Email Security Deployment Guide

SBA FOR GOVERNMENT

Revision: H2CY10

Who Should Read This Guide

This guide is intended for the reader with any or all of the following:

- 100–1000 connected employees
- Up to 20 branches with approximately 25 employees each
- Email services that are hosted either locally or co-located
- CCNA® certification or equivalent experience

The reader may be looking for any or all of the following:

- To understand the benefits of deploying email security
- To understand more about the Cisco Email Security solution
- To learn the benefits of Cisco® Email Security
- To deploy email filtering
- To filter email for spam
- To filter email for viruses
- To reduce cost by optimizing email bandwidth and improve employee productivity
- To gain the assurance of a tested solution

Related Documents

Before reading this guide

BN — Foundation Design Overview

BN — Foundation Deployment Guide

BN — Foundation Configuration Files Guide

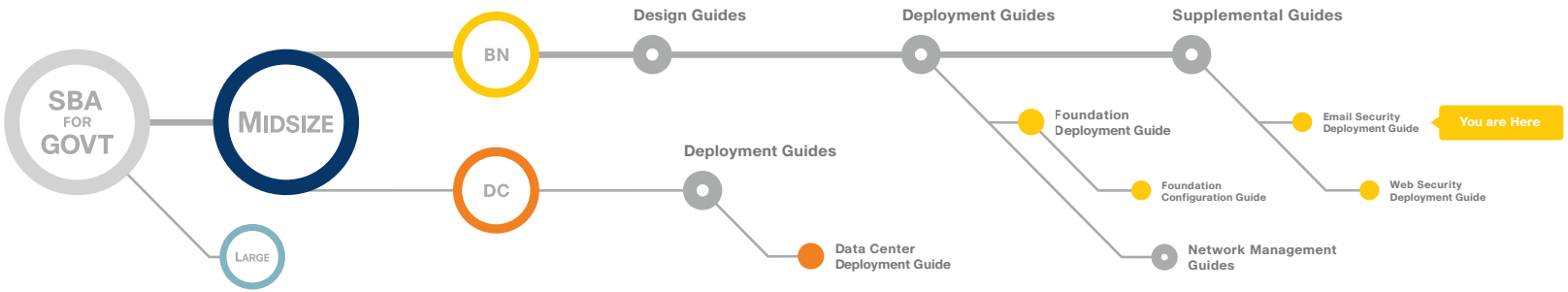


Table of Contents

Architectural Overview

The Cisco® Smart Business Architecture (SBA) for Government is a comprehensive design for networks with up to 1000 users. This out-of-the-box design is simple, fast, affordable, scalable, and flexible.

The Cisco SBA for Midsize Agencies incorporates LAN, WAN, wireless, security, WAN optimization, and unified communication technologies tested together as a solution. This solution-level approach simplifies the system integration normally associated with multiple technologies, allowing you to select the modules that solve your agency's problems rather than worrying about the technical details.

We have designed the Cisco SBA to be easy to configure, deploy, and manage. This architecture:

- Provides a solid network foundation
- Makes deployment fast and easy
- Accelerates ability to easily deploy additional services
- Avoids the need for re-engineering of the core network

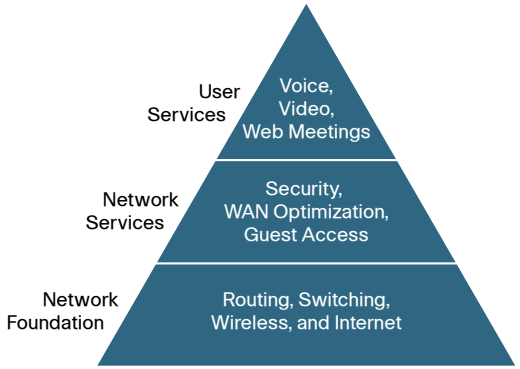
By deploying the Cisco SBA, your agency can gain:

- A standardized design, tested and supported by Cisco
- Optimized architecture for midsize agencies with up to 1000 users and up to 20 branches
- Flexible architecture to help ensure easy migration as the agency grows
- Seamless support for quick deployment of wired and wireless network access for data, voice, teleworker, and wireless guest
- Security and high availability for agency information resources, servers, and Internet-facing applications
- Improved WAN performance and cost reduction through the use of WAN optimization
- Simplified deployment and operation by IT workers with CCNA® certification or equivalent experience
- Cisco enterprise-class reliability in products designed for midsize agencies

Guiding Principles

We divided the deployment process into modules according to the following principles:

- **Ease of use:** A top requirement of Cisco SBA was to develop a design that could be deployed with the minimal amount of configuration and day-two management.
- **Cost-effective:** Another critical requirement as we selected products was to meet the budget guidelines for midsize agencies.
- **Flexibility and scalability:** As the agency grows, so too must its infrastructure. Products selected must have the ability to grow or be repurposed within the architecture.
- **Reuse:** We strived, when possible, to reuse the same products throughout the various modules to minimize the number of products required for spares.



The Cisco SBA can be broken down into the following three primary, modular yet interdependent components for the midsize agency.

- **Network Foundation:** A network that supports the architecture
- **Network Services:** Features that operate in the background to improve and enable the user experience without direct user awareness
- **User Services:** Applications with which a user interacts directly

The Purpose of this Guide

This deployment guide introduces the Email Security solution.

It explains the requirements that were considered when building the Cisco SBA design and introduces each of the products that were selected.

Agency Overview

Due to a need for a functional and reliable email solution, many agencies have made an email security solution requirement. This solution must handle the common threats while not introducing new issues like blocking legitimate emails.

The two major threats to the email system:

- Floods of unsolicited and unwanted emails, called spam, that waste employee time through their sheer volume, and use valuable resources like bandwidth and storage.
- Malicious emails that come 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 trick employees to release sensitive information like credit card numbers, social security numbers, or intellectual property, or to browse to malicious websites.

Notes

Technology Overview

An email solution will become unusable if spam—unsolicited and unwanted emails—is not filtered properly. The sheer volume of spam messages can crowd out legitimate mail. A side effect of some anti-spam solutions is false positives or email that is incorrectly identified as spam. When this occurs, the agency must expend resources to sift through the junk email looking for legitimate messages or reduce the level of filtering, which allows more messages to go to users, making the user responsible for determining whether emails are spam.

Spam is also likely to include embedded attacks. Criminal organizations have found that using attacks in email is an effective and cheap way to attack a user's machine. These attacks may take the form of viruses that attempt to infect the user's host, or counterfeit URLs that trick users into going to a website where criminals can steal bank login credentials or infect the user's host. These types of attacks, known as phishing, are used to gather social security numbers, credit card numbers, or compromise the host to use it as a launch point to send spam and other attacks.

Filtering Spam

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

One technique used to combat spam and phishing attacks is reputation-based filtering checks. If a server is a known spam sender, then 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 processes can be applied to emails carrying viruses and other threats.

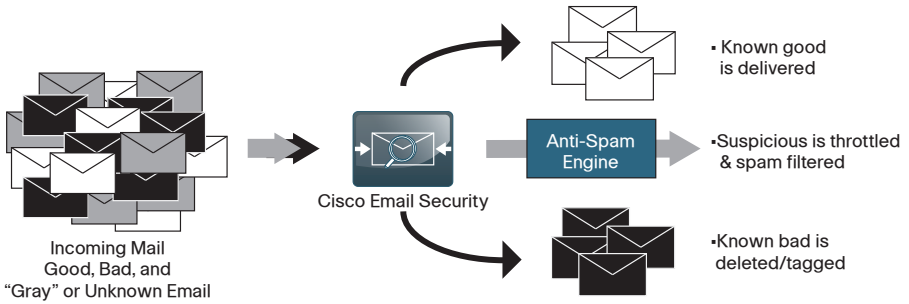
The goal of the solution is to filter out positively identified spam and quarantine or discard emails sent from untrusted or potentially hostile locations. Anti-virus (AV) scanning is applied to emails and attachments from all servers to remove known malware.

Reputation filters provide the first layer of defense by looking at the source IP address of the email server and comparing this to the reputation data downloaded from Cisco SenderBase®. SenderBase is the world's largest repository for security data including spam sources, 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 Email Security Appliance (ESA), receive updates from SenderBase several times a day. When ESA receives an email, it compares the source IP to the SenderBase database (see Figure 1). If the reputation of the sender is:

- Positive, the email gets forwarded on to the next layer of defense.
- Negative, the email is discarded.
- In between, the email is considered suspicious, is quarantined, and must wait for inspection before being delivered.

Context-based anti-spam inspection in ESA inspects the entire mail message, including attachments, looking for details like sender identity, message contents, embedded URLs, and email formatting. Using these algorithms, the ESA can identify spam messages without blocking legitimate email.

Figure 1. Email Filtering Overview



Fighting Viruses and Malware

Cisco Email Security Appliance uses a multilayer approach to fight viruses and malware.

The first layer is the Virus Outbreak Filters which are downloaded from SenderBase by the appliance. 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 anti-virus signatures are updated to counter the current threat.

The ESA second layer of defense involves using AV signatures to scan quarantined emails to ensure that they do not carry viruses into the network.

Cisco IronPort Email Security Appliance

The ESA protects the email infrastructure and the employees who use email at work. ESA integrates into the existing email infrastructures easily with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA), or mail relay, along the email delivery chain.

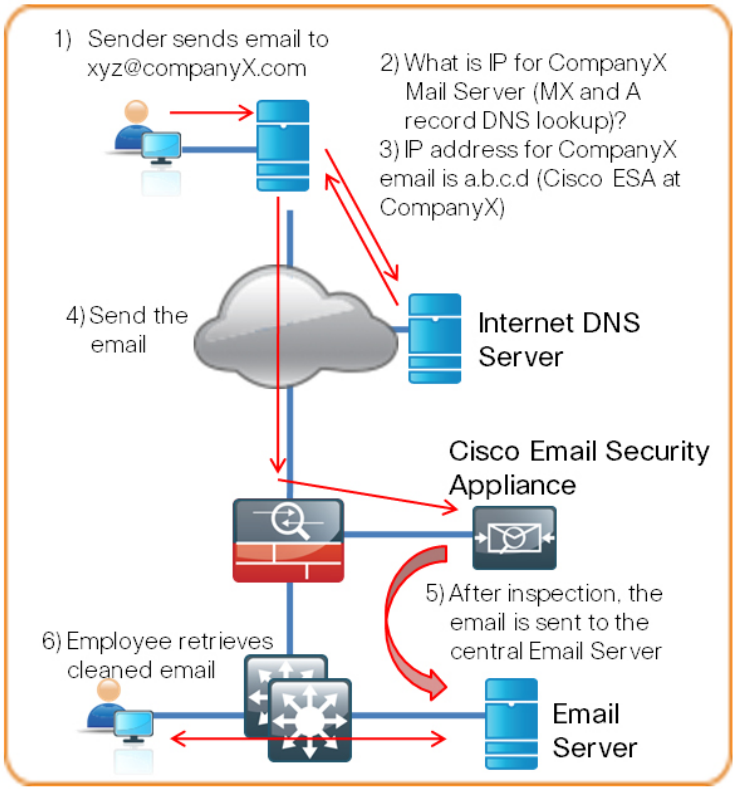
A normal email exchange, when an agency is using an MTA, might look like the email message flow depicted in Figure 2.

ESA can be deployed:

- With a single physical interface to filter email to and from the agency's mail servers.
- Using a two-interface configuration, one for email transfers to and from the Internet and the other for email transfers to and from the internal servers.

ESA uses a variety of mechanisms for spam and antivirus filtering.

Figure 2. Email Message Flow



Notes

Deploying the Cisco Email Security Appliance

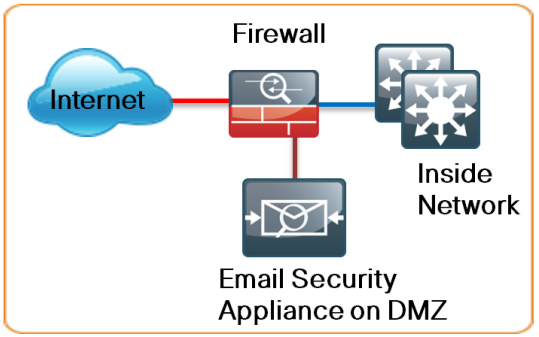
For deployment in the SBA, the ESA is configured for basic network access and an anti-spam and anti-virus policy is built and applied. The Domain Name System (DNS) was modified to support the ESA; the appliance software was updated, and the feature keys for the appliance were installed.

Some slight policy changes have been made, but a detailed policy configuration discussion, troubleshooting, and ongoing monitoring are beyond the scope of this document. Policy migration and advanced policy creation for the Cisco ESA device should be directed to your Cisco Partner or IronPort SE.

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

In this Deployment Guide, the ESA is physically deployed on the DMZ of the Internet Edge firewall using a single interface for simplicity (see Figure 3). This interface handles all incoming and outgoing email and carries management traffic. The port on the ESA is the M1 management interface.

Figure 3. Deployment Overview



It is important that the ESA be accessible via the public Internet and that the ESA is the "first hop" in your email infrastructure. The sender's IP address is used by several of the ESA's processes and is one of the primary identifiers SenderBase uses to determine the sender's reputation. If another device receives mail before forwarding it to the ESA, the ESA will not be able to determine the sender's IP address and filtering cannot be applied properly.

This section explains how to deploy the ESA, including the following processes:

- Preparing for ESA Deployment
- Completing the Basic Deployment
- Enabling Security Services
- Maintaining the ESA

Process

Preparing for ESA Deployment

1. Configure the DNS

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

Procedure 1 Configure the DNS

The ESA's hostname is the name carried in the DNS's Mail Exchange (MX) record, and it indicates that the ESA is the primary MTA; the DNS A (IP address) record corresponds to the IP address that the Cisco ASA 5500 Adaptive Security Appliance is statically translated to the ESA's address in the DMZ.

Process

Completing the Basic Deployment

1. Complete Basic ESA Setup
2. Complete the System Setup
3. Configure System Updates and Feature Keys

After physically installing and connecting the ESA to the network, the next step is basic setup.

Procedure 1 Complete Basic ESA Setup

The ESA supports two configuration interfaces: Web browser or CLI.

Complete the following steps to connect to an unconfigured ESA using a Web browser:

Step 1: Configure a PC with an IP address in the 192.168.42.x network.

Step 2: Connect both devices to the same VLAN on a switch (or directly connect a crossover Ethernet cable between the devices).

Step 3: Browse to the default IP address of 192.168.42.42.

Reader Tip

User documentation can be found here:
http://www.ironport.com/support/login.html

Work with your Cisco IronPort Channel Partner to obtain a login.

Tech Tip

The default username and password is admin/ironport.

To connect using the console port, complete the following steps to set up basic networking to configure connectivity. You will then finish configuring the ESA with the built-in Web GUI device management.

Step 1: Issue the following two commands in the device CLI:

```
interfaceconfig
setgateway
```

Step 2: Commit your changes after making them as follows:

```
ironport.example.com> interfaceconfig

Currently configured interfaces:
1. Management (192.168.42.42/24 on Data 1: ironport.example.
com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> edit

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

IP interface name (Ex: "InternalNet"):
[Management]> DMZ_Interface

IP Address (Ex: 192.168.1.2):
[192.168.42.42]> 192.168.30.100

Ethernet interface:
1. Data 1
2. Data 2
[1]> 1

Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> 255.255.255.192

Hostname:
[ironport.example.com]> email1.cisco.local

Do you want to enable FTP on this interface? [N]>

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]>

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]>

Do you want to enable HTTPS on this interface? [Y]>

Which port do you want to use for HTTPS?
[443]>

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

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

Do you want to enable IronPort Spam Quarantine HTTPS on this
interface? [N]> y

Which port do you want to use for IronPort Spam Quarantine
HTTPS?
[83]>

You have not entered an HTTPS certificate. To assure privacy,
run "certconfig" first. You may use the demo, but this will
not be secure.
Do you really wish to use a demo certificate? [Y]>

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

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

Do you want DMZ_Interface as the default interface for
IronPort Spam Quarantine? [N]> y

Do you want to use a custom base URL in your IronPort 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

Currently configured interfaces:
1. DMZ_Interface (192.168.30.101/26 on Data 1: email2.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.
[]>

Please run "systemsetup" or "sethostname" then "commit" before
sending mail.
ironport.example.com> setgateway

Warning: setting an incorrect def
ault gateway may cause the current connection to be interrupted
when the changes are committed.
Enter new default gateway:
[]> 192.168.30.65

ironport.example.com> commit

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

Changes committed: Mon Dec 14 17:04:49 2009 UTC
```

Step 3: Assuming the correct firewall rules have been applied, ping the appliance from the network to verify the configuration is complete.

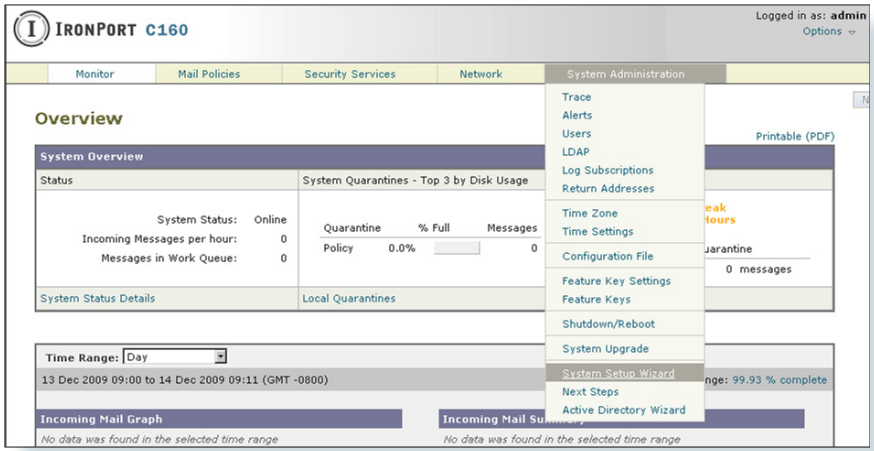
Step 4: To connect to the GUI device management, open a browser and browse via https (https://192.168.42.42/) to the address of the email appliance.

Procedure 2 Complete the System Setup

Step 1: After initial configuration is complete, connect to the appliance using a browser to access the device management application GUI (graphical user interface).

Run the System Setup Wizard from the GUI (see Figure 4).

Figure 4. System Setup Wizard

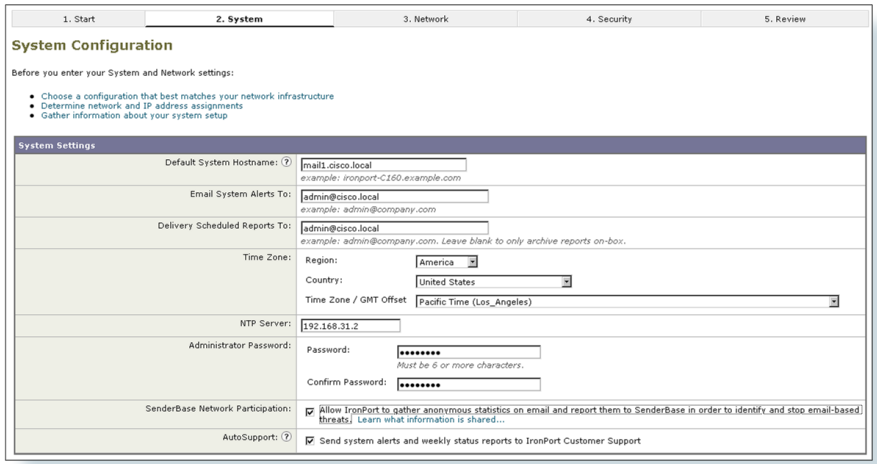


Step 2: Read the license and accept, then select the **Begin Setup** button.

Step 3: Answer the System Configuration questions to define the basic settings such as time settings, default hostname, and the default password.

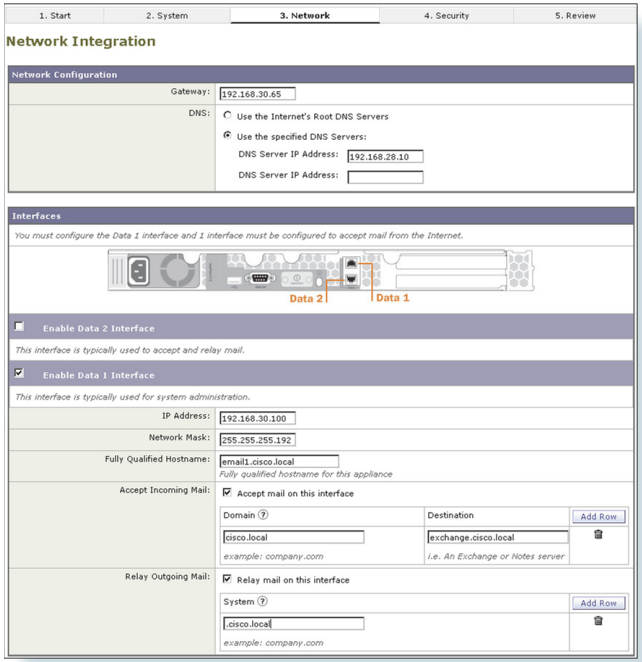
The last two questions ascertain your interest in participating in the SenderBase network by allowing your ESA to send anonymized reputation details about email traffic back to Cisco to improve SenderBase and the product in general (see Figure 5).

Figure 5. System Configuration



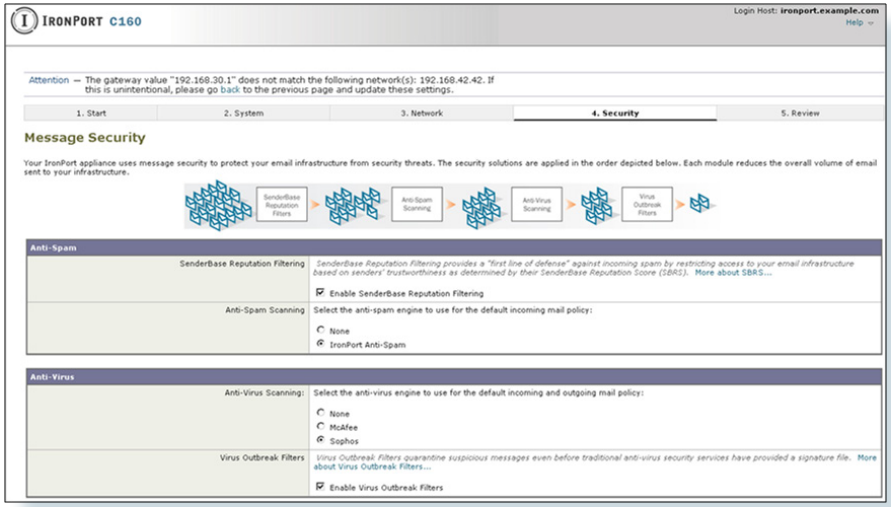
Step 4: Network Integration allows you to define your DNS server (or tell the appliance to use the Internet's Root DNS servers). This panel is also where the user sets up the network interface(s) used for mail processing (see Figure 6).

Figure 6. Network Integration



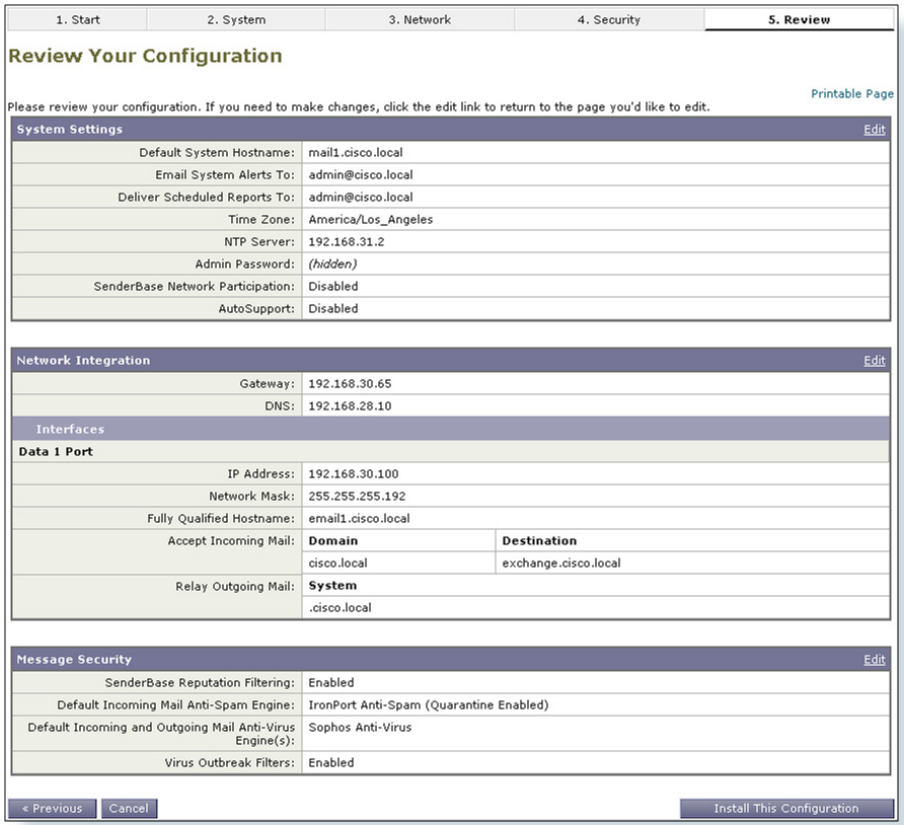
Step 5: Message Security selects whether anti-spam and anti-virus filtering are enabled and which engine is used for each function (see Figure 7).

Figure 7. Message Security



Step 6: Review allows you to review the configuration that you have defined, and to accept or modify the configuration. If you accept, the ESA will install the configuration onto your Email Security Appliance (see Figure 8).

Figure 8. Review



Tech Tip

If your environment requires proxies for HTTP or HTTPS communications, define these proxies here: Security Services->Service Updates. Select the **Edit Update Settings** button and then enter the proxy settings for HTTP and HTTPS at the bottom of this page and hit the **Submit** button and the **Commit** button.

Procedure 3 Configure System Updates & Feature Keys

It is important to look at two other areas on the box before you begin to use it: Feature keys and system upgrades.

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: To check whether your ESA has any licenses that are not currently enabled, select the **Check for New Keys** button. This will enable the ESA to connect to Cisco.com and determine if all purchased licenses are installed and enabled.

Step 3: To upgrade the code on the appliance, select the **System Administration->System Upgrade** button. This will display the current software version. Select the **Available Updates** button to determine if updates are available.

If newer versions are available, they can be selected and installed. While it is not necessary to load all updates in order, it is possible that the latest update will require interim updates before it can be loaded. If interim updates are required, the manager will notify you.

Tech Tip

It is not possible to downgrade software versions at this time, so be certain that an upgrade is desired before proceeding.

Process

Enabling Security Services

1. Set up Bounce Verification
2. Review Incoming Mail Policies

Now that the system setup is complete, you are ready to enable security services.

Procedure 1 Set Up Bounce Verification

Bounce verification is a process that allows the ESA to apply a specific tag to outgoing messages so that when bounce emails come back to the ESA, it can verify that the emails were actually originally sent out by the ESA. Spammers and hackers use fake bounced messages for many malicious purposes.

Step 1: Access **Mail Policies > Bounce Verifications** and select the **New Key** button.

Step 2: Enter an arbitrary text string that the ESA will apply in the Bounce verification process. Commit the changes.

Step 3: Access **Mail Policies > Destination Controls** and click on the Default in the first table.

Step 4: Change Bounce Verification to **on**.

Step 5: Submit and commit changes.

Procedure 2 Review Incoming Mail Policies

To complete the ESA set up, review the Incoming Mail Policies.

Step 1: Access **Mail Policies > Incoming Mail Policies**. Currently there is one default mail policy. The one default change we will make is to change a positive Antispam result from a Quarantine action to a Drop action.

Step 2: Select the policy definition under the Antispam column header.

Step 3: Change the Positively Identified Spam Settings from **Quarantine** to **Drop**.

Step 4: Submit and commit.

Process

Maintaining the ESA

1. Monitor the ESA
2. Troubleshoot the ESA

With your system fully deployed, you are ready to monitor and maintain the ESA.

Procedure 1 Monitor the ESA

There are a variety of reports available under Monitor to help you monitor the ESA's behavior. These reports make it possible to track activity and statistics for spam, virus types, incoming mail domains, outbound destinations, system capacity, and system status.

Procedure 2 Troubleshoot the ESA

Step 1: To determine why the ESA applied specific actions to a given email, you can run the Trace tool under **System Administration**.

By defining a search using details of a given email in question, you can test a specific email to determine how and why the ESA handled the message. This is especially useful if some of the more advanced features of the ESA are used (like DLP).

Reader Tip

User documentation can be found here:
http://www.ironport.com/support/login.html

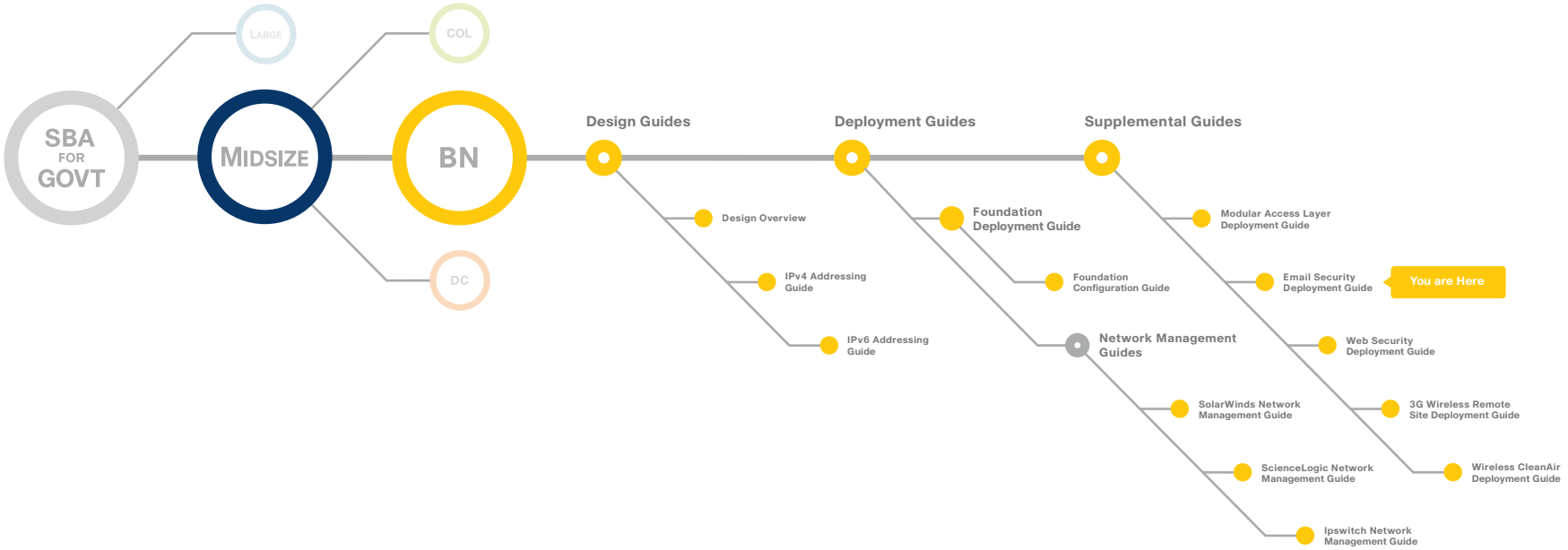
Work with your Cisco IronPort Channel Partner to obtain a login.

Appendix A: Product List

The following products and software version have been validated for the Cisco SBA:

Functional Area	Product	Part Numbers	Software Version
Internet Edge	Cisco Ironport C160 Email Security Appliance	C160-BUN-R-NA	6.5.3-007

Appendix B:
SBA for Midsize Agencies Document System



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.**

C07-641114-00 12/10