172.16.130.25</td>
</tr>
<tr>
<td>Secondary</td>
<td>mail-b.cisco.local</td>
<td>172.17.130.25</td>
</tr>
</tbody>
</table>

**Table 6 - Example MX records (External DNS)**

<table>
<thead>
<tr>
<th>ISP</th>
<th>FQDN</th>
<th>Mail server</th>
<th>Mail server priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>cisco.local</td>
<td>mail-a.cisco.local</td>
<td>10</td>
</tr>
<tr>
<td>Secondary</td>
<td>cisco.local</td>
<td>mail-b.cisco.local</td>
<td>20</td>
</tr>
</tbody>
</table>
Procedure 2  Connect to the Cisco ESA

Option 1: Connecting to a virtual Cisco ESA deployed on VMware ESXi

Step 1: Using vSphere, right click on the server name of the vESA and select “Open Console”

Tech Tip

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

Option 2: Connecting to a stand-alone Cisco ESA appliance

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.

Procedure 3  Deploy Cisco ESA

Tech Tip

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

Step 1: Run interfaceconfig and setgateway, which change the basic network settings, and then issue the commit command, which saves the changes to the running configuration.

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:
[1]> EDIT

Enter the number of the interface you wish to edit.
[1]> 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 "0xffffffff00"):
[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-ESA-c100v.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**
Do you want to enable RSA Enterprise Manager Integration on this interface? [N]> **n**
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-ESA-c100v.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.
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 4** 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 hostname. (Example: DMZ-ESA-c100v.cisco.local)

**Step 5:** In the Email System Alerts To box and the Deliver Scheduled Reports To box, enter the administrator 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.
On the Network tab, verify the IPv4 gateway is correct and proceed to choose **Use the specified DNS Servers** radio button.

**Step 9:** In the **DNS Server IP Address** box, enter the internal DNS. (Example: 10.4.48.10)

**Step 10:** Within the Enable Management Interface box select: **Accept mail on this interface**.

**Step 11:** In the **Domain** box, enter the organization’s email domain. (Example: cisco.local)

**Step 12:** In the **Destination** box, enter the internal email server. (Example internal-exchange.cisco.local)

**Step 13:** Also on the Management Interface select **Relay mail on this interface**.
Step 14: In the Mail Server box, enter the internal email server, and then click Next. (Example internal-exchange.cisco.local)

Step 15: On the Security tab, ensure anti-spam and anti-virus filtering are enabled, and then click Next.

Step 16: On the Review tab, review the configuration, and then click Install this Configuration.

Step 17: On the Confirm Install window, accept the warning by clicking Install. Cisco ESA installs the configuration.
Step 18: When the Active Directory wizard appears, click Cancel. In this example, you do not configure an Active Directory server.

**Procedure 5** 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 Upgrade Options. 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.
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.
Step 3: Click Commit Changes.

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.

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

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.

**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 Enable.

**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.

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.
## Email Security

In the following table, to determine the part number for a Cisco Email Security Premium Subscription license, use the values that you need for the term and quantity components of the part number. For example, if you need a license with a 1-year term for 5300 users, the part number would be ESA-ESP-1Y-S8.

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Security Appliance</td>
<td>Cisco Email Security Appliance C370</td>
<td>C370-BUN-R-NA</td>
<td>Async OS 8.5.5-280</td>
</tr>
<tr>
<td>Email Security Virtual Appliance</td>
<td>Cisco Email Security Premium Subscription License</td>
<td>ESA-ESP-[term]-[quantity]</td>
<td>Async OS 8.5.5-280</td>
</tr>
<tr>
<td></td>
<td>Term Based Subscription License – 1 year</td>
<td>term = 1Y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Term Based Subscription License – 3 year</td>
<td>term = 3Y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Term Based Subscription License – 5 year</td>
<td>term = 5Y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S1 (100–199 Users)</td>
<td>quantity = S1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S2 (200–499 Users)</td>
<td>quantity = S2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S3 (500–999 Users)</td>
<td>quantity = S3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S4 (1000–1999 Users)</td>
<td>quantity = S4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S5 (2000–2999 Users)</td>
<td>quantity = S5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S6 (3000–3999 Users)</td>
<td>quantity = S6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S7 (4000–4999 Users)</td>
<td>quantity = S7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S8 (5000–9999 Users)</td>
<td>quantity = S8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S9 (10,000–19,999 Users)</td>
<td>quantity = S9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S10 (20,000–49,999 Users)</td>
<td>quantity = S10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S11 (50,000–99,999 Users)</td>
<td>quantity = S11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S12 (100,000–249,999 Users)</td>
<td>quantity = S12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S13 (250,000–499,999 Users)</td>
<td>quantity = S13</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S14 (500,000–999,999 Users)</td>
<td>quantity = S14</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantity Based Subscription License – User Band S15 (More than 1,000,000 Users)</td>
<td>quantity = S15</td>
<td></td>
</tr>
</tbody>
</table>
### Internet Edge

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Cisco ASA 5545-X IPS Edition - security appliance</td>
<td>ASA5545-IPS-K9</td>
<td>ASA 9.1(5) IPS 7.1(8p2)E4</td>
</tr>
<tr>
<td></td>
<td>Cisco ASA 5525-X IPS Edition - security appliance</td>
<td>ASA5525-IPS-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASA 5515-X IPS Edition - security appliance</td>
<td>ASA5515-IPS-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASA 5512-X IPS Edition - security appliance</td>
<td>ASA5512-IPS-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASA 5512-X Security Plus license</td>
<td>ASA5512-SEC-PL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firewall Management</td>
<td>ASDM</td>
<td>7.1(6)</td>
</tr>
</tbody>
</table>

### Internet Edge LAN

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMZ Switch</td>
<td>Cisco Catalyst 2960-X Series 24 10/100/1000 PoE and 2 SFP+ Uplink</td>
<td>WS-C2960X-24PS</td>
<td>15.0(2)EX5 LAN Base feature set</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 2960-X FlexStack-Plus Hot-Swappable Stacking Module</td>
<td>C2960X-STACK</td>
<td></td>
</tr>
</tbody>
</table>
Appendix B: Changes

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

- We added the deployment of Cisco ESA as a virtual appliance within the DMZ.
- We upgraded the Cisco ESA Code to 8.5.5-280
- We improved usability of procedures for configuring firewall policy rules
ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, “DESIGNS”) IN THIS MANUAL ARE PRESENTED “AS IS,” WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

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

© 2014 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. 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)