

Document Number ENG-27621
Revision A
Author Brian Weis
Project Manager David McGrew

Cisco 3640 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 reference [FIPS-140] for a full list of the FIPS 140-1 requirements.

Department	Name	Acceptance Date
IOS Encryption	David McGrew, Manager	

Reviewers

Rev.	Date	Originator	Comment
A	11/24/99	Brian Weis	Initial Version

Modification History

Definitions

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

IPSEC A family of IETF protocols which provide network layer encryption.
IKE 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] 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:

- 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 such as ping, telnet, and etc. can be viewed in the console by typing “?” at the command prompt.

The following cryptographic services are available to the user:

Table 1: 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 invoking 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:

- 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
- Shutdown 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 such as network configuration and routing configuration 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 commnad “reload” for soft reboot

2.0 Security Rules

2.1 System Requirements

The following requirement 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 are tampered, there will be clear tampered evidence from the labels. The tamper-evident labels have two layers. Upon tampering, the second layer will be peeled with the word “VOID” and stay on the module. This will clearly show tamper evidence.
2. The IOS version must be an image of at the following type: Cisco IOS Version 12.1(1)T.
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. He 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. The Flash memory card will not be configured in FIPS mode.
12. 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 method that are 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 FIPS140-1 configuration.

- ah-sha-hmac
- esp-des
- esp-sha-hmac
- esp-3des

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 Passwords

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.

4.0 Tamper-evident Label Placements

Label 1: The tamper-evident label must be placed so that the 1/2 of the label must cover the front enclosure and the other 1/2 must cover the main body of the module. Any attempt to remove the front enclosure port shall leave tamper evidence by the tamper-evident label.

Label 2: The tamper-evident label must be placed so that the 3/4 of the label must cover the two PC slots and the rest must be attached to the main body of the module. Any attempts to remove the PC slots or the Main board of the module shall leave tamper evidence by the tamper-evident label.

Label 3, 4, 5, and 6: The tamper-evident label must be placed so that the half of the label must cover the enclosure and the other half must cover the Network module slot. Any attempt to remove the Network module slot shall leave tamper evidence by the tamper-evident label. Additional labels may be required if the Network module slot is separated into four WAN or LAN ports.

Note: The tamper-evident labels must be placed 24 hours minimum to be in FIPS mode.

Figure 1. Front Tamper-evident label placements

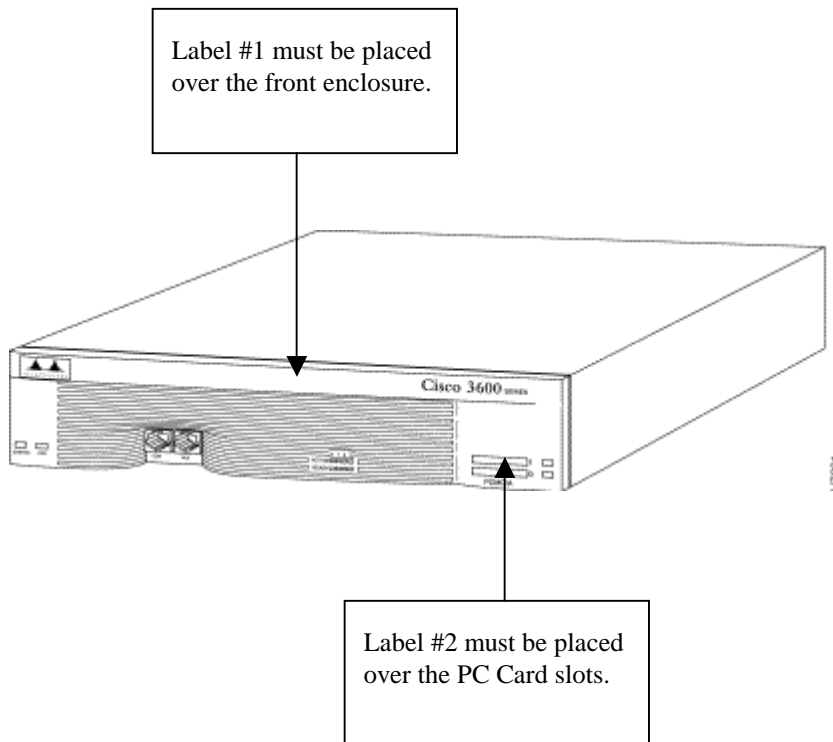
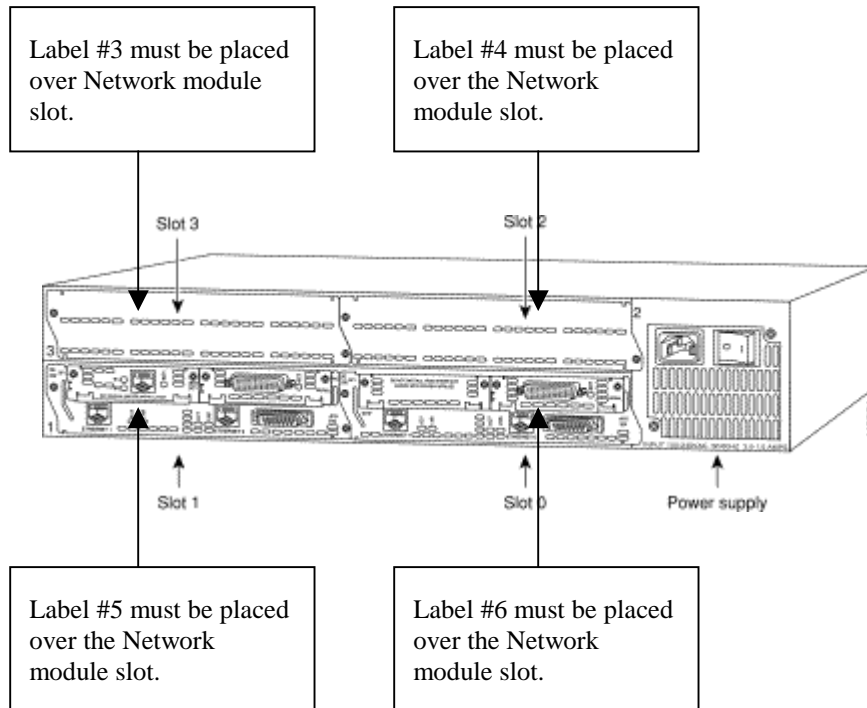


Figure 2. Rear Tamper-evident label placements



Reference Documents

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

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

Document Number ENG-27621
Revision A
Author Brian Weis
Project Manager David McGrew

Cisco 7140 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 reference [FIPS-140] for a full list of the FIPS 140-1 requirements.

Department	Name	Acceptance Date
IOS Encryption	David McGrew, Manager	

Reviewers

Rev.	Date	Originator	Comment
A	9/25/98	Brian Weis	Initial Version
B	11/17/98	Brian Weis	Changed authentication method

Modification History

Definitions

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

IPSEC A family of IETF protocols which provide network layer encryption.
IKE 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] 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:

- 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 such as ping, telnet, and etc. can be viewed in the console by typing “?” at the command prompt.

The following cryptographic services are available to the user:

Table 1: 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 invoking 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:

- 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
- Shutdown 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 such as network configuration and routing configuration 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 commnad “reload” for soft reboot

2.0 Security Rules

2.1 System Requirements

The following requirement 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 are tampered, there will be clear tampered evidence from the labels. The tamper-evident labels have two layers. Upon tampering, the second layer will be peeled with the word “VOID” and stay on the module. This will clearly show tamper evidence.
2. The IOS version must be an image of at the following type: Cisco IOS Version 12.1(1)T.
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. He 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. The Flash memory card will not be configured in FIPS mode.
12. 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 method that are 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 FIPS140-1 configuration.

- ah-sha-hmac
- esp-des
- esp-sha-hmac
- esp-3des

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 Passwords

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.

4.0 Tamper-Evident Label Placements

Label 1 and 2: The tamper-evident label must be placed over the enclosure. It must be placed at the location shown in Figure 1. One half of the tamper-evident label must cover the enclosure and the other half must cover the router. Any attempt to remove the enclosure shall leave tamper evidence by the tamper-evident label.

Label 3: The tamper-evident label must be placed so that the one half of the label must cover the enclosure and the other half must cover the Service module slot. Any attempt to remove the Service module slot shall leave tamper evidence by the tamper-evident label.

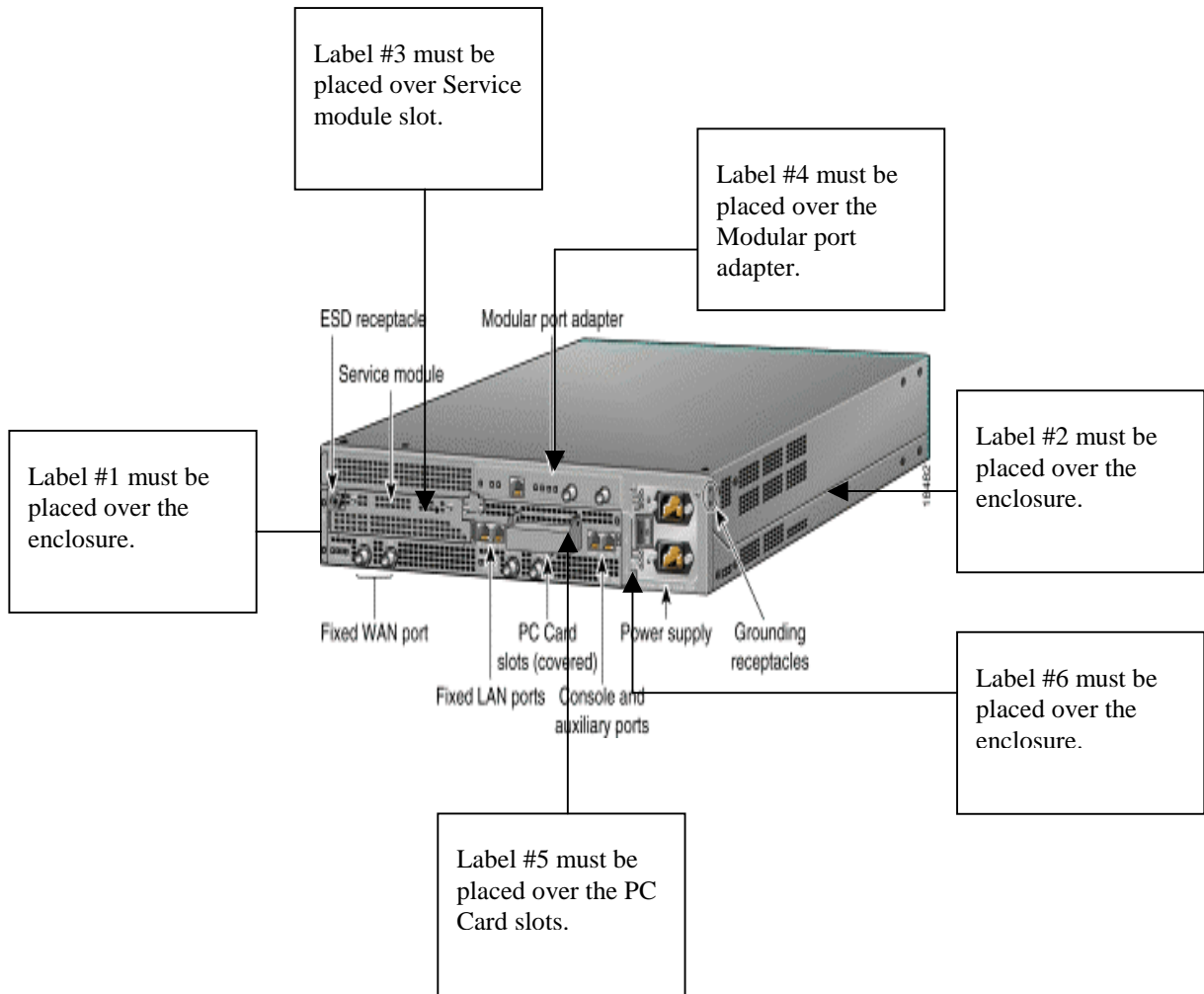
Label 4: The tamper-evident label must be placed so that the half of the label must cover the enclosure and the other half must cover the Modular port adapter. Any attempt to remove the Modular port adapter shall leave tamper evidence by the tamper-evident label.

Label 5: The tamper-evident label must be placed so that the half of the label must cover the enclosure and the other half must cover the PC Card slots. Any attempt to remove the PC Card slots shall leave tamper evidence by the tamper-evident label.

Label 6: The tamper-evident label must be placed so that the half of the label must cover the enclosure and the other half must cover the fixed WAN slot. Ensure that the label covers the screw as shown in figure 1. Any attempt to remove the fixed WAN slot shall leave tamper evidence by the tamper-evident labels.

Note: The tamper-evident labels must be placed 24 hours minimum to be in FIPS mode.

Figure 1. Tamper-evident label placements



Reference Documents

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

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

Document Number ENG-27621
Revision A
Author Brian Weis
Project Manager David McGrew

Cisco 7206 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 reference [FIPS-140] for a full list of the FIPS 140-1 requirements.

Department	Name	Acceptance Date
IOS Encryption	David McGrew, Manager	

Reviewers

Rev.	Date	Originator	Comment
A	11/24/99	Brian Weis	Initial Version

Modification History

Definitions

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

IPSEC A family of IETF protocols which provide network layer encryption.
IKE 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] 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:

- 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 such as ping, telnet, and etc. can be viewed in the console by typing “?” at the command prompt.

The following cryptographic services are available to the user:

Table 1: 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 invoking 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:

- 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
- Shutdown 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 such as network configuration and routing configuration 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 commnad “reload” for soft reboot

2.0 Security Rules

2.1 System Requirements

The following requirement 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 are tampered, there will be clear tampered evidence from the labels. The tamper-evident labels have two layers. Upon tampering, the second layer will be peeled with the word “VOID” and stay on the module. This will clearly show tamper evidence.
2. The IOS version must be an image of at the following type: Cisco IOS Version 12.1(1)T.
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. He 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. The Flash memory card will not be configured in FIPS mode.
12. 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 method that are 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 FIPS140-1 configuration.

- ah-sha-hmac
- esp-des
- esp-sha-hmac
- esp-3des

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 Passwords

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.

4.0 Tamper-Evident Label Placements

Label 1, 2, 3, 4, 5, and 6: The tamper-evident label must be placed next to the port adapter lever lock. It must be placed at the locations shown in Figure 1. The labels must be placed after the port adapter lever is in a lock position. The labels must be placed over the lock and unlock gap so that if attempts have been made to unlock the port adapter levers, the labels shall clearly leave tamper evidence.

Label 7: The tamper-evident label must be placed so that the 3/4 of the label must cover the two PC slots and the rest must be attached to the main body of the module. Any attempts to remove the PC slots or the Main board of the module shall leave tamper evidence by the tamper-evident label.

Label 8: The tamper-evident label must be placed so that the 1/2 of the label must cover the enclosure and the other 1/2 must cover the power supply filter plate. Any attempt to remove the power supply filter plate shall leave tamper evidence by the tamper-evident label.

Label 9: The tamper-evident label must be placed so that the 1/2 of the label must cover the enclosure and the other 1/2 must cover the power port. Any attempt to remove the power port shall leave tamper evidence by the tamper-evident label.

Label 10: The tamper-evident label must be placed so that the 1/2 of the label must cover the enclosure and the other 1/2 must cover the network processing engine board. Any attempt to remove the network processing engine board shall leave tamper evidence by the tamper-evident label.

Note: The tamper-evident labels must be placed 24 hours minimum to be in FIPS mode.

Figure 1. Front Tamper-evident label placements

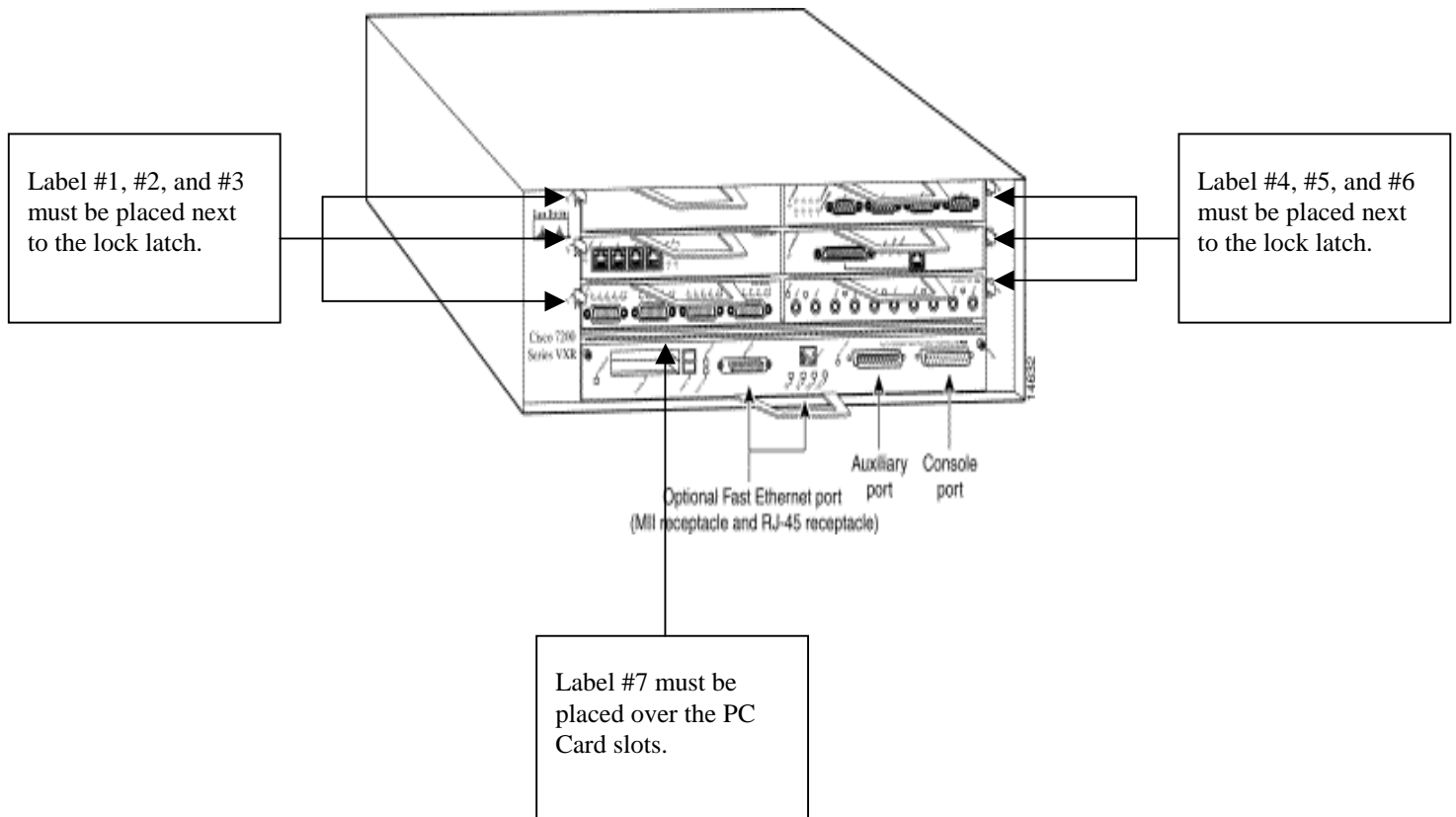
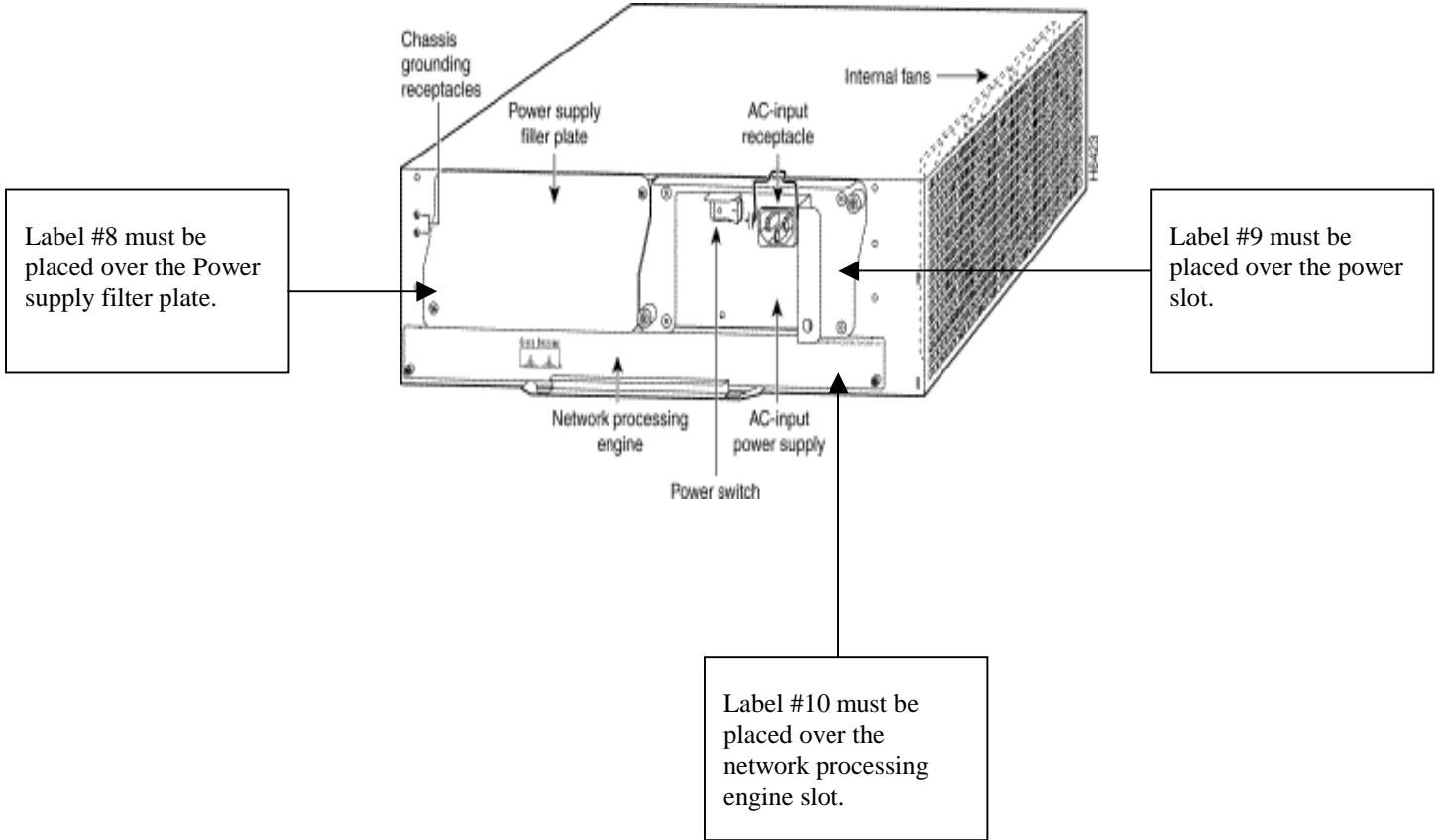


Figure 2. Back Tamper-evident label placements



Reference Documents

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

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