Cisco Web Security Appliance

CC Configuration Guide

Version 1.1

August 7, 2017
# Table of Contents

1 Introduction .................................................................................................................. 7
1.1 Audience ............................................................................................................... 7
1.2 Purpose ............................................................................................................... 7
1.3 Document References .......................................................................................... 7
1.4 Supported Hardware and Software ........................................................................ 8
1.5 Operational Environment ...................................................................................... 9
  1.5.1 Supported non-TOE Hardware/ Software/ Firmware .......................................... 9
2 Secure Acceptance of the TOE .................................................................................. 10
3 Secure Installation and Configuration ........................................................................ 13
  3.1 Physical Installation ........................................................................................... 13
  3.2 Pre-requisites of Virtual Appliance Installation .................................................. 13
  3.3 Initial Setup via Direct Console Connection ....................................................... 13
    3.3.1 Options to be chosen during the initial setup of the WSA ................................... 13
4 Secure Usage of the TOE ......................................................................................... 15
  4.1 Remote Administration Protocols ....................................................................... 15
    4.1.1 Enabling FIPS Mode ..................................................................................... 15
    4.1.2 Key Zeroization ............................................................................................ 17
    4.1.3 Disable telnet .................................................................................................. 18
    4.1.4 SSHv2 Configuration ..................................................................................... 18
    4.1.5 SSL/TLS Settings .......................................................................................... 20
  4.2 Authorized Administrators ................................................................................... 22
  4.3 Password Complexity ......................................................................................... 23
  4.4 Adding a Login Banner ....................................................................................... 23
  4.5 Configuring External Authentication ................................................................... 24
  4.6 Logging .............................................................................................................. 24
  4.7 Inactivity Session Termination ........................................................................... 26
  4.8 Product Updates ................................................................................................. 27
    4.8.1 Online Updates ............................................................................................. 27
    4.8.2 Offline Updates ............................................................................................. 28
5 Obtaining Documentation, Support & Security Guidelines ....................................... 28
6 Security Relevant Events ....................................................................................................................... 29
7 Network Services and Protocols ............................................................................................................. 43
8 Modes of Operation ................................................................................................................................. 45
9 Security Measures for the Operational Environment .............................................................................. 46
10 Related Documentation ......................................................................................................................... 46
10.1 World Wide Web .................................................................................................................................. 46
10.2 Ordering Documentation .................................................................................................................... 46
10.3 Documentation Feedback .................................................................................................................. 47
11 Obtaining Technical Assistance ............................................................................................................ 47
12 Appendix A ............................................................................................................................................ 49
12.1 Components ......................................................................................................................................... 49
12.2 Order of Operations ............................................................................................................................. 50
12.3 System Prerequisites .......................................................................................................................... 51
12.3.1 Public Internet facing Host ............................................................................................................ 51
12.3.2 Private Network Facing Host ........................................................................................................ 51
12.4 Tool Installation ................................................................................................................................... 53
12.4.1 Public Internet Facing Host ........................................................................................................ 53
12.4.2 Customer Private Network Host .................................................................................................. 53
12.5 Tool Configuration ............................................................................................................................. 54
12.5.1 Public Internet Facing Host ........................................................................................................ 54
12.5.2 On the Customer Private Network Server ................................................................................... 56
12.6 On the Customer Private Network Content Security Appliances ..................................................... 56
12.7 Cisco WSA .......................................................................................................................................... 56
12.8 Executing updates - Order of operation and commands to perform ................................................ 58
12.8.1 Command Prompt to execute the script on the Public Internet Facing Host ................................ 58
List of Tables

Table 1: Acronyms ........................................................................................................................................... 5
Table 2 Cisco Documentation and CI List ........................................................................................................ 7
Table 3 IT Environment Components ............................................................................................................ 9
Table 4 Excluded Functionality ..................................................................................................................... 9
Table 5 TOE External Identification ........................................................................................................... 10
Table 6 Evaluated Software Images ........................................................................................................... 12
Table 7 General Auditable Events ............................................................................................................... 30
Table 8 Protocols and Services .................................................................................................................... 43
Table 9 Operational Environment Security Measures ................................................................................... 46

List of Figures

Figure 1 FIPS mode dialog ............................................................................................................................... 16
Figure 2 CLI saveconfig sub-option when in FIPS mode ............................................................................. 17
Figure 3 GUI version of the save config ....................................................................................................... 17
Figure 4 sshconfig options via CLI ............................................................................................................. 19
Figure 5 sslconfig command dialog ........................................................................................................... 21
Figure 6 Setting Inactivity Timeout in GUI ................................................................................................. 26
Figure 7 Setting Inactivity Timeout in CLI .................................................................................................. 27
Figure 8 Offline Update Details .................................................................................................................... 49
List of Acronyms

The following acronyms and abbreviations are used in this document:

Table 1: Acronyms

<table>
<thead>
<tr>
<th>Acronyms / Abbreviations</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>CC</td>
<td>Common Criteria for Information Technology Security Evaluation</td>
</tr>
<tr>
<td>CI</td>
<td>Configuration Items</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>CSR</td>
<td>Certificate Signing Request</td>
</tr>
<tr>
<td>WSA</td>
<td>Web Security Appliance</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standards</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hyper-Text Transport Protocol Secure</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>MTA</td>
<td>Mail Transfer Agent</td>
</tr>
<tr>
<td>NDcPP</td>
<td>Network Device Collaborative Protection Profile</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>POST</td>
<td>Power On Self Test</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure Copy Protocol</td>
</tr>
<tr>
<td>SFP</td>
<td>Security Function Policy</td>
</tr>
<tr>
<td>SSHv2</td>
<td>Secure Shell (version 2)</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>TCP</td>
<td>Transport Control Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TOE</td>
<td>Target of Evaluation</td>
</tr>
<tr>
<td>TSF</td>
<td>TOE Security Function</td>
</tr>
<tr>
<td>UCS</td>
<td>Unified Computing System</td>
</tr>
</tbody>
</table>
DOCUMENT INTRODUCTION

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

DOCUMENT INTRODUCTION
This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the Web Security Appliance (WSA). This Operational User Guidance with Preparative Procedures addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration. Administrators of the TOE will be referred to as administrators, authorized administrators, TOE administrators, semi-privileged administrators, and privileged administrators in this document. All administrative actions that are relevant to the Common Criteria (CC) Evaluation and claimed Protection Profile(s) are described within this document. This document will include pointers to the official Cisco documentation in order to aid the administrator in easily identifying the CC relevant administrative commands, including subcommands, scripts (if relevant), and configuration files, that are related to the configuration (including enabling or disabling) of the mechanisms implemented in WSA that are necessary to enforce the requirements specified in the claimed PP.
1 Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Web Security Appliance (WSA), the TOE, as it was certified under Common Criteria. The Web Security Appliance (WSA) may be referenced below by the model number series or related acronym ex. WSA or TOE.

1.1 Audience

This document is written for administrators configuring the TOE. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, and understand your network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use the operating systems on which you are running your network.

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining WSA operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

1.3 Document References

This section lists the Cisco Systems documentation that is also the Common Criteria Configuration Item (CI) List. The documents used are shown below in Table 2. Throughout this document, the guides will be referred to by the corresponding “#”, such as [1].

<table>
<thead>
<tr>
<th>#</th>
<th>Title</th>
<th>Covers</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Title</td>
<td>Covers</td>
<td>Link</td>
</tr>
<tr>
<td>----</td>
<td>----------------------------------------------------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S670, S680</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 170 Series Hardware Installation Guide</td>
<td>S170, X1070</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco x90 Series Hardware Installation Guide</td>
<td>x90</td>
<td></td>
</tr>
</tbody>
</table>

### 1.4 Supported Hardware and Software

Only the hardware and software listed in section 1.5 of the Security Target (ST) is compliant with the Common Criteria evaluation. Using hardware not specified in the ST invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed in the ST will invalidate the secure configuration. The hardware is comprised of the following: S690, S690X, S680, S390, S380, S190, S170, and S100v, S300v running on Cisco UCS servers (blade or rack-mounted). The software is comprised of the AsyncOS software image Release 10.5.
1.5 Operational Environment

1.5.1 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 3 IT Environment Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Required</th>
<th>Usage/Purpose Description for TOE performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management workstation with SSH Client</td>
<td>Yes</td>
<td>This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.</td>
</tr>
<tr>
<td>Management workstation using web browser for HTTPS</td>
<td>Yes</td>
<td>This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through HTTPS protected channels. Any web browser that supports TLSv1.0 with the supported ciphersuites may be used.</td>
</tr>
<tr>
<td>Local Console</td>
<td>No</td>
<td>This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>No</td>
<td>The TOE supports communications with an NTP server in order to synchronize the date and time on the TOE with the NTP server’s date and time. A solution must be used that supports secure communications with up to a 32 character key.</td>
</tr>
<tr>
<td>Web Server</td>
<td>Yes</td>
<td>This includes the IT environment Web servers that the TOE receives and sends HTTP/HTTPS.</td>
</tr>
<tr>
<td>Syslog Server</td>
<td>Yes</td>
<td>This includes any syslog server to which the TOE would transmit syslog messages.</td>
</tr>
<tr>
<td>Update Server</td>
<td>No</td>
<td>This includes the Cisco IT environment update servers that are used to download the latest software updates for the TOE.</td>
</tr>
</tbody>
</table>

Table 4 Excluded Functionality

<table>
<thead>
<tr>
<th>Excluded Functionality</th>
<th>Exclusion Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-FIPS 140-2 mode of operation on the</td>
<td>This mode of operation includes non-FIPS allowed operations.</td>
</tr>
</tbody>
</table>

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the collaborative Protection Profile for Network Devices.
2 Secure Acceptance of the TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that that is has not been tampered with during delivery.

Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions:

**Step 1** Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

**Step 2** Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

**Step 3** Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

**Step 4** Note the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

**Step 5** Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

**Step 6** Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). Also verify that the unit has the following external identification as described in Table 5 below. The TOE version can be verified by the hardware appliance face plate model number.

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Model Number</th>
<th>External Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSA</td>
<td>S690</td>
<td>Cisco S690 Web Security Appliance</td>
</tr>
<tr>
<td>S690X</td>
<td></td>
<td>Cisco S690X Web Security Appliance</td>
</tr>
<tr>
<td>S680</td>
<td></td>
<td>Cisco S680 Web Security Appliance</td>
</tr>
<tr>
<td>S390</td>
<td></td>
<td>Cisco S390 Web Security Appliance</td>
</tr>
<tr>
<td>S380</td>
<td></td>
<td>Cisco S380 Web Security Appliance</td>
</tr>
</tbody>
</table>
### Table: Product Name, Model Number, External Identification

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Model Number</th>
<th>External Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>S370</td>
<td></td>
<td>Cisco S370 Web Security Appliance</td>
</tr>
<tr>
<td>S190</td>
<td></td>
<td>Cisco S190 Web Security Appliance</td>
</tr>
<tr>
<td>S170</td>
<td></td>
<td>Cisco S170 Web Security Appliance</td>
</tr>
<tr>
<td>S100v</td>
<td></td>
<td>Cisco S100v</td>
</tr>
<tr>
<td>S300v</td>
<td></td>
<td>Cisco S300v</td>
</tr>
</tbody>
</table>

**Step 7** Approved methods for obtaining a Common Criteria evaluated software images:

- Perform and Offline Update by downloading the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. Software images are available from Cisco.com at the following: [http://www.cisco.com/cisco/software/navigator.html](http://www.cisco.com/cisco/software/navigator.html). Refer to Appendix A for Offline Update process.
- Perform an Online Update where the TOE downloads the software image directly from Cisco and then installs the image. Refer to Section 5.10 for Online Update process.
- The TOE ships with the correct software images installed.

**Step 8** Once the file is downloaded, the authorized administrator verifies that it was not tampered with prior to moving it to the TOE by using a SHA-384 utility to compute an SHA-384 hash for the downloaded file and comparing this with the SHA-384 hash for the image listed in Table 6 below.

If installing software on the hardware appliance go to Step 9a. If installing a WSA Virtual Appliance skip to Step 9b.

**Step 9a** Install the downloaded and verified software image onto your WSA as described in [1] Click on Maintain and Operate → Cisco AsyncOS 10.0.0 for Web User Guide → chapter “Connect, Install, and Configure”. → section System Setup Wizard via the GUI. Using the Command Line Interface, see Appendix B "Access the Command Line Interface", Subsection First Access.

Start WSA as described in [1]. Confirm that your WSA loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

**Step 9b** Install the software appliance by following the steps outlined in [2] Security → Cisco Web Security Virtual Appliance → section “Deploy the Virtual Appliance” Open the VMware client and selected create new → Select Use Existing Virtual Disk → Browse and Select the WSA image that was unzipped xyz.vmdk file.

**Step 10** The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. Using the CLI type the “version” [3] command to display the currently running system image filename and the system software release version. See Table 6 below for the detailed hash value that must be checked to ensure the software has not been modified in anyway.
<table>
<thead>
<tr>
<th>Software Version</th>
<th>Image Name</th>
<th>SHA-512 hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>AsyncOS 10.5</td>
<td>phoebe-9-1-0-040.tgz</td>
<td>9cf31fba634978a06688acdee6dd88e6a47b3c36f04ec9927dedb4cda7611c1fba06271065907c5a61c1c8d76b83cea675fa5ac9085d1b632b0664e4ca41b239</td>
</tr>
<tr>
<td></td>
<td>phoebe-9-1-0-040-C600V.zip</td>
<td>d36a48feaa7b5159a34b75e1ddfe84a2a0ba618b0752708c78fcb76dd6cd369243b53cafd52fb33a37fbbf83f15da17bc710524269ee35d14106bebb42a9b44a</td>
</tr>
</tbody>
</table>
3 Secure Installation and Configuration

3.1 Physical Installation
Follow the appropriate Cisco Hardware Installation Guide for your model [3] for hardware installation instructions. For WSA "v" models, see the Cisco Content Security Virtual Appliance Installation Guide [2], section “Set Up the Virtual Appliance” for detailed instructions for setting up the Virtual Appliance.

During installation please ensure that the TOE is installed as follows:

- The WSA must be protected from unauthorized physical modification.
- The WSA must be located within controlled access facilities, which will prevent unauthorized physical access.

3.2 Pre-requisites of Virtual Appliance Installation

- In order to determine the compatible version of ESXi, confirm the model number you have to the listing of Supported Servers for ESXi in the Release Notes for the VMware ESXi Installable Cisco Custom ISO Image [8]. Once you have confirmed that your hardware is compatible, then download the Cisco Custom Image for ESXi:


  In the evaluated configuration ESXi 5.5 must be used and should be patched to the latest VMware release.

- The install guide for your (UCS) Unified Communications Server can be found here: http://www.cisco.com/c/en/us/support/servers-unified-computing/unified-computing-system/products-installation-guides-list.html. In the evaluated configuration, the UCS Server should only be managed locally.

- VMware vSphere ESXi Installation:
  1. Preferably use IE browser
  2. Download the ESXi version image, [8] includes links for a free download of ESXi which comes with 60 days Eval.
  3. Please find the video url that explains raid configuration on UCS server if you have single Hard Drive
  4. In the evaluated configuration, the ESXi configuration should only be managed locally.

3.3 Initial Setup via Direct Console Connection
The WSA must be given basic configuration via console connection prior to being connected to any network.

3.3.1 Options to be chosen during the initial setup of the WSA
An authorized administrator must use the System Setup Wizard for the initial setup in order to ensure a complete configuration. Follow the instructions in the [1] Cisco AsyncOS Web User Guide, chapter “Connect, Install, and Configure”, section “System Setup Wizard” via the Graphical User Interface (GUI) for initial setup instructions. An authorized administrator can run the System Setup Wizard using a browser [1].
The default password for the admin account must be changed during the initial setup configuration meeting the password complexity rules as described in section 3.3.1.3 below.

Note: The following changes must be made according to [1] in Chapter “Connect, Install, and Configure” during installation to put the WSA into its evaluated configuration:

### 3.3.1 Configuring System Alerts

Note: Other than configuring the TOE to create an email alert when the local audit storage is exhausted, the information within this section does not fall within the scope of NDcPP evaluation.

The WSA monitors web traffic received on port 80 and 443 containing Web traffic. The WSA can take actions in order to enforce a web based policy.

In order to configure settings related to alerts see Chapter "Perform System Administration Tasks", section Managing Alerts, subsection Configuring Alert Settings, specify an email address of an authorized administrator to use for System Alerts.

### 3.3.1.2 Setting the Time

This section contains information on setting the local hardware clock or optionally the NTP sources. Clock management is restricted to the Authorized Administrator and the Authorized System Administrator. See chapter “Perform System Administration Tasks” section System Date and Time Management [1] for configuring the time. Cisco AsyncOS allows an authorized administrator to use the Network Time Protocol (NTP) to synchronize time with other servers on the network, or to manually set the system clock. The time can be set manually via the Time Zone or Time Settings page from the System Administration menu in the GUI or by using the following commands in the CLI: ntpconfig, settime, and settz.

To use NTP, see section “Synchronizing the System Clock with an NTP Server” [1]. When Network Time Protocol (NTP) is configured, the time is synchronized with a NTP server over NTPv3. NTP runs on UDP, which in turn runs on IP. NTP Version 3 (NTPv3) is documented in RFC 1305.

### 3.3.1.3 Password Complexity

This section describes the required password complexity rules when setting the password during initial setup as well as for all subsequent administrator accounts that are created. See chapter “Perform System Administration Tasks”, section Setting Passphrase Requirements for Administrative Users [1] for instructions on setting password rules. All WSA Administrator accounts must meet the following password complexity rules:

1. The account password must be composed of any combination of characters that includes characters for at least 3 of these four character sets: upper and lower case letters, numbers, and one of the following special characters: [“!”,”@”,”#”,”$”,”^”,”&”,”*”,”(”,”)”] ;

2. Minimum password length of 15 characters or greater

### 3.3.1.4 Disable AutoSupport

Note: The information within this section does not fall within the scope of the NDcPP evaluation.

3.3.1.5 Disable Cloudmark

Note: The information within this section does not fall within the scope of NDcPP evaluation.

- Enable Anti-Spam Scanning

During Step 4: Security ("Enabling Anti-Spam Scanning"), enable Cisco Anti-Spam software. Third-party anti-spam software needs to be disabled, such as Cloudmark.

- Enable Anti-Virus Scanning

During Step 4: Security ("Enabling Anti-Virus Scanning"), enable Cisco’s integrated anti-virus scanning Sophos and disable McAfee Anti-Virus.

4 Secure Usage of the TOE

4.1 Remote Administration Protocols

Administrators access the TOE management functionality through the TOE Web GUI interface and also can run a subset of commands via the CLI interface. The GUI is web based and is accessed over HTTPS for remote sessions. The TOE CLI is accessed either via a directly connected console or remotely via a SSHv2 connection. In the evaluated configuration, WSA must be configured to run in FIPS mode in order to ensure that the Common Criteria evaluated ciphersuites and algorithms are used. Information regarding accessing the TOE CLI may be found in Appendix B "Access the Command Line Interface" of [1].

4.1.1 Enabling FIPS Mode

WSA must be run in the FIPS mode of operation. The use of the cryptographic engine in any other mode was not evaluated nor tested during the CC evaluation of the TOE. The fipsconfig command automatically configures the FIPS approved algorithms and key sizes putting WSA into FIPS mode. In addition, all stored passwords and keys will be encrypted in stored configuration files and also any email configuration files will be encrypted.

Before You Begin

Make sure that the appliance does not have any objects that are not FIPS compliant, for example, a DKIM verification profile with a key size of 512 bits. To enable FIPS mode, you must modify all the non-FIPS-compliant objects to meet FIPS requirements.

See Figure 1 FIPS mode dialog and chapter "Perform System Administration Tasks", section FIPS Compliance [1] for using the fipsconfig command. When enabling FIPS mode, the authorized administrator must say 'y' for the 'Do you want to enable encryption to sensitive data in configuration file when FIPS mode is enabled?' This will encrypt all stored passwords and keys.
m670e03.ibeng> fipsconfig

FIPS mode is currently disabled.

Choose the operation you want to perform:
- SETUP - Configure FIPS mode.

[]> setup

To finalize FIPS mode, the appliance will reboot immediately. No commit will be required.

Are you sure you want to enable FIPS mode and reboot now? [N]> y

Do you want to enable encryption to sensitive data in configuration file when FIPS mode is enabled? Changing the value will result in system reboot [N]> y

Enter the number of seconds to wait before forcibly closing connections.
[30]>

System rebooting. Please wait while the queue is being closed...

Closing CLI connection.
Rebooting the system...

Figure 1 FIPS mode dialog
4.1.1.1 Securing Passwords and Keys
As long as the authorized administrator selected 'y' for the 'Do you want to enable encryption to sensitive data in configuration file when FIPS mode is enabled?' then all passwords and keys will be encrypted. The below discussion is to describe further sub options that are available.

When the appliance is in FIPS mode, new sub-options will be displayed to the user asking whether to always save the configuration with encrypted passwords. In the CLI, the **saveconfig** command can be used to encrypt the passwords and keys. In the evaluated configuration, it is required to select **Encrypt passwords** in the **saveconfig** command dialog.

![Figure 2 CLI saveconfig sub-option when in FIPS mode](image)

**Configuration File**

![Figure 3 GUI version of the save config](image)

4.1.2 Key Zeroization
Although key zeroization is handled by the cryptographic module, a wipe command is available to ensure that the keys are zeroized within the old core dump files. As part of the reload command, an option to wipe the data is provided. The wipe option along with the **wipedata** command will overwrite the hard drive with zeros so that the keys are zeroized within the old core dump files.
WipeData(cli->wipedata) is a new command that will currently provide two options (“coredump” & “status”). Coredump will wipe the core dump files, status will display running, successful or unsuccessful for the last run of the command.

4.1.3 Disable telnet

By default telnet is disabled. To check that it is disabled an authorized administrator can go to [3] Chapter 3 (“The Commands: Reference Examples”), section “Networking Configuration/Network Tools” to use the interfaceconfig command. To verify that telnet is disabled on all interfaces (Data 1, Data 2, and Management) by selecting the interface.

```
Ethernet interface:
1. Data 1
2. Data 2
3. Management
[1]> Hostname: [mail3.example.com]> Do you want to enable Telnet on this interface? [Y]> n
```

4.1.4 SSHv2 Configuration

SSHv2 is enabled by default. This section describes the configuration of SSHv2 for remotely accessing the TOE CLI. The SSH keys are generated when using the hostkeyconfig command - NEW.

The administrator must choose a SSH client which supports SSHv2 using AES and HMAC-SHA-1 algorithms as well as ensure that diffie-hellman-group14-sha1 is the only allowed key exchange methods used for the SSH protocol. The administrator must configure the SSH client to use these algorithms when remotely connecting to the TOE.

In configuring SSHv2, at least one of the following data integrity algorithms for transport connection is required: hmac-sha1 and the "None" MAC algorithm is not allowed. These data integrity algorithms can be selected using the sshconfig command in the CLI. In addition, the diffie-hellman-group14-sha1 must be selected for the key exchange method used for SSH. SSH transport implementation must use SSH_RSA as its public key algorithm as well as AES-CBC-128, AES-CBC-256 for encryption. The algorithms and key sizes shown in Figure 4 are examples, please configure the TOE as described above.

Users accessing the CLI via SSH can be authenticated using public key cryptography. This requires the user’s public key to be entered into the TOE (using the sshconfig > userkey command) and associated with the user’s account. If there is no public key configured for the user, the user will instead be prompted to enter their username and password to authenticate.

For configuring SSH, the following algorithms and key sizes should be used:

Cipher Algorithms: aes256-cbc, aes128-cbc
MAC: hmac-sha1
Public key authentication algorithms: ssh-rsa
KEX Algorithms: diffie-hellman-group14-sha1
Minimum server key size: 2048
ssh server config settings:
Server key size: 1024

Cipher Algorithms: aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc,arcfour,rijndael-cbc@lysator.liu.se

MAC methods: hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com, hmac-md5-96

Public key authentication algorithms: ssh-rsa,ssh-dss

KEX Algorithms:
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha

Would you like to modify SSH Server configuration settings? (Yes/No) [N]> y

Enter the Minimum Server key size do you want to use
[1024]>

Enter the Cipher Algorithms do you want to use
[aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc,arcfour,rijndael-cbc@lysator.liu.se]>

Enter the MAC methods do you want to use
[hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-md5-96]>

Enter the Public key authentication algorithms do you want to use
[ssh-rsa,ssh-dss]>

Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha]>

ssh server config settings:
Server key size: 2048

Cipher Algorithms: aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc,arcfour,rijndael-cbc@lysator.liu.se

Figure 4 sshconfig options via CLI
The TOE supports uploading and downloading configuration files and accessing log files via SCP. When configuring the Log Retrieval Methods select SCP Push in the GUI or use the `logconfig` command in the CLI.

Note: The TOE also provides the option for accessing log files via FTP. By default, FTP (pull) downloading is disabled and may not be enabled in the evaluated configuration.

### 4.1.5 SSL/TLS Settings

When WSA is configured for FIPS mode, the below TLS ciphersuites are enforced by default.

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246

Use the `sslconfig` command to limit the ciphersuites. See Figure 5 below for more information regarding the `sslconfig` command. In order to limit the ciphersuites to just TLS_RSA_WITH_AES_128_CBC_SHA and TLS_RSA_WITH_AES_256_CBC_SHA the following steps should be followed:

1. `sslconfig`
2. `GUI`
3. 3 (TLS v1.1 or 1.2)
4. `AES256-SHA, AES128-SHA`
5. Leave sslconfig by clicking enter
6. `commit`
7. click enter
8. y

In the event that the validity of a peer certificate cannot be determined, then WSA does not accept the certificate. There is no action required by the administrator.
Fig. 5: $\text{sslconfig}$ dialog

4.1.5.1 Obtaining Certificates

To use TLS, the Cisco appliance must have an X.509v3 certificate and matching private key for receiving and delivery. An authorized administrator may use the same certificate for both SMTP receiving and delivery and different certificates for HTTPS services on an interface, and all outgoing TLS connections to destination domains, or use one certificate for all of them.

An authorized administrator may purchase certificates and private keys from a recognized certificate authority service. A certificate authority is a third-party organization or company that issues digital certificates used to verify identity and distributes public keys. This provides an additional level of assurance that the certificate is issued by a valid and trusted identity. Cisco does not recommend one service over another.

The Cisco appliance can generate a Certificate Signing Request (CSR) to submit to a certificate authority to obtain the public certificate. The certificate authority will return a trusted public certificate signed by a private
key. Use the Network > Certificates page in the GUI or the certconfig command in the CLI to generate the CSR and install the trusted public certificate.

If you are acquiring or creating a certificate for the first time, search the Internet for “certificate authority services SSL Server Certificates,” and choose the service that best meets the needs of your organization. Follow the service’s instructions for obtaining a certificate.

An authorized administrator can view the entire list of certificates on the Network > Certificates page in the GUI and in the CLI by using the print command after you configure the certificates using certconfig. Note that the print command does not display intermediate certificates. See [1] section “Obtaining Certificates” and [3] certconfig for more detailed information.

When the administrator is creating CSR, the subject should include the Name, country (optional), organization name, common name, and email address. When generating a new key, make sure 2048 bit is set for key size. For the Extensions, in the Basic constraints section, choose Certificate Authority for the Type. Note: Subsequent Certificate Signing Requests (CSRs) can be signed via this CA with the Type set to Not Defined. Add a Subject Alternative Name (SAN) for the Domain Name System (DNS).

4.1.5.2 Installing the Certificate from a Certification Authority

Step 1  The X.509v3 certificate must be received in PEM format before uploading to WSA.
Step 2  Navigate to the Network > Certificates page
Step 3  Click the name of the certificate that you sent to the Certification Authority for signing.
Step 4  Enter the path to the file on your local machine.

4.1.5.3 Enabling a Certificate for HTTPS

An authorized administrator can enable a certificate for HTTPS services on an IP interface using either the Network > IP Interfaces page in the GUI or the interfaceconfig command in the CLI. When adding an IP interface via the GUI, select a certificate that you want to use for the HTTPS service, check the HTTPS check box, and enter the port number.

In following example, the interfaceconfig command is used to edit the IP interface PublicNet to enable HTTPS services on port 443 (the default port). All other defaults for the interface are accepted. (Typing Enter at the prompt accepts the default value shown in brackets.)

Note that this example shows using the demonstration certificate that is pre-installed on the appliance. You may enable HTTPS services with the demonstration certificate for testing purposes, but it is not secure and is not recommended for general use.

In the event that the validity of a peer certificate cannot be determined, then WSA does not accept the certificate. There is no action required by the administrator.

4.2 Authorized Administrators

In the evaluated configuration, the administrator accounts must be created on the WSA itself. See chapter "Administering User Accounts" [1] and section Adding Local User Accounts for instructions on creating user accounts and assigning roles. WSA provides multiple pre-defined user roles with varying levels of permissions. The predefined administrative roles map to the Authorized Administrator role. The roles are
privileged and semi-privileged with varying administrative access. See Table 32-1 under Working with User Accounts > User Roles of [1] for a detailed listing of roles and associated privileges. Below is a brief listing of administrative roles and associated access:

- “admin” default user account that has full access to all system configuration settings.
- “Administrators” have full access to all system configuration settings.
- “Operators” are restricted from creating, editing, or removing user accounts and cannot use the following commands: resetconfig, upgradecheck, upgradeinstall, systemsetup or running the System Setup Wizard.
- “Technician” can perform system upgrades, reboot the appliance, and manage key features.

Below is a brief listing of user roles with limited associated access:

- “Read-only” can view administrative interfaces, but do not have the ability to commit configuration changes or to access the file system, or SCP, thus preventing them from accessing log files.
- “Guests” can only view system status information.
- “Help Desk” have access to system quarantines, end-user spam quarantines, and message tracking via the GUI.
- “Custom user role” can only access email security features assigned to the role. These features can be any combination of DLP policies, email policies, reports, quarantines, local message tracking, encryption profiles, and the Trace debugging tool. The users cannot access system configuration features. Only administrators can define custom user roles.

New users are created with the following procedures:

1. Navigate to the TOE web GUI and enter the administrator credentials.
2. Hover over “System Administration” and choose “Users.”
3. Choose “Add User.”
4. Enter a username, full name, role (Administrator), and password.
5. Choose “Commit Changes.”

4.3 Password Complexity
All administrator accounts must have the password configured to meet the complexity rules as defined in section 3.3.1.3

4.4 Adding a Login Banner
In the evaluated configuration a login banner must be created for all authorized administrator accounts accessing the TOE via the CLI or GUI locally and remotely. Instructions for configuring the login banner can be found in [1] section Additional Security Settings for Accessing the Appliance. In the CLI, use the adminaccessconfig > banner command to create the login banner. After creating the banner, commit your changes.
4.5 Configuring External Authentication

Note: The information within this section does not fall within the scope of NDcPP evaluation.

In support of authentication decisions and user authorizations, the TOE may leverage external authentication servers via LDAP and Radius. This is only for user accounts which have limited access to the TOE. This includes the following roles: “Read-only,” “Guests,” “Help Desk,” and the “Custom user role.” In the evaluated configuration, administrator user accounts must be created on WSA only.

Note: In the evaluated configuration, Administrator user accounts cannot be set up in Active Directory or RADIUS. This includes the following administrative user roles: “admin,” “Administrators,” “Operators,” and “Technician”.

Information regarding the use of this management functionality, including secure usage guidelines, can be found in [1] section External Authentication.

4.6 Logging

The TOE maintains audit records related to security-relevant operations of the TOE. Administrators and Operators can access all audit information. The administrators can manually download the log files by clicking a link to the log directory on the Log Subscriptions page, then clicking the log file to access. Depending on the browser as described in the WSA User Guide, an authorized administrator can view the file in a browser window, or open or save it as a text file. This method uses the HTTP(S) protocol and is the default retrieval method.

Information regarding the use of this management functionality, including secure usage guidelines, can be found in chapter “Monitor System Activity Through Logs” of [1]. In the evaluated configuration, the log files must be backed up to a remote computer. SCP Push must be configured to ensure the session is secured using SSHv2. See section Pushing Log Files to Another Server of [1]. An Authorized Administrator can configure the protocol used while creating or editing the log subscription in the GUI or via the logconfig command in the CLI.

This method periodically pushes log files to an SCP server on a remote syslog server, once an administrator configures the SCP Push. An authorized administrator defines a log subscription’s rollover settings when creating or editing the subscription using the System Administration > Log Subscriptions page in the GUI or the logconfig command in the CLI. The two settings available for triggering a log file rollover are:

- A maximum file size.
- A time interval.

To set the interval, it can be configured by file size or time. See the "Log Subscriptions" chapter and the section Adding and Editing Log Subscriptions. For example, enter 10m if you want AsyncOS to roll over the log file when it reaches 10 megabytes. Regarding the rollover by time, it can be customized using day, hour, minutes, and seconds. It could be backed up once a day or every hour depending on how the administrator wants to configure the audit backup policy.

This method requires an SSH SCP server on a remote computer using SSHv2 protocol. The subscription requires a username, SSH key, and destination directory on the remote syslog server. Log files are transferred based on a rollover schedule set by the authorized administrator.

The log files that must have a subscription configured are:

- AMP Engine Logs
- Audit Logs
- Access Logs
- CLI Audit Logs
- NTP Logs
- Auth Logs
- System Logs
- Updater Logs

Note that the TOE can also export various other log file’s audit records to an external syslog server, but these other log files do not contain logs that satisfy the TOE’s auditing requirements.

The TOE is capable of detecting when the SSH connection fails. The TOE also stores a local set of audit records on the TOE, and continues to do so if the communication with the syslog server goes down. The TOE stores the audit logs locally as configured with the logconfig command in the CLI and the Log Subscriptions page in the GUI. The size of the local log files are set by an authorized administrator using the 'Rollover by File Size' configuration setting. Once the file reaches the specified size it is sent to the syslog server using SCP. These transfers can also be configured based on configured time intervals.

If the SSH connection to the Syslog Server fails, then once the physical connection is restored, the log files will remain on the TOE. On the next SCP Push based on either the maximum log file size being exceeded or on the time interval, the current log file and the log files previously unsuccessfully transferred will be transferred.

In the event audit log storage is exhausted, then WSA will overwrite the oldest records in the audit trail, and generate an email alert to this effect and send it to an Administrator.
4.7 Inactivity Session Termination

Inactivity settings must trigger termination of the administrator session in the GUI and CLI. These settings are configurable as described in chapter "Perform System Administration Tasks", section User Network Access of [1]. Here the inactivity timeout can be set for both the GUI and CLI.

Step 1 Select System Administration > Network Access > Session Inactivity Timeout.

Step 2 Click Edit Settings.

Step 3 Enter the number of minutes users can be inactive before being logged out. You can define a timeout period between 5 and 1440 minutes.

Step 4 Submit and commit your changes.

![Network Access](image)

**Figure 6 Setting Inactivity Timeout in GUI**

Through the CLI, the adminaccessconfig > **timeout** command can be used to set the inactivity for the GUI and CLI.
Figure 7 Setting Inactivity Timeout in CLI

4.8 Product Updates
Verification of the authenticity of updated software is done in both a manual and automated manner depending on the update process chosen.

4.8.1 Online Updates
Perform an Online Update of your WSA via the GUI as described in [1] chapter “Perform System Administration Tasks” section Upgrading AsyncOS for Web”.

Perform an Online Upgrade of your WSA via the CLI using the System Administration > System Upgrade commands.
WSA automatically compares the hash received via the configuration file to the hash computed for the product update using SHA-384. If there is a checksum mismatch, the update will not be installed. Attempts to perform an illegitimate update onto the system will be logged into updater logs at INFO level. The sample log line will look as follows:

```
Wed Dec 11 05:50:07 2013 Info: repeng SHA384 Mismatch
```

After performing the update process, the administrator must confirm the software version the TOE is running. This can be accomplished by using the “version” command via the CLI to display the currently running system image filename and the system software release version.

### 4.8.2 Offline Updates

See Appendix A.

### 5 Obtaining Documentation, Support & Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


To find an HTML or PDF version of many Cisco titles go to www.cisco.com. Type the title in the ‘Search’ field and click **Go**.
6 Security Relevant Events

WSA is able to generate audit records that are stored internally within the TOE whenever an audited event occurs, as well as simultaneously offloaded to an external syslog server. The details for protection of that communication are covered in section 4.6.

WSA can generate many types of logs, recording varying types of information. Log files contain the records of regular activity and errors from various components of the system. A log subscription associates a log type with a name, logging level, and other constraints such as size and destination information; multiple subscriptions for the same log type are permitted.

The log type indicates what information will be recorded within the generated log such as message data, system statistics, binary, or textual data. An authorized administrator selects the log type when creating a log subscription. See chapter "Monitor System Activity Through Logs", section Adding and Editing Log Subscriptions [1].

To prevent log files on the appliance from becoming too large, AsyncOS performs a “rollover” and archives a log file when it reaches a user-specified maximum file size or time interval and creates a new file for incoming log data. Based on the retrieval method defined for the log subscription, the older log file is stored on the appliance for retrieval or delivered to an external computer. In the evaluated configuration, SCP Push must be configured see section 4.6 for more information.

The table below include the security relevant events that are applicable to the TOE. Table 7: General Auditable Events includes general applicable events.

Deleting Audit Records

Audit logs cannot directly be deleted through the administrator interfaces. To remove a log subscription, the logconfig command in the CLI or Log Subscriptions page on the System Administration menu can be used. See chapter "Monitor System Activity Through Logs", section Adding and Editing Log Subscriptions for more information.

The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table below). Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited.

The local audit trail consists of the individual audit records; one audit record for each event that occurred. The audit fields in each audit event will contain at a minimum the following:

Example Audit Event:

Date: Dec 1
Time: 21:37:18
Type of event: Info
**Subject identity:** Available when the command is run by an authorized TOE administrator user such as “User admin”. In cases where the audit event is not associated with an authorized user, an IP address may be provided for the Non-TOE endpoint and/or TOE.

**Outcome (Success or Failure):** Success may be explicitly stated with “success” or “passed” contained within the audit event or is implicit in that there is not a failure or error message. More specifically for failed logins, a “Login failed” will appear in the audit event. For successful logins, a “Login success” will appear in the associated audit event. For failed events “failure” will be denoted in the audit event. For other audit events a detailed description of the outcome may be given in lieu of an explicit success or failure. For example, for an IPsec session where the lifetime of the SA has expired a detailed description is given in the associated audit event: “SA lifetime threshold reached, expiring in 1412 seconds.”

**Additional Audit Information:** As described in Column 3 of Table 7 below.

As noted above, the information includes at least all of the required information. Example audit events are included in Table 7 below. The auditable events that result from administrative actions are included in Table 9 and are designated with “Administrative Event” within the Auditable Events column.

**Table 7: General Auditable Events**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
<th>Sample Log</th>
</tr>
</thead>
</table>
| FAU_GEN.1   | Administrative Actions: Configuration of Log Subscriptions. Changing logging settings. Clearing logs. | None | 1. Logs for startup and shutdown of auditing on WSA  
Tue Oct 23 22:34:36 2012 Info: System is shutting down.  
Tue Oct 23 22:13:33 2012 Info: System is coming up. |
|             |                  |                                  | 2. Logs for user activities performed on GUI on WSA  
Thu Nov 1 19:03:00 2012 Info: login:10.65.79.90 user:admin session:XtL50wp9GB92YyjVerYb  
Thu Nov 1 19:03:00 2012 Info: req:10.65.79.90 userid:XtL50wp9GB92YyjVerYb 303 POST /login HTTP/1.1 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.94 Safari/537.4 | |
|             |                  |                                  | 3. Logs for an interactive session being unlocked at GUI on WSA.  
Thu Nov 1 18:38:30 2012 Info: Session JwfASs1C35u8cxk4K0Lb user:admin expired  
Thu Nov 1 18:44:47 2012 Info: req:10.65.79.90 userid:kwrhGldJwOpcAt8TU3K 200 POST /login HTTP/1.1 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.94 Safari/537.4  
Thu Nov 1 18:44:48 2012 Info: login:10.65.79.90 | |
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
<th>Sample Log</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>user:admin session:kwrkGIJwOpcAl8TU3K</td>
</tr>
</tbody>
</table>

**Administrative Actions:**

Choose the operation you want to perform:
- NEW - Create a new log
- EDIT - Modify a log subscription
- DELETE - Remove a log subscription
- SETUP - General settings
- LOGHEADERS - Configure headers to log
- HOSTKEYCONFIG - Configure SSH host keys


Fri Aug 24 08:20:21 2012 Info: PID 3126: User admin entered 'mycli'; prompt was 'Please enter the name for the log:

Fri Aug 24 08:20:22 2012 Info: PID 3126: User admin entered ''; prompt was 'Choose the method to retrieve the logs:

Fri Aug 24 08:20:23 2012 Info: PID 3126: User admin entered ''; prompt was 'Filename to use for log files:

Fri Aug 24 08:20:24 2012 Info: PID 3126: User admin entered ''; prompt was 'Please enter the maximum file size. You can specify suffixes: "m" for megabytes, "k" for kilobytes. Suffixes are case-insensitive:

Fri Aug 24 08:20:24 2012 Info: PID 3126: User admin entered ''; prompt was 'Should an alert be sent when files are removed due to the maximum number of files allowed? [N]

Fri Aug 24 08:20:27 2012 Info: PID 3126: User admin entered 'n'; prompt was 'Do you want to configure time-
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
<th>Sample Log</th>
</tr>
</thead>
</table>
|              |                 | based log files rollover? [N]> ' | Fri Aug 24 08:20:43 2012 Info: PID 3126: User admin entered 'edit'; prompt was '{nCurrently configured logs:
Log Name Log Type Retrieval Interval {n |
| FAU_STG_EXT.1 | Administrative Actions: Configuration of syslog export settings | None | Fri Aug 24 08:20:49 2012 Info: PID 3126: User admin entered '{n'; prompt was '{nChoose the method to retrieve the logs:{n1. Download Manually: FTP/HTTP(S)/SCP\n2. FTP Push\n3. SCP Push\n4. Syslog Push\n[1]> ' |
| FCS_CKM.1    | Administrative Actions: Manual key generation | None | Fri Aug 24 08:35:10 2012 Info: PID 7135: User admin entered '{n'; prompt was '{nDo you want to enable SSH on this interface? [N]> ' |
| FCS_HTTPS_EXT.1 | Failure to establish an HTTPS Session. Establishment/Termination of an HTTPS Session. | Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures. | • **On successful establishment of HTTPS session:**
Tue Nov 26 03:58:45 2013 Info: login: 10.142.40.74 user:admin session:6lqctJzHrresnF7gny. The HTTPS session has been established successfully.

- **On HTTPS session failure:**
  - Tue Nov 26 02:56:39 2013 Info: Error in https connection from host 10.142.40.74 port 51840 - (336036069, 'error:140780E5:SSL routines:SSL23_READ:ssl handshake failure')
  - On logging out from a HTTPS session:
    - Tue Nov 26 03:58:49 2013 Info: Session vODemYvihaE7WQ0ZVyRx user:admin expired
    - Tue Nov 26 03:58:49 2013 Info: logout:10.142.40.74 user:admin session6lqctJzHrresnF7gny. The HTTPS session has been terminated.
  - **On successful establishment of HTTPS session(euqgui):**
    - Tue Dec 24 08:35:54 2013 Info: login:admin user:xY7S4BlslW34AqdBjgyR session:10.21.64.11 The HTTPS session has been established successfully.
    - **On logging out from a HTTPS session(euqgui):**
      - Tue Dec 24 08:35:54 2013 Info: logout:user:xY7S4BlslW34AqdBjgyR session:10.21.64.11 The HTTPS session has been terminated. |
<p>| FCS_SSHC_EXT.1 | Failure to establish an SSH Session. Establishment/Termination of an SSH | Failure to establish a SSH Session. IP address of remote host Reason for failure. | Thu Dec 19 04:52:19 2013 Info: An authentication attempt by the user ***** from 10.76.69.125 failed using an SSH |</p>
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
<th>Sample Log</th>
</tr>
</thead>
</table>
| Session.    | Administrative Actions: | Configuration of SSH settings: including certificates or passwords, algorithms, host names, users. | Establishment of a SSH session  
- IP address of remote host  
- Thu Dec 19 04:49:42 2013 Info: The user admin successfully logged on from 10.142.40.203 using an SSH connection.  
- Termination of a SSH session.  
Thu Dec 19 02:50:37 2013 Info: PID 80360: User admin logged out of Command Line Interface  
- Administrative Actions  
Fri Aug 24 08:20:43 2012 Info: PID 3126: User admin entered 'edit'; prompt was
\nCurrently configured logs:
<table>
<thead>
<tr>
<th>Log Name</th>
<th>Log Type</th>
<th>Retrieval Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\nChoose the operation you want to perform:
\- NEW - Create a new log.  
\- EDIT - Modify a log subscription.  
\- DELETE - Remove a log subscription.  
\- SETUP - General settings.  
\- LOGHEADERS - Configure header fields to log.  
\- HOSTKEYCONFIG - Configure SSH host keys.\n| FCS_SSHS_EXT.1 | Failure to establish an SSH Session. Establishment/Termination of an SSH Session. Administrative Actions: Configuration of SSH settings: including certificates or passwords, algorithms, host names, users. | Reason for failure: Non-TOE endpoint of connection (IP address) for both successes and failures. | Failure to establish a SSH Session.  
- IP address of remote host  
- Reason for failure.  
Thu Dec 19 04:52:19 2013 Info: An authentication attempt by the user ***** from 10.76.69.125 failed using an SSH connection.  
- Establishment of a SSH session  
- IP address of remote host  
- Thu Dec 19 04:49:42 2013 Info: The user admin successfully logged on from 10.142.40.203 using an SSH connection.  
- Termination of a SSH session.  
Thu Dec 19 02:50:37 2013 Info: PID 80360: User admin logged out of Command Line Interface |
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
<th>Sample Log</th>
</tr>
</thead>
</table>
| FCS_TLS_EXT.1     | Failure to establish a TLS Session. Establishment/Termination of a TLS Session.  | Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.  | **Failure to establish a TLS Session.**  
  o IP address of remote host  
  o Reason for failure.  
Tue Nov 26 02:56:39 2013 Info: Error in https connection from host 10.142.40.74 port 51840 - (336036069, 'error:140780E5:SSL routines:SSL23_READ:ssl handshake failure')  
**Establishment of a TLS session**  
  o IP address of remote host  
Fri Dec 13 11:42:27 2013 Info: New TLS connection from 10.76.69.66 has been established successfully.  
**Termination of a TLS session.**  
Fri Dec 13 11:44:27 2013 Info: TLS connection from 10.142.40.74 has been closed.  
<ssl>  
  <ssl_inbound_method>tlsv1</ssl_inbound_method>  
  <ssl_inbound_ciphers>FIPS</ssl_inbound_ciphers>  
  <ssl_outbound_method>tlsv1</ssl_outbound_method>  
  <ssl_outbound_ciphers>FIPS:aNULL</ssl_outbound_ciphers>  
  <ssl_gui_method>tlsv1</ssl_gui_method>  
  <ssl_gui_ciphers>FIPS</ssl_gui_ciphers>  
</ssl>  
<encryption>  
  <encryption_enabled>1</encryption_enabled>  
</encryption> |
| FIA_PMG_EXT.1     | Administrative Actions: Setting length requirement for passwords.                | None.                                                                                              | XML generated by configuration change.  
  Change comment:  
  User: admin  
  Configuration changes are described as:  
  The log subscriptions for the qlogd server.  
  Product: IronPort C660 Messaging Gateway(tm) Appliance  
  Model Number: C660  
  Version: 7.5.2-017  
  Serial Number: 002219240BBE-BQXFLJ1  
  Number of CPUs: 2  
  Memory (GB): 4  
  Current Time: Sat Aug 25 01:11:45 2012 |
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
<th>Sample Log</th>
</tr>
</thead>
</table>
| FIA_UIA_EXT.1     | All use of the identification and authentication mechanism.                       | Provided user identity, origin of the attempt (e.g., IP address).                                  | • **Successful Login from Serial Port/Console:**
Wed Jan 29 10:49:28 2014 Info: The user admin successfully logged on from cuau0  

• **Failed Login from Serial Port/Console:**
Wed Jan 29 10:51:02 2014 Info: An authentication attempt by the user ***** from cuau0 failed  
(For all authentication attempts via serial/console port, there will be no IP information that will be logged.)  

• **Successful login from GUI:**
Tue Nov 26 11:26:48 2013 Info: The user admin successfully logged on from 10.142.40.203 using an HTTPS connection.  

• **Failed login attempt from GUI:**
Tue Nov 26 11:27:12 2013 Info: An authentication attempt by the user admin from 10.142.40.203 failed.  

See FCS_SSH_EXT.1 for remote CLI login audit events. |
| FIA_UAU_EXT.2     | All use of the authentication mechanism.                                          | Origin of the attempt (e.g., IP address).                                                        | See FIA_UIA_EXT.1 for sample logs for serial port/console and GUI  

See FCS_SSH_EXT.1 for remote CLI login audit events. |
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
<th>Sample Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIA_X509_EXT.1</td>
<td>Unsuccessful attempt to validate a certificate</td>
<td>Reason for failure</td>
<td></td>
</tr>
<tr>
<td>FMT_MOF.1 (1)/TrustedUpdate</td>
<td>Any attempt to initiate a manual update</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>FMT_MTD.1</td>
<td>Administrative Actions: See all other rows in table.</td>
<td>None</td>
<td>See all other rows in table.</td>
</tr>
<tr>
<td>FMT_SMF.1</td>
<td>Administrative Actions: See all other rows in table.</td>
<td>None</td>
<td>See all other rows in table.</td>
</tr>
<tr>
<td>FMT_SMR.2</td>
<td>Administrative Actions: Configuring administrative users with specified roles.</td>
<td>None</td>
<td>XML generated by configuration change.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Change comment:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User: admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuration changes are described as:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The log subscriptions for the qlogd server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Product: IronPort C660 Messaging Gateway(tm) Appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Model Number: C660</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Version: 7.5.2-017</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Serial Number: 002219240BEEE-BQXFLJ1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Number of CPUs: 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Memory (GB): 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Current Time: Sat Aug 25 01:11:45 2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;users&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;user&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;username&gt;admin&lt;/username&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;fullname&gt;Administrator&lt;/fullname&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;group&gt;admin&lt;/group&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;enc_password&gt;*****&lt;/enc_password&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;last_passwd_change&gt;1&lt;/last_passwd_change&gt;</td>
</tr>
<tr>
<td>Requirement</td>
<td>Auditable Events</td>
<td>Additional Audit Record Contents</td>
<td>Sample Log</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------</td>
<td>----------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;ignore_pw_expiration&gt;0&lt;/ignore_pw_expiration&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;lock_reason&gt;&lt;/lock_reason&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;delegated_id&gt;None&lt;/delegated_id&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;/user&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;/users&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;matched_content_visibility&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;group&gt;admin&lt;/group&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;group&gt;cloudadmin&lt;/group&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;group&gt;delegatedadmin&lt;/group&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;group&gt;helpdesk&lt;/group&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;group&gt;operators&lt;/group&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;group&gt;readonly&lt;/group&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;/matched_content_visibility&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;feature_key_status&gt;0&lt;/feature_key_status&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;information_upload_error&gt;&lt;/information_upload_error&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;core_watch_enabled&gt;1&lt;/core_watch_enabled&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;timezone&gt;America/Los_Angeles&lt;/timezone&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;admin_access&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;admin_acl&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;admin_acl_action&gt;allowall&lt;/admin_acl_action&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;admin_acl_allow_list&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;/admin_acl_allow_list&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;admin_acl_proxy_list&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;/admin_acl_proxy_list&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;admin_acl_origin_ip_header&gt;x-forwarded-for&lt;/admin_acl_origin_ip_header&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;/admin_acl&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;admin_login_banner&gt;&lt;/admin_login_banner&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;/admin_access&gt;</td>
</tr>
<tr>
<td>Requirement</td>
<td>Auditable Events</td>
<td>Additional Audit Record Contents</td>
<td>Sample Log</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------</td>
<td>----------------------------------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| FPT_STM.1   | Changes to the time.  
Administrative Actions:  
Manual changes to the system time.  
Changes to NTP settings. | The old and new values for the time.  
Origin of the attempt (e.g., IP address). | - **Manual Clock update via CLI:**  
Thu Dec 19 10:16:00 2013 Info: PID 16996: User admin entered 'User admin connected from remote ip 10.76.69.46 updated time from Thu Dec 19 09:46:54 2013 GMT to Thu Dec 19 15:16:00 2013 GMT  
- **Manual update from WebUI:**  
- **NTP changing the time:**  
Thu Dec 19 15:20:20 2013 Info: The system time was changed from Thu, 19 Dec 2013 10:18:42 to Thu, 19 Dec 2013 15:20:20 using information from 10.142.41.203. |
| FPT_TUD_EXT.1 | Administrative Actions:  
Initiation of update. | No additional information. | **Accepted Update:**  
* Fri May 9 15:01:14 2014 Debug: Acquiring dynamic manifest from stage-updates.ironport.com:443  
Fri May 9 15:01:14 2014 Debug: Sending client manifest: <?xml version="1.0" encoding="iso-8859-1"?>  
Fri May 9 15:01:14 2014 Debug: Network Participation: Attempting to connect to host: stage-updates.ironport.com port: 443  
Fri May 9 15:01:15 2014 Debug: Network Participation: Successfully connected to host: stage-updates.ironport.com port: 443  
<br>\n
<sha384>d696f0391f33a371685ba360cf292e922ef31f8f355dc7dd600f60cc3230baa614297a94e5fe0a46195b3e3762e079a9ff5</sha384>  

<path>case/1.0/case/default/1391719393485731</path>  
<scheme>http</scheme>  
<server>stage-updates.ironport.com</server>  
<server2>stage-updates.ironport.com</server2>  
<display_version>3.3.1-009</display_version>  
<application allow_from="7d27487716b7b8127c33c8930de0544537210931b39ad8360816c856888e5090937750718dh8d4d52e5a3f927c8b6ec4f696132c13fabae0942e65d757a1b78c519307a4910b20b20e7f797bade66755d9e14e372885e4f4a26fd1b777b4bda1f8bdecf055c555b00f4433ca9558ab989e566dc3351a612e1f23ab906954b08889c3f7fe0c799f711cc9e1a90d7a4b1de0c26df66fe2a746dbfd055bca691f3422b59a213ef24df5a921f8b04a4a044f1c7756e3134d8a427fc6a5" name="mcafee" version="5">
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
<th>Sample Log</th>
</tr>
</thead>
</table>
|             |                 |                                  | Fri May 9 15:01:17 2014 Info: Acquired server manifest, starting update 2  
Fri May 9 15:01:17 2014 Info: Server manifest specified an update for case |
|             |                 |                                  | **Rejected update:**  
Fri May 9 15:08:30 2014 Debug: Network Participation: Attempting to connect to host:  
updater01.ibqa.sgg.cisco.com port: 443  
Fri May 9 15:08:30 2014 Debug: Network Participation: Successfully connected to host:  
updater01.ibqa.sgg.cisco.com port: 443  
Fri May 9 15:08:30 2014 Info: The manifest was malformed.  
Fri May 9 15:09:30 2014 Debug: Skipping update request for "cloudmark"  
Fri May 9 15:09:30 2014 Debug: dlp updates disabled  
Fri May 9 15:09:30 2014 Debug: Skipping update request for "dlp" |
| FTA_SSL_EXT.1 | Any attempts at unlocking of an [local] interactive session.  
Administrative Actions:  
Specifying the inactivity time period. | No additional information. | **When user is logged out of CLI session because of inactivity timeout:**  
**Unlocking of an [local] interactive session:**  
See FIA_UIA_EXT.1 for sample logs for serial port/console  
**Administrator Action:**  
<?xml version="1.0" encoding="ISO-8859-1"?>  
<!DOCTYPE config SYSTEM "config.dtd">  
<!--  
XML generated by configuration change.  
Change comment:  
User: admin  
Configuration changes are described as:  
The log subscriptions for the qlogd server.  

Product: IronPort C660 Messaging Gateway(tm) Appliance -->
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
<th>Sample Log</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Model Number: C660</td>
<td>&lt;account_policies&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Version: 7.5.2-017</td>
<td>&lt;enable_failed_login_lock&gt;0&lt;/enable_failed_login_lock&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Serial Number: 002219240BBE-BQXFLJ1</td>
<td>&lt;account_lock_threshold&gt;5&lt;/account_lock_threshold&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of CPUs: 2</td>
<td>&lt;display_account_locked_message&gt;0&lt;/display_account_locked_message&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory (GB): 4</td>
<td>&lt;account_locked_message&gt;Your account is not available due to administrative action. Please contact your Administrator.&lt;/account_locked_message&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Current Time: Sat Aug 25 01:11:45 2012</td>
<td>&lt;force_pw_change_on_admin_reset&gt;0&lt;/force_pw_change_on_admin_reset&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;enable_password_expiration&gt;0&lt;/enable_password_expiration&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;password_expiration_period&gt;90&lt;/password_expiration_period&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;enable_password_expiration_warning&gt;0&lt;/enable_password_expiration_warning&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;password_expiration_warning_period&gt;14&lt;/password_expiration_warning_period&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;/account_policies&gt;</td>
</tr>
<tr>
<td>FTA_SSL.3</td>
<td>The termination of a remote session by the session locking mechanism. Administrative Actions: Specifying the inactivity time</td>
<td>No additional information.</td>
<td>* When user is logged out of WebUI session because of inactivity timeout: Tue Dec 3 05:42:44 2013 Info: User admin logged out from session rVXB6Wi7TpnS4BO3tbGV because of inactivity timeout. <strong>Administrator Action:</strong> See FTA_SSL_EXT.1 sample logs</td>
</tr>
<tr>
<td>Requirement</td>
<td>Auditable Events</td>
<td>Additional Audit Record Contents</td>
<td>Sample Log</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------</td>
<td>-------------------------------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| FTA_SSL.4   | The termination of an interactive session. Administrative Action: Logging out of TOE. | No additional information. | • Audit record generate when admin logs out of CONSOLE.  
  • CLI Logout of admin:  
    Thu Nov 1 18:52:30 2012 Info: PID 21630: User admin entered '<EOF>'; prompt was 'c660q04.ibqa>'  
    Thu Nov 1 18:52:30 2012 Info: PID 21630: User admin logged out of CLI session  
  • Audit record generated when the admin logs out of Web UI:  
    Thu Nov 1 18:45:19 2012 Info: logout:10.65.79.90 user:admin session:kwRhhGlJwOpcAl8TU3K |
| FTA_TAB.1   | Administrative Action: Configuring the banner displayed prior to authentication. | None | XML generated by configuration change.  
  Change comment:  
  User: admin  
  Configuration changes are described as:  
  The log subscriptions for the qlogd server.  
  Product: IronPort C660 Messaging Gateway(tm) Appliance  
  Model Number: C660  
  Version: 7.5.2-017  
  Serial Number: 002219240BBE-BQXFLJ1  
  Number of CPUs: 2  
  Memory (GB): 4  
  Current Time: Sat Aug 25 01:11:45 2012  
  <admin_access>  
    <admin_acl>  
      <admin_acl_action>allowall</admin_acl_action>  
      <admin_acl_allow_list>  
        </admin_acl_allow_list>  
      <admin_acl_proxy_list>  
        </admin_acl_proxy_list>  
    </admin_acl>  
    <admin_login_banner></admin_login_banner>  
  </admin_access> |
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
<th>Sample Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP_ITC.1</td>
<td>Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.</td>
<td>Identification of the initiator and target of failed trusted channels establishment attempt.</td>
<td>AUDIT: See logs provided in FCS_TLS_EXT.1, FCS_SSH_EXT.1</td>
</tr>
<tr>
<td>FTP_TRP.1</td>
<td>Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions. Administrative Action: Connecting to the TOE with SSH/TLS</td>
<td>Identification of the claimed user identity.</td>
<td>AUDIT: See logs provided in FCS_TLS_EXT.1, FCS_SSH_EXT.1</td>
</tr>
</tbody>
</table>
## 7 Network Services and Protocols

The table below lists the network services/protocols available on the Web Security Appliance as a client (initiated outbound) and/or server (listening for inbound connections), all of which run as system-level processes. The table indicates whether each service or protocol is allowed to be used in the certified configuration.

<table>
<thead>
<tr>
<th>Service or Protocol</th>
<th>Description</th>
<th>Client (initiating)</th>
<th>Allowed</th>
<th>Server (terminating)</th>
<th>Allowed</th>
<th>Allowed use in the certified configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No restrictions.</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>n/a</td>
<td>No restrictions.</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>n/a</td>
<td>Use SCP or HTTPS instead.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
<td>Yes</td>
<td>For OCSP or copy</td>
<td>Yes</td>
<td>No</td>
<td>Used implicitly for OCSP. For other HTTP functions, such as “copy”, recommend using HTTPS instead, or tunneling through IPsec.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No restrictions.</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No restrictions.</td>
</tr>
<tr>
<td>IMAP4S</td>
<td>Internet Message Access Protocol Secure version 4</td>
<td>Yes</td>
<td>Over TLS</td>
<td>No</td>
<td>n/a</td>
<td>No restrictions.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
<td>Yes</td>
<td>Over IPsec</td>
<td>No</td>
<td>n/a</td>
<td>Use LDAP-over-SSL instead.</td>
</tr>
<tr>
<td>LDAP-over-SSL</td>
<td>LDAP over Secure Sockets Layer</td>
<td>Yes</td>
<td>Over TLS</td>
<td>No</td>
<td>n/a</td>
<td>If used for authentication of TOE users, configure TLS as described in section 4.1.5 of this document.</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>n/a</td>
<td>Any configuration. Use of key-based authentication is recommended.</td>
</tr>
<tr>
<td>POP3S</td>
<td>Post Office Protocol version 3 over TLS</td>
<td>Yes</td>
<td>Over TLS</td>
<td>No</td>
<td>n/a</td>
<td>Configure TLS as described in section4.1.5 of this document.</td>
</tr>
<tr>
<td>Service or Protocol</td>
<td>Description</td>
<td>Client (initiating)</td>
<td>Allowed</td>
<td>Server (terminating)</td>
<td>Allowed</td>
<td>Allowed use in the certified configuration</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------</td>
<td>---------------------</td>
<td>--------</td>
<td>----------------------</td>
<td>--------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>n/a</td>
<td>If used for authentication of TOE users, secure through TLS.</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure Copy Protocol over SSH</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Configure SSH as described in section 4.1.4 of this document.</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>n/a</td>
<td>Recommended to use SMTPS instead.</td>
</tr>
<tr>
<td>SMTPS</td>
<td>SMTP over TLS</td>
<td>Yes</td>
<td>Over TLS</td>
<td>No</td>
<td>n/a</td>
<td>Configure TLS as described in section 4.1.5 of this document.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
<td>Yes (snmp-trap)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Outbound (traps) only. Recommended to tunnel through IPsec.</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>As described in the section 4.1.4 of this document.</td>
</tr>
<tr>
<td>SSL (not TLS)</td>
<td>Secure Sockets Layer</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Use TLS instead.</td>
</tr>
<tr>
<td>Telnet</td>
<td>A protocol used for terminal emulation</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Use SSH instead.</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>As described in the section 4.1.5 of this document.</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>n/a</td>
<td>Recommend using SCP or HTTPS instead.</td>
</tr>
</tbody>
</table>

The table above does not include the types of protocols and services listed here:

- OSI Layer 2 protocols such as CDP, VLAN protocols like 802.11q, Ethernet encapsulation protocols like PPPoE, etc. The certified configuration places no restrictions on the use of these protocols; however evaluation of these protocols was beyond the scope of the Common Criteria product evaluation. Follow best practices for the secure usage of these services.

- Protocol inspection engines that can be enabled with “inspect” commands because inspection engines are used for filtering traffic, not for initiating or terminating sessions, so they’re not considered network ‘services’ or ‘processes’ in the context of this table. The certified configuration places no restrictions on the use protocol inspection functionality; however evaluation of this functionality was beyond the scope of the Common Criteria product evaluation. Follow best practices for the secure usage of these services.
8 Modes of Operation

WSA has several modes of operation, these modes are as follows:

**Booting** – while booting, WSA does not allow access to the administrator interfaces until the WSA image and configuration has loaded. This mode of operation automatically progresses to the Normal mode of operation.

**Normal** - The WSA image and configuration is loaded and WSA is operating as configured. It should be noted that all levels of administrative access occur in this mode and that all WSA based security functions are operating while operating WSA has little interaction with the administrator.

Following operational error, the TOE reboots (once power supply is available) and enters booting mode. The only exception to this is if there is an error during the Power on Startup Test (POST) during bootup, then the TOE will shutdown. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen, and saved in the crashinfo file. Within the POST, self-tests for the cryptographic operations are performed.

The following POST tests are performed:

- AES Known Answer Test (Separate encrypt and decrypt)
- DRBG Known Answer Tests
  - HASH_DRBG Known Answer Test
  - HMAC_DRBG Known Answer Test
  - CTR_DRBG Known Answer Test
- HMAC Known Answer Tests
  - HMAC-SHA1 Known Answer Test
- ECC CDH KAT
- RSA Known Answer Test (Separate sign and verify)
- SHA-1 Known Answer Test
- Software Integrity Test (HMAC-SHA1)

If any of the POST fail, the following actions should be taken:

- If possible, review the crashinfo file. This will provide additional information on the cause of the crash
- Restart the TOE to perform POST and determine if normal operation can be resumed
- If the problem persists, contact Cisco Technical Assistance via [http://www.cisco.com/techsupport](http://www.cisco.com/techsupport) or 1 800 553-2447
- If necessary, return the TOE to Cisco under guidance of Cisco Technical Assistance.
9  Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions, and adheres to the environment security objectives listed below. The environment security objective identifiers map to the environment security objectives as defined in the Security Target.

Table 9  Operational Environment Security Measures

<table>
<thead>
<tr>
<th>Environment Security Objective</th>
<th>IT Environment Security Objective Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>OE_PHYSICAL</td>
<td>Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.</td>
</tr>
<tr>
<td>OE_NO_GENERAL_PURPOSE</td>
<td>There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.</td>
</tr>
<tr>
<td>OE_NO_THRU_TRAFFIC_PROTECTION</td>
<td>The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.</td>
</tr>
<tr>
<td>OE_TRUSTED_ADMIN</td>
<td>TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.</td>
</tr>
<tr>
<td>OE_UPDATES</td>
<td>The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.</td>
</tr>
<tr>
<td>OE_ADMIN_CREDENTIALS_SECURE</td>
<td>The administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.</td>
</tr>
</tbody>
</table>

10  Related Documentation

Use this document in conjunction with the WSA User Guide documentation at the following location:


Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

10.1  World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following site: [http://www.cisco.com](http://www.cisco.com)

10.2  Ordering Documentation

Cisco documentation is available in the following ways:
Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:


Registered Cisco.com users can order or download the Documentation through the online Subscription Store:

http://www.cisco.com

Non-registered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS (6387).

10.3 Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

11 Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.
To access Cisco.com, go to the following website:

http://www.cisco.com
12 Appendix A

Under certain circumstances, as in the case where customer networks are not connected to the public Internet, Cisco has an optional configuration to support local (or “offline”) updates to those appliances.

Using this local/off-line service, the Cisco Content Security appliances can retrieve needed update data and AsyncOS upgrades from a local source without requiring access to the public Internet.

This document is intended for Cisco Systems customers who require the use of this service configuration and is presented as a guide to deploy the service and to assist in the configuration for the most common scenarios.

12.1 Components

The offline updater consists of two parts. Part one is the updater service requestor (ipClient) that resides on a Linux host connected to the public Internet. There are 4 files associated with this part: the update script, ipClient-v9.pl for setting the proxy and urls, the equipment and licensed services list, and the required PKI certificate.

Part two is the customer network facing the update server that runs in the customer network and which Cisco Content Security servers are configured to receive updates and upgrades from.

Local-Updates / Updater Flow

![Local-Updates / Updater Flow Diagram]

Figure 8 Offline Update Details
The offline updater tool (ipClient) is designed to emulate the Cisco Content Security appliance update and upgrade mechanisms by querying the production Cisco Updater Service and then downloading updates for the local update feature.

The offline updater tool (ipClient) is currently written in Perl and all necessary Perl modules must be installed on the Internet facing host before the tool will run properly.

### 12.2 Order of Operations

1) The offline updater tool iterates through a list of models and asks for a server update and upgrade manifest request for each serial or VLN provided in the equipment list.

2) The offline updater tool uses a PKI Certificate to authenticate and make https requests to the hosted Cisco Updater Service. For valid requests the tool receives a server manifest request back from the Cisco Updater Service.

3) The tool reads the Server Manifest for location of the update files and downloads them.

4) The offline updater tool checks to verify the downloaded file by using the sha-384 checksum it received in Server Manifest against the one it generates to see if they match, if they don’t match the update file is deleted.

5) For easy transport of the smaller application “updates” between the unsecure and secure networks, the tool bundles all downloaded updates into a compressed file called Application.tar. This action is not performed for asyncos “upgrades” but these can be copied and transported as needed. This is just an artifact of this tool’s development history and there is no special reason for the different behavior.

6) The Application.tar and/or the Asyncos upgrades file can be copied via CD/DVD or USB to the appliance in a secure manner.

Notes: The offline updater tool uses a log feature to log responses received from the Cisco Updater Service.

All the Content Security Server Manifests received from the Updater are stored in the /manifest directory.

The ipClient-config file is used to set the HTTP Proxy (if necessary), Base Path, Updater URL, Port and Certification path Location.
12.3 System Prerequisites

12.3.1 Public Internet facing Host

The public Internet facing host should be running Linux kernel b3.5.0-17-generic. The Ubuntu 64 bit Linux OS was used for testing, though any variant should work provided all necessary perl modules are loaded.

Perl Modules required and installed using a terminal shell:

- Ubuntu Linux server
  
  ```bash
  sudo apt-get install libconfig-tiny-perl
  sudo apt-get install libanyevent-dbi-perl
  sudo apt-get install liblwp-protocol-https-perl
  sudo apt-get install libxml-opml-simplegen-perl
  sudo apt-get install libdbd-csv-perl
  sudo apt-get install libanyevent-db-dbd-pg-perl
  sudo apt-get install libwww-perl
  ```

LWP::UserAgent;
LWP::Simple;
XML::Simple;
Compress::Zlib;
DBI;
Getopt::Long;
Config::Tiny;
Digest::MD5;
Net::SSLey
IO::Socket::SSL

12.3.2 Private Network Facing Host

The host on the customer network should be running Apache and Perl. Linux Ubuntu 64 bit was used for testing, although other variants should work. The Apache configuration requires the following modules:

Architecture: 64-bit
Server MPM: Prefork
threaded: no
forked: yes (variable process count)

Server compiled with:

-D APACHE_MPM_DIR="server/mpm/prefork"
-D APR_HAS_SENDFILE
-D APR_HAS_MMAP
-D APR_HAVE_IPV6 (IPv4-mapped addresses enabled)
-D APR_USE_SYSVSEM_SERIALIZE
-D APR_USE_PTHREAD_SERIALIZE
-D APR_HAS_OTHER_CHILD
-D AP_HAVE_RELIABLE_PIPED_LOGS
-D DYNAMIC_MODULE_LIMIT=128
-D HTTPD_ROOT="/etc/apache2"
-D SUEXEC_BIN="/usr/lib/apache2/suexec"
-D DEFAULT_PIDLOG="/var/run/apache2.pid"
-D DEFAULT_SCOREBOARD="logs/apache_runtime_status"
-D DEFAULT_LOCKFILE="/var/run/apache2/accept.lock"
-D DEFAULT_ERRORLOG="logs/error_log"
-D AP_TYPES_CONFIG_FILE="mime.types"
-D SERVER_CONFIG_FILE="apache2.conf"

To use the transport perl script, load these perl modules using sudo: sudo apt-get install libbencode-perl
sudo apt-get install libconfig-tiny-perl sudo apt-get install libanyevent-dbi-perl
sudo apt-get install liblwp-protocol-https-perl sudo apt-get install libxml-opml-simplegen-perl sudo apt-get install libdbd-csv-perl
sudo apt-get install libanyevent-db-announce-perl sudo apt-get install libwww-perl
12.4 Tool Installation

12.4.1 Public Internet Facing Host

- Create all the directories below using root. The script will deal with creating the specific package directories (i.e., ASYN COS, CASE, etc)
  /chosen installation directory/ipclient
  /chosen installation directory/ipclient/logs
  /chosen installation directory/ipclient/cert
  /chosen installation directory/ipclient/httpd
  /chosen installation directory/ipclient/httpd/manif ests
  /chosen installation directory/ipclient/DATABASE
  /chosen installation directory/ipclient/transferPackage

- Create a user called ipClient
- Copy the ipClient.pl, equipment, and ipClient.config files into the home directory for that user.

NOTE: The script can be executed from any given directory, /chosen installation directory/ipclient is only an example.

12.4.2 Customer Private Network Host

The server side script will populate the app directories and AsyncOS builds into /var/www/

(Please edit the updater.cgi script if you wish to use different directories.)

Using root, create the directories below:
  /chosen installation directory/ipclient/updater
  /chosen installation directory/ipclient/updater/logs
  /chosen installation directory/ipclient/updater/transferPackage

NOTE: The script can be executed from any given directory, since the script will write to the base directory of Apache, /var/www, the user that runs the script needs to have read/write rights to the www directory.
12.5 Tool Configuration

12.5.1 Public Internet Facing Host

1) Modify the Equipment file in <BasePath>/DATABASE to include all customer necessary information. A sample equipment file is listed below, this file is located under <BasePath>/DATABASE. It has all the data of the appliances or LVN that are located in the secure facility. ipClient uses this to make a request to the Ironport Updater and in return receives a Server Manifest.

- **type**: can only be **serials** or **vln**.
- **serial_number**: can be a single or multiple full serial numbers for either a VLN or appliance separated by a pipe (|).
  - **Serial number**: physical appliances
  - **VLN numbers**: Virtual Email or Web appliances
- **model**: holds the model number for the appliance
- **applications**: is the list of applications that are on that appliance or VLN separated by a pipe (|).
- **version**: is the version or tag release of the appliance or VLN

Sample Customer Equipment list entries

```plaintext
 type,serial_number,model,applications,version
serials,xyz123xyw-123456,C170,case|cloudmark|mcafee|postx|sophos|timezones,phoebe-7-6-1-022
serials,xyz123xyw-123456,C160,case|cloudmark|mcafee|postx|sophos|timezones,phoebe-7-6-1-022
serials,xyz123xyw-123456,C360,repeng|case,phoebe-8-0-0-671 vln,VLNWSA1111,S660,wbrs,coeus-7-5-0-101
```

2) Modify the ipclient-config file as necessary to conform to the customer host specific environment.

3) Open the PKI Certificate file delivered to the customer and copy the key section into a file named to match the parameters defined in the ipClient-config file. Copy the Certificate component of the file into a file named to match the parameters in the ipClient-config file.

```
CERTIFICATE_PATH=/usr/cert/CustomerCertificate.crt
CERTIFICATE_KEY=/usr/cert/Customerkeys.key
```
Configuration file is used to setup the ipClient tool on the Internet Facing Host. Below is the sample configuration these need to set up accordingly.

**HTTP_PROXY** declares the proxy url
HTTP_PROXY=proxy_example.com

**HTTP_PROXY_PORT**
Proxy Port to use
HTTP_PROXY_PORT=80

**UPDATE_SERVER** is for the url for the target Cisco Updater Service. UPDATE_SERVER=update-manifests.sco.cisco.com

**PORT** is port number to use for Cisco Updater Server. PORT=443

**Directory Structure**
**BASE_PATH** is the base directory for all the files and folders. BASE_PATH=/usr/ipclient
Below are calculated paths, these should not be changed since they fall under the BASE_PATH.
LOG_PATH=/logs
DATABASE=/DATA
BASE
MANIFEST_PATH=/httpd/manifests
HTTPD_PATH=/httpd

**CERTIFICATE_PATH** and **CERTIFICATE_KEY** are the full path to the certificate and key files used to authenticate with the Cisco Update Server.

CERTIFICATE_PATH=/usr/cert/CustomerCertificate.crt
CERTIFICATE_KEY=/usr/cert/Customerkeys.key
NUMBEROFRETRIES declares the number of times to try getting the Server Manifests before giving up.

NUMBEROFRETRIES=2

NUMBEROFFILERETRIES declares the number of times to try downloading the file before giving up.

NUMBEROFFILERETRIES=4

Notes: All downloaded updates are stored in the folder <BasePath>/httpd
Manifests are in the directory <BasePath>/httpd/manifests
Once all the updates are downloaded ipClient tool bundles them all up into the Application.tar file and places it into /transferPackage directory.

12.5.2 On the Customer Private Network Server

1) Modify the processuploads.pl script to match customer Apache directory structure as necessary

12.6 On the Customer Private Network Content Security Appliances

Customer Content Security Appliance configurations:

Using the CLI>updateconfig command, point the appliances to the internal local update/upgrade server

12.7 Cisco WSA

Service (images): Update URL:

<table>
<thead>
<tr>
<th>Feature Key updates</th>
<th>http://Private_Update_Server_IP:80/asyncos</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Anti-Virus definitions</td>
<td>http://Private_Update_Server_IP:80</td>
</tr>
<tr>
<td>RSA DLP Engine Updates</td>
<td>http://Private_Update_Server_IP:80</td>
</tr>
<tr>
<td>PXE Engine Updates</td>
<td>http://Private_Update_Server_IP:80</td>
</tr>
<tr>
<td>Cloudmark SP Engine Updates</td>
<td>http://Private_Update_Server_IP:80</td>
</tr>
</tbody>
</table>
Sophos Anti-Virus definitions http://Private Update
Server IP:80 Intelligent Multi-Scan rules http://Private Update
Server IP:80 Outbreak Filters rules http://Private Update
Server IP:80 Timezone rules http://Private Update
Server IP:80


IMS Secondary Service rules
Cloudmark SP Edition rules
Service (list): Update URL:
------------------------------------------------------------------------------
McAfee Anti-Virus definitions http://Private Update
Server IP:80/manifests/C100.phoebe-9-1-0-671.updates_manifest.xml
RSA DLP Engine Updates http://Private Update
Server IP:80/manifests/C100.phoebe-9-1-0-671.updates_manifest.xml
PXE Engine Updates http://Private Update
Server IP:80/manifests/C100.phoebe-9-1-0-671.updates_manifest.xml
Cloudmark SP Engine Updates http://Private Update
Server IP:80/manifests/C100.phoebe-9-1-0-671.updates_manifest.xml
Sophos Anti-Virus definitions http://Private Update
Server IP:80/manifests/C100.phoebe-9-1-0-671.updates_manifest.xml
IronPort Anti-Spam rules http://Private Update
Server IP:80/manifests/C100.phoebe-9-1-0-671.updates_manifest.xml
Intelligent Multi-Scan rules http://Private Update
Server IP:80/manifests/C100.phoebe-9-1-0-671.updates_manifest.xml
Outbreak Filters rules http://Private Update
Server IP:80/manifests/C100.phoebe-9-1-0-671.updates_manifest.xml
Timezone rules http://Private Update
Server IP:80/manifests/C100.phoebe-9-1-0-671.updates_manifest.xml

Service (list): Update URL:
------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades http://Private Update
Server IP:80/manifests/C100.phoebe-9-1-0-671.upgrades_manifest.xml

Update interval: 5m

Proxy server: not enabled
HTTPS Proxy server: not enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.

12.8 Executing updates - Order of operation and commands to perform

Scripts can be executed from the command prompt or the customer can have a crontab set up in linux to execute it on a configurable basis that satisfies the customer requirement.

12.8.1 Command Prompt to execute the script on the Public Internet Facing Host

12.8.1.1 For Apps Updates
perl ipClient-v9.pl --apps

12.8.1.2 For Asyncos Upgrades
perl ipClient-v9.pl --asyncos

After the ipClient tool has run and the .tar file has been created on the Public Internet facing host, copy it to removable media and carry it to the customer site update server.

Copy the .tar file into the /usr/ipclient/updater/transferPackage directory and run the processUploads.pl script.
perl processUploads.pl

This script will then write the contents of the file and move all updates, upgrades and appropriate files into appropriate directories for the Content Security Appliances to retrieve.

Run the cli updateall command on the Content Security appliances.

VITAL NOTES

*****After performing the update process, the administrator must confirm the software version the TOE is running. This can be accomplished by using the “version” command via the CLI to display the currently running system image filename and the system software release version. *****

*****After every upgrade to the Content Security Appliances performed under this protocol, the equipment list file will need to be edited to reflect the most current downloaded information.*****