# Cisco 900 Series Integrated Services Routers (ISR) running IOS v15.9

# Common Criteria Operational User Guidance And Preparative Procedures

**Version 0.9**

**28 November 2022**

**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Table of Contents

1. Introduction....9
1.1 Audience....9
1.2 Purpose....9
1.3 Document References....9
1.4 Supported Hardware and Software....12
1.4.1 Supported Configurations....12
1.5 Operational Environment....13
1.6 Excluded Functionality....13
2. Secure Acceptance of the TOE....15
3. Secure Installation and Configuration....18
3.1 Physical Installation....18
3.2 Initial Setup via Direct Console Connection....19
3.2.1 Options to be chosen during the initial setup of the Cisco 900 Series Integrated Services Routers....19
3.2.2 Saving Configuration....20
3.2.3 Enabling FIPS Mode....20
3.2.4 Administration of Cryptographic Self-Tests....20
3.2.5 Administration of Non-Cryptographic Self-Tests....22
3.2.6 Access Control and Lockout....22
3.2.7 Session Termination....24
3.2.8 User Lockout....24
3.3 Network Protocols and Cryptographic Settings....25
3.3.1 Remote Administration Protocols....25
3.3.2 Authentication Server Protocols....27
3.3.3 Routing Protocols....28
3.3.4 Basic Firewall Packet Filtering Configuration....28
3.3.5 Information Flow Policies....30
3.3.6 X.509 Certificates....31
3.3.6.1 Generate a Key Pair....31

3.3.6.2 Creation of the Certificate Signing Request ..... 32
3.3.6.3 Securely Connecting to a Certificate Authority for Certificate Signing ..... 33
3.3.6.4 Authenticating the Certificate Authority ..... 34
3.3.6.5 Storing Certificates to a Local Storage Location ..... 35
3.3.6.6 How to Specify a Local Storage Location for Certificates ..... 35
3.3.6.7 Configuring a Revocation Mechanism for PKI Certificate Status Checking ..... 36
3.3.6.8 Configuring Certificate Chain Validation ..... 36
3.3.6.9 Certificate Validation ..... 37
3.3.6.10 Setting X.509 for use with IKE ..... 37
3.3.6.11 Deleting Certificates ..... 37
3.3.7 IPsec Overview ..... 38
3.3.8 Configuration of IPsec ..... 39
3.3.8.1 Configure Reference Identifier ..... 39
3.3.8.2 IKEv2 Transform Sets ..... 40
3.3.8.3 IPsec Transform and Lifetimes ..... 42
3.3.8.4 NAT Traversal ..... 42
3.3.8.5 Tunnel Mode vs. Transport Mode ..... 43
3.3.8.6 IKEv2 Parameters Permitted in the Evaluated Configuration ..... 44
3.3.8.7 IPSEC Session Interruption Recovery ..... 45
3.3.9 Session Protection ..... 45
3.3.9.1 Syslog Server Running on an IPsec Endpoint ..... 45
3.3.9.2 Syslog Server Adjacent to an IPsec Peer ..... 46
3.4 Logging Configuration ..... 47
3.4.1 Managing Audit Records ..... 49
3.4.2 Usage of Embedded Event Manager ..... 49
3.4.3 Remote Logging ..... 50
3.4.4 Logging Protection ..... 50
4. Secure Management ..... 51
4.1 User Roles ..... 51
4.2 Passwords ..... 51
4.3 System Clock Management ..... 54
4.4 Identification and Authentication ..... 54
4.5 Administrative Banner Configuration ..... 55

4.6 Administrative Session Termination ..... 55
4.7 Administrative Session Lock-out ..... 55
4.8 Product Updates ..... 56
5. Security Relevant Events ..... 57
5.1 Deleting Audit Records ..... 58
5.2 Reviewing Audited Events ..... 58
6. Network Services and Protocols ..... 68
7. Modes of Operation ..... 72
7.1 Network Processes Available During Normal Operation ..... 73
8. Security Measures for the Operational Environment ..... 75
9. Obtaining Documentation and Submitting a Service Request ..... 76
9.1 Documentation Feedback ..... 76
9.2 Obtaining Technical Assistance ..... 76

# List of Tables

Table 1 Acronyms ..... 6
Table 2 Terminology ..... 7
Table 3 Reference Documents ..... 10
Table 4 Required non-TOE Hardware/ Software/ Firmware ..... 13
Table 5 Excluded Functionality ..... 13
Table 6: Evaluated Products and their External Identification ..... 15
Table 7: Evaluated Software Images ..... 17
Table 8 AAA Commands ..... 24
Table 9 Reference Identifier Configuration ..... 40
Table 10 IKEv2 Parameters in the Evaluated Configuration ..... 44
Table 11 IPsec Parameters Permitted in the Evaluated Configuration ..... 44
Table 12 Auditable Events ..... 58
Table 13 Audit Records (sample) ..... 60
Table 14 Protocols and Services ..... 69
Table 15 Security Objective for the Operational Environment ..... 75

# Acronyms

The following acronyms and abbreviations are common and may be used in this document:

**Table 1 Acronyms**

| Acronyms / Abbreviations | Definition |
|---|---|
| AAA | Administration, Authorization, and Accounting |
| AES | Advanced Encryption Standard |
| BRI | Basic Rate Interface |
| CC | Common Criteria for Information Technology Security Evaluation |
| CEM | Common Evaluation Methodology for Information Technology Security |
| CM | Configuration Management |
| CSU | Channel Service Unit |
| DHCP | Dynamic Host Configuration Protocol |
| DSU | Data Service Unit |
| EAL | Evaluation Assurance Level |
| EHWIC | Ethernet High-Speed WIC |
| ESP | Encapsulating Security Payload |
| ESPr | Embedded Services Processors |
| GE | Gigabit Ethernet port |
| IT | Information Technology |
| NDcPP | collaborative Protection Profile for Network Devices |
| OS | Operating System |
| PoE | Power over Ethernet |
| PP | Protection Profile |
| SA | Security Association |
| SFP | Small–form-factor pluggable port |
| SHS | Secure Hash Standard |
| ST | Security Target |
| TCP | Transport Control Protocol |
| TSC | TSF Scope of Control |
| TSF | TOE Security Function |
| TSP | TOE Security Policy |
| WAN | Wide Area Network |
| WIC | WAN Interface Card |

# Terminology

The following terms are common and may be used in this document:

**Table 2 Terminology**

| Term | Definition |
|---|---|
| Authorized Administrator | Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions. |
| Peer | Another router on the network that the TOE interfaces with. |
| Remote VPN Peer | A remote VPN Peer is another network device that the TOE sets up a VPN connection with. This could be a VPN client or another router. |
| Privileged Administrator | Synonymous with Authorized Administrator for the purposes of this evaluation. |
| User | Any entity (human user or external IT entity) outside the TOE that interacts with the TOE. |
| vty | vty is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term). |
| Vty | vty is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term). For configuration purposes vty defines the line for remote access policies to the router. |

# DOCUMENT INTRODUCTION

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

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco 900 Series Integrated Services Routers (ISR) running IOS 15.9. 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.

# 1. Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco 900 Series Integrated Services Routers (ISR) running IOS 15.9 TOE certified under Common Criteria. The TOE may be referenced below as the ISR900 Series, TOE, or simply router.

## 1.1 Audience

This document is written for administrators configuring the TOE, specifically the ISR 900 IOS 15.9 software. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, 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 IOS software and the various 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, 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 ISR900 Series operations. It is recommended that you read all instructions in this document and any references before performing steps outlined and entering commands. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

## 1.3 Document References

This document refers to several Cisco Systems documents. The documents used are shown below in Table 3 Reference Documents. Throughout this document, the guides will be referred to by the "#", such as **[1]**.

**Table 3 Reference Documents**

| Reference number | Document Name | Link |
|---|---|---|
| [1] | Release Notes for Cisco 900 Series Integrated Services Routers (ISR) running Cisco IOS Release 15.9(3)M | https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/15-8m/release/notes/15-8-3-m-rel-notes.html |
| [2] | Hardware Installation Guide for the Cisco 900 Series Integrated Services Router | https://www.cisco.com/c/en/us/td/docs/routers/access/900/hardware/installation/guide/b-cisco-ISR900-series-hig.html |
| [3] | Cisco 900 Series ISR Software Configuration Guide | https://www.cisco.com/c/en/us/td/docs/routers/access/900/software/configuration/guide/900SCG.html<br><br>https://gzhls.at/blob/ldb/e/0/9/2/28dfe39365458bd39f88a4e95413c1ac3607.pdf |
| [4] | Cisco IOS Security Configuration Guide: Securing User Services, Release 15.1S | https://www.cisco.com/c/dam/en/us/td/docs/ios/sec_user_services/configuration/guide/15_1s/sec_user_svcs_15_1S_cg_book.pdf |
| [5] | Cisco Networking Services Configuration Guide, Cisco IOS Release 15M&T | https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cns/configuration/15-mt/cns-15-mt-book.html |
| [6] | Cisco IOS Security Command Reference A to Z | http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html<br><br>http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-d1-cr-book.html<br><br>http://www.cisco.com/en/US/docs/ios-xml/ios/security/m1/sec-m1-cr-book.html<br><br>http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-s1-cr-book.html<br><br>(master list)<br>http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html |
| [7] | FIPS Certificate | https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program |

| Reference number | Document Name | Link |
|---|---|---|
| [8] | IP Routing: Protocol-Independent Configuration Guide, Cisco IOS Release 15M&T | https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/15-mt/iri-15-mt-book.html |
| [9] | Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS Release 15M&T | https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ikevpn/configuration/15-mt/sec-ike-for-ipsec-vpns-15-mt-book.html |
| [10] | Cisco IOS Configuration Fundamentals Command Reference | https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book.html |
| [11] | Configuration Fundamentals Configuration Guide | https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xe-16/fundamentals-xe-16-book.html |
| [12] | Secure Shell Configuration Guide, Cisco IOS Release 15M&T | https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/15-mt/sec-usr-ssh-15-mt-book.pdf |
| [13] | Cisco System Messages | https://www.cisco.com/c/en/us/td/docs/ios/system/messages/guide/consol_smg/sm_cnovr.html |
| [14] | Public Key Infrastructure Configuration Guide, Cisco IOS Release 15MT | https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book.html |
| [15] | Loading and Managing System Images Configuration Guide | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sys-image-mgmt/configuration/xe-16/sysimgmgmt-xe-16-book.html |
| [16] | Basic System Management Configuration Guide, Cisco IOS Release 15M&T | https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/15-mt/bsm-15-mt-book.html |
| [17] | Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS Release 15M&T | https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book.html |
| [18] | Security for VPNs with IPsec Configuration Guide, Cisco IOS Release15M&T | https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configur |

| Reference number | Document Name | Link |
|---|---|---|
| | | ation/15-mt/sec-sec-for-vpns-w-ipsec-15-mt-book.pdf |

## 1.4 Supported Hardware and Software

Only the following hardware and software listed in Section 1.4 Supported Hardware and Software is compliant with the Common Criteria Cisco 900 Series Integrated Services Routers (ISR) collaborative Protection Profile for Network Devices v2.2e (NDcPP v2.2e) and PP-Module for Virtual Private Network (VPN) Gateways v1.1 (MOD_VPNGW v1.1) 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 TOE is the hardware and software solution that makes up the Cisco Integrated Service Routers 900 Series (ISR900) models. The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS software image Release 15.9. In addition, the software image is also downloadable from the Cisco web site.

The TOE guidance documentation that is also considered to be part of the TOE is the Cisco 900 Series Integrated Services Routers (ISR) Common Criteria Operational User Guidance And Preparative Procedures. This document is downloadable from the http://cisco.com web site at:

> https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/common-criteria.html.

In Table 1 Common Criteria Certified Product Guidance Enter the certified product name or simply click on the certification date for the product. A PDF version of the document will be displayed, which can be downloaded and saved.

### 1.4.1 Supported Configurations

The TOE is comprised of both software and hardware. The hardware is comprised of the following Cisco 900 Series Integrated Services Routers (ISR) (herein after referred to as the ISR900); C921-4P, C921J-4P, C931-4P, C926-4P and C927-4P.

The software is comprised of the Universal Cisco Internet Operating System (IOS) software image Release IOS 15.9.

The ISR900 that comprises the TOE has common hardware characteristics. These characteristics affect only non-TSF relevant functions of the router (such as throughput and amount of storage) and therefore support security equivalency of the routers in terms of hardware.

The ISR900 primary features include the following:

- Hardware LAN ports to connect multiple devices; ready to support secure broadband and Metro Ethernet connectivity;
- Dedicated management port on the router, RJ-45 console port and a USB B console connection;
- Dynamic memory, used by the central processor for all system operation;
- Flash memory (EEPROM), used to store the Cisco IOS-XE image (binary program);
- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs and

- Non-volatile random-access memory (NVRAM) is used to store router configuration parameters that are used to initialize the system at start-up.

Cisco IOS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in this document.

## 1.5 Operational Environment

The TOE supports the following hardware, software, and firmware components in its operational environment. Each component is identified as being required or not based on the claims made in this Security Target. All the following environment components are supported by all TOE evaluated configurations.

**Table 4 Required non-TOE Hardware/ Software/ Firmware**

| Component | Usage/Purpose Description for TOE performance |
|---|---|
| Management Workstation with SSH Client | 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. |
| Local Console | 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. |
| RADIUS AAA Server | This includes any IT environment RADIUS AAA server that provides single-use authentication mechanisms. This can be any RADIUS AAA server that provides single-use authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide single-use authentication to administrators. |
| Syslog Server | The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE. The syslog server will need to act as an IPsec peer or as an IPsec endpoint. |
| Certification Authority (CA) | This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment. |
| VPN Peer | A remote VPN Peer is another network device that the TOE sets up a VPN connection with. This could be a VPN client or another router. |

## 1.6 Excluded Functionality

The exclusion of this functionality does not affect the compliance to the NDcPP v2.2e and MOD_VPNGW v1.1.

**Table 5 Excluded Functionality**

| Excluded Functionality | Exclusion Rationale |
|---|---|
| Non-FIPS 140-2 mode of operation on the router. | This mode of operation includes non-FIPS allowed operations. |

# 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** Record 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 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:

**Table 6: Evaluated Products and their External Identification**

| Product Name | External Identification |
|---|---|
| Cisco 900 Series Integrated Service Routers | ISR 900 |

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

- Download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. The reason to download to a trusted system within your

organization, such as the management workstation, is to ensure the file has not been tampered with prior to securely copying to the TOE for installation.

- Software images are available from Cisco.com at the following:

  https://www.cisco.com/c/en/us/support/routers/900-series-integrated-services-routers-isr/tsd-products-support-series-home.html

- The TOE ships with the correct software images installed, however this may not be the evaluated version.

**Step 8** Once the file is downloaded **[15],** verify that it was not tampered with by using a SHA-512 utility to compute a SHA-512 hash for the downloaded file and comparing this with the SHA-512 hash for the image listed in Table 7 below as described in Image Verification **[3]**. If the SHA-512 hashes do not match, contact Cisco Technical Assistance Center (TAC) https://tools.cisco.com/ServiceRequestTool/create/launch.do.

Once the file has been copied, it is recommended that you read and familiarize yourself Overview Basic Configuration of a Cisco Networking Device and Using Auto Install to Remotely Configure Cisco Networking Devices **[11]** before proceeding with the install. You may also want to familiarize yourself with **[1]** Release Notes, **[6]** basic commands and **[11]** Using the Cisco IOS Command-Line Interface concepts before proceeding with the installation and configuration of the TOE.

**Step 9** In the evaluated configuration, the published hash is used to ensure the image has not been tampered. The TOE will automatically display the hash verification on boot or by using the reload command. The successful hash verification message will display on the successful verification of the boot image. If the image was tampered with in any way, an error would be displayed, and the image will not boot. Confirm that the TOE loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

To verify the published hash, you can use a checksum utility of your choice to compute the hash for the downloaded image file and then comparing the results against the image hash listed below in Table 7: Evaluated Software Images.

If the hashes do not match, contact Cisco Technical Assistance Center (TAC) http://tools.cisco.com/ServiceRequestTool/create/launch.do. Login to CCO is required.

The image authenticity can also be verified using the digital signature. To verify the digital signature prior to installation, the show software authenticity file command allows you to display software authentication related information that includes image credential information, key type used for verification, signing information, and other attributes in the signature envelope, for a specific image file. The command handler will extract the signature envelope and its fields from the image file and dump the required information **[15]** Loading and Maintaining System Images -> Digitally Signed Cisco Software using the **show software authenticity file [6]**

> Router# **show software authenticity file** {bootflash0:filename | bootflash1:filename | bootflash:filename | nvram:filename | usbflash0:filename | usbflash1:filename}

To display the software public keys that are in the storage with the key types, use the **show software authenticity keys** command in privileged EXEC mode.

To display information related to software authentication for the current ROM monitor (ROMMON), monitor library (monlib), and Cisco IOS image used for booting, use the **show**

**software authenticity running** command in privileged EXEC mode. If there was an issue with the digital signature verification, an error message would be displayed, and the image will not boot.

Once the image is loaded into bootflash, to display information related to software authenticity for a specific image file, use the verify command. For example:

<900># verify <image name>

The image name and hash are listed below in Table 7: Evaluated Software Images

If the output from the show software authenticity file command does not provide expected output as described in **[1]**, contact Cisco Technical Assistance Center (TAC) https://tools.cisco.com/ServiceRequestTool/create/launch.do.

**Step 10** To Install and configure your ISR900 Series router follow the instructions as described in **[3]** Overview Basic Configuration of a Cisco Networking Device, depending on your organization and current network environment, select either IOS AutoInstall or IOS Setup mode ’.

Start your ISR900 Series router as described in **[3]**. Confirm that your ISR900 Series router loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

**Step 11** The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. Use the “**show version**” command **[6]** (master list) show mvrp interface through snmp-server enable traps ospf rate-limit to display the currently running system image filename and the system software release version. See below for the detailed hash value that must be checked to ensure the software has not been modified in anyway.

**Table 7: Evaluated Software Images**

| Software Version | Image Name / Description | SHA512 Checksum Hash |
|---|---|---|
| IOS 15.9 | c900-universalk9-mz.SPA.159-3.M4.bin | ddd26f4c7808e2bf851821191ded0540<br>86c2bee276de0012d1ebcbbf97ef2e7ec<br>df8c344eb3f53272410b82122eb217044<br>6638e3ef8b01117fd550b9f8056df0 |

When updates, including psirts (bug fixes) to the evaluated imagine are posted, customers are notified that updates are available (if they have purchased continuing support), information provided how to download updates and how to verify the update is the same as described above.

# 3. Secure Installation and Configuration

To ensure the TOE is in its evaluated configuration, the configuration settings outlined in the following sections need to be followed and applied. The evaluated configuration includes the following security features that are relevant to the secure configuration and operation of the TOE.

- Security audit – ensures that audit records are generated for the relevant events and are securely transmitted to a remote syslog server
- Cryptographic support – ensures cryptography support for secure communications.
- Identification and authentication – ensures the warning banner is displayed at login, that all users are successfully identified and authenticated prior to gaining access to the TOE, the users can only perform functions in which they have privileges, and terminates users after a configured period of inactivity
- Secure Management – provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection.
- Packet Filtering - The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers and the TOE. More accurately, these tunnels are sets of security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to interfaces using crypto map sets.
- Protection of the TSF - protects against interference and tampering by untrusted subjects by implementing identification, authentication, the access controls to limit configuration to Authorized Administrators and the TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software. TOE performs testing to verify correct operation of the router itself and that of the cryptographic module. Finally, the TOE maintains the date and time.
- TOE Access - terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE can also be configured to lock the Authorized Administrator account after a specified number of failed logon attempts until an authorized administrator can enable the user account. The TOE can also display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.
- Trusted Path/Channel - allows trusted channels to be established to itself from remote administrators over SSHv2 and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session between the TOE and the authentication servers as well as to protect communications with a CA.

## 3.1 Physical Installation

Follow the Cisco 900 Series Integrated Services Routers Hardware Installation Guide **[2]** for preparation of the physical site, and hardware installation.

## 3.2 Initial Setup via Direct Console Connection

The Cisco 900 Series Integrated Services Routers must be given basic configuration via console connection prior to being connected to any network. The console can be any environment console that is physically connected to the router, via the Serial Console Port (RJ-45).

### 3.2.1 Options to be chosen during the initial setup of the Cisco 900 Series Integrated Services Routers

The setup starts automatically when a device has no configuration file in NVRAM. When setup completes, it presents the System Configuration Dialog. This dialog guides the administrator through the initial configuration with prompts for basic information about the TOE and network and then creates an initial configuration file. After the file is created, an authorized administrator can use the CLI to perform additional configuration. *Performing Device Setup Configuration* in **[3]** describes how to use Setup to build a basic configuration and to make configuration changes. The following items must be taken into consideration during setup:

- The account created during the initial installation of the TOE is considered the privileged administrator and has been granted access to all commands on the TOE (privilege level 15).
- The privilege levels are not necessarily hierarchical in the sense they are configurable. The privilege level determines the functions the user can perform. Privilege levels 0 and 1 are defined by default, while levels 2-14 are undefined by default. Levels 0-14 are considered the semi-privileged administrator and can be set to include any of the commands available to the level 15 administrators.
- The number of administrators created, and their various levels of access are based on organizational requirements and policies.
- The term "Authorized Administrator" is used in this document to refer to any administrator that has successfully authenticated to the router and has access to the appropriate privileges to perform the requested functions.

Refer to the IOS Command Reference Guide for available commands, associated roles and privilege levels **[3] [4] [6] [10]**.

1 – Enable Secret – Must adhere to the password complexity requirements. This setting can be confirmed after "setup" is complete by examining the configuration file for "enable secret 5 …" in Cisco IOS Security Command Reference: Commands D to L -> select E -> select enable secret -> **[6]**

2 – Enable Password - Must adhere to the password complexity requirements. This must be set to something different than the enable secret during "setup", however after setup this will not be used within the evaluated configuration. In Cisco IOS Security Command Reference: Commands D to L -> select E -> select enable password **[6]**

3 – Virtual Terminal Password - Must adhere to the password complexity requirements. Securing the virtual terminal (or vty) lines with a password in the evaluated configuration is suggested. This password allows access to the device through only the console port. Later in this guide steps will be given to allow ssh into the vty lines. Reference password (line configuration) In Cisco IOS Security Command Reference: Commands M to R -> select pac key through port-misuse -> select password (line configuration) **[6]**

4 – Configure SNMP Network Management – No (this is the default). This setting can be confirmed after "setup" is complete by examining the configuration file to ensure that there is no "snmp-

server" entry. To ensure there is no snmp server agent running, use the "**no snmp-server**' command. In the evaluated configuration, SNMP should remain disabled, as it was not tested during the evaluation.

### 3.2.2 Saving Configuration

IOS uses both a running configuration and a starting configuration. Configuration changes affect the running configuration, in order to save that configuration, the running configuration (held in memory) must be copied to the startup configuration. This may also be achieved by either using the **write memory** command **[6]** or the **copy system:running-config nvram:startup-config** command in **[6]** These commands should be used frequently when making changes to the configuration of the router. If the router reboots and resumes operation when uncommitted changes have been made, these changes will be lost, and the router will revert to the last configuration saved. To see the current configuration, use the **show running-config** command in **[6]** Cisco IOS Security Commands Reference: Commands S to Z -> show parameter-map type consent through show users -> show running-config.

### 3.2.3 Enabling FIPS Mode

The TOE must be run in the FIPS mode of operation by ensuring the cryptographic functions are operating correctly. The use of the cryptographic engine in any other mode was not evaluated nor tested during the CC evaluation of the TOE. This is done by setting the following in the configuration:

The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots the IOS image. From the ROMMON command line enter the following**:**

**confreg 0x0102**

The self-tests for the cryptographic functions in the TOE are run automatically during power-on as part of the POST. The same POST self-tests for the cryptographic operations can also be executed manually at any time by the Authorized Administrator using the command:

**test crypto self-test**

If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen, saved in the crashinfo file, and all secure data transmission is halted.

- 

### 3.2.4 Administration of Cryptographic Self-Tests

The TOE provides Power on Startup Test (POST) that are consistent with the FIPS 140-2 requirements. These POST tests for the cryptographic functions in the TOE are run automatically during the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software).. These tests include the following:

- AES Known Answer Test
- HMAC Known Answer Test
- RNG/DRBG Known Answer Test
- SHA-1/256/512 Known Answer Test

- ECDSA Self-Test
- RSA Signature Known Answer Test (both signature/verification)
- Software Integrity Test

Additionally, the power-on self-tests are performed after the cryptographic systems are initialized but prior to the underlying OS initialization of external interfaces; this prevents the security appliances from passing any data before completing power-on self-tests (POST) and entering FIPS mode.

The tests include:

- AES Known Answer Test –

For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly.

- RSA Signature Known Answer Test (both signature/verification) –

This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly.

- RNG/DRBG Known Answer Test –

For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly.

- HMAC Known Answer Test –

For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly.

- SHA-1/256/512 Known Answer Test –

For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match, and the hash operations are operating correctly.

- ECDSA Self-Test –

This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This

value is compared to the original plaintext value to ensure the decrypt operation is working properly.

In addition, the Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms that the image file that's about to be loaded has maintained its integrity. Prior to installing the image, the Authorized Administrator can verify the public hash to ensure the files has not been tampered.

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. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic.

If an error occurs during the self-test, a SELF_TEST_FAILURE system log is generated. Following is an example:

> Example Error Message _FIPS-2-SELF_TEST_IOS_FAILURE: "IOS crypto FIPS self test failed at %s."
>
> Explanation FIPS self test on IOS crypto routine failed.

These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected because any deviation in the TSF behavior will be identified by the failure of a self-test.

### 3.2.5 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 Authorized 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

The Authorized Administrator can also run the **show diagnostic** command to display the diagnostic test results and the supported test **[6]**. For troubleshooting any error messages received while running the tests, messages from running diagnostic and actions to take, refer to System Message Overview **[13].**

### 3.2.6 Access Control and Lockout

The ISR900 Series must be configured to use a username and password for each administrator and one password for the enable command. Ensure all passwords are stored encrypted by using the following command **[6]:**

Commands S to Z -> sa ipsec through sessions maximum ->service password-encryption:

**service password-encryption**

When creating administrator accounts, all individual accounts are to be set to a privilege level of one. This is done by using the following commands:

Commands S to Z -> traffic-export through zone security -> username (with parameters listed below)

**username** <name> **password** <password>

to create a new username and password combination, and

**username** <name> **privilege 1**

to set the privilege level of <name> to 1. If combining to one command, the password must be the last parameter:

**username <name> privilege 1 password <password>**

To prevent administrators from choosing insecure passwords, each password must be at least 15 characters long. You may use the following command to set the minimum length to 15 if available on the TOE model or set using the **aaa-common-criteria policy** command.

**security passwords min-length** *<length>* **[6]** Cisco IOS Security Commands Reference: Commands S to Z -> sa ipsec through sessions maximum -> security passwords min-length

Refer to Section 4.2 in this document or **[6]** for configuring strong passwords and setting the minimum password length using the **aaa-common-criteria policy** command. Also refer to **[6]** for any of the following commands:

To ensure the plain text password is securely stored, use the **password encryption aes** command **[6]** Cisco IOS Security Commands Reference: Commands M to R -> password encryption aes

Identification and authentication on the console/auxiliary port is required for Users. In the configuration mode, enter the following command **[6]**:

Router(config)#**aaa authentication login via-console**

Router(config)#**line console 0**

Router(config-line)#**login authentication via-console**

Administrator account access is to be restricted to a specified number of authentication attempts before the administrator account in question is locked out. The account then requires unlocking by an authorized administrator before it can be used again. The evaluated configuration requires that the lockout occurs after a specified threshold for unsuccessful authentication attempts. Use the following command, with '<x>' being the required number of attempts before lockout, to set the authentication failure threshold (the authentication threshold must be non-zero):

Commands A to C -> aaa accounting -> aaa local authentication attempts max-fail (with parameters listed below)

**aaa local authentication attempts max-fail <**x>

A locked user account may be unlocked by a privileged administrator by using the following command **[6]**:

Commands A to C -> ca trust-point -> clear aaa local user lockout (with parameters listed below)

**clear aaa local user lockout** <username>

You can enter a single username, or you can enter 'all' to specify all locked users are to be unlocked.

### 3.2.7 Session Termination

Inactivity settings must trigger termination of the administrator session. These settings are configurable using the following listed commands. See **[6]** *Cisco IOS Security Command References: Commands A to Z for the following commands.*

**line vty <first> <last>**

**exec-timeout <time>**

where first and last are the range of vty lines on the box (i.e. "0 4"), and time is the period of inactivity after which the session should be terminated for remote administration access via SSH.

See **[4]** under Authentication, Authorization, and Accounting Configuration Guide, section User Security Configuration and/or **[10]** D through E to set the local line console and time out

**line console**

**exec-timeout <time>**

The line console setting is not immediately activated for the current session. The current console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session.

In addition to session timeouts, an administrator can manually logout from the TOE with the following command: **exit**

### 3.2.8 User Lockout

User accounts must be configured to lockout after a specified number of authentication failures. See **[6]** *Cisco IOS Security Command References: Commands A to Z for the following commands.*

**aaa local authentication attempts max-fail [*number of failures*]**

where number of failures is the number of consecutive failures that will trigger locking of the account. Configuration of these settings is limited to the privileged administrator (see 4.1 User Roles).

Related commands:

**Table 8 AAA Commands**

| AAA Command | AAA Command Result |
|---|---|
| clear aaa local user fail-attempts | Clears the unsuccessful login attempts of the user. |
| clear aaa local user lockout | Unlocks the locked-out user. |
| show aaa local user lockout | Displays a list of all locked-out users. |

This applies to consecutive failures on the TOE during a given session and is not affected by the SSH session disconnections after their default number of failures.

To ensure the privileged administrator account does not get locked out by the number of failed attempts it is essential that an additional Administrator account be created to only be used in an emergency at the local console to unlock the locked Administrator account. Although, it is noted that the lockout is not applicable to the local console administrators.

## 3.3 Network Protocols and Cryptographic Settings

The router provides secure transmission when TSF data is transmitted between separate parts of the TOE (encrypted sessions for remote administration (via SSHv2)).

The router also supports the use of a remote AAA server (RADIUS), provided by the environment that is used as the enforcement point for identifying and authenticating users, including login and password dialog, challenge and response, and messaging support. Encryption of the packet body is provided using RADIUS (RADIUS only encrypts the password within the packet body). This AAA server should be on an internal protected network, such as a network isolated behind a VPN gateway, through which the ISR900 Series can reach the AAA server using an IPsec tunnel.

**Note:** if any of the network protocol connections are unintentionally broken, the connection will need to be re-established following the steps described below for each of the following protocols, IPsec and SSH.

### 3.3.1 Remote Administration Protocols

Telnet should not be used for management purposes as there is no protection for the data that is transmitted. To ensure the administrator does not use Telnet for management purposes, the following commands sets the vty port to only accept ssh connections **[6] [12]**.

**line vty 0 10**

**transport input ssh**

SSHv2 must be used to secure the trusted path for remote administration for all SSHv2 sessions. To enable sshv2, use the "**ip ssh version 2**" command **[6]** Commands D to L -> ip source-track through ivrf -> ip ssh version.

Before SSH is configured, the rsa keys need to be generated for the SSH server using the following command:

**crypto key generate rsa** with an RSA key size of **2048 bits [6]** Commands A to C -> crypto isakmp aggressive-mode disable -> crypto key generate.

RSA keys are generated in pairs—one public RSA key and one private RSA key. This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

Only one set of keys can be configured using the **crypto key generate** command at a time. Repeating the command overwrites the old keys.

If the configuration is not saved to NVRAM with a "**copy run start**", the generated keys are lost on the next reload of the router.

If the error "% Please define a domain-name first" is received, enter the command '**ip domain-name [domain name]**'.

SSH must be configured to require use of as a minimum, Diffie-Hellmann group 14. IOS allows the required DH groups to be specified by their modulus size. The default is modulus 1024 (DH Group 1). To require use of DH Group 14, specify a minimum modulus size of 2048 using the following command **[12]** or **[6]** Commands D to L -> ip source-track through ivrf:

**ip ssh dh min size 2048**

In addition, configure your ssh client for dh-group-14, in Putty, configure the SSH client to support only diffie-hellman-group14-sha1 key exchange. To configure Putty, do the following:

- Go into Putty Configuration Select > Connection > SSH > Kex;
- Under Algorithm selection policy: move Diffie-Hellman group 14 to the top of the list;
- Move the "warn below here" option to right below DH group14

When SSHv2 is enabled the TOE can be configured to limit the algorithms and ciphers that can be used for the secure SSH connection.

To secure and control SSH sessions, the evaluated configuration requires SSHv2 session to only use AES-CBC-128 and AES-CBC-256 encryption key algorithms. To set, use the following command **[12]** How to Configure SSH Algorithms for Common Criteria Certification -> Configuring an Encryption Key Algorithm for a Cisco IOS SSH Server and Client:

**ip ssh server algorithm encryption aes128-cbc aes256-cbc**

The TOE also needs to be configured to only support hmac-sha1, hmac-sha256, and hmac-sha512 MAC algorithms using the following command **[12]** How to Configure SSH Algorithms for Common Criteria Certification -> Configuring a MAC Algorithm for a Cisco IOS SSH Server and Client:

**ip ssh server algorithm mac hmac-sha1 hmac-sha256 hmac-sha512**

To secure and control SSH sessions, the evaluated configuration requires that the SSHv2 session timeout period and maximum number of failed login attempts to be set. This is done by using the following command:

**ip ssh timeout <seconds>** (in the evaluated configuration this is set to 120 seconds. The default and maximum is 120 seconds) **[6]**. Commands D to L -> ip source-track through ivrf (with the parameters listed above) and **[12]**

**ip ssh authentication-retries <integer>** (in the evaluated configuration is limited to 3. The default is 3, with a maximum of 5) **[6]**. Commands D to L -> ip source-track through ivrf (with the parameters listed above) and **[12]**

The evaluated configuration also requires the TOE to re-key of no longer than one hour (time 60) and no more than one gigabyte (volume 1000000) of transmitted data. This can be initiated by the client of by issuing the following command **[6]** and **[12]**

**ip ssh rekey** { **time** *time* | **volume** *volume* }

Note, the TOE will react to first threshold limit reached and perform an ip-ssh rekey.

To verify the proper encryption algorithms are used for established SSHv2 connections; use the "**show ssh sessions**" command **[6]**. To disconnect SSH sessions, use the **ssh disconnect** command **[6]**.

The TOE acting as the SSH server supports three types of user authentication methods and sends these authentication methods to the SSH client in the following predefined order:

- Public-key authentication method
- Keyboard-interactive authentication method (note this method is not included nor allowed in the evaluated configuration and must be disabled using the following command **no ip ssh server authenticate user keyboard**
- Password authentication method

By default, all the user authentication methods are enabled. Use the **no ip ssh server authenticate user {publickey | keyboard | pasword}** command to disable any specific user authentication method so that the disabled method is not negotiated in the SSH user authentication protocol. This feature helps the SSH server offer any preferred user authentication method in an order different from the predefined order. The disabled user authentication method can be enabled using **the ip ssh server authenticate user {publickey | keyboard | pasword}** command. Refer to Secure Shell -> Configuring User Authentication Methods **[12]**.

In addition, the following configurations also need to be set for the excluded functionality.

HTTP server was not evaluated and must be disabled **[6]** and **[4]**. Securing User Services Overview

**no ip http server [4]**. Securing User Services Overview

HTTPS server was not evaluated and must be disabled **[6]** and **[4]**. Securing User Services Overview:

**no ip http secure-server**

SNMP server was not evaluated and must be disabled **[6]**

**no snmp-server**

### 3.3.2 Authentication Server Protocols

RADIUS (outbound) for authentication of TOE administrators to remote authentication servers is disabled by default but can be enabled by administrators in the evaluated configuration. Use best practice for selection and protection of a key to ensure that the key is not easily guessable and is not shared with unauthorized users.

For further information about configuring RADIUS, refer to Cisco IOS Security Command Reference: Commands M to R -> radius attributes nas-port-type through rd -> radius server **[6]** or Securing User Services Overview **->** RADIUS and TACACS+ **[4]**.

If using RADIUS for remote authentication, the connection must be secured using IPsec

It is recommended to read the referenced sections to become familiar with remote authentication concepts prior to configuration.

Refer to 3.3.7 IPsec Overview and 3.3.9 Session Protection in this document.

### 3.3.3 Routing Protocols

The routing protocols are used to maintain routing tables. The routing tables can also be configured and maintained manually. Refer to the applicable sections in **[8]** for configuration of the routing protocols.

Note, this functionality was not claimed or tested in the evaluated configuration.

### 3.3.4 Basic Firewall Packet Filtering Configuration

The TOE supports the following packet filtering firewall rule set of the following protocols:

- IPv4 (RFC 791)
- IPv6 (RFC 2460)
- TCP (RFC 793)
- UDP (RFC 768)
- IKEv2 (RFC 5996)
- IPsec ESP (RFCs 4301, 4303)
- SSH (RFCs 4251, 4252, 4253, 4254, 6668)

The following attributes, at a minimum, are configurable within Packet filtering rules for the associated protocols:

- IPv4
  - Source address
  - Destination Address
  - Protocol
- IPv6
  - Source address
  - Destination Address
  - Next Header (Protocol)
- TCP
  - Source Port
  - Destination Port
- UDP
  - Source Port
  - Destination Port

Traffic matching is done based on a top-down approach in the access list. The first entry that a packet matches will be the one applied to it. The MOD_VPNGW requires that the TOE Access control lists (ACLs) are to be configured to drop all packet flows as the default rule and that traffic matching the acl be able to be logged. The drop all default rule can be achieved by including an ACL rule to drop all I ch as the last rule in the ACL configuration. The logging of matching traffic is done by appending the key word “log-input” per the command reference at the end of the acl statements, as done below.

A privileged authorized administrator may manipulate the ACLs using the commands ip inspect, access-list, crypto map, and access-group as described **[6] [10]**.

Access lists must be configured on the TOE to meet the requirements of the MOD_VPNGW.

***Note:*** These access lists must be integrated with the defined security policy for your TOE router. Enabling just these access lists with no permits will result in traffic being dropped. Ensure that your access list entries are inserted above the default deny acl.

In this example, it is assumed that interface GigabitEthernet0/0 is the external interface, and is assigned an IP address of 10.200.1.1. Interface GigabitEthernet0/1 is the internal interface and is assigned an IP address of 10.100.1.1.

If remote administration is required, ssh has to be explicitly allowed through either the internal or external interfaces.

TOE-common-criteria# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

TOE-common-criteria(config)# **access-list 199 permit tcp host 10.200.1.1 host 10.200.0.1 eq 22 log-input**

To include the port numbers within the logs and activate it on an interface, use the following extended access list configuration:

TOE-common-criteria(config)# **ip access-list extended <name of list>**

TOE-common-criteria(config-ext-nacl)# **permit tcp 10.200.1.1 0.0.0.0 range 2020 2021 10.200.0.1 0.0.0.0 range 20 21 log-input**

TOE-common-criteria(config-ext-nacl)# **interface <interface name>**

TOE-common-criteria(config-if)# **ip access-group <name of list> in**

To log connections to the Certificate Authority, implement the following acl:

TOE-common-criteria(config)# **access-list 100 permit ip any host [IP of CA] log-input**

TOE-common-criteria(config)# **access-list 199 permit ip any host [IP of CA] log-input**

To close ports that don't need to be open and may introduce additional vulnerabilities, implement the following acl:

TOE-common-criteria(config)# **access-list 100 deny 132 any any log-input**

TOE-common-criteria(config)# **access-list 199 deny 132 any any log-input**

To explicitly create the default deny acl for traffic with no other match, implement the following acl:

TOE-common-criteria(config)# **access-list 100 deny any any log-input**

TOE-common-criteria(config)# **access-list 199 deny any any log-input**

***Note:*** Logging of all traffic hitting the default deny acl can generate a large number of logs, and a determination should be made whether it is necessary prior to entering this at the end of all access lists.

To apply the acls to the interfaces (note, the following is an example and as such the actual interface name may be different based on the model):

TOE-common-criteria(config)# **interface GigabitEthernet0/0**

TOE-common-criteria(config-if)# **ip access-group 199 in**

TOE-common-criteria(config)# **interface GigabitEthernet0/1**

TOE-common-criteria(config-if)# **ip access-group 100 in**

Additional information on creation of packet filtering and VPN information flow policies is given in Section 3.3.5 below

NOTE: If using an IPv6 ACL with the **deny ipv6 any any** rule, then the following permit rules must be added to enable IPv6 neighbor discovery:

TOE-common-criteria(config)#**permit icmp any any nd-na**

TOE-common-criteria(config)#**permit icmp any any nd-ns**

### 3.3.5 Information Flow Policies

The TOE may be configured by the privileged administrators for information flow control/ firewall rules as well as VPN capabilities using the access control functionality. Configuration of information flow policies is restricted to the privileged administrator. The MOD_VPNGW requires that the TOE be able to support options for information flow policies that include discarding, bypassing, and protecting. On the TOE, an authorized administrator can define the traffic rules on the box by configuring access lists (with permit, deny, and/or log actions) and applying these access lists to interfaces using access and crypto map sets:

- The 'discard' option is accomplished using access lists with deny entries, which are applied to interfaces within access-groups. Guidance for configuration of IOS Information Flow Policies is located in the **[3]** Configuring Security Features -> Zone-based Policy Firewalls and **[17]**.
- The 'bypassing' option is accomplished using access lists, which are applied to interfaces within crypto maps for IPsec and the 'filter tunnel' command for SSL VPN. If no explicit 'permit' exists within the crypto map, but there is no explicit or implicit deny, then the packet is allowed to bypass the tunnel in plaintext. Guidance for configuration of entries for IPsec is in **[9] [14]**
- The 'protecting' option is accomplished using access lists with permit entries, which are applied to interfaces within crypto maps for IPsec and the 'filter tunnel' command for SSL VPN.

The criteria used in matching traffic in all of these access lists includes the source and destination address, and optionally the Layer 4 protocol and port.

The TOE enforces information flow policies on network packets that are receive by TOE interfaces and leave the TOE through other TOE interfaces. When network packets are received on a TOE interface, the TOE verifies whether the network traffic is allowed or not and performs one of the following actions, pass/not pass information, as well as optional logging.

**Create an ACL:**

Router(config)# access-list 100 < deny | permit> ip <source address> <source wildcard bits> <destination address> <destination wildcard bits>

**Create crypto map:**

Router(config)# crypto map <MAP_NAME> isakmp-profile

Router(config-crypto-map)# set peer 10.0.0.1

Router(config-crypto-map)# set transform-set SAMPLE_SET

Router(config-crypto-map)# match address 100

**Apply the crypto map to an interface:**

Router(config)# interface GigabitEthernet0/0

Router(config-if)# crypto map <MAP_NAME>

Please refer to the "Cisco IOS Security Command Reference: Commands A to C" for additional information on configuring crypto maps refer to:

https://www.cisco.com/c/en/us/td/docs/iosxml/ios/security/a1/sec-a1-cr-book.html

## 3.3.6 X.509 Certificates

The TOE may be configured by the privileged administrators to use Privacy Enhanced Mail (PEM) X.509v3 certificates to authenticate IPsec peers. Both RSA and ECDSA certificates are supported.

Creation of these certificates and loading them on the TOE is covered in **[14]**, and a portion of the TOE configuration for use of these certificates follows below.

CRL is used for certificate revocation checking. The authorized administrator can use the "revocation-check" command to specify at least one method of revocation checking; CRL is not the default method and must be selected in the evaluated configuration. The authorized administer sets the trust point and its name and the revocation-check method. If the TOE does not have the applicable CRL and is unable to obtain one, the TOE will reject the peer's certificate.

Checking is done for the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE. The local certificate that was imported must contain the basic constraints extension with the CA flag set to true, the check also ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set. If they are not, the certificate is not accepted.

The certificate chain path validation is configured on the TOE by first setting crypto pki trustpoint name and then configuring the level to which a certificate chain is processed on all certificates, including subordinate CA certificates using the chain-validation command. If the connection to determine the certificate validity cannot be established, the certificate is not accepted, and the connection will not be established.

NOTE: Certificate revocation check is performed when certificates are loaded on the device and on each use during the authentication step and is the same process for all certificates.

### 3.3.6.1 Generate a Key Pair

RSA and ECDSA keys are generated in pairs, one public key and one private key:

(config)# **crypto key generate rsa modulus 2048**

**-or-**

(config)# **crypto key generate ec keysize <256 | 384> exportable**

The keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

***Note:*** Only one set of keys can be configured using the crypto key generate command at a time. Repeating the command overwrites the old keys.

***Note:*** If the configuration is not saved to NVRAM with a "copy run start", the generated keys are lost on the next reload of the router.

***Note:*** If the error "% Please define a domain-name first" is received, enter the command 'ip domain-name [domain name].

### 3.3.6.2 Creation of the Certificate Signing Request

The certificate signing request for the TOE will be created using the RSA key pair and the domain name configured in Section 3.3.1 above.

In order for a certificate signing request to be generated, the TOE must be configured with a hostname, trustpoint, enrollment method and revocation checking. This is done by using the following commands **[6]**:

- To specify the hostname for the peer in the IKE keyring exchange, use the **hostname** *name* in configuration mode

  **Hostname** <**name**>

  Where the <**name**> is the name of the peer (**hostname routerTOE**)

- To declare the trustpoint that the TOE should use, use the **crypto pki trustpoint** *name* command in configuration mode

  **crypto pki trustpoint** <**name**>

  Where the <**name**> creates the name of the trustpoint (**crypto pki trustpoint ciscotest**)

- To specify the enrollment parameters of a certification authority (CA), use the enrollment [terminal or url] command in ca-trustpoint configuration mode

  **enrollment url** <**url**>

  Where the <**url**> specifies the URL of the file system where the TOE should send certificate requests (**enrollment url http://192.168.2.137:80**)

- To specify the subject name settings in the certificate request, use the subject-name command in ca-trustpoint configuration mode.

  **subject-name** <**x.900-name**>

  Where the <**x.900-name**> specifies the subject name used in the certificate request. If the <**x.900-name**> argument is not specified, the fully qualified domain name (FQDN),

which is the default subject name, will be used (**subject-name CN=routerTOE.cisco.com,OU=TAC**).

***Note:*** SAN extension is not supported in the evaluated configuration.

- All of the certificates include at least the following information:

  public key and (Common Name, Organization, Organizational Unit, Country) <**subject-name**> **CN=routerTOE.cisco.com,O=cisco,OU=TAC,C=U**

- To specify the revocation check method, use the revocation-check command in ca-trustpool configuration mode.

  **revocation-check <method1>** [ *method2 method3* ]

  Where the **<method1>** specifies the method used by the TOE to check the revocation status of the certificate. Available methods are identified by the following keywords:

  - crl--Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior.
  - ocsp--Certificate checking is performed by an online certificate status protocol (OCSP) server.

  If a second and third method is specified, each method is used only if the previous method returns an error, such as a server being down.

  **NOTE:** In the evaluated configuration, only the "crl" method is to be used

  **NOTE:** In the evaluated configuration, the certificates shall be generated using RSA with a modulus of at least 2048 bits

  **NOTE:** The TOE accepts PEM formatted certificates

- To create the certificate signing request, use the crypto pki enroll command in global configuration mode.

  **crypto pki enroll <name>**

  Where **<name>** is the CA that was set above using the **crypto pki trustpoint** command (**crypto pki enroll ciscotest**)

#### 3.3.6.3 Securely Connecting to a Certificate Authority for Certificate Signing

The TOE must communicate with the CA for Certificate Signing over IPSEC. This authentication will use pre-shared keys.

Following are sample instructions to configure the TOE to support an IPSec tunnel with aes encryption, with 10.10.10.102 as the IPSec peer IP on the CA, 10.10.10.110 as the local TOE IP.

TOE-common-criteria#**configure terminal**

TOE-common-criteria(config)#**crypto isakmp policy 1**

TOE-common-criteria(config-isakmp)#**encryption aes**

TOE-common-criteria(config-isakmp)#**authentication pre-share**

TOE-common-criteria(config-isakmp)#**group 14**

TOE-common-criteria(config-isakmp)#**lifetime 86400**

TOE-common-criteria(config)#**crypto isakmp key** [*insert 22 - 127 character preshared key*] **address 10.10.10.101**

TOE-common-criteria(config)#**crypto ipsec transform-set sampleset esp-aes esp-sha-hmac**

TOE-common-criteria(cfg-crypto-trans)#**mode tunnel**

TOE-common-criteria(config)#**crypto map sample 19 ipsec-isakmp**

TOE-common-criteria(config-crypto-map)#**set peer 10.10.10.102**

TOE-common-criteria(config-crypto-map)#**set transform-set sampleset**

TOE-common-criteria(config-crypto-map)#**set pfs group14**

TOE-common-criteria(config-crypto-map)#**match address 170**

TOE-common-criteria(config-crypto-map)#**exi**t

TOE-common-criteria(config)#**interface g0/0**

TOE-common-criteria(config-if)#**ip address 10.10.10.110 255.255.255.0**

TOE-common-criteria(config-if)#**crypto map sample**

TOE-common-criteria(config-if)#**exit**

TOE-common-criteria(config)#**access-list 170 permit ip 10.10.10.0 0.255.255.255 10.10.10.0 0.255.255.255**

#### 3.3.6.4 Authenticating the Certificate Authority

The TOE must authenticate the CA by acknowledging its attributes match the publicly posted fingerprint.

- To authenticate the certification authority (by getting the certificate of the CA), use the crypto ca authenticate command in global configuration mode.

  **crypto ca authenticate** <**trustpoint-name**>

  Where <**trustpoint-name**> specifies the name of the CA that was set above using the **crypto pki trustpoint** command (**crypto ca authenticate ciscotest**)

The TOE administrator must verify that the output of the command below matches the fingerprint of the CA on its public site.

Device (config)#**crypto ca authenticate ciscotest**

Certificate has the following attributes:

Fingerprint MD5: 8DE88FE5 78FF27DF 97BA7CCA 57DC1217

Fingerprint SHA1: 271E80EC 30304CC1 624EEE32 99F43AF8 DB9D0280

% Do you accept this certificate? [yes/no]: **yes**

Trustpoint CA certificate accepted.

### 3.3.6.5 Storing Certificates to a Local Storage Location

Certificates are stored to NVRAM by default; however, some routers do not have the required amount of NVRAM to successfully store certificates. All Cisco platforms support NVRAM and flash local storage. Depending on the platform, an authorized administrator may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token. During run time, an authorized administrator can specify what active local storage device will be used to store certificates. For more detailed information see the *Public Key Infrastructure Configuration Guide* Guidance document **[14]** Storing PKI Credential, section "How to Configure PKI Storage."

### 3.3.6.6 How to Specify a Local Storage Location for Certificates

The summary steps for storing certificates locally to the TOE are as follows:

1. Enter configure terminal mode:

   TOE-common-criteria# **configure terminal**

2. Specify the local storage location for certificates: **crypto pki certificate storage *location-name***

   Device(config)# **crypto pki certificate storage flash:/certs**

3. Exit:

   Device(config)# **exit**

4. Save the changes made:

   Device# **copy system:running-config nvram:startup-config**

5. Display the current setting for the PKI certificate storage location:

   Device# **show crypto pki certificates storage**

The following is sample output from the show crypto pki certificates storage command, which shows that the certificates are stored in the certs subdirectory of disk0:

```
Device# show crypto pki certificates storage
Certificates will be stored in disk0:/certs/
```

The authorized administrator can also configure one or more certificate fields together with their matching criteria to match. Such as:

- expires-on
- issuer-name
- name
- serial-number
- subject-name
- unstructured-subject-name
- valid-start

This allows for installing more than one certificate from one or more CAs on the TOE. For example, one certificate from one CA could be used for SSH connections, while another certificate from

another CA could be used for IPsec connections. However, the default configuration is a single certificate from one CA that is used for all authenticated connections.

### 3.3.6.7 Configuring a Revocation Mechanism for PKI Certificate Status Checking

Perform this task to set up the certificate revocation mechanism CRL that is used to check the status of certificates in a PKI.

Use the **revocation-check** command to specify the method (CRL) that is to be used to ensure that the certificate of a peer has not been revoked.

(ca-trustpoint)#**revocation-check crl**

If the TOE does not have the applicable CRL and is unable to obtain one, the TOE will reject the peer's certificate.

### 3.3.6.8 Configuring Certificate Chain Validation

Perform this task to configure the processing level for the certificate chain path of peer certificates.

Prerequisites:

- The device must be enrolled in your PKI hierarchy.
- The appropriate key pair must be associated with the certificate.

1. Enter configure terminal mode:

   TOE-common-criteria# **configure terminal**

2. Set the crypto pki trustpoint name:

   TOE-common-criteria(config)# **crypto pki trustpoint ca-sub1**

3. Configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates using **the chain-validation [{stop | continue} [parent-trustpoint]] command**:

   TOE-common-criteria(ca-trustpoint)# **chain-validation continue ca-sub1**

   - Use the **stop** keyword to specify that the certificate is already trusted. This is the default setting.
   - Use the **continue** keyword to specify that the subordinate CA certificate associated with the trustpoint must be validated.
   - The **parent-trustpoint** argument specifies the name of the parent trustpoint the certificate must be validated against.

   ***Note:*** A trustpoint associated with the root CA cannot be configured to be validated to the next level. The **chain-validation** command is configured with the continue keyword for the trust point associated with the root CA, an error message will be displayed, and the chain validation will revert to the default **chain-validation** command setting.

4. Exit:

TOE-common-criteria(ca-trustpoint)# **exit**

### 3.3.6.9 Certificate Validation

By default, the TOE will validate the certificate of the IPsec peer including a Basic Constraints extension. No configuration is required by the administrator. Optionally as a way to test a Basic Constraints extension, the administrator can add subject name restrictions to the CA root trustpoint. Refer to How to Configure Certificate Enrollment for a PKI" in **[14]**. A portion of an example TOE configuration follows below.

TOE-common-criteria (config)# crypto pki certificate map <certificate map name> 1 subject-name co example

TOE-common-criteria (config)# crypto pki trustpoint CAroot

TOE-common-criteria (ca-trustpoint)# enrollment terminal

TOE-common-criteria (ca-trustpoint)# match certificate <certificate map name>

TOE-common-criteria (ca-trustpoint)#end

TOE-common-criteria (config)# crypto pki trustpoint CA sub

TOE-common-criteria (ca-trustpoint)# enrollment terminal

TOE-common-criteria (ca-trustpoint)# subject-name
CN=example.organization.com,OU=Spiral Dept,O=Example

TOE-common-criteria (ca-trustpoint)# match certificate <certificate map name>

TOE-common-criteria (ca-trustpoint)#end

The administrator should find an error message stating that certificate chain validation has failed because a certificate in the chain was not a valid CA certificate.

### 3.3.6.10 Setting X.509 for use with IKE

Once X.509v3 keys are installed on the TOE, they can be set for use with IKEv2 with the commands:

TOE-common-criteria (config-isakmp)# **authentication ecdsa-sig**

**IKE2:**

TOE-common-criteria (config)#**crypto ikev2 proposal sample**

TOE-common-criteria(config-ikev2-profile)#**authentication [remote | local] rsa-sig**

**-or-**

TOE-common-criteria(config-ikev2-profile)#**authentication [remote | local] ecdsa-sig**

If an invalid certificate is loaded, authentication will not succeed.

### 3.3.6.11 Deleting Certificates

If the need arises, certificates that are saved on the router can be deleted. The router saves its own certificates and the certificate of the CA.

To delete the router's certificate from the router's configuration, the following commands can be used in global configuration mode:

Router# **show crypto ca certificates** [Displays the certificates stored on router]

Router(config)# **crypto ca certificate chain name** [Enters certificate chain configuration mode]

Router(config-cert-cha)# **no certificate certificate-serial-number** [deletes the certificate]

To delete the CA's certificate, the entire CA identity must be removed, which also removes all certificates associated with the CA—router's certificate and the CA certificate. To remove a CA identity, the following command in global configuration mode can be used:

Router(config)# **no crypto ca identity** *name* [Deletes all identity information and certificates associated with the CA]

### 3.3.7 IPsec Overview

The TOE allows all privileged administrators to configure Internet Key Exchange (IKE) and IPsec policies. IPsec provides the following network security services:

- Data confidentiality--The IPsec sender can encrypt packets before transmitting them across a network.
- Data integrity--The IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission.
- Data origin authentication--The IPsec receiver can authenticate the source of the sent IPsec packets. This service is dependent upon the data integrity service.
- Anti-replay--The IPsec receiver can detect and reject replayed packets.

IPsec provides secure tunnels between two peers, such as two routers. The privileged administrator defines which packets are considered sensitive and should be sent through these secure tunnels and specifies the parameters that should be used to protect these sensitive packets by specifying the characteristics of these tunnels. When the IPsec peer recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

More accurately, these tunnels are sets of security associations (SAs) that are established between two IPsec peers. The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used by the two peers. SAs are unidirectional and are established per security protocol (AH or ESP).

With IPsec, privileged administrators can define the traffic that needs to be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces using crypto map sets. Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port. However, the access lists used for IPsec are only used to determine the traffic that needs to be protected by IPsec, not the traffic that should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface.

A crypto map set can contain multiple entries, each with a different access list for the interface. The crypto map entries are searched in a sequence and as such, the router attempts to match the packet to the access list specified in that entry, for example:

- The ‘discard’ option is accomplished using access lists with deny entries, which are applied to interfaces within access-groups.
- The ‘bypassing’ option is accomplished using access lists with deny entries, which are applied to interfaces within crypto maps for IPSec.
- The ‘protecting’ option is accomplished using access lists with permit entries, which are applied to interfaces within crypto maps for IPsec.

When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged as cisco, connections are established, if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry as described above.

Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the router. "Applicable" packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer.

Access lists associated with IPsec crypto map entries also represent the traffic that the router needs protected by IPsec. Inbound traffic is processed against crypto map entries. If an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet.

Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings that can be applied to IPsec-protected traffic. During the IPsec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

## 3.3.8 Configuration of IPsec

IPsec tunnels must be used for remote administration, transmission of audit records, and whenever connecting to AAA servers (RADIUS). If an IPsec tunnel terminates in a router (rather than a syslog or RADIUS) then the connection from the server to the router must be physically secure. Refer to **[9]** for detailed guidance to configure IPsec tunnels. To ensure the IPsec tunnels will be consistent with the evaluated configuration, use parameters as described in this section. Configuring IPsec tunnels requires configuration of the following elements:

- **Layer-3 Interfaces:** IP-enabled interfaces that can be local tunnel endpoints.
- **Crypto Access Lists:** Any access lists that will be applied to Crypto Maps.
- **Crypto Maps:** An association of a crypto access list (a “match address”), one or more IPsec peers (accessible from a valid local layer-3 interface), and with one or more transforms or transform sets.
- **IPsec Transforms:** Administratively-specified parameters to be permitted during IPsec SA negotiation (see tables below for permitted parameters).

### 3.3.8.1 Configure Reference Identifier

This section describes configuration of the peer reference identifier, which is achieved through a certificate map.

Certificate maps provide the ability for a certificate to be matched with a given set of criteria. You can specify which fields within a certificate should be checked and which values those fields may or may not have. There are six logical tests for comparing the field with the value: equal, not equal, contains, does not contain, less than, and greater than or equal. ISAKMP and ikev2 profiles can bind themselves to certificate maps, and the TOE will determine if they are valid during IKE authentication.

NOTE: SAN is not supported for reference identifiers.

**Table 9 Reference Identifier Configuration**

| Sequence | Command | Action |
|---|---|---|
| Step1 | (config)# **crypto pki certificate map** *label sequence-number* | Starts certificate-map mode |
| Step2 | *(ca-certificate-map)# field-name match-criteria match-value* | In ca-certificate-map mode, you specify one or more certificate fields together with their matching criteria and the value to match.<br>*field-name*—Specifies one of the following case-insensitive name strings (CN: Fully Qualified Domain Name (FQDN), CN: user FQDN, CN: IP Address. Distinguished Name (DN)) or a date:<br>–subject-name<br>–issuer-name<br>–name<br>–valid-start<br>–expires-on<br>Note Date field format is dd mm yyyy hh:mm:ss or mm dd yyyy hh:mm:ss.<br>*match-criteria*—Specifies one of the following logical operators:<br>–eq—Equal (valid for name and date fields)<br>–ne—Not equal (valid for name and date fields)<br>–co—Contains (valid only for name fields)<br>–nc—Does not contain (valid only for name fields)<br>–lt —Less than (valid only for date fields)<br>–ge —Greater than or equal (valid only for date fields)<br>*match-value*—Specifies the name or date to test with the logical operator assigned by match-criteria. |
| Step3 | (ca-certificate-map)# **exit** | Exits ca-certificate-map mode. |
| Step4 | For IKEv2:<br>crypto ikev2 profile ikev2-profile1<br>match certificate *label* | Associates the certificate-based ACL defined with the crypto pki certificate map command to the profile. |

### 3.3.8.2 IKEv2 Transform Sets

An Internet Key Exchange version 2 (IKEv2) proposal is a set of transforms used in the negotiation of IKEv2 SA as part of the IKE_SA_INIT exchange. An IKEv2 proposal is regarded as complete only when it has at least an encryption algorithm, an integrity algorithm, and a Diffie-Hellman (DH) group configured. If no proposal is configured and attached to an IKEv2 policy, then the default proposal is used in the negotiation, and it contains selections that are not valid for the TOE. Therefore, the following settings must be set in configuring the IPSec with IKEv2 functionality for the TOE:

Router#**conf t**

Router(config)#**crypto ikev2 proposal sample**

Router(config-ikev2-proposal)#**integrity sha1**

Router(config-ikev2-proposal)#**encryption aes-cbc-128**

**Note:** AES key sizes of 192 and 256 are allowed in the evaluated configuration. AES-GCM mode with key sizes of 128, and 256 are allowed in the evaluated configuration. The authorized administrator may configure the TOE to use aes-cbc or aes-gcm.

**Note:** The authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128 (either CBC or GCM).

**Note:** Both confidentiality and integrity are configured with the hash sha and encryption aes commands respectively. As a result, confidentiality-only mode is disabled.

Router(config-ikev2-proposal)#**group 14**

This selects DH Group 14 (2048-bit MODP) for IKE. DH Groups 19 and 20 can also be used in the evaluated configuration.

Router(config-ikev2-proposal)#**lifetime 86400**

The default time value for Phase 1 SAs is 24 hours (86400 seconds), but this setting can be changed using the command above with different values.

Router (config)#**crypto ikev2 keyring keyring-1**

Router (config-ikev2-keyring)#**peer peer1**

Router (config-ikev2-keyring-peer)#**address 0.0.0.0 0.0.0.0**

Router (config-ikev2-keyring-peer)#**pre-shared-key cisco123!cisco123!CISC**

This section creates a keyring to hold the pre-shared keys referenced in the steps above. In IKEv2 these pre-shared keys are specific to the peer.

Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper-case letters (A-Z), lower case letters (a-z), numbers (0-9), and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

The TOE supports pre-shared keys up to 127 bytes in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time.

HEX keys generated off system can also be input for IKEv2 using the following instead of the pre-shared-key command above: ‘**pre-shared-key hex [hex key]**’. For example: **pre-shared-key hex 0x6A6B6C**, refer to **[9]** for more information on this command.

This configures IPSec to use pre-shared keys. X.509 v3 certificates are also supported for authentication of IPSec peers. See Section 4.6.3 below for additional information.

Router(config)#**crypto logging ikev2**

This setting enables IKEv2 syslog messages.

The configuration above is not a complete IKE v2 configuration, and additional settings will be needed. See **[18]** Configuring Internet Key Exchange Version 2 (IKEv2) for additional information on IKE v2 configuration.

#### 3.3.8.3 IPsec Transform and Lifetimes

Regardless of the IKE version selected, the TOE must be configured with the proper transform for IPsec ESP encryption and integrity as well as IPsec lifetimes.

To configure IPsec ESP to use HMAC-SHA-1 and AES-CBC-128 use the following command:

**crypto ipsec transform-set example esp-aes 128 esp-sha-hmac**

NOTE: In the evaluated configuration esp-aes also supports 192- and 256-bit key sizes and AES-GCM 128-, 192-, and 256-bit key sizes. HMAC-SHA 256 and HMAC-SHA 512 are supported.

The default time value for Phase 2 SAs is 1 hour. There is no configuration required for this setting since the default is acceptable; however to change the setting to 8 hours as claimed in the Security Target the "**crypto ipsec security-association lifetime"** command can be used as specified below:

**crypto ipsec security-association lifetime seconds 28800**

The following command configures a lifetime of 100 MB of traffic for Phase 2 SAs. The default amount for this setting is 2560KB, which is the minimum configurable value for this command. The maximum configurable value for this command is 4GB. Therefore, the security association lifetime range is 2560KB - 4GB (100,000 to 4,000,000 Kilobytes).

**crypto ipsec security-association lifetime kilobytes 100000**

Additional information regarding configuration of IPsec can be found in the **[18]**. The IPSEC commands are also dispersed within the Security Command References **[6]**.

This functionality is available to the Privileged Administrator. Configuration of VPN settings is restricted to the privileged administrator.

#### 3.3.8.4 NAT Traversal

For successful NAT traversal over an IOS-XE NAT device for an IPsec connection between two IOS-XE peers, the following configuration needs to be used (Also refer to Chapter 7 of [18])–

On an IOS NAT device (router between the IPsec endpoints):

config terminal

ip nat service list <ACL-number> ESP spi-match

access-list <ACL-number> permit <protocol> <local-range> <remote-range>

end

On each IOS peer (IPsec router endpoints):

config terminal

crypto ipsec nat-transparency spi-matching

end

### 3.3.8.5 Tunnel Mode vs. Transport Mode

Tunnel mode is the default mode for all IKE connections. The mode setting is applicable only to traffic whose source and destination addresses are the IPsec peer addresses; the mode setting is ignored for all other traffic. This mode ensures secure connectivity between the TOE and the authorized remote entity (i.e. syslog server).

Tunnel mode can be specified with the following command in crypto ipsec transform set mode:

**mode tunnel**

However, in the evaluated configuration transport mode is required. Transport mode provides end-to-end communications between a client and server.

Transport mode can be specified with the following command in crypto ipsec transform set mode:

**mode transport**

### 3.3.8.6 IKEv2 Parameters Permitted in the Evaluated Configuration

**Table 10 IKEv2 Parameters in the Evaluated Configuration**

| IKEv2 Transform Types | IKEv2 Transform Options | Permitted in the Evaluated Configuration | Required in the Evaluated Configuration |
|---|---|---|---|
| Authentication | rsa-sig (default) (RSA signature)<br>rsa-encr (RSA encrypted nonces)<br>pre-share<br>ecdsa-sig | rsa-sig (default) (RSA signature)<br>pre-share<br><br>ecdsa-sig (ECDSA signature)<br>pre-share | Yes.<br>While rsa-encr (RSA encrypted nonces) may be offered for use, it is known for weakness and is not allowed for use in the evaluated configuration |
| Encryption | des (default)<br>3des<br>aes-cbc 128, 192, 256<br>aes-gcm 128, 192, 256 | aes-cbc 128, 192, 256<br>aes-gcm 128, 256 | Yes. |
| Group | 1, 2, 5, 14, 15, 16, 19, 20, 24 | 14, 19, 20 | Yes. |
| Hash | sha (default sha 1)<br>sha256<br>sha512 | sha (default sha 1)<br>sha256<br>sha512 | Yes. |
| Lifetime | number of seconds | Yes. | Any time limit is acceptable. The recommended limit for IKEv2 SA (IKE Phase 1 SA) lifetimes is 24 hours (86,400 seconds). |

Following are the allowable IPsec parameters.

**Table 11 IPsec Parameters Permitted in the Evaluated Configuration**

| IPsec Transform Types | IPsec Transform Options | Permitted in the Evaluated Configuration | Required in the Evaluated Configuration |
|---|---|---|---|
| AH Transform | ah-md5-hmac<br>ah-sha-hmac | No | No.<br>Use of AH is irrelevant to evaluated security functionality. |
| ESP Encryption Transform | esp-3des<br>esp-aes<br>esp-des<br>esp-null<br>esp-seal | esp-aes | Yes.<br>AES must be used in the evaluated configuration. IPsec protocol ESP is implemented using the cryptographic algorithms AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, and AES-GCM-256 |
| ESP Authentication Transform | esp-md5-hmac<br>esp-sha-hmac | esp-sha-hmac | Yes, IPsec protocol ESP is implemented using the HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512<br><br>Not specifying an ESP Authentication Transform would equate to using ESP in “confidentiality only” mode, which |

| IPsec Transform Types | IPsec Transform Options | Permitted in the Evaluated Configuration | Required in the Evaluated Configuration |
|---|---|---|---|
| | | | is not permitted in the evaluated configuration. |
| IP Compression Transform | comp-lzs | Yes. | No. |
| Mode | tunnel (default) transport | Yes. | Tunnel mode is always preferred. |
| Lifetime | Seconds and/or kilobytes | Yes. | IPsec SAs (IKEv2 Phase 2 SAs) can be restricted within the range of 2560KB - 4GB (100,000 to 4,000,000 Kilobytes).<br>The recommended time limit for IKEv2 Phase 2 SAs is no more than 8 hours (28,800 seconds). |

#### 3.3.8.7 IPSEC Session Interruption Recovery

If an IPsec session with a peer is unexpectedly interrupted, the connection will be broken. In these cases, no administrative interaction is required. The IPsec session will be reestablished (a new SA set up) once the peer is back online.

### 3.3.9 Session Protection

TOE communications with the AAA server (RADIUS) and the syslog server must be secured using IPsec. If an authorized administrator wants to authenticate using a RADIUS server, then the session between the TOE and AAA server must be protected to ensure the authentication data is not passed in the clear. If an authorized administrator wants to back-up the audit logs to a syslog server, then protection must be provided for the syslog server communications so that audit data is protected.

This session protection can be provided in one of two ways:

1. With a syslog/AAA server acting as an IPsec peer of the TOE and the records tunneled over that connection, or
2. With a syslog/AAA server that is not an IPsec peer of the TOE but is physically co-located with an IPsec peer of the TOE within a trusted facility, and the records are tunneled over the connection to that IPsec peer.

The syslog/AAA servers will need to act as an IPsec peer or as an IPsec endpoint where there would be a direct connection from the TOE to the syslog/AAA servers.

If the syslog/AAA server is not capable of acting as an IPsec peer or as an IPsec endpoint, then the syslog/AAA server must be located in a physically protected facility and connected to a router capable of establishing an IPsec tunnel with the TOE.

#### 3.3.9.1 Syslog Server Running on an IPsec Endpoint

For deployments where the syslog/AAA server is able to operate as an IPsec peer of the TOE, the IPsec tunnel will protect events as they are sent to the server. Examples of free VPN endpoint products that can be installed on a syslog server to allow it to be an IPsec peer include the Racoon

tool that is part of the IPsec Tools on many Linux systems, strongSwan, Openswan, FreeS/WAN, Social VPN, tcpcrypt, tinc and Cloudvpn.

Following are sample instructions to configure the TOE to support an IPsec tunnel with aes encryption, with 10.10.10.101 as the IPsec peer IP on the syslog server, 10.10.10.110 and 30.0.0.1 as the local TOE IPs, and the syslog server running on 40.0.0.1 (a separate interface on the syslog server). For the following commands see the **[6]**.

Changes to the IP addressing scheme and routing policies may need to be changed to support the organization network.

Router #**configure terminal**
Router (config)#**crypto isakmp policy 1**
Router (config)#**encryption aes**
Router (config)#**authentication pre-share**
Router (config)#**group 14**
Router h(config)#**lifetime 86400**
Router (config)#**crypto isakmp key {*keystring*} address 10.10.10.101**
Router (config)#**crypto isakmp key {*keystring*} address 40.0.0.1**
Router (config)#**crypto ipsec transform-set sampleset esp-aes esp-sha-hmac**
Router (config)#**mode tunnel**
Router h(config)#**crypto map sample 19 ipsec-isakmp**
Router (config-crypto-map)#**set peer 10.10.10.101**
Router (config-crypto-map)#**set transform-set sampleset**
Router (config-crypto-map)#**set pfs group14**
Router (config-crypto-map)#**match address 170**
Router (config-crypto-map)#**exit**
Router h (config)#**interface g0/0**
Router (config-if)#**ip address 10.10.10.110 255.255.255.0**
Router (config-if)#**crypto map sample**
Router (config-if)#**interface Loopback1**
Router (config-if)#**ip address 30.0.0.1 255.0.0.0**
Router (config-if)#**exit**
Router h(config)#**ip route 40.0.0.0 255.0.0.0 10.10.10.101**
Router (config)#**access-list 170 permit ip 30.0.0.0 0.255.255.255 40.0.0.0 0.255.255.255**
Router (config)#**logging source-interface Loopback1**
Router (config)#**logging host 40.0.0.1**

### 3.3.9.2 Syslog Server Adjacent to an IPsec Peer

If the syslog server is not directly co-located with the TOE, then the syslog server must be located in a physically protected facility and connected to a router capable of establishing an IPsec tunnel with the TOE. This will protect the syslog records as they traverse the public network.

Following are sample instructions to configure the TOE to support an IPsec tunnel with aes encryption, with 11.1.1.4 as the IPsec peer, 10.1.1.7 and 11.1.1.6 as the local IPs, and the syslog server on the 12.1.1.0 /28 subnet. For the following commands see the **[6]**.

Changes to the IP addressing scheme and routing policies may need to be changed to support the organization network.

Router#**configure terminal**
Router#**crypto isakmp policy 1**
Router(config-isakmp)#**encryption aes**
Router(config-isakmp)#**authentication pre-share**
Router(config-isakmp)#**group 14**
Router(config-isakmp)#**lifetime 28800**
Router(config)#**crypto isakmp key {*keystring*} address 10.10.10.101**
Router(config)#**crypto ipsec transform-set sampleset esp-aes esp-sha-hmac**
Router(cfg-crypto-trans)#**mode tunnel**
Router(config)#**crypto map sample 1 ipsec-isakmp**
Router(config-crypto-map)#**set peer 11.1.1.4**
Router(config-crypto-map)#**set transform-set sampleset**
Router(config-crypto-map)#**match address 115**
Router(config-crypto-map)#**exit**
Router(config)#**interface g0/1**
Router(config-if)#**ip address 10.1.1.7 255.255.255.0**
Router(config-if)#**no ip route-cache**
Router(config-if)#**crypto map sample**
Router(config-if)#**interface g0/0**
Router(config-if)#**ip address 11.1.1.6 255.255.255.0**
Router(config-if)#**crypto map sample**
Router(config-if)#**exit**
Router(config)#**ip route 12.1.1.0 255.255.255.0 11.1.1.4**
Router(config)#**access-list 115 permit ip 10.1.1.0 0.0.0.255 12.1.1.0 0.0.0.255 log**
Router(config)#**logging host 12.1.1.1**

## 3.4 Logging Configuration

The router can be configured to generate an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include events related to the enforcement of information flow policies, identification and authentication related events, and administrative events. Additionally, the startup and shutdown of the TOE generates an audit record to indicate the TOE is up and operational or is shutting down and all processes are stopping. A complete list of available audit messages for the ISR 900 series, beyond what is required for the evaluated configuration can be found in **[13]**.

To ensure audit records are generated for the required auditable events, the TOE must be configured in its evaluated configuration as specified in this document. This is to ensure that auditing is enabled so that the audit records are being generated for the required auditable events. If the command 'no logging on' is entered the TOE is deemed no longer in the evaluated configuration.

- Logging of command execution must be enabled **[6] [10]**:

  Router(config)#**archive**

  Router(config)#**no logging console**

  Router(config-archive)#**log config**

  Router(config-archive-log-cfg)#**logging enable**

Router(config-archive-log-cfg)**#hidekeys** (this ensures that keys and passwords are not displayed in the clear)

Router(config-archive-log-cfg)#**logging size *entires*** (number of entries to be retained in the configuration log. The range is from 1 to 1000; the default is 100)

Router(config-archive-log-cfg)#**notify syslog** (this enables the sending of notifications of configuration changes to a remote syslog server if configured. See Remote Logging below for configuring the syslog server)

Router(config-archive-log-cfg)#**end**

Router(config-archive)#**exit**

- Timestamps, including the year must be enabled for the audit records:

  Router(config)#**service timestamps log datetime year**

- Set the size logging file size. The range is 4096 to 2147483647, it is recommended to set at least 150000000:

  **Router (config)# logging buffer 150000000**

- To generate logging messages for failed and successful login attempts in the evaluated configuration, issue the login on-failure and login on-success commands:

  Router(config)**#login on-failure log**

  Router(config)**#login on-success log**

- Enable radius debugging:

  Router**#debug radius authentication**

- Enable IPsec related debugging

  Router**#debug crypto isakmp**

  Router**#debug crypto ipsec**

  Router**#debug crypto ikev2**

  Router**#debug crypto pki validation**

- Enable logging of ssh session establishment, authentication request, terminations and timeouts in privileged EXEC mode enter the following:

  Router**#debug ip ssh detail**

- To enable remote logging of debugging information after a reboot, use the following command in privileged EXEC mode.

  Router**#logging trap debugging**

Debug level auditing is required for specific protocols and events to ensure the audit records with the level of information are generated to meet the requirements in the Security Target. When that level of auditing is required, it is annotated as such throughout this AGD document.

Before you start a debug command, always consider the output that this command will generate and the amount of time this can take. Before debugging, look at your CPU load with the "**show processes cpu"** command **[6]**. Verify that you have ample CPU available before you begin the debugs and use the debug commands with caution.

### 3.4.1 Managing Audit Records

The TOE provides the Authorized Administrator the ability to manage local audit records stored within the TOE. Audit logging is enabled by default on the TOE.

Configuring the audit log severity level is done with the logging buffered command.

Router(config)# **logging buffered <0-7>**

Severity levels:

1 – Alerts

2 – Critical

3 – Errors

4 – Warnings

5 – Notifications

6 – Informational

7 – Debugging

Viewing the audit log is done with the show logging command.

Router# **show logging**

Clearing the audit log is done with the clear logging command.

Router# **clear logging**

### 3.4.2 Usage of Embedded Event Manager

In order to ensure that all commands executed by a level 15 user are captured in a syslog record, the following Cisco Embedded Event Manager script can be used. Enter it at the CLI as follows:

Router(config)#**event manager applet cli_log**

Router(config-applet)#**event cli pattern "." *mode exec enter**

Router(config-applet)#**action 1.0 info type routername**

Router(config-applet)#**action 2.0 syslog msg "User:$_cli_username via Port:$_cli_tty Executed[$_cli_msg]"**

Router(config-applet)#**action 3.0 set _exit_status "1"**

Router(config-applet)#**end**

See https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-embedded-event-manager-eem/index.html for more information on EEM scripting.

### 3.4.3 Remote Logging

To protect against audit data loss the TOE must be configured to send the audit records securely (through an IPsec tunnel) to an external TCP syslog server. For instance, all emergency, alerts, critical, errors, and warning message can be sent to the console alerting the administrator that some action needs to be taken as these types of messages mean that the functionality of the router is affected. All notifications and information type message can be sent to the syslog server, whereas message is only for information and the router functionality is not affected.

Configure IPsec tunnel(s) to transport the syslog messages to syslog server(s). Without using IPsec, the syslog connection would not have confidentiality and integrity of the audit data secured in transit. For guidance on configuration of IPsec tunnels, refer to Session Protection in this document. The set of logging messages sent to the remote syslog server with the **logging host <ip address of syslog server>** command **[6]**, can be the same or different from the set written to the local logging buffer. To specify the severity level for logging to the syslog host, use the **logging trap** command **[6]**. Level 7 will send all logs required in the evaluation up to the debug level logs, as configured above to the syslog server.

When connection to the remote audit server is down (either because the IPsec tunnel is down, or the syslog server is unavailable), the TOE will continue to log messages to the logging buffer. Messages in the logging buffer can be viewed with the "**show logging buffer**" command **[10]** show gsr through show monitor event trace -> **show logging**. When the buffer is full, the oldest messages will be overwritten with new messages. The buffer size can be increased from the default using the command, "**logging buffered [buffer size in bytes]**". You will also need to set the command, **logging buffer debug** to ensure an audit record is generated if there is an issue with the logging buffer.

### 3.4.4 Logging Protection

If an authorized administrator wants to back-up the logs to a syslog server, then protection must be provided for the syslog server communications. This can be provided in one of two ways:

1. With a syslog server operating as an IPsec peer of the TOE and the records tunneled over that connection, or
2. With a syslog server is not directly co-located with the TOE but is adjacent to an IPsec peer within a trusted facility, and the records are tunneled over the public network.

In either configuration the IPsec peer must, at a minimum support peer authentication using RSA and pre-shared keys and the following algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) and DH Groups 14 (2048-bit MODP).

Refer to 3.3.9 Session Protection for deployment configuration examples where the syslog server is able to operate as an IPsec peer of the TOE or if the syslog server is not directly co-located with the TOE, then the syslog server must be located in a physically protected facility and connected to a router capable of establishing an IPsec tunnel with the TOE. This will protect the syslog records as they traverse the public network.

# 4. Secure Management

## 4.1 User Roles

The ISR900 series has both privileged and semi-privileged administrator roles as well as non-administrative access. Non-administrative access is granted to authenticated neighbor routers for the ability to receive updated routing tables. There is no other access or functions associated with non-administrative access. These privileged and semi-privileged roles are configured in the Access Control and Session Termination section above. The TOE also allows for customization of other levels. Privileged access is defined by any privilege level entering an 'enable secret 5' after their individual login. The command 'enable secret' is a replacement for the 'enable password' command since the 'enable secret' creates the password and stores it in encrypted. Privilege levels are number 0-15 that specifies the various levels for the user. The privilege levels are not necessarily hierarchical. Privilege level 15 has access to all commands on the TOE. Privilege levels 0 and 1 are defined by default, while levels 2-14 are undefined by default. Levels 0-14 can be set to include any of the commands available to the level 15 administrators and are considered the semi-privileged administrator for purposes of this evaluation. The privilege level determines the functions the user can perform; hence the authorized administrator with the appropriate privileges.

To establish a username-based authentication system, use the username command in global configuration mode.

TOE-common-criteria(config)# **username name** [privilege level]

When a user no longer requires access to the TOE, the user account can be removed. To remove an established username-based authentication account, use the "no" form of the command.

TOE-common-criteria(config)# **no username name**

Refer to the IOS Command Reference Guide for available commands and associated roles and privilege levels. **[3] [4] [6] [10]**.

## 4.2 Passwords

The password complexity is not enforced by the router by default and must be administratively set in the configuration. To prevent administrators from choosing insecure passwords, each password must be at least 15 characters.

Use the following command **[6]** to set the minimum length to 15.

**security passwords min-length** <length>

You can also set the password minimum length in the **aaa common-criteria policy** using the **min-length** <length> option **[6]** Cisco IOS Security Command Reference: Commands A to C -> aaa accounting through aaa local authentication attempts max-fail -> aaa common-criteria policy. See below for syntax.

The password can be composed of any combination of characters that includes characters for at least 3 of these four character sets: upper case letters, lower case letters, numerals, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")".

Configure the TOE to enforce that complexity requirement by enabling **aaa password restriction** command that will also enforce the following restrictions:

1. The new password cannot have any character repeated more than three times consecutively.
2. The new password cannot be the same as the associated username.
3. The password obtained by capitalization of the username or username reversed is not accepted.
4. The new password cannot be “cisco”, “ocsic”, or any variant obtained by changing the capitalization of letters therein, or by substituting “1”, “|”, or “!” for i, or by substituting “0” for “o”, or substituting “$” for “s”.

The **aaa password restriction** command **[6]** can only be used after the **aaa new-model** command is configured (described below).

To prevent users from choosing insecure passwords, password should meet the following requirements:

- Does not contain more than three consecutive characters, such as abcd
- Does not contain more than two repeating characters, such as aaabbb
- Does not contain dictionary words
- Does not contain common proper names

The above items are recommended but are not enforced by the TOE:

The ISR900 Series can enforce the use of strong passwords by using options listed below with the “**aaa common-criteria policy**” command **[6]** Cisco IOS Security Command Reference: Commands A to C -> aaa accounting through aaa local authentication attempts max-fail -> aaa common-criteria policy. To view the current policy use, “**show aaa common-criteria policy”** command **[6]** Cisco IOS Security Command Reference: Commands S to Z-> set aggressive-mode client-endpoint through show content-scan -> show aaa common-criteria policy.

The following are common criteria policy guidelines and password options that are available:

- First enable the authentication, authorization, and accounting (AAA) access control model with the “**aaa new-model”** command **[6]** Cisco IOS Security Command Reference: Commands A toC -> Cisco IOS Security Command Reference: Commands A to C aaa max-sessions through algorithm -> aaa new-model.

  **aaa new-model**

- Configure authentication, authorization, and accounting (AAA) common criteria security policies with the “**aaa common-criteria policy**” command **[6]** Cisco IOS Security Command Reference: Commands A toC -> aaa accounting through aaa local authentication attempts max-fail -> aaa common-criteria policy

  **aaa common-criteria policy** <policy>

- Passwords must be set to a minimum length of 15 characters. To set the password minimum length use the min-length option use the aaa common-criteria policy command to enter the common criteria configuration policy mode.

  Router(config)#**aaa common-criteria** <policy>

  Router(config-cc-policy)#**min-length** 15

- The aaa common criteria policy cannot be assigned to a user account without also setting a password within the same "**username**" command **[6]** Cisco IOS Security Command Reference: Commands S to Z -> traffic-export through zone security -> username. Following is an example command to set username, password and policy

  **username** <username> **common-criteria-policy** <policy> **password** <password>

To store passwords in encrypted form in the configuration file, use the "**service password-encryption**" command **[6]** Cisco IOS Security Command Reference: Cisco IOS Security Command Reference: Commands S to Z -> sa ipsec through sessions maximum -> service password-encryption.

**service password-encryption**

Whether or not "service password-encryption" has been enabled, a password for an individual username can be entered in either plaintext or as a SHA-256 hash value and be stored as a SHA-256 hash value in the configuration file when using the "**username**" command. **[6]** Cisco IOS Security Command Reference: Commands S to Z -> traffic-export through zone security -> username. Following is an example command to set username, password and password encryption service

**username** *name* **secret** {**0** *password* | **4** *secret-string* | **5** *SHA256 secret-string*}

*password* is the password that a user enters.

0 - Specifies an unencrypted clear-text password. The password is converted to a SHA256 secret and gets stored in the router.

4 - Specifies an SHA256 encrypted secret string. The SHA256 secret string is copied from the router configuration.

5 - Specifies a message digest alogrithm5 (MD5) encrypted secret

To store the enable password in non-plaintext form, use the '**enable secret'** command when setting the enable password. The enable password can be entered as plaintext, or as an MD5 hash value. Example:

**enable secret** [**level** *level*] {*password* | **0** | **4** | **5** [*encryption-type*] *encrypted-password*}

level - (Optional) Specifies the level for which the password applies. You can specify up to sixteen privilege levels, using the numerals 0 through 15.

password – password that will be entered

0 - Specifies an unencrypted clear-text password. The password is converted to a SHA256 secret and gets stored in the router.

4 - Specifies an SHA256 encrypted secret string. The SHA256 secret string is copied from the router configuration.

5 - Specifies a message digest alogrithm5 (MD5) encrypted secret.

encryption-type - (Optional) Cisco-proprietary algorithm used to encrypt the password. The encryption types available for this command are 4 and 5. If you specify a value for *encryption-type* argument, the next argument you supply must be an encrypted password (a password encrypted by a Cisco router).

encrypted-password - Encrypted password that is copied from another router configuration.

Use of enable passwords are not necessary, so all administrative passwords can be stored as SHA-256 if enable passwords are not used.

***Note:*** Cisco no longer recommends that the 'enable password' command be used to configure a password for privileged EXEC mode. The password that is entered with the 'enable password' command is stored as plain text in the configuration file of the networking device. If passwords were created with the 'enable password' command, it can be hashed by using the 'service password-encryption' command. Instead of using the 'enable password' command, Cisco recommends using the 'enable secret' command because it stores a SHA-256 hash value of the password.

To have IKE preshared keys stored in encrypted form, use the **password encryption aes** command **[6]** to enable the functionality and the **key config-key password-encrypt** {*text*} command **[6]** to set the master password to be used to encrypt the preshared keys. The preshared keys will be stored encrypted with symmetric cipher Advanced Encryption Standard [AES].

## 4.3 System Clock Management

The basis of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the date and time. The TOE system clock keeps track of time internally based on Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). The Authorized Administrator can configure information about the local time zone and summer time (daylight saving time) so that the time appears correctly for the local time zone.

Use the commands below to configuring the time and date:

router(config)# **clock timezone** zone hours-offset [minutes-offset]

router(config)# **clock summer-time zone recurring** [week day month hh:mm week day month hh:mm [offset]]

router(config)# **clock summer-time zone date** date month year hh:mm:ss date month year hh:mm:ss [offset]

router(config)# **exit**

router# **clock set** hh:mm:ss date month year

For further details refer to Setting Time and Calendar Services -> Hardware Clock -> Setting The Hardware Clock in **[16]** or Using the Cisco IOS Command-Line Interface (CLI) in **[11]**.

## 4.4 Identification and Authentication

Configuration of Identification and Authentication settings is restricted to the privileged administrator.

The ISR900 Series can be configured to use local authentication and authorization secured using SSHv2 or RADIUS secured using IPsec.

Refer to Securing User Services Overview -> RADIUS and TACACS+ Attributes **[4]**. It is recommended to read this section to become familiar with remote authentication concepts prior to configuration. You can also refer to the specific commands in **[6]** regarding configuring RADIUS commands.

## 4.5 Administrative Banner Configuration

The TOE provides the Authorized Administrator the ability to configure a banner that is displayed on the CLI management interface prior to the user name and password prompts allowing any administrative access to the TOE.

This functionality is facilitated using the "**banner login**" command **[6]**

For example, to create a banner of text "This is a banner" use the command

**banner login** d This is a banner d

## 4.6 Administrative Session Termination

The TOE allows the Authorized 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.

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

Router(config)# **line vty <first> <last>**

Router(config-line)# **exec-timeout <time>**

Router(config)**# line console**

Router(config-line)**# exec-timeout <time>**

To save these configuration settings to the startup configuration:

**copy run start**

where first and last are the range of vty lines on the box (i.e. "0 15"), and time is the period of inactivity after which the session should be terminated. Configuration of these settings is limited to the Authorized Administrator (see Section 4.1).

The line console setting is not immediately activated for the current session. The current console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session.

## 4.7 Administrative Session Lock-out

Administrative user accounts must be configured to lockout after a specified number of authentication failures using the following command:

Router(config)# **aaa local authentication attempts max-fail [*number of failures*]**

Where number of failures is the number of consecutive failures that will trigger locking of the account. Configuration of these settings is limited to the Authorized Administrator.

> ***Note:*** This applies to consecutive failures on the TOE during a given session and is not affected by the SSH session disconnections of their default number of failures.
>
> ***Note:*** Administrator lockouts are not applicable to the local console. Local administrators cannot be locked out and therefore have the ability to unlock other users by using the local console.

To unlock the account, the Authorized Administrator uses the following commands:

> **clear aaa local user fail-attempts [username username | all]** (Clears the unsuccessful login attempts of the user)
>
> **clear aaa local user lockout username [username] (**Unlocks the locked-out user)
>
> **show aaa local user lockout** (Displays a list of all locked-out users)

***Note: Privilege 15 administrators cannot be locked out of the device. SSH public key authentication shall also be used in the evaluated configuration to ensure that the Administrator does not lose access to the TOE.**

## 4.8 Product Updates

Verification of authenticity of updated software is done in the same manner as ensuring that the TOE is running a valid image. See 2 Secure Acceptance of the TOE above in this document; specially steps 7 and 9 for the method to download and verify an image prior to running it on the TOE. Once the image is verified perform the following upgrade steps:

1. Enter Enable mode

   ```
   Enable
   <password>
   ```

2. Copy the image to flash

   ```
   Copy tftp : flash:
   ```

3. When prompted, enter the IP address of the TFTP

   ```
   Address or name of remote host []? <tftp ip address>
   ```

4. When prompted, enter filename of the Cisco IOS software image to be installed

   ```
   Source filename []? <source filename>
   ```

5. When prompted, enter the filename name to be used for the router, typically this is the same name as entered in step 4

   ```
   Destination filename []? <source filename>
   ```

6. Enter **no** when prompted to erase flash memory before copying

7. Once the software is loaded, enter Configure mode

```
Configure terminal
```

8. Delete all entries in the bootable image list

```
no boot system
```

9. Specify the new image to be loaded

```
Boot system flash: <system image file name from Step 5 above>
```

10. Exit configuration mode

```
Exit
```

11. Reload the device

```
Reload
```

12. Once the device has reloaded and is operational, verify the version to ensure the upgrade was successful

```
Show version
```

# 5. Security Relevant Events

The TOE 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 Logging Protection above.

The administrator can set the level of the audit records to be stored in a local buffer, displayed on the console, sent to the syslog server, or all the above. The details for configuration of these settings are covered in the relevant section above in this document.

The local log buffer is circular. Newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer.

When configured for a syslog backup the TOE will simultaneously offload events from a separate buffer to the external syslog server. This buffer is used to queue events to be sent to the syslog server if the connection to the server is lost. It is a circular buffer, so when the events overrun the storage space overwrites older events.

Refer to the relevant section below in this document that include the security relevant events that are applicable to the TOE.

## 5.1 Deleting Audit Records

The TOE provides the privileged administrator the ability to delete audit records stored within the TOE. This is done with the "**clear logging"** command **[10]** C commands -> clear logging.

## 5.2 Reviewing Audited Events

The ISR900 Series maintains logs in multiple locations: local storage of the generated audit records, and simultaneous offload of those events to the external syslog server. For the most complete view of audited events, across all devices, and to view the auditable events defined in the Security Target administrators should review the Audit Log on a regular basis.

Using the ISR900 Series Command Line Interface (CLI) administrators can review audited events. The information provided in the audit records include the date and time of the event, the type of event, subject identity that caused the event, the outcome of the event, and additional information related to the event. The types of events that are audited include, the start-up and shut-down of the audit functions; administrators' login and logout, changes to TSF data related to configuration changes, generating and importing of, changing, or deleting of cryptographic keys, resetting passwords and starting and stopping services. The following table includes all of the required auditable events and additional information that is required based on the type of event.

**Table 12 Auditable Events**

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| FAU_GEN.1 | None. | None. |
| FAU_GEN.2 | None. | None. |
| FAU_STG_EXT.1 | None. | None. |
| FCS_CKM.1 | None. | None. |
| FCS_CKM.1/IKE | None. | None. |
| FCS_CKM.2 | None. | None. |
| FCS_CKM.4 | None. | None. |
| FCS_COP.1/DataEncryption | None. | None. |
| FCS_COP.1/SigGen | None. | None. |
| FCS_COP.1/Hash | None. | None. |
| FCS_COP.1/KeyedHash | None. | None. |
| FCS_IPSEC_EXT.1 | Failure to establish an IPsec SA.<br><br>Session establishment with peer. | Reason for failure.<br><br>Enter packet contents of packets transmitted/received during session establishment. |
| FCS_RBG_EXT.1 | None. | None. |
| FCS_SSHS_EXT.1 | Failure to establish an SSH session. | Reason for failure. |
| FIA_AFL.1 | Unsuccessful login attempts limit is met or exceeded. | Origin of the attempt (e.g., IP address). |
| FIA_PMG_EXT.1 | None. | None. |
| FIA_UIA_EXT.1 | All use of the identification and authentication mechanism. | Origin of the attempt (e.g., IP address). |
| FIA_UAU_EXT.2 | All use of the identification and authentication mechanism. | Origin of the attempt (e.g., IP address). |
| FIA_UAU.7 | None. | None. |

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| FIA_X509_EXT.1/Rev | Unsuccessful attempt to validate a certificate.<br>Any addition, replacement or removal of trust anchors in the TOE's trust store.<br>Session Establishment with a CA | Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.<br>Entire packet contents of packets transmitted/received during session establishment. |
| FIA_X509_EXT.2 | None. | None. |
| FIA_X509_EXT.3 | None. | None. |
| FMT_MOF.1/ ManualUpdate | Any attempt to initiate a manual update | None. |
| FMT_MOF.1/Services | Starting and stopping of services. | None. |
| FMT_MTD.1/CoreData | None. | None. |
| FMT_MTD.1/CryptoKeys | None. | None |
| FMT_SMF.1 | All management activities of TSF data. | None. |
| FMT_SMR.2 | None. | None. |
| FPF_RUL_EXT.1 | Application of rules configured with the 'log' operation | Source and destination addresses<br>Source and destination ports<br>Transport Layer Protocol |
| FPT_SKP_EXT.1 | None. | None. |
| FPT_APW_EXT.1 | None. | None. |
| FPT_STM_EXT.1 | Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1) | For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address). |
| FPT_TUD_EXT.1 | Initiation of update; result of the update attempt (success and failure) | None. |
| FPT_TST_EXT.1 | None. | None. |
| FPT_TST_EXT.3 | Indication that TSF self-test was completed | None. |
| | Failure of self-test | Reason for failure (including identifier of invalid certificate) |
| FTA_SSL_EXT.1 | The termination of a local session by the session locking mechanism. | None. |
| FTA_SSL.3 | The termination of a remote session by the session locking mechanism. | None. |
| FTA_SSL.4 | The termination of an interactive session. | None. |
| FTA_TAB.1 | None. | None. |
| FTP_ITC.1 | Initiation of the trusted channel.<br>Termination of the trusted channel. | Identification of the initiator and target of failed trusted channels establishment attempt |

| SFR | Auditable Event | Additional Audit Record Contents |
|---|---|---|
| | Failure of the trusted channel functions. | |
| FTP_TRP.1/Admin | Initiation of the trusted channel.<br>Termination of the trusted channel.<br>Failures of the trusted path functions. | None. |

To review locally stored audit records, enter the command "**show logging**" **[6]** or **[10]** -> show gsr through show monitor event trace -> show logging (*). Also, to monitor and maintain the log messages see **[16]** Configuring System Message Logs -> Monitoring and Maintaining System Message Logs.

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information. The part of the message preceding the percent sign depends on the setting of the service sequence-numbers, service timestamps log datetime, service timestamps log datetime [localtime] [msec] [show-timezone], or service timestamps log uptime global configuration command. The following information is basic information that is included in an audit/log record.

- Element - Description
- seq no: - Stamps log messages with a sequence number only if the service sequence-numbers global configuration command is configured. For more information, see the "Enabling and Disabling Sequence Numbers in Log Messages" section.
- timestamp formats:
    - mm/dd hh:mm:ss or hh:mm:ss (short uptime) or d h (long uptime)
- Date and time of the message or event. This information appears only if the service timestamps log [datetime | log] global configuration command is configured. For more information, see the "Enabling and Disabling Time Stamps on Log Messages" section.
- Facility - The facility to which the message refers (for example, SNMP, SYS, and so forth). For a list of supported facilities, see Table 34-4.
- severity - Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 34-3.
- MNEMONIC - Text string that uniquely describes the message.
- description - Text string containing detailed information about the event being reported.
- hostname-n - Hostname of a stack member and its router number in the stack. Though the stack master is a stack member, it does not append its hostname to system messages.

Below is a sample of audit records for the various required auditable events; these records are a sample and not meant as an exact record for the particular event. In addition, for some cryptographic failures producing an audit record would require extensive manipulation and therefore snippets of source code is provided to illustrate what would be displayed in an audit record. The indication that the TSF self-test was completed successful is indicated by reaching a log-in prompt. If TSF self-test did not complete successfully, a system failure error message would be displayed.

**Table 13 Audit Records (sample)**

| Requirement | Auditable Events | Additional Audit Record Contents | Sample Record |
|---|---|---|---|
| FAU_GEN.1: Audit data generation | Changing logging settings<br><br>Clearing logs | None | **Changing logging settings:**<br>Feb 17 2019 16:29:07: %PARSER-5CFGLOG_LOGGEDCMD: User:test_admin logged command:logging enable<br><br>Feb 17 2019 16:34:02: %PARSER-5CFGLOG_LOGGEDCMD: User:test_admin logged command:logging informational<br><br>**Clearing logs:**<br>Feb 17 2019 17:05:16: %PARSER-5CFGLOG_LOGGEDCMD: User:test_admin logged command:clear logging |
| FAU_STG_EXT.1: External audit trail storage | Configuration of syslog export settings | None | **Configuration of syslog:**<br>Feb 17 2010 17:05:16: %PARSER-5CFGLOG_LOGGEDCMD: User:test_admin logged command:logging host |
| FCS_CKM.1: Cryptographic key generation (for asymmetric keys) | Manual key generation | None | **Manual key generation:**<br>Feb 17 2019 16:14:47: %PARSER-5CFGLOG_LOGGEDCMD: User:test_admin logged command:crypto key *****<br><br>Jan 24 2019 03:10:08.878: %GDOI-5KS_REKEY_TRANS_2_UNI: Group getvpn transitioned to Unicast Rekey.ip |
| FCS_CKM_EXT.4: Cryptographic key zeroization | Manual key zeroization | None | **Manual key zeroization:**<br>Feb 17 2019 16:37:27: %PARSER-5CFGLOG_LOGGEDCMD: User:test_admin logged command:crypto key zeroize |
| FCS_IPSEC_EXT.1 | Failure to establish an IPsec SA | Reason for failure | **Attempted aggressive mode:**<br>Jan 22 2019 13:17:19 UTC: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Aggressive mode failed with peer at 21.0.0.3<br>Feb 1 2019 10:15:36.555: %CRYPTO-5-IKMP_AG_MODE_DISABLED: Unable to initiate or respond to Aggressive Mode while disabled<br>Unsupported algorithms:<br>[debug - similar to] Jan 21 2019 09:28:02.468: IPSEC(ipsec_process_proposal): transform proposal not supported for identity: {esp-aes }<br><br>**Administrator Action:**<br>Feb 17 2019 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: crypto isakmp policy 1 |

| Requirement | Auditable Events | Additional Audit Record Contents | Sample Record |
|---|---|---|---|
| FCS_SSHS_EXT.1 | Failure to establish an SSH session | Reason for failure | **Failure to establish an SSH Session:**<br>Jun 18 2019 11:19:06 UTC: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: anonymous] [Source: 100.1.1.5] [localport: 22] [Reason: Login Authentication Failed] at 11:19:06 UTC Mon Jun 18 2019<br>Establishment of an SSH session<br>IP address of remote host<br>Jun 18 2019 11:31:35 UTC: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ranger] [Source: 100.1.1.5] [localport: 22] at 11:31:35 UTC Mon Jun 18 2019<br>Jun 18 2019 06:47:17.041: %SSH-5-SSH2_CLOSE: SSH2 Session from 1.1.1.1 (tty = 0) for user 'cisco' using crypto cipher 'aes256-cbc', hmac 'hmac-sha1-96' closed |
| FIA_AFL.1 | Unsuccessful login attempts limit is met or exceeded | Origin of the attempt (e.g., IP address) | **Unsuccessful login attempts limit is met or exceeded:**<br>Nov 25 2019 10:52:47.652: \%SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 10.21.0.101] [localport: 22] [Reason: Login Authentication Failed] at 10:52:47 EST Sat Nov 25 2019<br>Nov 25 2019 10:52:49.655: \%SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 10.21.0.101] [localport: 22] [Reason: Login Authentication Failed] at 10:52:49 EST Sat Nov 25 2019<br>Nov 25 2019 10:53:05.678: \%SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ] [Source: 10.21.0.101] [localport: 22] [Reason: Login Authentication Failed] at 10:53:05 EST Sat Nov 25 2019<br>Nov 25 2019 10:53:26.693: \%AAA-5-USER_LOCKED: User testuser locked out on authentication failure |
| FIA_PMG_EXT.1: Password management | Setting length requirement for passwords | None | **Setting length requirement for passwords:**<br>Feb 15 2019 13:12:25.055: %PARSER-5CFGLOG_LOGGEDCMD: User:cisco logged command: security passwords min-length 15 |
| FIA_PSK_EXT.1: Pre-Shared Key Composition | Creation of a pre-shared key | None | **Creation of a preshared key:**<br>Feb 15 2019 13:12:25.055: %PARSER-5CFGLOG_LOGGEDCMD: User:cisco logged command: crypto isakmp key ***** |

| Requirement | Auditable Events | Additional Audit Record Contents | Sample Record |
|---|---|---|---|
| FIA_UIA_EXT.1 | All use of the identification and authentication mechanism<br><br>Administrative Actions: Logging into TOE | Provided user identity, origin of the attempt (e.g., IP address) | **Login failure:**<br>Jan 17 2019 05:15:14.912: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: anonymous] [Source: 21.0.0.3] [localport: 22] [Reason: Login Authentication Failed] at 00:15:14 EST Thu Jan 17 2019<br>Jan 17 2019 05:05:49.460: %SEC_LOGIN-5-<br><br>**Login success:**<br>Login Success [user: ranger] [Source: 21.0.0.3] [localport: 22] at 00:05:49 EST Thu Jan 17 2019<br>Jan 21 2019 04:00:57 UTC: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 0.0.0.0] [localport: 0] at 23:00:57 EST Sun Jan 20 2019<br>Administrator Action:<br>Jan 21 2019 04:00:57 UTC: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 0.0.0.0] [localport: 0] at 23:00:57 EST Sun Jan 20 2019 |
| FIA_UAU_EXT.2 | All use of the authentication mechanism | Origin of the attempt (e.g., IP address) | **Login failure:**<br>Jan 17 2019 05:15:14.912: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: anonymous] [Source: 21.0.0.3] [localport: 22] [Reason: Login Authentication Failed] at 00:15:14 EST Thu Jan 17 2019<br><br>**Login success:**<br>Jan 17 2019 05:05:49.460: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ranger] [Source: 21.0.0.3] [localport: 22] at 00:05:49 EST Thu Jan 17 2019 |
| FIA_X509_EXT.1/Rev | Unsuccessful attempt to validate a certificate<br><br>Any addition, replacement or removal of trust anchors in the TOE's trust store | Reason for failure of certificate validation<br><br>Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store | **Unsuccessful attempt to validate a certificate**<br>Jan 22 2019 13:17:19 UTC: * Jan 22 2014 13:17:19: %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from 10.100.100.2 is bad: certificate invalid<br><br>**Addition of trust anchors:**<br>Sep 18 11:38:06.256: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named cryptokeytest has been generated or imported by crypto-engine |
| FMT_MOF.1/Services | Starting and stopping of Services | None | **Stopping of Services:**<br>Jul 19 12:10:00 toe-loopback 289: *Jul 19 2019 12:10:00.678: \%SYS-6LOGGINGHOST_STARTSTOP: Logging to host 10.24.0.1 port 514 started - CLI initiated<br><br>Jul 19 12:09:51 toe-loopback 282: *Jul 19 2019 12:09:51.963: \%SYS-6LOGGINGHOST_STARTSTOP: Logging to host 10.24.0.1 port 514 stopped - CLI initiated |

| Requirement | Auditable Events | Additional Audit Record Contents | Sample Record |
|---|---|---|---|
| FMT_MOF.1(1)/Manual Update | Any attempt to initiate a manual update | None | See FPT_TUD_EXT.1 |
| FMT_MTD.1/Crypto Keys | Management of Cryptographic keys | None | **Crypto keys (generating and deleting):**<br>Feb 17 2019 16:14:47: %PARSER-5CFGLOG_LOGGEDCMD: User:test_admin logged command: crypto key generate Feb 17 2019 16:37:27: %PARSER-5CFGLOG_LOGGEDCMD: User:test_admin logged command:crypto key zeroize<br><br>See all other records in Table 8 “Auditable Administrative Events”. |
| FMT_SMF.1 | All management activities of TSF data | None | **Resetting of passwords:**<br>Nov 21 2019 15:06:53.679: \%PARSER-5CFGLOG_LOGGEDCMD: User:admin logged command:no enable password<br>Nov 21 2019 15:06:53.724: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no username script privilege 15 password 0 password<br>Nov 21 2019 15:08:54.042: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:username script privilege 15 password 0 secret<br>Nov 21 2019 15:08:54.070: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:enable password secret<br><br>**Services:**<br>Jul 19 12:10:00 toe-loopback 289: *Jul 19 2019 12:10:00.678: \%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.24.0.1 port 514 started - CLI initiated<br><br>Jul 19 12:09:51 toe-loopback 282: *Jul 19 2019 12:09:51.963: \%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.24.0.1 port 514 stopped - CLI initiated<br><br>See all records with ‘Administrator Actions’ |

| Requirement | Auditable Events | Additional Audit Record Contents | Sample Record |
|---|---|---|---|
| FPF_RUL_EXT.1 | Application of rules configured with the 'log' operation | Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface | **ACL Configuration**:<br>Aug 6 10:53:48 toe-loopback 327: *Aug 6 2019 10:53:47.403: \%PARSER-5-CFGLOG_LOGGEDCMD: User:script logged command:ip access-list extended FPF_RUL_EXT.1-deny Aug 6 10:53:48 toe-loopback 328: *Aug 6 2019 10:53:47.572: \%PARSER-5-CFGLOG_LOGGEDCMD: User:script logged command:deny icmp 10.22.0.203 0.0.0.0 10.21.0.101 0.0.0.0 log Aug 6 10:53:48 toe-loopback 329: *Aug 6 2019 10:53:47.748: \%PARSER-5-CFGLOG_LOGGEDCMD: User:script logged command:permit icmp 10.22.0.203 0.0.0.0 10.21.0.101 0.0.0.0 log Aug 6 10:53:48 toe-loopback 330: *Aug 6 2019 10:53:47.878: \%PARSER-5-CFGLOG_LOGGEDCMD: User:script logged command:interface GigabitEthernet0/0/1<br>Aug 6 10:53:48 toe-loopback 331: *Aug 6 2019 10:53:48.010: \%PARSER-5-CFGLOG_LOGGEDCMD: User:script logged command:ip access-group FPF_RUL_EXT.1-deny in **Packets denied by ACL**: Aug 6 10:53:54 toe-loopback 335: *Aug 6 2019 10:53:53.601: \%FMANFP-6-IPACCESSLOGDP: R0/0: fman_fp_image: list FPF_RUL_EXT.1-deny denied icmp 10.22.0.203 -> 10.21.0.101 (0/0), 1 packet Aug 6 10:53:54 toe-loopback 336: *Aug 6 2019 10:53:53.853: \%FMANFP-6-IPACCESSLOGDP: R0/0: fman_fp_image: list FPF_RUL_EXT.1-deny denied icmp 10.22.0.203 -> 10.21.0.101 (0/0), 1 packet<br>Aug 6 10:53:54 toe-loopback 337: *Aug 6 2019 10:53:54.104: \%FMANFP-6-IPACCESSLOGDP: R0/0: fman_fp_image: list FPF_RUL_EXT.1-deny denied icmp 10.22.0.203 -> 10.21.0.101 (0/0), 1 packet |
| | Indication of packets dropped due to too much network traffic | TOE interface that is unable to process packets | **Indication of packets:**<br>May 6 2019 04:04:28.279: %HA_EM-6-LOG: test2: value GigabitEthernet0/2 output_packets_dropped increased from 1058406890 to 1061078215 |

| Requirement | Auditable Events | Additional Audit Record Contents | Sample Record |
|---|---|---|---|
| FPT_STM_EXT.1 | Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1 ) | For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address) | **Local Clock Update:** Feb 5 2019 06:28:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 11:27:52 UTC Tue Feb 5 2019 to 06:28:00 UTC Tue Feb 5 2019, configured from console by admin on console.<br><br>**Administrator Actions:** Manual changes to the system time: Feb 5 2019 06:28:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 11:27:52 UTC Tue Feb 5 2019 to 06:28:00 UTC Tue Feb 5 2019, configured from console by admin on console. |
| FPT_TUD_EXT.1 | Initiation of update. result of the update attempt (success or failure)<br><br>Administrative Actions: Software updates | No additional information | **Initiation of the update command - success:** *Jul 10 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:upgrade *Jul 10 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:copy tftp .... *Jul 10 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged<br><br>**Initiation of the update command – failure:** autoboot: boot failed, restarting... |
| FPT_TST_EXT.1 | Indication that TSF self-test was completed | Any additional information generated by the tests beyond “success” or “failure” | **Indication that TSF self-test was completed:** Jan 23 2019 06:53:24.570: %CRYPTO-6SELF_TEST_RESULT: Self test info: (Self test activated by user: admin) Jan 23 2019 06:53:24.670: %CRYPTO-6SELF_TEST_RESULT: Self test info: (Software checksum ... passed) *Jul 16 19:37:58.339: %DIGISIGN-4SIGNATURE_NOT_PRESENT: %WARNING: Digital signature is not found in file isr900-monouniversalk9.16.09.01.SPA.pkg.BAD.SPA |
| FPT_TST_EXT.3 | Failure of self-test | Reason for failure (including identifier of invalid certificate) | **Failure of self-test:** Validating dev_mode signature dev_mode validation failed for token 0006F66C59BF dev_mode is PRIV Unsupported package header version (0) Failed to boot file bootflash:images/c921-4p-universalk9mz.158-1.E1.bin ..... autoboot: boot failed, restarting... |

| Requirement | Auditable Events | Additional Audit Record Contents | Sample Record |
|---|---|---|---|
| FTA_SSL_EXT.1 | The termination of a local session by the session locking mechanism<br><br>Administrative Actions: Specifying the inactivity time period | No additional information | **In the TOE this is represented by login attempts that occur after the timeout of an administrative user:**<br>Feb 6 2019 04:37:59.190: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 0.0.0.0] [localport: 0] at 04:37:59 UTC Wed Feb 6 2019<br>Administrator Action:<br>Feb 6 2019 04:32:07.609: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)), user admin |
| FTA_SSL.3 | The termination of a remote session by the session locking mechanism<br><br>Administrative Actions: Specifying the inactivity time period | No additional information | **Session termination due to time expired:**<br>Feb 6 2019 04:32:07.609: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)), user admin<br><br>**Administrator Action:**<br>Feb 15 2019 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: exec-timeout 60 |
| FTA_SSL.4 | The termination of an interactive session | No additional information | **Audit record generate when admin logs out of CONSOLE:**<br>Feb 15 2019 16:29:09: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:exit<br>Or (if Embedded Event Manager is used)<br>Aug 30 2019 00:33:13 30.0.0.1 239: Aug 30 2019 00:33:12.452: \%HA_EM-6-LOG: cli_log: host[CC_TOE] user[script] port[0] exec_lvl[15] command[logout ] Executed<br><br>**Audit record generated when the admin logs out of SSH:**<br>Jun 18 2019 11:17:36.653: SSH0: Session terminated normally<br><br>**Administrator Action:**<br>Feb 15 2019 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: exit |
| FTA_TAB.1 | Administrative Action: Configuring the banner displayed prior to authentication. | None | **Configure login banner:**<br>Feb 15 2019 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: banner login d This is a banner d |

| Requirement | Auditable Events | Additional Audit Record Contents | Sample Record |
|---|---|---|---|
| FTP_ITC.1 | Initiation of the trusted channel<br><br>Termination of the trusted channel<br><br>Failure of the trusted channel functions | Identification of the initiator and target of failed trusted channels establishment attempt | See events for FCS_IPSEC_EXT.1 above. |
| FTP_ITC.1/VPN | Initiation of the trusted channel<br><br>Termination of the trusted channel<br><br>Failure of the trusted channel functions | Identification of the initiator and target of failed trusted channels establishment attempt | See events for FCS_IPSEC_EXT.1 above. |
| FTP_TRP.1/Admin | Initiation of the trusted channel. Termination of the trusted channel<br><br>Failures of the trusted path functions | Identification of the claimed user identity | See events for FCS_SSH_EXT.1 above. |

# 6. Network Services and Protocols

The table below lists the network services/protocols available on the TOE 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.

For more detail about each service, including whether the service is limited by firewall mode (routed or transparent), or by context (single, multiple, system), refer to the ***Command Reference*** guides listed above in this document.

**Table 14 Protocols and Services**

| Service or Protocol | Description | Client (initiating) | Allowed | Server (terminating) | Allowed | Allowed use in the certified configuration |
|---|---|---|---|---|---|---|
| AH | Authentication Header (part of IPsec) | Yes | No | Yes | No | No, ESP must be used in all IPsec connections. |
| DHCP | Dynamic Host Configuration Protocol | Yes | Yes | Yes | Yes | No restrictions. |
| DNS | Domain Name Service | Yes | Yes | No | n/a | No restrictions. |
| ESP | Encapsulating Security Payload (part of IPsec) | Yes | Yes | Yes | Yes | Configure ESP as described in relevant section of this document. |
| FTP | File Transfer Protocol | Yes | No | No | n/a | Use tunneling through IPsec |
| HTTP | Hypertext Transfer Protocol | Yes | No | Yes | No | Use tunneling through IPsec |
| HTTPS | Hypertext Transfer Protocol Secure | Yes | No | Yes | No | Use tunneling through IPsec |
| ICMP | Internet Control Message Protocol | Yes | Yes | Yes | Yes | No restrictions. |
| IKE | Internet Key Exchange | Yes | Yes | Yes | Yes | As described in the relevant sections of this document. |
| IMAP4S | Internet Message Access Protocol Secure version 4 | Yes | Over IPsec | No | n/a | No restrictions. |
| IPsec | Internet Protocol Security (suite of protocols including IKE, ESP and AH) | Yes | Yes | Yes | Yes | Only to be used for securing traffic that originates from or terminates at the TOE, not for "VPN Gateway" functionality to secure traffic through the TOE. See IKE and ESP for other usage restrictions. |

| Service or Protocol | Description | Client (initiating) | Allowed | Server (terminating) | Allowed | Allowed use in the certified configuration |
|---|---|---|---|---|---|---|
| Kerberos | A ticket-based authentication protocol | Yes | Over IPsec | No | n/a | If used for authentication of TOE administrators, tunnel this authentication protocol secure with IPsec. |
| LDAP | Lightweight Directory Access Protocol | Yes | No, use RADIUS | No | n/a | Use RADIUS instead |
| LDAP-over-SSL | LDAP over Secure Sockets Layer | Yes | No, use RADIUS | No | n/a | Use RADIUS instead |
| NTP | Network Time Protocol | Yes | No | No | n/a | Use local clock instead |
| RADIUS | Remote Authentication Dial In User Service | Yes | Yes | No | n/a | If used for authentication of TOE administrators, secure through IPsec. |
| SNMP | Simple Network Management Protocol | Yes (snmp-trap) | Yes | Yes | No | Outbound (traps) only. Recommended to tunnel through IPsec. |
| SSH | Secure Shell | Yes | Yes | Yes | Yes | As described in the relevant section of this document. |
| SSL (not TLS) | Secure Sockets Layer | Yes | No | Yes | No | Use IPsec instead. |
| TACACS+ | Terminal Access Controller Access-Control System Plus | Yes | No, use RADIUS | No | n/a | Use RADIUS instead |
| Telnet | A protocol used for terminal emulation | Yes | No | Yes | No | Use SSH instead. |
| TLS | Transport Layer Security | Yes | No | Yes | No | Not claimed; use IPsec instead |
| TFTP | Trivial File Transfer Protocol | Yes | Yes | No | n/a | Recommend using SCP or HTTPS instead or tunneling through IPsec. |

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.

- Routing protocols such as EIGRP, OSPF, and RIP. 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, so follow best practices for the secure usage of these protocols.
- 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.
- Network protocols that can be proxied through/by the TOE. Proxying of services by the TOE does not result in running said service on the TOE in any way that would allow the TOE itself to be remotely accessible via that service, nor does it allow the TOE to initiate a connection to a remote server independent of the remote client that has initiated the connection. The certified configuration places no restrictions on enabling of proxy functionality; however, the evaluation of this functionality was beyond the scope of the Common Criteria product evaluation. Follow best practices for the secure usage of these services.

# 7. Modes of Operation

An IOS router has several modes of operation, these modes are as follows:

**Booting** – while booting, the routers drop all network traffic until the router image and configuration has loaded. This mode of operation automatically progresses to the Normal mode of operation. During booting, a user may press the break key on a console connection within the first 60 seconds of startup to enter the ROM Monitor mode of operation. This Booting mode is referred to in the IOS guidance documentation as "ROM Monitor Initialization". Additionally, if the Router does not find a valid operating system image it will enter ROM Monitor mode and not normal mode therefore protecting the router from booting into an insecure state.

**Normal** - The IOS image and configuration is loaded and the router is operating as configured. All levels of administrative access occur in this mode and that all route-based security functions are operating. Once in the normal operating mode and fully configured, there is little interaction between the router and the administrator. However, the configuration of the router can have a detrimental effect on security; therefore, adherence to the guidelines in this document should be followed. Misconfiguration of the router could result in the unprotected network having access to the internal/protected network

**ROM Monitor** – This mode of operation is a maintenance, debugging and disaster recovery mode. While the router is in this mode, no network traffic is transmitted between the network interfaces. In this state the router may be configured to upload a new boot image from a specified TFTP server, perform configuration tasks and run various debugging commands.

If nvram is empty and a reload is done, IOS will try to boot automatically from an image top down that is in the flash directory. Make sure the valid IOS image is listed above any other images in flash.

To ensure the correct image is booted on startup use the boot system command **[6] [10]**:

#**boot system flash**:<image filename>

To return to EXEC mode from ROM monitor mode, use the "continue" command in ROM monitor mode.

rommon 1> **continue**

While no administrator password is required to enter ROM monitor mode, physical access to the router is required, therefore the router should be stored in a physically secure location to avoid unauthorized access which may lead to the router being placed in an insecure state.

Following operational error, the router 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 shut down or reboot to try to correct the issues. 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 same cryptographic POSTs can also be run on-demand as described above in this document and when the tests are run on-demand after system

startup has completed (and the syslog daemon has started), error messages will be written to the log.

All ports are blocked from moving to forwarding state during the POST. Only when all components of all modules pass the POST is the system placed in FIPS PASS state and ports are allowed to forward data traffic.

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 or 1 800 553-2447
- If necessary, return the TOE to Cisco under guidance of Cisco Technical Assistance.

If a software upgrade fails, the ISR900 Series will display an error when an authorized administrator tries to boot the system. The ISR900 Series then boots into the rommon prompt.

```
Directory an_image.bin not found
Unable to locate an_image.bin directory
Unable to load an_image.bin
boot: error executing "boot harddisk:an_image.bin"
autoboot: boot failed, restarting
```

## 7.1 Network Processes Available During Normal Operation

The following network-based processes may be running, or can be run in the evaluated configurations of the ISR900 Series, except where explicitly stated:

- ICMP is supported inbound and outbound for detection and troubleshooting of network connectivity.
- IPsec including ESP and IKE is supported for encryption of syslog traffic to an external audit server, and potentially to secure other traffic to/from external entities.
- RADIUS is supported for authentication of administrative connections to the console and/or via SSH.
- Routing protocols: The evaluated configuration supports use of BGPv4, EIGRP, EIGRPv6 for IPv6, PIM-SMv2, and OSPFv2, OSPFv3 for IPv6 and RIPv2. The routing protocols, BGPv4, EIGRP, EIGRPv6 for IPv6, PIM-SMv2, and OSPFv2, OSPFv3 for IPv6 supports routing updates with IPv4 or IPv6, while RIPv2 routing protocol support routing updates for IPv4 only. All these routing protocols support authentication of neighbor routers using MD5. Neither the authentication functions of those protocols, nor the use of MD5 were evaluated under Common Criteria.
- SSHv2 sessions secured connection is supported inbound and outbound for remote administrative access to the TOE, or to initiate administrative access to an external network device or other device/server running SSHv2.
- Syslog is supported outbound for transmission of audit records to a remote syslog server (syslog connections must be tunneled through IPsec).
- SSL (not TLS) may be running, however there are no claims being made, was not evaluated and should not be used in the evaluated configuration.

- TLS to secure communications may be running, however there are no claims being made, was not evaluated and should not be used in the evaluated configuration.

Infrastructure services

- Cisco IOS software; to be configured for use as described in this document.
- Redundant components, such as power supplies and fans.
- Automation through Embedded Event Manager (EEM); no claims are made in the evaluated configuration. This may not be supported on all TOE models due to limited space.
- AutoQoS (quality of services responding to traffic flows); no claims are made in the evaluated configuration.

Borderless services

- Rich layer 2/3/4 information (MAC, VLAN, TCP flags); no claims are made in the evaluated configuration.

# 8. 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.

**Table 15 Security Objective for the Operational Environment**

| Security Objective for the Operational Environment | Definition of the Security Objective | Responsibility of the Administrators |
|---|---|---|
| OE.PHYSICAL | Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. | The TOE must be installed to a physically secured location that only allows physical access to authorized personnel. |
| OE.NO_GENERAL_PURPOSE | 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. | None. IOS is a purpose-built operating system that does not allow installation of additional software. |
| OE.NO_THRU_TRAFFIC_PROTECTION | 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. | Administrators will ensure protection of any critical network traffic (administration traffic, authentication traffic, audit traffic, etc.) and ensure appropriate operational environment measures and policies are in place for all other types of traffic. |
| OE.TRUSTED_ADMIN | TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. | Administrators must read, understand, and follow the guidance in this document to securely install and operate the TOE and maintain secure communications with components of the operational environment. |
| OE.UPDATES | 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. | Administrators must download updates, including psirts (bug fixes) to the evaluated image to ensure that the security functionality of the TOE is maintained |
| OE.ADMIN_CREDENTIALS_SECURE | The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside. | Administrators must securely store and appropriately restrict access to credentials that are used to access the TOE (i.e. private keys and passwords) |
| OE.RESIDUAL_INFORMATION | The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. | Administrators must securely wipe the TOE of any and all sensitive information prior to removing from the operational environment. |

# 9. Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at:

With CCO login:
http://www.cisco.com/en/US/partner/docs/general/whatsnew/whatsnew.html

Without CCO login:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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

## 9.1 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.

## 9.2 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 any time, 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