

Cisco 2621 Security Policy

Project Headline

This document describes the rules for an IOS system using software-based IPSec encryption when used in accordance with FIPS 140-1 level 2 requirements. Please see [FIPS 140-1] for a full list of the FIPS 140-1 requirements.

Definitions

This section defines words, acronyms, and actions which may not be readily understood.

IPSec - Internet Protocol Security, a family of IETF protocols which provide network layer encryption.

IKE - Internet Key Exchange, a key management protocol used by IPSec for authentication and secret key derivation.

1.0 Roles and Services

Role-based authentication is used by the IOS. Two roles are defined: a User role, and a Crypto-Officer role. There is no maintenance role. Services available for each role are listed. Please see [UNIVERCD -found at the last page underReference Documents] for a detailed configuration description.

1.1 User Role

A user enters the system by accessing the console port with a terminal program.

The IOS prompts the user for their password, entered in plaintext. If it matches the plaintext password stored in IOS memory, the user is allowed entry to the IOS executive program. The non-cryptographic services available to the User role include the following:

- Obtain non-encryption router status (e.g., state of an interface, state of layer 2 protocols, version of IOS currently running)
- Connect to other network devices (e.g., outgoing Telnet, PPP)
- Initiate diagnostic network services (e.g., ping, mtrace)
- Adjust the terminal session (e.g., lock the terminal, adjust flow control)
- Display a directory of files kept in Flash memory
- Other non-cryptographic services can be viewed in the console by typing "?" at the command prompt.

The following cryptographic services are available to the user:

Crypto User Encryption Services

Description of Service	Executive Command
Attempt to enter the crypto officer role	Enable

1.2 Crypto-Officer Role

The Crypto-Officer role is entered from the User role by typing the `enable` command and responding with an appropriate password. The enable password entered by the Crypto-Officer is compared to a password stored in the router memory. If two passwords match, the Crypto-Officer enters the Crypto-Officer role.

The non-cryptographic services available to the Crypto-Officer role include the following:

- Perform router configuration (e.g., defining IP addresses, enabling interfaces, enabling network services)
- Reload and shut down the router
- Display full status of the router
- Shut down and restart network services
- Display the router configuration stored in memory, and also the version saved in NVRAM, which is used to initialize a router following a reboot.
- Other non-cryptographic services can be viewed in the console by typing “?” at the command prompt.

The following cryptographic services are available to the Crypto-Officer:

Crypto-Officer Cryptographic Services: Configuration

Description of Service	Configuration Command
Add/delete crypto users, and assign passwords to users	line console 0 (to enable user role and password) password (enter password) login
Create the crypto officer password	enable password
Set IPSec security association parameters	crypto ipsec security-association
Set an IPSec transform set	crypto ipsec transform-set
Create access-lists to match encrypted traffic	access-list <100-199>
Define IPSec policy and keys for a connection	crypto map
Set IPSec policy on a network interface	interface <interface name> crypto map

Executive commands in the User role are also available in the Crypto-Officer role. The following commands are only available to the Crypto-Officer:

Crypto-Officer Cryptographic Services: Executive Commands

Description of Service	Executive Command
Show the current IPSec security associations	show crypto ipsec sa
Show the current IPSec security association lifetimes	show crypto ipsec security- association-lifetime
Show the current IPSec transforms	show crypto ipsec transform-set
Show the number of encrypted and decrypted packets on a router	show crypto engine connections active
Clear an IPSec security association	clear crypto sa
Execute encryption self tests	Power regeneration or command “reload” for soft reboot

2.0 Security Rules

2.1 System Requirements

The following requirements relate to how the IOS system must be configured.

1. The tamper-evident labels must be placed according to the “Tamper-evident Label Placements” documentation prior to starting any of the services of the module. There are five tamper-evident labels that must be placed according to the documentation. If any of the labels were tampered with, the labels will clearly indicate that tampering has occurred. The tamper-evident labels have to two layers. Upon tampering, the second layer will be peeled with the word “VOID” appearing on the first layer, which will stay on the module. This will clearly show tamper evidence.
2. The IOS version must be an image of the following type: c2600-ik25-mz, release ___ or later.
3. The IOS version which is shipped with a router is the *only* allowable image. The loading of any other image is not allowed.
4. The value of the `config-register` which affects booting must be 0x0101 (the factory default). This setting disables “break” from the console to the ROM monitor, and specifies the first file in Flash to be the boot IOS image.
5. The Crypto-Officer must be present when the system is initialized and perform the initial configuration. The Crypto-Officer must create at least one Crypto-Officer role, as well as define the enable password for the Crypto-Officer role.
6. The Crypto-Officer shall always assign passwords to users.
7. The Crypto-Officer shall only assign users to a privilege level 1 (the default)
8. The Crypto-Officer shall not assign a command to any privilege level other than its default.
9. The following network services affect the security data items and must not be configured: SNMP, NTP, TACACS+, RADIUS, Kerberos.
10. Using RSA will take the module out of FIPS mode under IKE.
11. All terminal services must be disabled, except for the console. The following configuration disables login services on the auxiliary console line:
line aux 0
no exec
To disallow Telnet and x.29 access to the router, the following configuration must be used:
line vty 0 4
transport input none

2.2 IPSec Requirements and Cryptographic Algorithms

There are two types of key management methods allowed in FIPS mode:

- IPSec manually entered keys
- Internet Key Exchange with Pre-shared keys

Although the IOS implementation of IKE allows a number of algorithms, only the following transforms using FIPS approved algorithms are allowed in a FIPS 140-1 configuration:

- ah-sha-hmac
- esp-des
- esp-sha-hmac
- esp-3des (approved for government use)

Other non-FIPS approved algorithms include:

- RSA
- MD-4
- MD-5

3.0 Security Data Items

The following sections describe security relevant data items, and any restrictions on the user-configurable data items.

3.1 Passwords

The Crypto-Officer shall set user passwords to be at least 8 characters in length.

- User Passwords
- Enable Password

3.2 Keys

- IPSec DES Session Keys
- IPSec SHA HMAC Keys
- IKE Pre-shared Keys

The cryptographic keys are physically protected by the tamper-evident labels. The cryptographic keys are also protected with passwords.

Reference Documents

[FIPS 140-1] FIPS PUB 140-1 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION. Available online at <http://csrc.ncsl.nist.gov/fips/fips1401.htm>

[UNIVERCD] Cisco IOS documentation. Available online at <http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm>



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
<http://www-europe.cisco.com>
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

Americas
Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
<http://www.cisco.com>
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Connection Online Web site at <http://www.cisco.com/offices>.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela