Aggregation Services Router (ASR) 1000 Series

Common Criteria

Operational User Guidance

and

Preparative Procedures

Version 0.7

April 2011

Table of Contents

DOCUMENT INTRODUCTION

This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the Aggregation Services Router (ASR) 1000 Series software version IOS XE 2.4.2t solution. This Operational User Guidance and 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.

1. Introduction

This Operational User Guidance and Preparative Procedures documents the administration of the Aggregation Services Router (ASR) 1000 Series software version IOS XE 2.4.2t TOE certified by Common Criteria with functional conformance to the following Protection Profiles,

Table 1: Protection Profiles

Protection Profile	Version	Date
U.S. Government Router Protection Profile For Medium Robustness Environments	1.1	July 25, 2007
U.S. Government Virtual Private Network (VPN) Boundary Gateway Protection Profile For Medium Robustness Environments	1.2	Jan 30, 2009
U.S. Government Protection Profile for Traffic Filter Firewall For Medium Robustness Environments	1.1	July 25, 2007

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 and 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 ASR operations. This document makes reference to several Cisco Systems documents. The documents used are shown below.

[1] Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation and Initial Configuration Guide, Text Part Number: OL-13208-06, November 2009

[2] Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide, Text Part Number: OL-14126-06, February 26, 2010

[3] Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide, Text Part Number: OL-16506-06, February 26, 2010

[4] Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide, Text Part Number: OL-14127-06, February 26, 2010

[5] Cisco ASR 1000 Series Aggregation Services Routers Operations and Maintenance Guide, Text Part Number: OL-17665-03, June, 2009

[6] Cisco IOS Security Command Reference, April 2010

[7] Cisco IOS IP Routing: BGP Command Reference, November 2009

[8] Cisco IOS IP Routing: ISIS Command Reference, November 2009

[9] Cisco IOS IP Routing: OSPF Command Reference, November 2009

[10] Cisco IOS IP Routing: RIP Command Reference, November 2009

[11] FIPS 140-2 Non-Proprietary Security Policy for the Cisco ASR 1002f, ASR 1002 with ESP5 or ESP10, ASR 1004 with RP 1 or RP 2 and ESP10 or ESP20, and ASR 1006 with dual RP 1 or RP 2 and dual ESP10 or ESP20

[12] Aggregation Services Router (ASR) 1000 Series Security Target, Revision 0.17, March 2011

[13] Cisco IOS XE Network Management Configuration Guide, Release 2

1.3. Supported Hardware and Software

Only the following hardware and software listed below is compliant with the Common Criteria EAL4 evaluation. Using hardware not specified invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed below will invalidate the secure configuration.

The hardware and software solution included within the scope of this evaluation are:

Table 2: Physical Scope of the TOE

TOE Configuration	Hardware Configurations	Software Version
ASR 1002f	No configuration options	IOS XE 2.4.2t software
ASR 1002	ESP5 or ESP10	IOS XE 2.4.2t software
ASR 1004	RP 1 or RP 2	IOS XE 2.4.2t software
	ESP10 or ESP20	
ASR 1006	RP 1 or RP 2	IOS XE 2.4.2t software
	Dual ESP10 or ESP20	

Additionally, each TOE hardware model is configured to include one or more SPAs to facilitate network connectivity. The following table identifies the number of SPAs supported by each TOE hardware model.

Table 3: Physical Scope of the TOE

TOE Configuration	SPA Slots
ASR 1002f	1 SPA slot
ASR 1002	3 SPA slots
ASR 1004	8 SPA slots
ASR 1006	12 SPA slots

The following SPAs included within the TOE:

Cisco 8-Port Channelized T1/E1 Shared Port Adapter
Cisco 4-Port Channelized T3 (DS0) Shared Port Adapter
Cisco 2-Port Channelized T3 (DS0) Shared Port Adapter
Cisco 1-port Channelized STM-1/OC-3c to DS0 Shared Port Adapter
Cisco 2-Port Clear Channel T3/E3 Shared Port Adapter
Cisco 4-Port Clear Channel T3/E3 Shared Port Adapter
Cisco 4-Port Serial Interface Shared Port Adapter
Cisco 4-Port 10BASE-T/100BASE Fast Ethernet Shared Port Adapter
Cisco 8-Port 10BASE-T/100BASE Fast Ethernet Shared Port Adapter
Cisco 2-Port Gigabit Ethernet Shared Port Adapter
Cisco 5-Port Gigabit Ethernet Shared Port Adapter
Cisco 8-Port Gigabit Ethernet Shared Port Adapter
Cisco 10-Port Gigabit Ethernet Shared Port Adapter
Cisco 1-Port 10 Gigabit Ethernet Shared Port Adapter
Cisco 2-Port OC3c/STM-1c POS Shared Port Adapter
Cisco 4-Port OC3c/STM-1c POS Shared Port Adapter
Cisco 8-port OC3/STM4 POS Shared Port Adapter
Cisco 1-Port OC12c/STM-4c POS Shared Port Adapter
Cisco 2-port OC12/STM4 POS Shared Port Adapter
Cisco 4-port OC12/STM4 POS Shared Port Adapter
Cisco 8-port OC12/STM4 POS SPA Shared Port Adapter
Cisco 1-port OC48/STM16 POS/RPR Shared Port Adapter
Cisco 2-port OC48/STM16 POS/RPR Shared Port Adapter
Cisco 4-port OC48/STM16 POS/RPR Shared Port Adapter
Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with XFP Optics

1.4. TOE Operational Environment

The TOE optionally supports the following hardware, software, and firmware in its environment:

Table 4: IT Environment Components

IT Environment Component	Required	Usage/Purpose Description for TOE performance
VPN Peer	No	This includes any peer with which the TOE participates in VPN communications. VPN peers may be any device or software client that supports IPSec communications. Both VPN clients and VPN gateways are considered VPN peers by the TOE.

1.4.1. Excluded Functionality

Excluded Functionality	Exclusion Rationale
Dual IOS mode – dual instances on a single	This functionality provides software

ASR 1000 of the system software	redundancy within the TOE. Software redundancy is not a security functionality required by the Protection Profiles for which conformance is claimed.
In-Service Software Upgrade (ISSU)	This functionality provides the ability to upgrade the TOE software without taking the TOE out of commission. The functionality is not a security functionality required by the Protection Profiles for which conformance is claimed.
Any TLS communication with the TOE	TLS communications with the TOE were excluded from FIPS 140-2 validations. These types of connections would include HTTPS connections with external servers. The TOE does not require any communication with external servers via HTTPS to provide the functionality described in the ST.
SNMP and Web User Interface management	These management interfaces do not enforce the required role privileges.
Access to the Linux shell within the ASR 1000 Series router	The Linux shell access could be used to execute other (non-TOE) applications within the router. This access is disabled by compiling out access to the "platform shell" command.
The physical auxilary port, the BITS Ethernet Port, and the USB port.	They have no current use with the TOE.
External NTP server	The TOE must rely upon its own internal timestamp per the PP requirements.
External Authentication server	The TOE must rely upon local authentication mechanisms per the PP requirements.
Management via telnet and ftp	These protocols send authentication data in the clear.
Usage of debug.conf	The FIPS 140-2 validation restricts usage of the debug.conf file to set environment variable values.
Level-based privilege separation in IOS XE.	This evaluation creates custom non-hierarchical roles that are not level-based but command access based.

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:

TOE Model	External Identification
ASR 1002f	“ASR1000-2” in the upper right hand corner of the faceplate.

ASR 1002	"ASR1002" in the upper left-hand corner of the faceplate, and "ASR1000-ESP5" or "ASR1000-ESP10" on the ESP blade.
ASR 1004	"Cisco ASR 1004" on the upper right-hand corner of the chassis, "ASR1000-RP1" or "ASR1000-RP2" on the routing processor blade, and "ASR1000-ESP10" or "ASR1000-ESP20" on the ESP blade.
ASR 1006	"Cisco ASR 1006" on the upper right-hand corner of the chassis, "ASR1000-RP1" or "ASR1000-RP2" on the routing processor blades, and "ASR1000-ESP10" or "ASR1000-ESP20" on the ESP blades.

Step 7 There are three alternatives for obtaining a Common Criteria evaluated software IOS XE 2.4.2t image:

- Download the IOS XE 2.4.2t 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/web/download/index.html.
- The TOE ships with the current IOS XE software images installed.

Step 8 Once the file is downloaded, verify that it was not tampered with by using an MD5 utility to compute an MD5 hash for the downloaded file and comparing this with the MD5 hash for the image listed in Table 5 below. If the MD5 hashes do not match, contact Cisco Technical Assistance Center (TAC) http://tools.cisco.com/ServiceRequestTool/create/launch.do.

Step 9 The end-user must confirm once the TOE has booted that they are indeed running the evaluated version using the **show running-config** command as indicated in the Secure Installation of the TOE section below.

Step 10 Download the required TOE TCL scripts as documented in the TCL Scripts chapter in http://www.cisco.com/en/US/docs/routers/asr1000/operations/guide/asr1000ops.html.

Table 5: Evaluated Software Images

Platform	Image Name	MD5 hash
ASR 1002	asr1000rp1-adventerprisek9.02.04.02t.122-	69e745fe4842df432065500344e4ecb4

ASR 1002f ASR 1004 (RP1) ASR 1006 (RP1)	33.XND2t.bin	
ASR 1004 (RP2) ASR 1006 (RP2)	asr1000rp2-adventerprisek9.02.04.02t.122-33.XND2t.bin	4f87c2acd383c1c959d680bcb47d6338

3. Secure Installation of the TOE

Use the instructions in **[1]** and/or **[2]** for hardware installation of the TOE. After the TOE hardware has been installed, perform the following software package installing steps.

Step 1 Connect to the CLI of the TOE by following "Using Cisco IOS XE Software" → "Accessing the CLI Using a Router Console" → "Accessing the CLI Using a Directly-Connected Console" in **[3]**.

Step 2 Install the downloaded and verified software image onto TOE as described in the steps in "Consolidated Packages and Sub-Package Management" → "Managing and Configuring the Router to Run Using Consolidated Packages and Individual Sub-Packages" → "Quick Start Software Upgrade" in **[3]**. Be sure to complete the instructions with the **reload** command in step 7.

Note that the evaluated image binaries are consolidated packages, and are to be installed in their entirety. They should not be extracted and installed as individual sub-packages as steps 2, 4, and 5 in this section offer.

Step 3 Once the TOE comes back up after its reload, at the prompt, enter the **show running-config** command. Verify that the version is IOS XE 2.4.2t. If the ASR image fails to load, or if the ASR software version is not IOS XE 2.4.2t contact Cisco TAC.

Note that the show version command will also indicate IOS-XE Software Version 12.2(33)XND2t,

4. Initial TOE Configuration

The ASR TOE includes a strict role division with separate permissions assigned. There are three roles that will be defined in this initial configuration that must be used going forward. During this initial configuration reference will be made to a generic administrator that must perform the configuration.

Steps 1 through 6 below relate to settings in the FIPS Security Policy [11] that must be configured, while step 7 applies the evaluated base configuration.

Step 1 Reload the TOE and hit the break sequence (CTRL-Break) during the first 60 seconds to enter ROM Monitor mode.

Step 2 At the ROM Monitor (ROMMON) CLI: The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots. From the ROMMON command line, the administrator enters the following syntax:

confreg 0x0102

Step 3 Also at the ROMMON CLI: Dual IOS mode is not allowed. ROMMON variable IOSXE_DUAL_IOS must be set to 0 using the **IOSXE_DUAL_IOS = 0** command. Issue the **continue** command to exit ROMMON.

Step 4 The administrator must apply tamper evidence labels as described in **[11]**.

Step 5 In service software upgrade (ISSU) is not allowed. The administrator should not perform in service software upgrade of an ASR1000 FIPS validated firmware image

Step 6 Use of the debug.conf file is not allowed. The administrator should not create the bootflash:/debug.conf file and use it for setting environment variables values.

Step 7 During initial configuration of the TOE, the base configuration must be created by entering the following commands in configuration mode:

```
service timestamps debug datetime msec
service timestamps log datetime localtime
service timestamps log datetime year
no service password-encryption
service sequence-numbers
hostname <router name>
security passwords min-length 8
logging userinfo
logging console filtered
logging monitor filtered
logging buffer filtered
logging message-counter log
```

```
enable password lab
aaa new-model
aaa authentication login Administrators local
aaa authorization console
aaa authorization exec default local if-authenticated
no ip domain lookup
login on-success log
login on-failure log
key config-key password-encrypt secret1234
password encryption aes
crypto key generate rsa exportable label sshv2 modulus 3072
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
username <audit admin username> view auditadmin password <secret>
username <security admin username> view securityadmin password <secret>
username <crypto admin username> view cryptoadmin password <secret>
redundancy
 mode sso
file scripts-url harddisk:/cc_scripts
ip tftp source-interface GigabitEthernet0
ip ssh version 2
no crypto ipsec default transform-set



line con 0
 authorization exec default
 login authentication Administrators
 stopbits 1
line aux 0
 stopbits 1
line vty 0 10
 authorization exec default
 login authentication Administrators
```

```
 transport input ssh
```

!Defines commands that are available to all of the TOE administrators

```
parser view all_admin
 secret secret
 commands exec include all ping
 commands configure include event manager environment
 commands configure include event manager
 commands configure include event
 commands configure include no event manager environment
 commands configure include no event manager
 commands configure include no event
 commands configure include no
 commands exec include configure terminal
 commands exec include configure
 commands exec include terminal monitor
 commands exec include terminal
 commands exec include all show clock
 commands exec include all show logging
 commands exec include show running-config
 commands exec include show
 commands exec include all copy
 commands exec include all delete
 commands exec include all dir
 commands exec include all more
 commands exec include reload
!
```

!Defines commands that are available to both the Security Admin and the Crypto Admin

```
parser view security_crypto_admin
 secret secret
 commands exec include write memory
 commands exec include write
 commands exec include all show crypto
 commands exec include show ip
!
```

!Defines commands that are available to the audit administrator

```
parser view audit
 secret secret
 commands exec include all clear logging
 commands exec include clear
 commands exec include all logging persistent move
!
```

!Defines commands that are available to the security administrator

```
parser view security
 secret secret
 commands crypto-keyring include-exclusive all local-address
 commands crypto-ipsec-profile exclude set transform-set
 commands crypto-ipsec-profile include set
 commands crypto-map exclude set transform-set
 commands crypto-map exclude set pfs
 commands crypto-map include set
 commands route-map include all set
 commands route-map include all continue
 commands route-map include all match
 commands route-map include all description
 commands route-map include all default continue
 commands route-map include all default
 commands route-map include all no set
 commands route-map include all no continue
 commands route-map include all no match
 commands route-map include all no description
 commands route-map include all no
 commands configure include all event
 commands configure include all time-range
 commands configure include all monitor drop
 commands configure include monitor
 commands configure include all line
 commands configure include banner login
 commands configure include banner
 commands configure include all route-map
 commands configure include all ip as-path
 commands configure include ip access-list resequence
 commands configure include all router
```

```
commands configure include all interface
commands configure include all zone-pair
commands configure include all zone
commands configure include all policy-map type inspect
commands configure include policy-map type
commands configure include policy-map
commands configure include all class-map type inspect
commands configure include class-map type
commands configure include class-map
commands configure include all crypto map
commands configure include all crypto dynamic-map
commands configure include all crypto call
commands configure include all crypto identity
commands configure include allcrypto gdoi
commands configure include all crypto ipsec profile
commands configure include all crypto ipsec nat-transparency
commands configure include all crypto ipsec df-bit
commands configure include all crypto ipsec fragmentation
commands configure include all crypto ipsec security-association
commands configure include crypto ipsec
commands configure include all crypto logging
commands configure include all crypto keyring
commands configure include ip access-list extended
commands configure include ip access-list standard
commands configure include ip access-list match-local-traffic
commands configure include ip access-list log-update
commands configure include ip access-list logging
commands configure include all ip access-list
commands configure include all access-list
commands configure include crypto
commands configure include all parameter-map type inspect
commands configure include parameter-map type
commands configure include parameter-map
commands configure include all login
commands configure include ip verify
commands configure include all ip
commands configure include all clock summer-time
```

```
 commands configure include clock timezone
 commands configure include clock
 commands configure include all logging
 commands configure include all no event
 commands configure include all no time-range
 commands configure include all no monitor drop
 commands configure include no monitor
 commands configure include all no line
 commands configure include no banner login
 commands configure include no banner
 commands configure include all no route-map
 commands configure include all no ip as-path
 commands configure include no ip access-list resequence
 commands configure include all no router
 commands configure include all no interface
 commands configure include all no zone-pair
 commands configure include all no zone
 commands configure include all no policy-map type inspect
 commands configure include no policy-map type
 commands configure include no policy-map
 commands configure include all no class-map type inspect
 commands configure include no class-map type
 commands configure include no class-map
 commands configure include no crypto map
 commands configure include no crypto dynamic-map
 commands configure include no crypto call
 commands configure include no crypto identity
 commands configure include no crypto gdoi
 commands configure include all no crypto ipsec profile
 commands configure include all no crypto ipsec nat-transparency
 commands configure include all no crypto ipsec df-bit
 commands configure include all no crypto ipsec fragmentation
 commands configure include all no crypto ipsec security-
association
 commands configure include no crypto ipsec
 commands configure include no crypto logging
 commands configure include no crypto keyring
 commands configure include no ip access-list extended
```

```
commands configure include no ip access-list standard
commands configure include no ip access-list match-local-traffic
commands configure include no ip access-list log-update
commands configure include no ip access-list logging
commands configure include all no ip access-list
commands configure include all no access-list
commands configure include no crypto
commands configure include all no parameter-map type inspect
commands configure include no parameter-map type
commands configure include no parameter-map
commands configure include all no login
commands configure include no ip verify
commands configure include all no ip
commands configure include all no clock summer-time
commands configure include no clock timezone
commands configure include no clock
commands configure include all no logging
commands configure include no
commands exec include all crypto gdoi
commands exec include all crypto ipsec
commands exec include crypto
commands exec include all hw-module
commands exec include clock set
commands exec include clock
commands exec include all test
commands exec include all show zone-pair
commands exec include all show zone
commands exec include all show class-map type inspect
commands exec include show class-map type
commands exec include show class-map
commands exec include all show policy-map type inspect
commands exec include show policy-map type
commands exec include show policy-map
commands exec include all show parameter-map type inspect
commands exec include show parameter-map type
commands exec include show parameter-map
commands exec include all show ip
```

```
 commands exec include all show users
 commands exec include all show interfaces
 commands exec include all show platform
 commands exec include show
 commands exec include all clear counters
 commands exec include clear zone-pair
 commands exec include all clear interface
 commands exec include clear
 commands exec include show ip access-lists
 commands exec include all show access-lists
 commands exec include all set platform hardware qfp active
feature ipsec event type



!
```

!Defines commands that are available to the crypto administrator

```
parser view crypto
 secret secret
 commands exec include all crypto key
 commands crypto-keyring exclude local-address
 commands configure include crypto ipsec profile
 commands crypto-ipsec-profile include set
 commands crypto-map include set
 commands crypto-ipsec-profile include-exclusive all set
transform-set
 commands crypto-ipsec-profile include-exclusive all set pfs
 commands configure include crypto map
 commands configure include crypto dynamic-map
 commands crypto-map include-exclusive all set transform-set
 commands crypto-map include-exclusive all set pfs
 commands configure include all crypto key
 commands configure include all crypto ipsec transform-set
 commands configure include all crypto isakmp
 commands configure include all crypto keyring
 commands configure include all crypto pki
 commands configure include all kron occurrence
 commands exec include all show kron
 commands exec include-exclusive test crypto self-test
```

```
 commands exec include test platform software fips fP standby kat
 commands exec include test platform software fips fP active kat
 commands exec include all debug crypto
 commands exec include all no debug crypto
!
!
```
!Assigns the commands to the Audit administrator
```
parser view auditadmin superview
 secret secret
 view all_admin
 view audit
!
```
!Assigns the commands to the Security administrator
```
parser view securityadmin superview
 secret secret
 view all_admin
 view security_crypto_admin
 view security
!
```
!Assigns the commands to the Crypto administrator
```
parser view cryptoadmin superview
 secret secret
 view all_admin
 view security_crypto_admin
 view crypto

kron policy-list crypto_test
 cli test crypto self-test
 cli test platform software fips fP standby kat
 cli test platform software fips fP active kat

end
```

5. TOE Administrative User Roles

Note that all roles are configured during setup of the TOE and may not be changed while the TOE is operational.

Also note that the FIPS roles defined in [11] overlap with these roles. For purposes of Common Criteria operation, the following roles are to be used instead of the FIPS User and Crypto Officer roles. Note that the FIPS Crypto Officer duties are split between the Common Criteria Security Administrator and Cryptographic Administrator roles, and that the FIPS User functionality falls across all three Common Criteria roles. The FIPS roles need not be created separately.

5.1. Security Administrator;

5.1.1. Role Description

The Security Administrator is responsible for the following administrative tasks,

- Management of Self-Tests
- Management of TOE audit functionality
- Management of Information Flow Policies
- Management of authentication failure handling
- TOE clock management

5.1.2. User Interfaces

The Security Administrator uses the TOE CLI to interact with and configure the TOE. The TOE CLI is access over SSH or via a directly connected console.

5.2. Cryptographic Administrator (i.e., users authorized to perform cryptographic initialization and management functions);

5.2.1. Role Description

The Cryptographic Administrator is responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the TOE. These include,

- Management of cryptographic self-tests
- Invoke the non-cryptographic self-test
- Management of TOE audit functionality (ability to view audit records)

5.2.2. User Interfaces

The Cryptographic Administrator uses the TOE CLI to interact with and configure the TOE. The TOE CLI is access over SSH or via a directly connected console.

5.3. Audit Administrator

5.3.1. Role Description

The Audit Administrator is responsible for the regular review of the TOE's audit data and Audit trail deletion. The Audit Administrator can also invoke the non-cryptographic self-test.

5.3.2. User Interfaces

The Audit Administrator uses the TOE CLI to interact with and configure the TOE. The TOE CLI is access over SSH or via a directly connected console.

6. Security Relevant Events

6.1.1. Secure Remote Management

The TOE provides SSH-protected communications for remote management sessions.

The Initial TOE Configuration section, step 7, above includes the base configuration for the evaluated TOE. This configuration enables SSH managmenet on the TOE, with the **hostname**, **crypto key generate rsa**, and **ip ssh version 2** commands, and restricts remote access with the **line vty 0 10** and **transport input ssh** commands. Note that these settings are not to be changed, although the **crypto key generate rsa** command can be used to generate new rsa keys of 3072 bits or larger.

For additional information on configuring SSH see the "Configuring Secure Shell" chapter of the Cisco IOS Security Configuration Guide at http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.pdf.

6.1.2. Administration of Cryptographic Self-Tests

The TOE provides self-tests consistent with the FIPS 140-2 requirements. These self-tests include the following:

Power-on Self-Tests:

- Route Processor
    - Known Answer Tests: AES KAT, SHS KAT, HMAC KAT, Triple-DES, RNG KAT, RSA KAT
    - Firmware Integrity Test
- Embedded Services Processor
    - Known Answer Tests: AES KAT, SHS KAT, HMAC KAT, Triple-DES, RNG KAT, RSA KAT
    - Firmware Integrity Test

Conditional Self-Tests:

- Route Processor
    - Continuous Random Number Generator test for the FIPS-approved RNG
    - Continuous Random Number Generator test for the non-approved RNG
    - Pair-Wise Consistency Test
    - Conditional Bypass Test

- Embedded Services Processor
    - Continuous Random Number Generator test for the FIPS-approved RNG
    - Continuous Random Number Generator test for the non-approved RNG
    - Conditional Bypass Test

The TOE provides the ability to invoke Cryptographic Self-Tests on-demand.

- This functionality is available to the Cryptographic administrator.
- This functionality is facilitated using the test crypto self-test command

Additional information regarding Administration of Cryptographic Self-Tests review can be found in the "SELF-TESTS" section of **[11]**.

6.1.3. Administration of Non-Cryptographic Self-Tests

The TOE provides self-tests to verify the correct image is running on the TOE. This functionality is available to all administrators and can be executed on demand by reloading the TOE via the **reload** command and observing the following output:

Calculating SHA-1 hash...done

validate_package: SHA-1 hash:

calculated [hash value]

expected [same hash value as above]

Image validated

This functionality cannot be disabled by any administrator.

6.1.4. Configuration of Security Audit

The base configuration in Initial TOE Configuration step 7 includes the commands to setup basic security audit for the TOE. The commands in the following sections must also be applied to set the TOE up for the functionality defined in the Security Target **[12]**.

The TOE provides the ability for the authorized administrator to Review audit records: **show logging persistent**

- This functionality is available to the Audit, Cryptographic, and Security administrator.

Enable/disable persistent logging in a "logs" folder on bootflash (the command will create this folder if it does not already exist): **logging persistent url bootflash:logs immediate protected notify**

- This functionality is available to the Security administrator.

Sorting/searching audit records: **more bootflash:filter** and **show logging persistent selector-url bootflash:filter**

- This functionality is available to the Audit, Cryptographic, and Security administrator.

6.1.4.1. Excluding/Including Auditable Events

The TOE provides the Security Administrator the ability to explicitly exclude or include auditable events that are maintained by the TOE. The TOE accomplishes this using the Tcl scripts, "logging filter <script-url>syslog_include.tcl [args <*string*>]" and "logging filter <script-url>syslog_exclude.tcl [args <*string*>]".

The usage guidelines the "*string*" argument of "logging filter <script-url>syslog_include.tcl [args <*string*>]" are:

- **string** – an arbitrary character string. Any syslog message which contains the configured character string is propagated to the auditable events repository. Syslog messages which do not contain the configured character strings are dropped.

The usage guidelines the "*string*" argument of "logging filter <script-url>syslog_exclude.tcl [args <*string*>]" are:

- **string** – an arbitrary character string. Any syslog message which contains the configured character string is dropped. Syslog messages which do not contain the configured character string are propagated to the auditable events repository.

Usage guidelines that apply to both commands include the following:

- If a desired string value contains special characters such as space (ASCII 0x20), backslash ("\"), single or double quotes such value should be formatted according to the common CLI values formatting rules.

- Inclusive or exclusive filtering of multiple patterns is achieved by providing multiple syslog filter commands. The order of commands execution is determined by the order in which the filters are configured. The number of individual syslog filters is limited by the device memory size only.

6.1.4.2. Deleting Audit Records

The TOE provides the Audit Administrator the ability to delete audit records audit records stored within the TOE. This is accomplished using the **clear logging persistent** command.

6.1.4.3. Configuring lossless/circular auditing

The TOE provides the Security Administrator the ability to configure the TOE to stop all auditable events when an audit storage threshold is met (lossless auditing) or configure the TOE to overwrite the oldest audit records when the audit trail becomes full.

Configure lossless (including audit storage threshold) or circular auditing:

- **logging persistent url bootflash:logs protected immediate threshold 95** sets the TOE to send the box to a secure state once 95% of the available log space has been exhausted, and
- **logging persistent url bootflash:logs protected immediate** sets the TOE to overwrite the oldest records when the audit trail becomes full
- This functionality is available to the Security administrator.

WARNING: if the lossless auditing threshold is triggered (as specified by the "threshold" parameter on the logging persistent command) in combination with the setting of 'config-register 0x0102' (in Section 4, step 2 above) will enter an endless reload→crash cycle. If this occurs, contact the Cisco TAC.

6.1.4.4. Configuring Logging of IPSec modifications

The TOE provides the Security Administrator the ability to configure the TOE to log when modifications are detected to IPSec traffic. This is done with the following commands:

```
>set platform hardware qfp actactive feature ipsec event type decrypt-failed count 1
>set platform hardware qfp actactive feature ipsec event type encrypt-failed count 1
>set platform hardware qfp actactive feature ipsec event type replay count 1
```

NOTE: This is not a persistent setting. It must be reset every time the box is reloaded.

6.1.5. Configuration of Alarms

The following events can be monitored for the purpose of issuing alarms:

1. Security Administrator specified number of authentication failures;
2. Security Administrator specified number of Information Flow policy violations by an individual presumed source network identifier (e.g., IP address) within an administrator specified time period;
3. Security Administrator specified number of Information Flow policy violations to an individual destination network identifier within an administrator specified time period;
4. Security Administrator specified number of Information Flow policy violations to an individual destination subject service identifier within an administrator specified time period;
5. Security Administrator specified Information Flow policy rule, or group of rule violations within an administrator specified time period;
6. Any detected replay of TSF data or security attributes;

7. Any failure of the cryptomodule/cryptographic self-tests;
8. Any failure of the other key generation self-tests;
9. Any failure of the other TSF self-tests;
10. Security Administrator specified number of encryption failures;
11. Security Administrator specified number of decryption failures;
12. Security Administrator specified number of Phase 1 authentication failures when negotiating the Internet Key Exchange protocol; and
13. Security Administrator specified number of failures occur during Phase 2 negotiation.

Alarms are implemented using TCL scripts similar to those used for filtering the audit events. Each alarm is based on specific audit records, when those records are generated – a series of TCL scripts, including those for filtering, are executed.

Enable/disable alarms: **logging filter harddisk:cc_scripts/*[tcl script name]*** see TCL Script information later in this document for the listing of TCL scripts and their associated functionality. Also, in **[13]** the "Cisco IOS Scripting with Tcl" section contains additional details on the TCL functionality.

- This functionality is available to the Security administrator.

Enable audible alarms: **logging filter harddisk:cc_scripts/alarms_db.tcl args alarm_audible** or **logging filter harddisk:cc_scripts/alarms_db.tcl args alarm_not_audible** to disable audible alarms

- This functionality is available to the Security administrator.

Confirm alarms: **event manager environment confirm_alarm XXXXX** (where XXXXX is the alarm number identified)

- This functionality is available to the Audit, Cryptographic, and Security administrator.

6.1.6. Configuration of Quotas on Transport Layer Connections and Connection-oriented Resources

The TOE allows the security administrator to define the number of existing half-open sessions that will cause the Cisco IOS firewall to start and stop deleting half-open sessions. This is accomplished by using the "max-incomplete" command. This functionality is provided in conjunction with firewall policies.

Additional information regarding Configuration of Quotas on Transport Layer Connections (including Connection-oriented resources) can be found in the "max-incomplete" section of **[6]**.

6.1.7. Configuration of Authentication Failure Handling

The TOE provides the Security Administrator two options for handling authentication failure. The TOE allows the Security Administrator to either disable the ability to authenticate to the TOE remotely (via SSH) for a specified period of time or to disable the ability to authenticate to the TOE remotely until it

is re-enabled by an administrator directly connected via a serial cable whenever a threshold of unsuccessful authentication attempts is met.

Information regarding disabling the ability to authenticate remotely into the TOE for a specific period of time can be found in the "login block-for" section of **[6]**.

Information regarding disabling the ability to authenticate remotely until it is re-enabled by an administrator directly connected via a serial cable can be found in the information on the em_login_failure.tcl script in TCL Script information below. To re-enable remote access after lockout the Security Administrator executes the following commands:

line vty 0 10

authorization exec default

login authentication Administrators

transport input ssh

Note that this section does not refer to allowing authentication via a remote server. All authentication to the TOE is via the local database.

6.1.8. Use of Administrative Session Lockout and Termination

The TOE allows the Security Administrator to configure the length of time that an inactive administrative session remains open. After the configured period of time, the administrative session is locked and the screen is flushed. No further activity is allowed to until the administrator has successfully re-authenticated to the TOE. This is the same functionality as user session termination. The administrator is required to re-authenticate after the session becomes locked and the screen is cleared.

The **exec-timeout** command is used to configure this locking of the session after the administrator is inactive for the specified number of minutes and seconds on the vty lines:

line vty 0 10

exec-timeout ***minutes*** **[*seconds*]**

Use the **no** form of this command (**no exec-timeout**) to remove the timeout definition.

The TOE allows each administrative user of the TOE to locally lock their administrative sessions. After the session is locked, the screen is flushed. No further activity is allowed to until the administrator has successfully re-authenticated to the TOE.

The **exit** command is used for this on-demand locking of administrator sessions.

6.1.9. Use of Administrative Time and Location-based Restrictions

The TOE allows the Security Administrator to configure settings that deny administrative access to the TOE management CLI based on the location (IP address) of the requesting administrator, and the time and day of the connection request.

The **time-range** command is used to configure the time range restrictions and the **ip access-list** command is used to apply them to interfaces. The **ip access-list** command is also used to specify IP addresses from which to restrict administration (all traffic):

time-range restrict_07_09

periodic daily 07:00 to 09:00

ip access-list extended block_10_56_8_18

deny ip host 10.56.8.18 any log-input time-range restrict_07_09

Use the **no** form of this command (**no ip access-list**) to remove the time based-restrictions.

6.1.10. Configuration of the System Time

The TOE provides the Security Administrator the ability to set the time and date maintained within the TOE. The TOE date and time is set using the "clock set" command.

Additional information regarding configuration of the TOE clock can be found in the "Basic System Management" → "Performing Basic System Management" → "Setting Time and Calendar Services" → "Configuring Time and Date Manually" section of **[13]**.

Note that NTP is not to be used with the TOE.

6.1.11. Configuration Information Flow Policies

The TOE provides the ability to for the Security Administrator to configuration traffic flows through the TOE using Zone-Based Policy Firewall (also known as Zone-Policy Firewall, or ZFW).

ZFW changes the firewall configuration from the older interface-based model to a more flexible, more easily understood zone-based model. Interfaces are assigned to zones, and inspection policy is applied to traffic moving between the zones. Inter-zone policies offer considerable flexibility and granularity, so different inspection policies can be applied to multiple host groups connected to the same router interface.

Zones establish the security borders of your network. A zone defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your network. ZFW's default policy between zones is 'deny all'. If no policy is explicitly configured, all traffic moving between zones is blocked.

Traffic destined to the TOE itself is destined for a predefined zone known as the "self" zone.

Additional information regarding Configuration of Information Flow Policies can be found in the Zone-based Firewall commands of **[6]**.

6.1.12. Configuration of VPN Information Flow Policies

6.1.12.1. Internet Key Exchange Configuration

The TOE all allows the Cryptographic Administrator to configure Internet Key Exchange (IKE) settings, while restricting IKE traffic policies to the Security Administrator IKE is a key management protocol standard that is used in conjunction with the IP Security (IPSec) standard. IPSec is a feature that provides robust authentication and encryption of IP packets.

IKE is a hybrid protocol that implements the Oakley key exchange and the Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.) IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.

Additional information regarding Configuration of IKE Policies can be found in Internet Key Exchange Security Protocol Commands of **[6]**.

6.1.12.2. IPSec Configuration

IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices ("peers"), such as Cisco routers.

With IPSec, data can be sent across a public network without observation, modification, or spoofing, which enables applications, such as Virtual Private Networks (VPNs).

Additional information regarding configuration of IPSec can be found in the IPSec Network Security Commands of **[6]**.

6.1.13. ICMP Configuration

The TOE provides the Security Administrator the ability to configure how the TOE handles ICMP messages destined for the TOE itself. This is accomplished by using Zone-based Firewall policies and the self-zone described above. Zone-based firewall policies allow protocols to be specified as allowed or denied for a particular zone. To ensure that ICMP messages are accepted by the TOE, the

Security Administrator configures a permit policy for ICMP message to the self-zone.

Additional information regarding Configuration of Information Flow Policies can be found in the Zone-based Firewall commands of **[6]**.

6.1.14. Administrative Banner Configuration

The TOE provides the authorized administrator the ability to configure a banner that displays on the CLI management interface prior to allowing any administrative access to the TOE.

- This functionality is available to the Security administrator.
- This functionality is facilitated using the "banner login" command

Information regarding Administrative Banner Configuration can be found in the "banner" command section of **[6]**.

6.1.15. Failure handling

One of the key goals of the ASR is to minimize the impact of failures, particularly in configurations with redundant RP and ESP components. The "failure" may be due to card HW failure, SW exception/crash, card removal or CLI initiated.

The following table summarizes the recovery that occurs for various RP failures and their impact:

Table 6: RP Failure Scenarios

	Failure type	Configuration	Description/Impact
1.	RP transient hardware or software kernel (resulting in a reload of the RP)	Single RP (ASR 1002, ASR 1002f, or only a single RP installed in the ASR 1004 or ASR 1006)	Active ESP continues forwarding traffic while RP restarts. RP then reinitializes the other parts of the device. All state (routes, sessions, interfaces, flow, etc.) will be lost.
2.	RP permanent hardware	Single RP (ASR 1002, ASR 1002f, or only a single RP installed in the ASR 1004 or ASR 1006)	Active ESP continues forwarding traffic but eventually times out waiting for RP restart. Traffic stops until RP replaced.
3.	Active RP transient hardware or software kernel (resulting in a reload of the RP)	Dual RP (ASR 1004 or ASR 1006)	Active ESP continues forwarding traffic. Standby RP takes over using state synced with the active RP prior to failure. Carrier cards switch over to directions from standby RP. The new RP resends its state to active ESP (and redundant ESP if present). Active ESP maintains state (routes, sessions, interfaces, flow, etc.) found in common and discards any of its old state not known by new RP. The newly active RP rebuilds the checkpoint state of failed RP when it restarts.

4.	Active RP permanent hardware	Dual RP (ASR 1004 or ASR 1006)	Active ESP continues forwarding traffic. Standby RP takes over using state synced by active RP prior to failure. Carrier cards switch over to directions from standby RP. The new RP resends its state to active ESP (and redundant ESP if present). Active ESP maintains state (routes, sessions, interfaces, flow, etc.) found in common and discards any of its old state not known by new RP. The newly active RP rebuilds the checkpoint state of failed RP once it is replaced and restarts.
5.	Standby RP transient Hardware, permanent Hardware or Software kernel	Dual RP (ASR 1004 or ASR 1006)	Active ESP continues forwarding traffic. Active RP continues network control and legacy protocol forwarding. Active RP rebuilds checkpoint state of standby RP once it restarts (including after any repair).

The following table summarizes the recovery that occurs for various ESP failures and their impact:

Table 7: ESP Failure Scenarios

	Failure type	**Configuration**	**Description/Impact**
1.	Active ESP transient hardware or software kernel (resulting in a reload of the ESP)	Single ESP (ASR 1002, ASR 1002f, or only a single ESP installed in the ASR 1004 or ASR 1006)	Forwarding stops. ESP restarts and reinitializes its forwarding engine. Active RP resends its current state to ESP which rebuilds forwarding engine tables and its checkpoint state. Link keep-alives and sessions may time out. Local session state maintained by ESP is lost.
2.	Active ESP permanent hardware	Single ESP (ASR 1002, ASR 1002f, or only a single ESP installed in the ASR 1004 or ASR 1006)	Forwarding stops until ESP is replaced.
3.	Active ESP transient hardware or software kernel (resulting in a reload of the ESP)	Redundant ESP (ASR 1004 or ASR 1006)	Standby ESP takes over forwarding with momentary loss of traffic. Active sessions, flows, etc. are maintained except for those in transient condition. ESP restarts as standby. Active RP then resends its current state to ESP, which rebuilds forwarding engine tables and its checkpoint state as standby.
4.	Standby ESP transient hardware, permanent hardware or software kernel	Redundant ESP (ASR 1004 or ASR 1006)	Active ESP continues forwarding. If/when failed ESP restarts, active RP resends its current state to ESP which rebuilds forwarding engine tables and its checkpoint state as standby.

There are also possible SPA failure scenarios. While there are no redundant SPAs as might be the case for RPs and ESPs, the failure of SPAs do not necessarily

cause a complete system failure. Failures on a single card have no affect on the other cards. Note that the recovery action for the removal of a card (or its reset or power-down by the active RP) is the same as if the card had a permanent HW failure.

7. Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized users of the TOE to ensure that the TOE environment provides the necessary functions. The following identifies the requirements and the associated security measures of the authorized users.

7.1. OE.CRYPTANALYTIC

Cryptographic methods used in the IT environment shall be interoperable with the TOE, should be FIPS 140-2 validated and should be resistant to cryptanalytic attacks (i.e., will be of adequate strength to protect unclassified Mission Support, Administrative, or Mission Critical data).

1. Security Administrator: These users must be properly trained in the usage and proper operation of the ASR TOE and all the provided functionality per the implementing organization's operational security policies. These users must utilize SSH clients that are capable of SSHv2 connections with the TOE. These users must configure peer routers as VPN peers that utilize FIPS validated IPSEC crypto.
2. Cryptographic Administrator: These users must be properly trained in the usage and proper operation of the ASR TOE and all the provided functionality per the implementing organization's operational security policies. These users must utilize SSH clients that are capable of SSHv2 connections with the TOE. These users must configure peer routers as VPN peers that utilize FIPS validated IPSEC crypto.
3. Audit Administrator: These users must be properly trained in the usage and proper operation of the ASR TOE and all the provided functionality per the implementing organization's operational security policies. These users must utilize SSH clients that are capable of SSHv2 connections with the TOE. These users must configure peer routers as VPN peers that utilize FIPS validated IPSEC crypto.

7.2. OE.NO_GENERAL_PURPOSE

The Administrator ensures there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

1. Security Administrator: These users must be properly trained in the receipt of, installation, management, usage and proper operation of the ASR TOE component and all the provided functionality per the implementing organization's operational security policies. These users must follow the provided guidance that dictates registry settings that disallow access to the ROMMON and loading of non-certified images. The certified image has no general-purpose computing capabilities. Also note that the the Linux

shell access has been disabled in the TOE to prevent other non-TOE applications from executing on the router.

2. Cryptographic Administrator: These users must be properly trained in the receipt of, installation, management, usage and proper operation of the ASR TOE component and all the provided functionality per the implementing organization's operational security policies. These users must follow the provided guidance that dictates registry settings that disallow access to the ROMMON and loading of non-certified images. The certified image has no general-purpose computing capabilities.
3. Audit Administrator: These users must be properly trained in the receipt of, installation, management, usage and proper operation of the ASR TOE component and all the provided functionality per the implementing organization's operational security policies. These users must follow the provided guidance that dictates registry settings that disallow access to the ROMMON and loading of non-certified images. The certified image has no general-purpose computing capabilities.

7.3. OE.NO_TOE_BYPASS

Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.

1. Security Administrator: These users must be properly trained in the receipt of, installation, management, usage and proper operation of the ASR TOE component and all the provided functionality per the implementing organization's operational security policies. These users must install the ASR in such a location on their network that it is the only path between connected networks.
2. Cryptographic Administrator: These users must be properly trained in the receipt of, installation, management, usage and proper operation of the ASR TOE component and all the provided functionality per the implementing organization's operational security policies. These users must install the ASR in such a location on their network that it is the only path between connected networks.
3. Audit Administrator: These users must be properly trained in the receipt of, installation, management, usage and proper operation of the ASR TOE component and all the provided functionality per the implementing organization's operational security policies. These users must install the ASR in such a location on their network that it is the only path between connected networks.

7.4. OE.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.

1. Security Administrator: These users should ensure that the ASR is being physically protected in a manner consistent with the implementing organization's security policies.
2. Cryptographic Administrator: These users should ensure that the ASR is being physically protected in a manner consistent with the implementing organization's security policies.
3. Audit Administrator: These users should ensure that the ASR is being physically protected in a manner consistent with the implementing organization's security policies.

7.5. OE.AVAILABILITY

Network resources will be available to allow clients to satisfy mission requirements and to transmit information.

1. Security Administrator: These users must install the ASR in such a location on their network that it has access to transmit information on the networks.
2. Cryptographic Administrator: These users must install the ASR in such a location on their network that it has access to transmit information on the networks.
3. Audit Administrator: These users must install the ASR in such a location on their network that it has access to transmit information on the networks.

8. TCL Script information

The following table provides a list of Common Criteria specific TCL scripts, which were installed per 'Secure Acceptance of the TOE' step 10, and briefly explains each script's purpose.

Table 8: TCL Descriptions

Script file name	Description
timer.tcl	Timer events support for other scripts
alarms_db.tcl	Alarms database manager script
em_ike_phase1_failure.tcl	IKE Phase 1 negotiations failures watcher script
em_ike_phase2_failure.tcl	IKE Phase 2 negotiations failures watcher script
em_login_failure.tcl	User login failures watcher script
em_monitor_violation.tcl	An information flow violation monitors watcher script. Respective ACL-based event monitors must

	be configured for this watcher to fire
em_monitor_vpn_event.tcl	VPN encryption, decryption faults and packet replay event monitors watcher script
monitor_ipsec.tcl	This script configures VPN event monitors
syslog_exclude.tcl	Syslog messages which contain keywords passed to this script are not written to the persistent syslog database
syslog_include.tcl	Only syslog messages which contain keywords passed to this script are written to the persistent syslog database
esm_conf_vty.tcl	This script configures syslog messages output to connected VTY devices

In the following CC TCL scripts descriptions <script-url> is a directory in the IOS file system which contains the CC TCL scripts files. In the base configuration identified in 'Initial TOE Configuration' step 7 this directory is set to harddisk:/cc_scripts.

8.1.1.1. timer.tcl: Common Criteria alarms confirmation timer

Repetitive CC alarms confirmation requests are managed by the timer.tcl script:

logging filter <script-url>timer.tcl [args <interval>]

interval – an interval, in seconds, between two successive CC alarm prompts. A default interval between two successive CC alarm prompts is 60 seconds.

Example:

logging filter bootflash:timer.tcl args 120

Administrator is prompted to confirm pending CC alarms each 120 seconds (2 minutes).

8.1.1.2. alarms_db.tcl: Common Criteria alarms database manager

CC alarms database manager maintains a repository of unconfirmed CC alarms:

logging filter <script-url>alarms_db.tcl [args <audible-property>]

audible-property = alarm_audible | alarm_not_audible

Setting the alarm-property argument to "alarm_audible" enables emitting an audible signal while presenting each CC alarm confirmation prompt. By default an audible signal is not emitted.

8.1.1.3. em_ike_phaseX_failure.tcl: IKE Phase 1 and 2 failures catcher

In order to alert the administrator to IKE Phase 1 negotiation failures the following CLI entry should be configured:

logging filter <script-url>em_ike_phase1_failure.tcl [args threshold [interval]]

In similar fashion IKE Phase 1 negotiation failures monitoring requires the following CLI entry:

logging filter <script-url>em_ike_phase2_failure.tcl [args threshold [interval]]

threshold – a number of failures after which a CC alarm is raised

interval – time interval, in seconds, during which the number of failures must reach a set threshold which triggers a CC alarm

If the interval value is not specified it's considered to be indefinite and a CC alarm is raised after a set threshold number of failures occurred. By default the threshold value is 1 and the interval value is indefinite.

When the interval value is set and if less that the threshold number of events occurred during a given interval the failure counter is reset and a corresponding CC alarm is not raised.

Example:

logging filter bootflash:em_ike_phase1_failure.tcl args 3 300

This configuration raises a CC alarm after 3 IKE Phase 1 failures occurred within a 5 min (300 sec) interval. A CC alarm is not raised and the failure counter is reset if less than 3 failures (1 or 2) occurred during a given 5 min interval.

8.1.1.4. em_login_failure.tcl: Common Criteria alarms database manager

The following CLI configuration command allows configuring a watcher for a given category of IPsec policy violations:

bootflash:em_login_failure.tcl [args threshold [interval]]

1. The first argument is the alarm threshold which means how many times the relevant events happen before raising the alarm

2. The second is the time period (in seconds) in which all relevant events happens at.

Note:

- If no arguments are set, the default threshold is 1, and there is no meaning to the time period.
- If only one argument is given it is the alarm threshold, and there is no meaning to the time period.
- The em_login_failure.tcl script also executes the following commands to automatically disable the remote administration until the administrator takes an action to re-enable it:

line vty 0 10
transport input none

Examples:

logging filter bootflash:em_login_failure.tcl args 3

This configuration raises a CC alarm user fails to login in 3 successive attempts.

logging filter bootflash:em_login_failure.tcl args 3 300

This configuration raises a CC alarm user fails to login in 3 successive attempts in the last 5 minutes. A CC alarm is not raised and the failure counter is reset if less than 3 failures (1 or 2) occurred during a given 5 min interval.

8.1.1.5. syslog_in(ex)clude.tcl: syslog filter

Inclusive filtering of syslog messages is managed by configuring the following CLI command:

logging filter <script-url>syslog_include.tcl [args <string>]

string – an arbitrary character string. Any syslog message which contains the configured character string is propagated to the auditable events repository. Syslog messages which do not contain the configured character strings are dropped.

Exclusive filtering of syslog messages is managed by configuring the following CLI command:

logging filter <script-url>syslog_exclude.tcl [args <string>]

string – an arbitrary character string. Any syslog message which contains the configured character string is dropped. Syslog messages which do not contain the configured character string are propagated to the auditable events repository.

If a desired string value contains special characters such as space (ASCII 0x20), backslash (“\”), single or double quotes such value should be formatted according to the common CLI values formatting rules.

Inclusive or exclusive filtering of multiple patterns is achieved by providing multiple syslog filter commands. The order of commands execution is determined by the order in which the filters are configured. The number of individual syslog filters is limited by the device memory size only.

Example:

logging filter bootflash:syslog_include.tcl args ALARM

logging filter bootflash:syslog_include.tcl args LINK

Syslog messages which has character strings ALARM or LINK in them are propagated to the configured auditable events repositories (including terminal devices).

8.1.1.6. em_monitor_violation.tcl: information flow violations watcher

The following CLI configuration command allows raising a CC alarm when an information flow violation occurs:

logging filter <script-url>em_monitor_violation.tcl

8.1.1.7. monitor_ipsec.tcl: IPsec policy violation category configuration[1]

The following CLI configuration command allows configuring a watcher for a given category of IPsec policy violations:

logging filter <script-url>monitor_ipsec.tcl args <esp> <category> <threshold>

esp = active | standby - ASR1000 ESP on which IPsec policy violation is watched

category = decrypt-failed | encrypt-failed | replay – watch for decryption or encryption failures or IPsec packets replay events

threshold – a count of watched events after which a cumulative event is reported. The threshold value must be greater than 0.

All command arguments must be specified. Multiple CLI command lines may be configured for watching multiple categories of the IPsec policy violations.

Example:

logging filter bootflash:monitor_ipsec.tcl args active replay 100000

This CLI command line configures a watcher for the IPsec packets replay violations. The watcher fires each time after 100000 replayed IPsec packets were detected.

8.1.1.8. em_monotor_vpn_event.tcl: VPN policy violations catcher

In order to alert the administrator to previously configured VPN policy violations the following CLI entry should be configured:

logging filter <script-url> em_monotor_vpn_event.tcl

8.1.1.9. esm_conf_vty.tcl: Syslog messages output replication

The following CLI command configures syslog messages replication to all connected terminal devices:

---

[1] Implementation of this Common Criteria functional requirement is ASR1000 platform specific and cannot be utilized in a generic IOS environment.

logging filter <script-url>esm_conf_vty.tcl

8.1.1.10. TCL scripts configuration

Of all CC TCL scripts only the esm_conf_vty.tcl script is mandatory for configuration in all Common Criteria compliant environments. Other CC TCL scripts are deployed when administrator decides to utilize respective optional features.

When optional CC TCL scripts are configured the order of configuration is important. The **timer.tcl** script must always be configured *first* and the **alarms_db.tcl** script must always be configured *last* in the configuration sequence. The order in which all other CC TCL scripts are configured is irrelevant.

Example.

logging filter bootflash:timer.tcl 60

logging filter bootflash:esm_conf_vty.tcl

<… other scripts are configured here …>

logging filter bootflash:alarms_db.tcl alarm_audible

See individual scripts descriptions above for any additional CLI configuration required for a script to function properly.

9. Related Documentation

Use this document in conjunction with the IOS Router documentation at the following locations:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/index.htm

Obtaining Documentation

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

9.1. World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

9.2. Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

9.3. Ordering Documentation

Cisco documentation is available in the following ways:

Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

http://www.cisco.com/cgi-bin/order/order_root.pl

Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

http://www.cisco.com/go/subscription

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).

9.4. 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.

10. 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