National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Cisco IOS-IPSEC on the Integrated Service Routers, VPN Services Module (VPNSM) and IPSec VPN Shared Port Adapter (SPA), including VLAN separation

Report Number: CCEVS-VR-VID10116-2008
Dated: 31 May 2008
Version: 1.4

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road Suite 6740
Fort George Meade, MD 20755-6740

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the Cisco IOS-IPSEC on the Integrated Service Routers, VPN Services Module (VPNSM) and IPSec VPN Shared Port Adapter (SPA), including VLAN separation was performed by the ARCA Common Criteria Testing Laboratory in the United States and was completed on 31 May 2008. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.3, Evaluation Assurance Level 4, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Part 2, Version 2.3.

The ARCA Common Criteria Testing Laboratory is an approved National Information Assurance Partnership (NIAP) Common Criteria Testing Laboratory (CCTL). The CCTL concluded that the Common Criteria assurance requirements for Evaluation Assurance Level 4 (EAL4) have been met and that the conclusions in its Evaluation Technical Report are consistent with the evidence produced.

This Validation Report is not an endorsement of the Cisco IOS-IPSEC on the Integrated Service Routers, the VPN Services Module or the IPSec VPN Shared Port Adapter by any agency of the US Government and no warranty of the product is either expressed or implied.

The cryptography used in this product was not analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

1.1 Cisco IOS-IPSEC Functionality

The TOE consists of hardware and software used to construct Virtual Private Networks (VPNs) between networks or a remote access client. The TOE is made up of a single Cisco router or Catalyst 6500 switch, inclusive of IOS software and hardware modules used to accelerate the performance of the IPSEC protocol. The included Cisco hardware provides options for deploying VPNs from the small office to the large Enterprise

IPSec provides confidentiality, authenticity and integrity for IP data transmitted between trusted (private) networks or remote clients over untrusted (public) links or networks. The TOE therefore provides confidentiality, authenticity and integrity for IP data transmitted between a combination of Cisco Systems routers, Catalyst switches, VPN clients (within the IT Environment), VPNSM and IPSec VPN SPA.

1.2 Evaluation Details

Table 1 provides the required evaluation identification details.

Table 1: Evaluation Details

Item	Identification
Evaluation Scheme	US Common Criteria Evaluation and Validation Scheme (CCEVS)
Target of Evaluation	Cisco IOS-IPSEC on the Integrated Service Routers, VPN Services

	Module (VPNSM) and IPSec VPN Shared Port Adapter (SPA), including VLAN separation
EAL	EAL4
Protection Profile	None
Security Target	Security Target for IOS IPSEC on the Integrated Services Routers, VPN Services Module (VPNSM) and IPSec VPN Shared Port Adapter (SPA), including VLAN separation, Version 1.0, 5 May 2008
Developer	Tresys Technology, LLC 8840 Stanford Blvd., Suite 2100 Columbia, MD 21045
Evaluators	Rick West, Maria Tadeo, and Ken Dill ARCA CCTL 45901 Nokes Boulevard Sterling, VA 20166
Validators	John Nilles, The Aerospace Corporation Ken Elliott, The Aerospace Corporation
Dates of Evaluation	August 5, 2005 to 31 May 2008
Conformance Result	Part 2 extended; and Part 3 EAL 4 augmented with ALC_FLR.1.
Common Criteria (CC) Version	CC, version 2.3, August 2005

1.3 Interpretations

No NIAP or CCIMB interpretations are applicable to the ST

The Evaluation Team also complied with the CCEVS Precedents identified in Table 2

Table 2: CCEVS Precedents Applied to the Evaluation

Precedent	Precedent Title
PD-0108	Correctly specify remote administration

2. Identification of the TOE

The TOE consists of the Cisco router/switch hardware, Internetwork Operating System software and its guidance information. The table below contains the hardware and software compliant with Common Criteria evaluated Cisco IOS/IPSec. Only these specific models, hardware acceleration modules, and IOS Releases may be used. the Administration Guide contains information on other configuration limitations that must be enforced when using the device in the evaluated configuration.The VPN Client is not considered part of the TOE.

Model Family	Models	IPSec Hardware Acceleration Module	IOS Release	Additional Interface Cards or Modules
870	c871, c876, c877, c878	On board	12.4(11)T3	None
1800	c1801, c1802, c1803, c1811, c1812	On board	12.4(11)T3	None
1800	1841	On board or AIM-VPN/BPII-PLUS or AIM-VPN/SSL-1	12.4(11)T3	None
2800	2801	On board or AIM-VPN/EPII-PLUS or AIM-VPN/SSL-2	12.4(11)T3	None
	2811	On board or AIM-VPN/EPII-PLUS or AIM-VPN/SSL-2	12.4(11)T3	None
	2821	On board or AIM-VPN/EPII-PLUS or AIM-VPN/SSL-2	12.4(11)T3	None
	2851	On board or AIM-VPN/EPII-PLUS or AIM-VPN/SSL-2	12.4(11)T3	None
3800	3825	On board or AIM-VPN/EPII-PLUS or AIM-VPN/SSL-3	12.4(11)T3	None
	3845	On board or AIM-VPN/HPII-PLUS or AIM-VPN/SSL-3	12.4(11)T3	None
7200	7204VXR, 7206VXR	NPE-G1 and SA-VAM2 or SA-VAM2+	12.4(11)T3	None

		NPE-G2 and SA-VAM2, SA-VAM2+ or VSA		
7300	7301	SA-VAM2, SA-VAM2+	12.4(11)T3	None
		VSA		
6500	6503, 6506, 6509, 6513, all with Supervisor 720	• VPNSM • IPSec VPN SPA with SPA Carrier-400 (SSC-400)	12.2(18)SXF10	See section 5.1
7600	7603, 7606, 7609 and 7613, all with Supervisor 720	• VPNSM • IPSec VPN SPA with SPA Carrier-400 (SSC-400)		

Table 3 Evaluated Hardware and Software

870 Exclusions

The Cisco Systems 870 family of routers is a fixed configuration and does not provide any additional slots for interfaces.

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port, USB ports, and ISDN Dial Backup. There is no PC Card Slot or V.90 Analog modem on this family.

1800 (1801 – 1812) Exclusions

The Cisco Systems 1800 fixed configuration family of routers does not provide any additional slots for interfaces.

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port, USB ports, V.90 Analog Modem Dial Backup, and ISDN Dial Backup. There is no PC Card slot in this family.

1841 Exclusions

The Cisco Systems 1841 Router provides HWIC slots for additional interfaces. These slots may not be populated with any interfaces in the evaluated configuration. The AIM slot may only be populated with a AIM-VPN/BPII-PLUS or AIM-VPN/SSL-1.

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port and USB ports. There is no PC Card slot or V.90 analog modem in this Router.

2800 Exclusions

The Cisco Systems 2800 Family provides DSP, HWIC, and Network Module slots for additional interfaces. These slots may not be populated with any interfaces in the evaluated configuration. The AIM slots may only be populated with an AIM-VPN/EPII-PLUS or AIM-VPN/SSL-2.

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port and USB ports. There is no PC Card slot or V.90 analog modem in this family.

3800 Exclusions

The Cisco Systems 3800 Family provides PVDM, HWIC, and Network Module slots for additional interfaces. These slots may not be populated with any interfaces in the evaluated configuration. The AIM slots may only be populated with an AIM-VPN/EPII-PLUS or AIM-VPN/SSL-3.

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port and USB ports. There is no PC Card slot or V.90 analog modem in this family.

7200 / 7300 Exclusions

The Cisco Systems 7200 and 7300 Families provide Port Adapter slots for additional interfaces. These slots may not be populated with any interfaces in the evaluated configuration. The security module slots may only be populated with an SA-VAM2, SA-VAM2+, or VSA.

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port and USB ports. There is no PC Card slot or V.90 analog modem in these families.

6500 / 7600 Exclusions

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port. There is no V.90 analog modem, or USB ports contained within the Supervisor engine.

The following Cisco 6500 / 7600 Modules are specifically excluded from use in the evaluated configuration:

- Application Control Engine (ACE) Module ACE10-6500-K9
- Communication Media Module and associated Port Adapters WS-SVC-CMM=, WS-SVC-CMM-6E1=, WS-SVC-CMM-6T1=, WS-SVC-CMM-ACT=, WS-SVC-CMM-24FXS=
- Content Switching Module WS-X6066-SLB-APC=
- Content Switching Module with Secure Sockets Layer (SSL) WS-X6066-SLB-S-K9 =
- Firewall Services Module WS-SVC-FWM-1-K9=
- Intrusion Detection System (IDSM-2) Module WS-SVC-IDS2=
- Network Analysis Module (NAM -1/NAM -2) WS-SVC-NAM-1=, WS-SVC-NAM-2=
- Wireless Services Module (WiSM) WS-SVC-WISM-1-K9=
- Cisco 7600 Series Session Border Controller SBC
- Cisco 7600 Series / Catalyst 6500 Series WebVPN Services Module
- Cisco 7600 Series / Catalyst 6500 Series Anomaly Guard Module
- Cisco 7600 Series / Catalyst 6500 Series Traffic Anomaly Detector Module

3. Security Policy

The TOE provides the following security functions:

- Packet Filtering
  - PACKETFILTER.1 - Packet Filtering
- Configuration and Management
  - CONFIG.1 – System Messages
  - CONFIG.2 - Management Interfaces
  - CONFIG.3 – Management of Time
- IPSec Implementation
  - IPSEC.1 – IPSec Internet Key Exchange (IKE)
  - IPSEC.2 – IPSec Encapsulating Security Payload (ESP)
  - IPSEC.3 – Cryptographic Maps
- VLAN Management
  - VLAN.1 – VLAN Processing
- Key Management
  - KEYMGT.1 - Key Management
- Remote Management
  - REMOTE.1 - Remote Management
- Self Protection
- PROTECT.1 – Self Protection

3.1 IPSec Implementation

The TOE implements the IETF IPSec protocols (RFCs 2401-2404, 2406-2409) to provide confidentiality, authenticity and integrity for packet flows transmitted from and received by the TOE. The TOE IPSec implementation contains a number of functional components that meet the IPSec TSF.

IPSec provides secure *tunnels* between two VPN (IPSec) peers, such as a pair of security gateways (TOEs), a TOE and a security gateway, or a TOE and a host (VPN Client). With IPSec, the administrator defines what traffic should be protected between two IPSec peers by configuring crypto access control lists and applying these access lists to interfaces by way of cryptographic (crypto) map sets. Therefore, traffic may be selected on the basis of source and destination address, and optionally Layer 4 protocol, and port. (The crypto access control lists used for IPSec are used only to determine which traffic should be protected by IPSec, not which traffic should be blocked or

permitted through the interface. Separate access control lists define blocking and permitting at the interface.)
A crypto map set can contain multiple entries, each with a different crypto access control list. The crypto map entries are searched in order and the TOE attempts to match the packet to the crypto access control list specified in that entry.

When a packet matches a **permit** entry in a particular crypto access control 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 no security association (SA) exists that 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 crypto access control list entry.

Once established, the set of SAs (outbound, to the peer) are then applied to the triggering packet and to subsequent applicable packets as those packets exit the TOE. "Applicable" packets are packets that match the same access control 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. Multiple IPSec tunnels can exist between two peers to secure different data streams, with each tunnel using a separate set of SAs.
Crypto access control lists associated with IPSec crypto map entries also represent which traffic the TOE requires to be protected by IPSec. Inbound traffic is processed against the crypto map entries—if an unprotected packet matches a **permit** entry in a particular access control 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 to apply to IPSec protected traffic. During the IPSec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

IPSEC.1 - IPSec Internet Key Exchange (IKE)

IKE is a key management protocol standard that is used in conjunction with the IPSec. IKE automatically negotiates IPSec security associations (SAs) and enables IPSec secure communications without manual pre-configuration. Specifically, IKE provides the following benefits:

- Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
- Allows specification of a lifetime for the IPSec SA.
- Allows encryption keys to change during IPSec sessions.
- Allows IPSec to provide anti-replay services.
- Permits certification authority (CA).
- Allows dynamic authentication of peers.

IKE has two phases of key negotiation: phase 1 and phase 2. Phase 1 negotiates a security association (a key) between two IKE peers. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During phase 2 negotiation, IKE establishes keys (security associations) for IPSec. The TOE destroys keys by overwriting them.

Because IKE negotiations must be protected, each IKE negotiation begins by agreement of both peers on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations and mandates how the peers are authenticated. After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these SAs apply to all subsequent IKE traffic during the negotiation.

IKE authenticates IPSec peers using pre-shared keys, RSA keys or digital certificates. It also handles the generation and agreement of secure session keys using the Diffie-Hellman algorithm and negotiates the parameters used during IPSec ESP (IPSEC.2)
IKE maintains a trusted channel, referred to as a Security Association (SA), between IPSec peers that is also used to manage IPSec connections, including:

- The negotiation of mutually acceptable IPSec options between peers,
- The establishment of additional Security Associations to protect packets flows using ESP (as per IPSEC.2), and
- The agreement of secure bulk data encryption 3DES (168-bit) /AES (128, 192 or 256 bit) keys for use with ESP (IPSEC.2).
-

Implementation of the various cryptographic standards and RFCs ensure that only appropriate secure values are used for the cryptographic functions performed.

IKE extended authentication (Xauth) is a draft RFC based on the IKE protocol and requires username and password to perform user authentication in a separate phase after the IKE authentication phase 1 exchange. Xauth does not replace IKE. IKE allows for device authentication (using pre-shared keys, RSA keys or digital certificates) and Xauth allows for user authentication, which occurs after IKE device authentication. Xauth occurs after IKE authentication phase 1 but before IKE IPSec SA negotiation phase 2. The TOE can be configured to use the local authentication mechanism or an external authentication server for Xauth user authentication. To configure Xauth on the TOE, the administrator defines a client authentication list for a crypto map and applies the crypto map to an interface. The client authentication list identifies the authentication method (local and/or external authentication server) to use for user authentication. The administrator creates username and password entries into the local username database or the external authentication server.

IPSEC.2 - IPSec Encapsulating Security Payload (ESP)

The TOE uses ESP to protect packet flows between IPSec peers across interconnected untrusted networks in accordance with a TOE security policy (TSP). ESP is a method of encapsulating IP Packets and provides confidentiality using the 3DES and AES ciphers, integrity and authenticity using the MD5 and SHA-1 algorithms, and a mechanism to detect the capture and retransmission of packets (replay attacks) ensuring proof of origin cannot be repudiated. Implementation of the various cryptographic standards and RFCs ensure that only appropriate secure values are used for the cryptographic functions performed.

The parameters used by ESP, including session encryption keys, are negotiated via IPSec security associations (SAs) established via IKE (IPSEC.1) in accordance with the TSP. Note that security associations are unidirectional so that between IPSec peers protecting a packet flow (labeled A and B for example) there are at least two SA's - one from A to B and one from B to A. Each SA, and associated session encryption key, has a lifetime, which upon expiry results in a new SA and session encryption key being established by the SA peers.

The packet flows between two remote IPSec peers that are to be protected by the TOE are defined by way of cryptographic maps (IPSEC.3).

IPSEC.3 - Cryptographic Maps

Cryptographic (crypto) Maps are used by the routers/switch to pull together the various parts used to setup IPSec SAs, including:

a) Which packet flow (i.e. IP packets) that are to be protected by encryption, identified by a crypto access control list that can include IP protocol, source/destination IP address and source/destination UDP/TCP port number;
b) the granularity of the flow to be protected by a set of SAs;
c) how to identify the peer TOE that will decrypt the packet flow;
d) the interface(s) that are enabled for IPSec using the parameters specified above
e) what IPSec SA should be applied to the packet flow (by selecting from a list of one or more transform sets)
f) other parameters that might be necessary to define an IPSec SA.

Crypto map entries with the same crypto map name (but different map sequence numbers) are grouped into a crypto map set. The administrator applies these crypto map sets to interfaces; then, all IP traffic passing through the interface is evaluated against the applied crypto map set. If a crypto map entry sees outbound IP traffic that should be protected and the crypto map specifies the use of IKE, a SA is negotiated with the remote peer according to the parameters included in the crypto map entry; otherwise, if the crypto map entry specifies the use of manual SAs, an SA should have already been established via configuration. (If a dynamic crypto map entry sees outbound traffic that should be protected and no security association exists, the packet is dropped.)

The policy described in the crypto map entries is used during the negotiation of SAs. If the local router initiates the negotiation, it uses the policy specified in the static crypto map entries to create the offer to be sent to the specified IPSec peer. If the IPSec peer initiates the negotiation, the local router checks the policy from the static crypto map entries, as well as any referenced dynamic crypto map entries to decide whether to accept or reject the peer's request (offer). For IPSec to succeed between two IPSec peers, both peers' crypto map entries must contain compatible configuration statements.

Dynamic crypto maps ease IPSec configuration and are recommended for use with networks where the VPN peers are not always predetermined. A dynamic crypto map entry is essentially a static crypto map entry without all the parameters configured. It acts as a policy template where the missing parameters are later dynamically configured (as the result of an IPSec negotiation) to match a remote peer's requirements. This allows remote peers to exchange IPSec traffic with the router even if the router does not have a crypto map entry specifically configured to meet all of the remote peer's requirements.

For both static and dynamic crypto maps, if unprotected inbound traffic matches a **permit** statement in a crypto access list, and the corresponding crypto map entry is tagged as "IPSec," then the traffic is dropped because it is not IPSec-protected. (This is because the security policy as specified by the crypto map entry states that this traffic must be IPSec-protected.)

For static crypto map entries, if outbound traffic matches a **permit** statement in an access list and the corresponding SA is not yet established, the router initiates new SAs with the remote peer. In the case of dynamic crypto map entries, if no SA existed, the traffic would simply be dropped (because dynamic crypto maps are not used for initiating new SAs).

The functionality provided by cryptographic maps are modeled in the IPSec Information Flow SFP.

3.2 Packet Filtering

The TOE prevents attempts to establish management control connections to the TOE itself by rejecting packet flows (i.e. IP packets) that are not consistent with the information flow SFP.

PACKETFILTER.1- Packet Filtering

The TOE performs input packet filtering by applying an access control list (ACL) to specific interfaces of the TOE-enabled router / switch. ACLs filter network traffic by controlling whether routed packets are forwarded or blocked at the router’s interfaces. The router examines each packet to determine whether to forward or drop the packet, on the basis of the criteria the administrator specified within the access lists. The ACL can include IP protocol, source/destination IP address and source/destination UDP/TCP port number. Packets not matching the ACL are logged and discarded by the router / switch. The functionality provided by ACLs is modeled in the Packet Filter Information Flow SFP. The TOE rejects requests for access or services where the information arrives on a network interface, and the presumed address of the source subject is an external IT entity on a different network interface, this includes broadcast and loopback networks. This allows for traffic from known spoofed addresses, broadcasts and loopbacks to be blocked. By implementing this form of policy enforcement, the TOE ensures that the TSP cannot be bypassed as long as the TOE is correctly configured.

Individual rules that make up an IP ACL can have various values that control whether a packet results in a hit or miss on the ACL. See Appendix D, Table 3 for the details on all the ACL options that were specifically tested for Common Criteria and Table 4 for the details of the options available for use with an access control list that were not specifically tested for Common Criteria.

This table describes options to an IP Access Control List specifically tested with this version of the TOE for Common Criteria. Common Criteria specific testing represents a small percentage of the total regression testing that is performed against Cisco IOS.

ACL Option	**Description**
deny | **permit**	Denies or permits access if the conditions are matched.
Protocol	Name or number of an Internet protocol, expressed as an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP) the **ip** keyword is used.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. Each wildcard bit 0 indicates the corresponding bit position in the source. Each wildcard bit set to 1 indicates that both a 0 bit and a 1 bit in the corresponding position of the IP address of the packet will be considered a match to this access list entry. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:

	• Use a 32-bit quantity in four-part dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

Table 4: ACL Options Specifically Tested

This table describes additional options available for use with an access control list but were not specifically tested for Common Criteria.

ACL Option	Description
precedence *precedence*	Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name: critical, flash, flash-override, immediate, internet, network, priority, or routine
tos *tos*	Packets can be filtered by type of service level, as specified by a number from 0 to 15, or by name: max-reliability, max-throughput, min-delay, min-monetary-cost or normal .
log	Causes an informational logging message about the packet that matches the entry to be generated.
log-input	Includes the input interface and source MAC address in the logging output.
time-range *time-range-name*	Name of the time range that applies to this statement.
icmp-type	ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name: administratively-prohibited, alternate-address, conversion-error, dod-host-prohibited, dod-net-prohibited, echo, echo-reply, general-parameter-problem, host-isolated, host-precedence-unreachable, host-redirect, host-tos-redirect, host-tos-unreachable, host-unknown, host-unreachable, information-reply, information-request, mask-reply, mask-request, mobile-redirect, net-redirect, net-tos-redirect, net-tos-unreachable, net-unreachable, network-unknown, no-room-for-option, option-missing, packet-too-big, parameter-problem, port-unreachable, precedence-unreachable, protocol-unreachable, reassembly-timeout, redirect, router-advertisement, router-solicitation, source-quench, source-route-failed, time-exceeded, timestamp-reply, timestamp-request, traceroute, ttl-exceeded, or unreachable

igmp-type	IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15 or names: dvmrp, host-query, host-report, pim and trace.
Operator	Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
Port	The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names are: **bgp**, chargen, daytime, discard, domain, drip, echo, finger, ftp, ftp-data, gopher, hostname, irc, klogin, kshell, lpd, nntp, pop2, pop3, smtp, sunrpc, syslog, tacacs-ds, talk, telnet, time, uucp, whois or www . UDP port names are: biff, bootpc, bootps, discard, dnsix, domain, echo, mobile-ip, nameserver, netbios-dgm, netbios-ns, non500-isakmp, ntp, rip, snmp, snmptrap, sunrpc, syslog, tacacs-ds, talk, tftp, time, who, or xdmcp
TCP Flags	Uses the **match-all** or **match-any** CLI options to specify specific TCP flags to filter on: ACK, FIN, PSH, RST, SYN, URG.
fragments	The access list entry applies to non-initial fragments of packets; the fragment is either permitted or denied accordingly.
Established	For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST control bits set. The non-matching case is that of the initial TCP datagram to form a connection.
ttl *value*	Uses the TTL value of packets arriving at or leaving an interface. Packets with any possible TTL values 0 through 255 may be permitted or denied..

Table 5: ACL Options Not Specifically Tested for Common Criteria

3.3 VLAN Management

The TOE controls the logical connections between combinations of internal Virtual Local AreaNetworks(VLANs) by rejecting packet flows (i.e. IP packets) that are not consistent with the VLAN information flow SFP.

VLAN.1 – VLAN Processing

Network interfaces are grouped into VLANs, so Layer 2 broadcast packets will be issued to only interfaces within that VLAN. Packets will have a VLAN ID associated to them indicating which VLAN they are allowed to access. The TOE will enforce VLAN separation by only allowing packets onto the VLAN that matches the VLAN ID. VLAN traffic will not be forwarded to interfaces not in that VLAN. The functionality provided by VLAN Processing is modeled in the VLAN Information Flow SFP.

On the Catalyst 6500 series switch or 7600 series router where a packet is routed at Layer 3 or undergoes IPSec processing by the VPNSM / IPSec VPN SPA, it may have its VLAN ID modified so that it can forwarded on to the appropriate network (and VLAN). This is the expected processing at Layer 3 and does not violate VLAN separation.

3.4 Configuration and Management

The TOE includes functions that allow the configuration and operation of the security functions of the TOE to be controlled and monitored. The TOE also supports the ability to maintain real time.

CONFIG.1 - System Messages

The TOE generates audit messages (system messages) that identify specific TOE operations – For each event, the TSF shall record the date and time of each event, the type of event, the subject identity, the affected subject identity and the outcome of the event. Audited events include; all configuration changes, successful or failed authentication attempts, information flow events, changes to system time, use of security management functions, modifications to role assignments, and startup and shutdown of audit functions. (FAU_GEN.1).

Logged messages for these events can be directed to a combination of an interactive management session, a buffer within the TOE or to an external system outside of the TOE using the SYSLOG protocol. Use of a SYSLOG server is not supported in the evaluated configuration. Logged messages are sent to the console or directed to an internal buffer in the evaluated configuration. Using the "**show logging**" command, the authorized user can review the audit messages stored in the buffer on the TOE and act upon them as required (FAU_SAR.1).

CONFIG.2 - Management Interfaces

The TOE can be configured, managed and operated using the command line interface (CLI) either via direct local connection to a physical console port, or remotely via an in-band network connection. No management interfaces other than that provided via the console port are available in the IOS default configuration. The remote management connection to the CLI via SSH must be explicitly enabled to be used and all other remote management connections that IOS is capable of using, such as telnet, are disallowed in the evaluated configuration. The management interface presented at the console port is always enabled. Access to the CLI requires valid authentication. SNMP, telnet, and XML management interfaces are not enabled in the evaluated configuration described in this ST.

The TOE maintains all IOS administrator and VPN Client user roles. The TOE can and shall be configured to authenticate both unprivileged (administrator role) and privileged access (privilege administrator role) to the command line interface using a username and password. The TOE shall be configured to require an access password, which provides unprivileged access (administrator role) and an enable password which provides privileged access (administrator role). Privileged access is defined by any privilege level entering an enable password after their individual login. The router restricts the ability to create, modify and delete user accounts to administrators. No router CLI functions are accessible to an unauthenticated user, with the exception of the authentication functions. Additionally unprivileged access restricts the administrator from accessing any CLI commands that modify the security configuration of the TOE.

The administrator has control over all TOE functions, attributes, and data, either by executing commands, viewing status and configuration, or editing the TOE configuration settings. The default configuration will be secure so that packet flows will not occur. The administrator has the right to change from the default to allow packet flows. Implementation of the various cryptographic standards and RFCs ensure that only appropriate secure values can be entered by the administrator for cryptographic functions.

The VPN Client user role is maintained by the CONFIG.2 function by maintaining the list of allowed remote users that can establish an IPSec connection.

The TOE will conduct self-tests upon startup to verify that it is operating correctly.

CONFIG.3 - Management of Time

The TOE maintains real time using a reliable software clock that interfaces to an internal hardware clock. The TOE restricts the ability to change the system time to an authorized administrator. Hardware clocks are not available in the 800 series of routers, in this situation the administrator is required to update the software clock in the event of power failure or system restart.

3.5 Key Management

To support the authentication of one TOE to another TOE or router / switch to VPN Client, the TOE supports the use of public key cryptography.

KEYMGT.1 - Key Management

The TOE generates secure RSA public/private keys (512 and 1024 bit key lengths) for use with a Public Key Infrastructure (PKI). The TOE interacts with a certificate authority using the Simple Certificate Enrollment Protocol (SCEP) to download a certificate authority's digital certificate and to request and download a digital certificate for the TOE itself. The TOE can destroy keys it creates by overwriting them. Implementation of the various cryptographic standards ensure that only appropriate secure values are used for the key management functions performed.

3.6 Remote Management

REMOTE.1 – Remote Management

The TOE implements Secure Shell (SSH) using 192 bit 3DES encryption for the purposes of remote management. The implementation of SSH provides an integrated single use mechanism in that the transport protocol provides a unique session identifier that is bound to the key exchange process. This is used by higher level protocols to bind data to a given session and prevent replay of data from prior sessions. See section 9.2.3 *Replay* of the SSH Protocol Architecture internetworking draft for more information on the SSH protocol (http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-21.txt). Implementation of the various cryptographic standards ensure that only appropriate secure values are used for the cryptographic functions performed.
Remote management via SSH provides full access to the CLI command set.

3.7 Self Protection

PROTECT.1 – Self Protection

To enforce the protection of the TOE configuration through the distinction and separation of information flows. All traffic arriving at a TOE interface is mediated by the TSF by the IPSec, VLAN, and Packet Filtering information flow policies. The TOE protects itself from interference and tampering by untrusted subjects by implementing authentication and access controls to limit configuration to authorized administrators. The TOE complies with IPSec protocol (RFCs 2401-2410) and is designed to work with other VPN peers implementing the functionality detailed in the SFs IPSEC.1 and IPSEC.2. For IPSec, the TOE-enabled router / switch functions only as responder. Initiators propose Security Associations (SAs); responders accept, reject, or make counter-proposals—all in accordance with configured SA parameters. The IPSec policy to allow the IPSec VPN tunnel requires the VPN peer to be successfully authenticated. The VPN peer must be installed and configured with authentication credentials and connection details necessary to authenticate to the router / switch. The VPN peer and TOE-enabled router / switch negotiate how to build the IPSec security association by first authenticating each other using the pre-shared keys or certificates (RSA or DSA). In addition, the TOE-enabled router / switch uses username/password to authenticate remote VPN clients (IKE extended authentication). Once the security associations are negotiated and the IPSec tunnel is successfully established, the TOE-enabled router / switch encrypts packets based on the crypto access list associated with the cryptographic map that was used to negotiate the security associations. The crypto access lists used for IPSec are used only to determine which traffic should be protected by IPSec, not which traffic should be blocked or permitted through the interface. Separate firewall access control lists define blocking and permitting at the interface as configured by the authorized administrator. The IOS is not a general purpose operating system and access to IOS memory space is restricted to only IOS functions. Additionally, IOS is the only software running on the TOE enabled routers/ switch.

4. Assumptions and Clarification of Scope

This section describes the security aspects of the environment in which the TOE is expected to operate.

4.1 Secure Usage Assumptions

The following assumptions are made in relation to the TOE:

Name	Description

A.NoEvil	As the security functions of the TOE can be compromised by an authorised administrator, administrators are assumed to be non-hostile and trusted to perform their duties correctly.
A.PhySec	As the security functions of the TOE can be compromised by an attacker with physical access to the internetworking device containing the TOE, it is assumed that the internetworking device containing the TOE is located in a physically secure environment.
A.Training	As the security functions of the TOE can be compromised due to errors or omissions in the administration of the security features of the TOE, it is assumed that administrators of the TOE have been trained to enable them to securely configure the TOE.
A.Trusted-CA	As the security functions of the TOE when configured to use digital certificates can be comprised if the Certificate Authority (CA) that issued the certificates is not operated in a trusted manner, it is assumed that if the TOE is configured to use digital certificates, the issuing CA is trusted or evaluated to at least the same level as the TOE.
A.PSK	Pre-shared keys are assumed to be securely communicated between disparate administrators.

4.2 Threats to Security

The Threat agents against the TOE are attackers with expertise, resources, and motivation that combine to be a low attack potential. The TOE addresses the following threats:

Name	Description
T.Attack	An attacker may gain access to the TOE and compromise its security functions by altering its configuration.
T.Untrusted-Path	An attacker may attempt to disclose, modify or insert data within packet flows transmitted/received by the TOE over an untrusted network. If such an attack was successful, then the confidentiality, integrity and authenticity of packet flows transmitted/received over an untrusted path would be compromised.
T.VLAN-Hopping	An attacker forces a packet destined for one VLAN to cross into another VLAN for which it is not authorized compromising the confidentiality and integrity of information.
T.Mediate	An attacker may send impermissible information through the TOE which results in the exploitation of resources on the protected network.

4.3 Other

The organisational security policy will:

a) Specify whether networks connected to the TOE are trusted or untrusted (including VLANs and subnets),
b) Define which packet flows are to be protected by the TOE, and
c) Associate each protected packet flow with a VPN peer that will decrypt/encrypt the flow. [P.Connectivity]

5. Architectural Information

The following table contains the hardware and software compliant with Common Criteria evaluated Cisco IOS/IPSec. Only these specific models, hardware acceleration modules, and IOS Releases may be used.

Model Family	Models	IPSec Hardware Acceleration Module	IOS Release	Additional Interface Cards or Modules
870	c871, c876, c877, c878	On board	12.4(11)T3	None
1800	c1801, c1802, c1803, c1811, c1812	On board	12.4(11)T3	None
1800	1841	On board or AIM-VPN/BPII-PLUS or AIM-VPN/SSL-1	12.4(11)T3	None
2800	2801	On board or AIM-VPN/EPII-PLUS or AIM-VPN/SSL-2	12.4(11)T3	None
	2811	On board or AIM-VPN/EPII-PLUS or AIM-VPN/SSL-2	12.4(11)T3	None
	2821	On board or AIM-VPN/EPII-PLUS or AIM-VPN/SSL-2	12.4(11)T3	None
	2851	On board or AIM-VPN/EPII-PLUS or AIM-VPN/SSL-2	12.4(11)T3	None
3800	3825	On board or AIM-VPN/EPII-PLUS or AIM-VPN/SSL-3	12.4(11)T3	None
	3845	On board or AIM-VPN/HPII-PLUS or AIM-VPN/SSL-3	12.4(11)T3	None

7200	7204VXR, 7206VXR	NPE-G1 and SA-VAM2 or SA-VAM2+	12.4(11)T3	None
		NPE-G2 and SA-VAM2, SA-VAM2+ or VSA		
7300	7301	SA-VAM2, SA-VAM2+	12.4(11)T3	None
		VSA		
6500	6503, 6506, 6509, 6513, all with Supervisor 720	• VPNSM • IPSec VPN SPA with SPA Carrier-400 (SSC-400)	12.2(18)SXF10	See section 5.1 below
7600	7603, 7606, 7609 and 7613, all with Supervisor 720	• VPNSM • IPSec VPN SPA with SPA Carrier-400 (SSC-400)		

870 Exclusions

The Cisco Systems 870 family of routers is a fixed configuration and does not provide any additional slots for interfaces.

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port, USB ports, and ISDN Dial Backup. There is no PC Card Slot or V.90 Analog modem on this family.

1800 (1801 – 1812) Exclusions

The Cisco Systems 1800 fixed configuration family of routers does not provide any additional slots for interfaces.

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port, USB ports, V.90 Analog Modem Dial Backup, and ISDN Dial Backup. There is no PC Card slot in this family.

1841 Exclusions

The Cisco Systems 1841 Router provides HWIC slots for additional interfaces. These slots may not be populated with any interfaces in the evaluated configuration. The AIM slot may only be populated with a AIM-VPN/BPII-PLUS or AIM-VPN/SSL-1.

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port and USB ports. There is no PC Card slot or V.90 analog modem in this Router.

2800 Exclusions

The Cisco Systems 2800 Family provides DSP, HWIC, and Network Module slots for additional interfaces. These slots may not be populated with any interfaces in the evaluated configuration. The AIM slots may only be populated with an AIM-VPN/EPII-PLUS or AIM-VPN/SSL-2.

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port and USB ports. There is no PC Card slot or V.90 analog modem in this family.

3800 Exclusions

The Cisco Systems 3800 Family provides PVDM, HWIC, and Network Module slots for additional interfaces. These slots may not be populated with any interfaces in the evaluated configuration. The AIM slots may only be populated with an AIM-VPN/EPII-PLUS or AIM-VPN/SSL-3.

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port and USB ports. There is no PC Card slot or V.90 analog modem in this family.

7200 / 7300 Exclusions

The Cisco Systems 7200 and 7300 Families provide Port Adapter slots for additional interfaces. These slots may not be populated with any interfaces in the evaluated configuration. The security module slots may only be populated with an SA-VAM2, SA-VAM2+, or VSA.

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port and USB ports. There is no PC Card slot or V.90 analog modem in these families.

6500 / 7600 Exclusions

The following physical ports are specifically excluded from use in the evaluated configuration: Auxiliary port. There is no V.90 analog modem, or USB ports contained within the Supervisor engine.

The following Cisco 6500 / 7600 Modules are specifically excluded from use in the evaluated configuration:

- Application Control Engine (ACE) Module ACE10-6500-K9
- Communication Media Module and associated Port Adapters WS-SVC-CMM=, WS-SVC-CMM-6E1=, WS-SVC-CMM-6T1=, WS-SVC-CMM-ACT=, WS-SVC-CMM-24FXS=
- Content Switching Module WS-X6066-SLB-APC=
- Content Switching Module with Secure Sockets Layer (SSL) WS-X6066-SLB-S-K9 =
- Firewall Services Module WS-SVC-FWM-1-K9=
- Intrusion Detection System (IDSM-2) Module WS-SVC-IDS2=
- Network Analysis Module (NAM -1/NAM -2) WS-SVC-NAM-1=, WS-SVC-NAM-2=
- Wireless Services Module (WiSM) WS-SVC-WISM-1-K9=
- Cisco 7600 Series Session Border Controller SBC
- Cisco 7600 Series / Catalyst 6500 Series WebVPN Services Module
- Cisco 7600 Series / Catalyst 6500 Series Anomaly Guard Module
- Cisco 7600 Series / Catalyst 6500 Series Traffic Anomaly Detector Module

5.1 Ethernet Interfaces in the Cisco 6500 or Cisco 7600

When the Cisco 6500 or Cisco 7600 platforms are used in the evaluated configuration, at least one Supervisor 720 is required and at least one Ethernet line card. The available options for Ethernet line cards are listed in the table below.

The 802.3af standard defines how power is delivered to 10BASE-T, 100BASE-T or 1000BASE-T attached devices and is not security relevant. It defines a physical mechanism to use wires contained within an Ethernet cable to carry DC current. When Power over Ethernet ports are being used signalling continues to occur at higher levels in the OSI model to pass data.

XENPAK, SFP and GBIC are all Ethernet transceiver technologies. These transceivers must be plugged into specific line cards identified in the table. The use of Ethernet transceivers is optional for the TOE.

Name / Description	Ethernet	802.3af	Transceiver	XENPAK, SFP, or GBIC Line Card
Cisco 2-Port Gigabit Ethernet Shared Port Adapter	X			
Cisco 5-Port Gigabit Ethernet Shared Port Adapter	X			
Cisco 10-Port Gigabit Ethernet Shared Port Adapter	X			
Cisco 1-Port 10-Gigabit Ethernet Shared Port Adapter	X			
Cisco 7600 Series 4-Port Gigabit Ethernet WAN + LAN OSM GE-WAN-2	X			
Cisco 7600 Series / Catalyst 6500 Series 4-Port 10 Gigabit Ethernet Module	X			
Cisco 7600 Series Ethernet Services 20 Gbps Line Card, 2-Port 10GE	X			
Cisco 7600 Series Ethernet Services 20 Gbps Line Card, 20-Port GE	X			
Cisco 7600 Series / Catalyst 6500 Series 10/100 & 10/100/1000 Ethernet Interface Modules	X			
Cisco 7600 Series / Catalyst 6500 Series 10 Gigabit Ethernet Interface Modules	X			
4-Port 10 Gigabit Ethernet WS-	X			

X6704-10GE				
8-port 10 Gigabit Ethernet WS-X6708-10G-3C WS-X6708-10G-3CXL	X			
48-Port Small Form-Factor Pluggable (SFP)-Based Gigabit Ethernet Module WS-X6748-SFP	X			X
Fabric-Enabled 24-Port SFP-Based Gigabit Ethernet Module WS-X6724-SFP	X			X
16-Port Gigabit Interface Converter (GBIC)-Based Gigabit Ethernet Module WS-X6516A-GBIC	X			X
8-Port GBIC-Based Gigabit Ethernet Module WS-X6408A-GBIC	X			X
48-Port 10/100/1000 Ethernet Module WS-X6748-GE-TX	X			
48-Port 10/100/1000 Ethernet Module WS-X6148A-GE-TX	X			
48-Port 10/100/1000 Ethernet Module with Power over Ethernet (PoE) 802.3af WS-X6148A-GE-45AF	X	X		
Fabric-Enabled 48-Port 10/100/1000 Ethernet Module WS-X6548-GE-TX	X			
Fabric-Enabled 48-Port 10/100/1000 Ethernet Module with PoE 802.3af WS-X6548-GE-45AF	X	X		
96-Port 10/100 Fast Ethernet RJ-45 Module (Upgradable to PoE 802.3af) WS-X6148X2-RJ-45 96-Port 10/100 Fast Ethernet RJ-45 Module with PoE 802.3af WS-X6148X2-45AF	X	X		
96-Port 10/100 Fast Ethernet RJ-21 Module (Upgradable to PoE 802.3af) WS-X6196-RJ21	X	X		
96-Port 10/100 Fast Ethernet RJ-21 Module with PoE 802.3af WS-X6196-21AF	X	X		
48-Port 10/100 Fast Ethernet RJ-45 Module (Upgradable to PoE 802.3af) WS-X6148A-RJ-45	X	X		
48-Port 10/100 Fast Ethernet RJ-45 Module with PoE 802.3af WS-	X	X		

X6148A-45AF				
48-Port 10/100 Fast Ethernet RJ-21 Module (Upgradable to PoE 802.3af) WS-X6148-RJ21	X	X		
48-Port 10/100 Fast Ethernet RJ-21 Module with PoE 802.3af WS-X6148-21AF	X	X		
48-Port 100 BASE-X (SFP) WS-X6148-FE-SFP	X	X		
XENPAK (10 Gigabit) WS-XENPAK-LR, WS-XENPAK-ER, WS-XENPAK-SR, WS-XENPAK-CX4, WS-XENPAK-LX4, WS-XENPAK-ZR, DWDM-XENPAK, WDM-XENPAK-REC	X		X	
SFP (Gigabit) GLC-SX-MM, GLC-LH-SM, GLC-ZX-SM, GLC-T, GLC-BX-D, GLC-BX-U	X		X	
GBIC (Gigabit) WS-G5483, WS-G5484, WS-G5486, WS-G5487	X		X	
CWDM GBIC (Gigabit) CWDM-GBIC-1470, CWDM-GBIC-1490, CWDM-GBIC-1510, CWDM-GBIC-1530, CWDM-GBIC-1550, CWDM-GBIC-1570, CWDM-GBIC-1590	X		X	
DWDM GBIC (Gigabit) DWDM-GBIC	X		X	
SFP (Fast Ethernet) GLC-FE-100FX, GLC-FE-100LX, GLC-FE-100BX-U, GLC-FE-100BX-D	X		X	

Table 6: Ethernet Interfaces in the Cisco 6500 or Cisco 7600

5.2 Cryptography Compliance

Note that although several TOE components are FIPS validated cryptographic modules, the software running on those FIPS validated cryptographic modules is not one of the specific software code versions for this evaluated configuration. The TOE for this evaluation does not formally claim to have FIPS validated TOE components within the TOE boundary. The cryptography used in the TOE has been FIPS certified as indicated in the table below.

TOE Model	TOE IPSEC Hardware Acceleration Module	FIPS Cert #	Pending Certification
c871	On Board	707	
c876	On Board	707	
c877	On Board	707	

c878	On Board	707	
c1801	On Board	702	
c1802	On Board	702	
c1803	On Board	702	
c1811	On Board	702	
c1812	On Board	702	
1841	On Board	616	
	AIM-VPN/BPII-PLUS	620	
	AIM-VPN/SSL-1		Yes
2801	On Board	616	
	AIM-VPN/EPII-PLUS	620	
	AIM-VPN/SSL-2		Yes
2811	On Board	612	
	AIM-VPN/EPII-PLUS	617	
	AIM-VPN/SSL-2		Yes
2821	On Board	612	
	AIM-VPN/EPII-PLUS	617	
	AIM-VPN/SSL-2		Yes
2851	On Board	613	
	AIM-VPN/EPII-PLUS	619	
	AIM-VPN/SSL-2		Yes
3825	On Board	596	
	AIM-VPN/EPII-PLUS	618	
	AIM-VPN/SSL-3		Yes
3845	On Board	596	
	AIM-VPN/HPII-PLUS	618	
	AIM-VPN/SSL-3		Yes
7204VXR NPE-G1	SA-VAM2		
	SA-VAM2+		
7206VXR NPE-G1	SA-VAM2	428	
	SA-VAM2+	877	
7204VXR NPE-G2	SA-VAM2		
	SA-VAM2+		
	VSA		
7206VXR NPE-G2	SA-VAM2		
	SA-VAM2+	877	
	VSA	877	
7301	SA-VAM2		
	SA-VAM2+	877	
	VSA		
6503 /w Sup 720	VPNSM		
	IPSec VPN SPA		
6506 /w Sup 720	VPNSM		
	IPSec VPN SPA	658	
6509 /w Sup 720	VPNSM	429	
	IPSec VPN SPA	658	
6513 /w Sup 720	VPNSM		
	IPSec VPN SPA		

7603 /w Sup 720	VPNSM		
	IPSec VPN SPA		
7606 /w Sup 720	VPNSM	429	
	IPSec VPN SPA	658	
7609 /w Sup 720	VPNSM	429	
	IPSec VPN SPA	658	
7613 /w Sup 720	VPNSM		
	IPSec VPN SPA		

Table 7: TOE - FIPS Conformance

6. Documentation

Specific to IOS 12.4(11)T3:

- *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4T* (http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_book09186a008072adae.html)
- *Cisco IOS Network Management Configuration Guide, Release 12.4T* (http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tnm_c/index.htm)
- *Cisco IOS Configuration Fundamentals Command Reference, Release 12.4T http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcr/tcf_r/index.htm*
- *Cisco IOS Security Configuration Guide, Release 12.4T* (http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_book09186a008049e249.html)
- *Cisco IOS Security Command Reference*, Release 12.4T (http://www.cisco.com/en/US/products/ps6441/products_command_reference_book09186a0080497056.html)
- *Cisco IOS IP Application Services Configuration Guide, Release 12.4T http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_book09186a0080773e84.html*
- *Cisco IOS IP Routing Protocols Command Reference, Release 12.4T http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcr/tirp_r/index.htm*
- *Cisco IOS Software System Messages, Release 12.4 http://www.cisco.com/en/US/products/ps6350/products_system_message_guide_book09186a008043c0bf.html*
- *Cross-Platform Release Notes Cisco IOS Release 12.4T* (http://www.cisco.com/en/US/products/ps6441/prod_release_notes_list.html)
- *Cross-Platform Release Notes for Cisco IOS Release 12.4T,Caveats http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124relnt/xprn124t/index.htm*
- *Cisco IOS LAN Switching Configuration Guide Release 12.4T http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tlsw_c/index.htm*
- *Cisco IOS LAN Switching Command Reference 12.4T http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcr/tlsw_r/index.htm*
- *IOS Interface and Hardware Component Configuration Guide, Release 12.4T http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tif_c/index.htm*
- Hardware Installation Guides for each router platform (Table 4)
- Regulatory Compliance and Safety Information specific to each router platform (Table 2)
- *Cisco IOS Software Release Notes 12.4T* (http://www.cisco.com/en/US/products/ps6441/prod_release_notes_list.html)

Specific to IOS 12.2(18)SXF8:

- *Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2* (http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a00801c8339.html)
- *Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.2SX* (http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a00801d4269.html)
- *Cisco 7600 Series Cisco IOS Command Reference, 12.2SX* (http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/122sx/cmdref/index.htm)
- *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* (http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/index.htm)
- *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* (http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/index.htm)
- *Cisco IOS Security Command Reference, Release 12.2* (http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/index.htm)
- *Cisco IOS Security Configuration Guide, Release 12.2* (http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080087df1.html)

7. IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. The cryptography used in this product was not analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

7.1 Developer Testing

The developer performed a testing and coverage analysis, which examined each SFR and developed one or more Cisco test cases that verify the function or command requirement. These tests were documented in the EAL4 Detailed Test Plan. The scope of the developer tests included all TOE Security Functions.

The developer testing addresses the following security functionality claimed by the TOE: acls, IPSec, logging, ability of administrators to carry out management functions.

The following hardware equivalence rationale addresses various TOE components and establishes what equivalent hardware is present in the test configuration and why that hardware subset is sufficient.

Group	Hardware Crypto Acceleration	Models	IOS version	Tested by Arca	Tested by Cisco
A	On-board only.	c87x, c18xx	12.4(11)T3	C871	C870
B	On-board or with optional module.	1841, 28xx, 38xx	12.4(11)T3	2851 with no accelerator	2811, 2821, and 3845 with no accelerator, and 2851 with AIM-VPN/EPII-PLUS,
C	Module-based only.	72xx and 7301	12.4(11)T3	7206VXR with NPE-G2 and VSA	7206VXR with VAM2, and 7301 with VAM2+
D	Module-based only.	76xx, and 65xx	12.2(18)SXF10	7606 with SPA	6506 with SPA, 7609 with SPA, and 6503 with VPNSM

The developer used an existing test suite to test the IPSec component of the product.

The evaluation team determined that the developer's test methodology met the coverage and depth requirements and that the actual test results matched the expected results.

7.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team also ensured that all subsystem interfaces were tested by the developer.

The evaluation team performed a sample of the developer's test suite and devised an independent set of team tests and penetration tests. The evaluation team reran a subset of the developer's test suite that tested all of eight of the TSF's.

The evaluation team also performed a penetration flaw hypothesis analysis of the product to prepare for a penetration testing effort. The analysis examined each SFR line by line to determine whether it was possible that the evaluated configuration could be susceptible to a vulnerability. The specific penetration tests executed include the following:

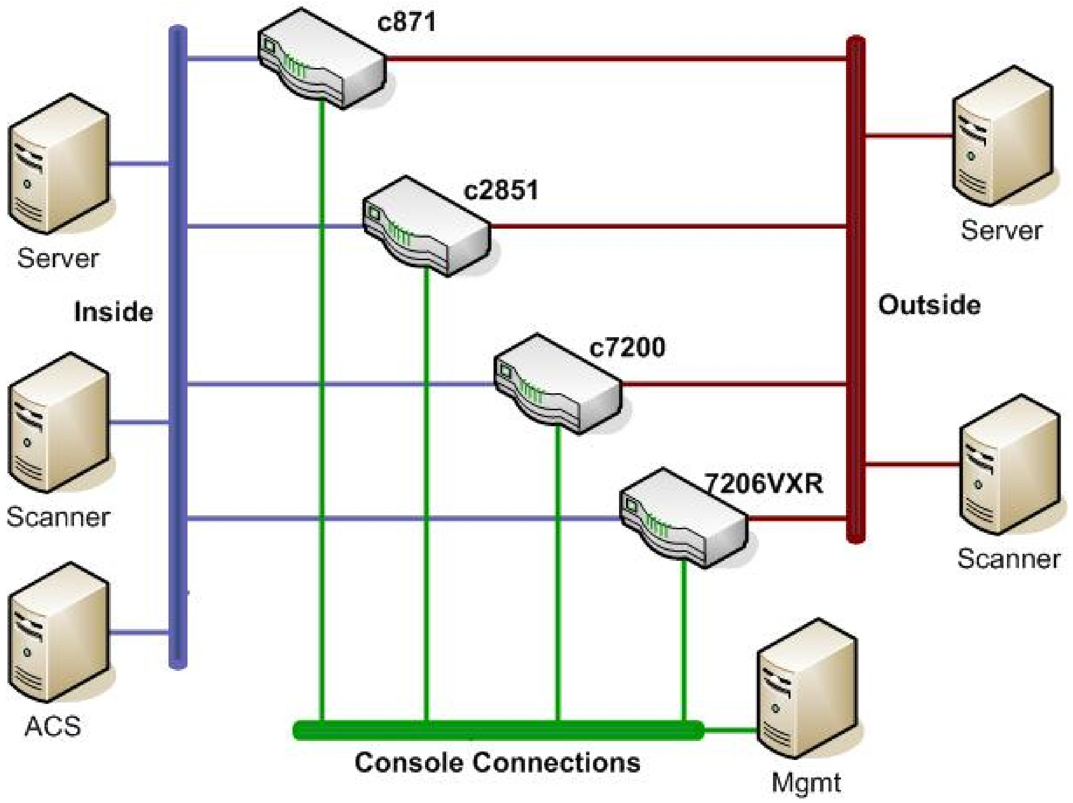
- Use a port scanner to check for open ports on the firewall unmanaged by a rule using Nessus..
- Test the different privilege levels and granting command access to the different levels.
- Determine whether mis-configuration of the TOE would allow traffic to pass through IOS from one VLAN to another without routing inspection (VLAN hopping).
- Test potential abuse privilege levels using the "autocommand" command.
- Test potential misuse of the "kron" command to run commands as another user.

The evaluation team constructed and ran each of the identified tests. The results of the penetration test execution verified that none of the hypothesized flaws was exploitable.

8.Evaluated Configuration

The evaluated configuration was tested in the configuration identified in Figure 1, below. The evaluation results are valid for all configurations of the TOE identified in section 5 of this report.

Figure 1: Testing Environment



Component	Description
Cisco 2851	Cisco 2851 running IOS version 12.4(11)T3
Cisco 871	Cisco 871 running IOS version 12.4(11)T3
Cisco 7200	Cisco 7200 running IOS version 12.4(11)T3
Cisco 7606	Cisco 7606 running IOS version 12.2(18)SXF10

9. Results of the Evaluation

The Cisco IOS-IPSec satisfies all of the EAL4 assurance requirements against which it was evaluated. The Security Target provides a detailed description of how Cisco IPSec meets each of the listed components.

10. List of Acronyms

ACL	Access Control List
API	Application Programming Interface
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US CC Validation Scheme)
CCIMB	Common Criteria Implementation Board
CCTL	Common Criteria Testing laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CMS	Certificate Management System
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
EOBC	Ethernet Out-of-Band Channel
ETR	Evaluation Technical Report
FW	Firewall
FIPS	Federal Information Processing Standard
ID	Identifier
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PC	Personal Computer
PD	Precedent Database
PFSS	PIX Firewall Syslog Server
RFC	Request for Comment
SAR	Security Functional Requirement
SFR	Security Assurance Requirement
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security

TOE	Target Of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VR	Validation Report

11. Validation Comments/Recommendations

Note that although several TOE components are FIPS validated cryptographic modules, the software running on those FIPS validated cryptographic modules is not one of the specific software code versions for this evaluated configuration. The TOE for this evaluation does not formally claim to have FIPS validated TOE components within the TOE boundary.