Security Target for Cisco IOS IPSEC on the Integrated Services Routers, VPN Services Module (VPNSM), and IPSec VPN Shared Port Adapter (SPA), Including VLAN Separation

Reference: ST
May 2008
Version: 1.0

Table of Contents

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

Conventions

The notation, formatting and conventions used in this Security Target are consistent with those used in Version 2.2 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the Security Target reader. The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment* and *iteration* are defined in Section 2.1.4 of Part 2 of the CC.

- Refinements are indicated by **bold** text and ~~strikethrough~~
- Selections are enclosed in [square brackets]
- Assignments are enclosed in [square brackets and underlined]
- Iterations are numbered in sequence as appropriate.

Terminology

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. A subset of those definitions is included in the list below with supplemental definitions that are exclusive to Cisco products. They are listed here to aid the reader of the Security Target.

Acronym	Expansion or Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function

Acronym	Expansion or Definition
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
TTP	Trusted Third Party

The following terminology specific to the TOE and its environment is also provided to aid the user of the Security Target.

Word	Definition
Assets	Data transmitted over a network
AH	Authentication Header, a security protocol that provides authentication. AH is embedded in the data to be protected (a full datagram).
Crypto access control list	Crypto access control lists are used to define which IP traffic is protected by crypto and which traffic is not protected by crypto. (These access lists are *not* the same as regular access control lists (ACL), which determine what traffic to forward or block at an interface.)
DMVPN	Dynamic Multipoint VPN. The DMVPN feature combines generic routing encapsulation (GRE) tunnels, IPSec encryption, and next hop resolution protocol (NHRP) routing to provide administrators an ease of configuration via crypto profiles, which override the requirement for defining static crypto maps, and dynamic discovery of tunnel endpoints.
End System	A client or server system with an IP address
ESP	Encapsulating Security Payload. A security protocol that provides data confidentiality services and optional authentication and replay-detection services. ESP encapsulates the data to be protected.
Extranet	The interconnection of two or more intranets interconnected with an untrusted network using internetworking devices compliant with the TOE to protect packet flows between the intranets.
IKE	Internet Key Exchange, which negotiates the security association between two entities and exchanges key material
Internetworking Device	A device that interconnects two or more network segments and forwards IP traffic between the end systems connected to the attached network segments (e.g.. a router or firewall).
Intranet	An organization's internal network, constructed from trusted networks (typically LAN's) interconnected with untrusted networks or network segments using internetworking devices

Word	Definition
MD5	Message Digest 5, a one-way hash that combines a shared secret and the message (the header and payload), to produce a 128-bit value. The recipient of the message runs the same hash of the message and compares it with the inserted hash value to yield the same result, indicating that nothing in the packet has been changed in transit.
Network	A single network segment or two or more network segments interconnected by internetworking devices
Network Segment	A single physical segment to which end systems are connected
Packet Flow	A unicast flow of IP packets identified by some combination of source/destination IP address, source/destination TCP/UDP port number, TOS field and input interface
SA	Security Association
SHA-1	Secure Hash Algorithm 1, similar to MD5, but produces a 160-bit hash value. Takes longer to calculate than MD5, but provides less chance of collision.
SPA	Shared Port Adapter
Replay Attack	An attempt by an eavesdropper to capture some portion of a transmission and retransmit it at a later time to gain authorized access to the receiver or to spoof the security functions of the receiver.
User	A human that interacts with the TOE to configure and operate the TOE, i.e. an administrator. End users (clients) do not interact with the TOE.
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

The following abbreviations are used when referring to Cisco routers.

Acronym	Expansion or Definition
AIM	Advanced Interface Module (an internal plug-in hardware accelerator)
E	Ethernet
PA	Port Adapter (a large, high performance, modular network interface)
VAM	VPN Accelerator Module (a hardware accelerator in port adapter format)
WIC	WAN Interface Card (a small modular network interface for Wide Area Networks)

Introduction

Identification

Title	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
Authors	Cisco Systems, Inc.
Last Updated	May 2008
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005. No NIAP or CCIMB interpretations are applicable to the ST as of August 8, 2005. This ST uses the CCEVS Precedents PD-0108 to correctly specify remote administration.
Keywords:	IPSec, VLAN

TOE Software Identification: The following Cisco IOS releases:

Cisco IOS 12.4(11)T3

Cisco IOS 12.2(18)SXF10

TOE Hardware Identification: The following hardware platforms and IPSec Hardware Acceleration Modules are included in the evaluated configuration:

- Cisco 870 Series Integrated Services Routers
- Cisco 1800 Series Integrated Services Routers (with optional AIM-VPN/EPII-PLUS or AIM-VPN/SSL-1)
- Cisco 2800 Series Integrated Services Routers (with optional AIM-VPN/EPII-PLUS or AIM-VPN/SSL-2)
- Cisco 3800 Series Integrated Services Routers (with optional AIM-VPN/EPII-PLUS or AIM-VPN/SSL-3)
- Cisco 7204VXR and 7206VXR Routers with NPE-G1 and (SA-VAM2 or SA-VAM2+)
- Cisco 7204VXR and 7206VXR Routers with NPE-G2 and (SA-VAM2, SA-VAM2+ or VSA)
- Cisco 7301 Router with SA-VAM2, SA-VAM2+ or VSA
- Cisco Catalyst 6500 Series Switches with VPNSM or IPSEC VPN SPA
- Cisco 7600 Series Routers with VPNSM or IPSEC VPN SPA

Security Target Overview

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 Cisco 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.

Hardware encryption acceleration modules are installed in slots within the 1800, 2800, 3800, 7200 and 7300 series routers. The VPN Service Module / IPSec VPN SPA are installed in a single slot on either the Cisco Catalyst 6500 series switches or Cisco 7600 series routers.

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, Cisco Catalyst switches, VPN clients (within the IT Environment), VPNSM and IPSec VPN SPA.

Virtual Local Area Networks (VLANs) group network devices together based on logical instead of physical connections. The VLAN functionality is configured using IOS Software and creates separate logical networks.

Configuring VPNs using the VPNSM or IPSec VPN SPA is similar to configuring VPNs on routers. When you configure VPNs with the VPNSM or IPSec VPN SPA on the Cisco Catalyst 6500 series switches or Cisco 7600 series routers, you attach crypto maps to VLANs (using interface VLANs); when you configure VPNs on routers running Cisco IOS software, you configure individual interfaces.

The TOE implements the following security functions: IPSEC, Packet Filtering, VLAN Management, Configuration and Management and Key Management.

CC Conformance Claim

The TOE conforms to the following parts of the CC (Version 2.3):

- Part 2 extended; and
- Part 3 EAL 4 augmented with ALC_FLR.1.

TOE Description

This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

Product Type

The TOE consists of hardware and software used to form Virtual Private Networks. The TOE is Cisco IOS 12.4(11)T3 executing on Cisco 870, 1800, 2800, and 3800 Integrated Services Routers, Cisco 7204VXR, 7206VXR, and 7301 and Cisco IOS 12.2(18)SXF10 executing on Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers. IPSec hardware modules (i.e., AIM-VPN/BPII-PLUS, VPNSM, and IPSec VPN SPA) are used to accelerate the performance of the IPSec protocol. The TOE is all inclusive of the routers and switches. No portion of the physical boundary of the included routers or switches is considered outside the scope of the TOE. The VPN peers for which the TOE is used to establish and maintain a VPN connection is considered part of the IT Environment. From hereon the TOE is referred to as the TOE, router, or router/ switch.

The routers are standalone with physical Ethernet and serial interfaces used to provide many different network interconnections. The routers receive power from their own power supply, and are standalone, self-supporting units. The routers are a board with CPU and memory enclosed within a chassis. The routers support the inclusion of a hardware cryptographic acceleration board which contributes to higher performance for IPSec.

On the Cisco Catalyst 6500 series switches or 7600 series routers, the VPNSM and IPSec VPN SPA do not have any physical network interfaces. They are housed within one of the host devices (6500 or 7600) and provide virtual interfaces (via interface VLANs) for communication. Both the VPNSM and the IPSec VPN SPA consist of a board with CPU and memory enclosed within the bigger 6500 or 7600 chassis. They both receive power from the host chassis.

Routers

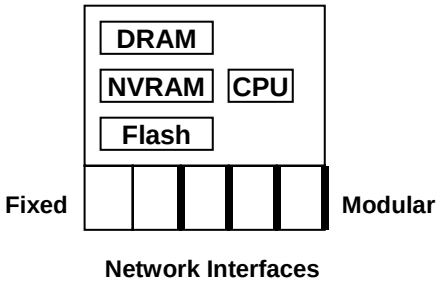
Routers forward packets from one network segment to another based on network layer information (e.g.. IP address). Interconnected routers will exchange information to determine the optimal path along which network traffic should be forwarded. The primary function of a router is to provide connectivity between networks of end systems. Routers filter packets to permit or deny packet flows.

The routers use a common operating system called Cisco IOS. Cisco IOS software is distributed using feature sets (IP Base, Enterprise, Advanced Security). The IOS software includes the necessary feature set for IPSec. The TOE-compliant software versions are identified in the "Identification " section on page 6.

Routers that support the TOE have a number of common hardware characteristics.

- Central processor that supports all system operations, e.g.. Intel Pentium, PowerPC, MIPS
- Dynamic memory, used by the central processor for all system operations
- Flash memory, used to store the operating system image
- Non-volatile memory, which stores configuration parameters used to initialize the system at system startup
- Multiple physical network interfaces (minimally two). Some models will have a fixed number and/or type of interfaces; some models will have slots that accept additional network interfaces.

Figure 1 Common Hardware Components of a Cisco Router



The basic operation of a router is as follows:

1. At system start-up the operating system is transferred from flash memory to dynamic memory using a built-in hardware bootstrap (some models execute the operating systems directly from flash memory).
2. The operating system reads the configuration parameters from non-volatile memory, builds the necessary data structures in dynamic memory and commences operation.
3. IP packets are forwarded to the router over one or more of it's physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the router. This processing typically results in the IP packets being forwarded out of the router over another interface, or dropped in accordance with a configured policy.

When you configure a VPN on the Cisco routers, a packet is sent to a routed interface that is associated with an IP address. If the interface has an attached crypto map, the software checks that the packet is on a crypto access control list that is specified by the crypto map. If a match occurs, the packet is transformed (encrypted) before it is routed to the appropriate IPSec peer; otherwise, the packet is routed in the clear (unencrypted) state.

VPNSM / IPSec VPN SPA

The TOE comprises the Cisco Catalyst 6500 series switches and Cisco 7600 series routers running Cisco IOS with the VPN Service Module (VPNSM) or IPSec VPN SPA installed. Although termed switches and routers, both platforms are identical in terms of functionality as they both run the same image of IOS. Both platforms support layer 2 switching and layer 3 routing, a capability which can be configured on a per port basis. Both platforms support multiple physical interfaces (typically Local Area Network (LAN) interfaces, but other interface types are supported) and multiple logical interfaces (or Virtual LANS).

In the context of the TOE the Cisco 6500 / 7600 chassis runs IOS under the control of the Supervisor 720. The supervisor 720 Engine is responsible for the configuration of Access Control Lists (ACLs), VLANs and crypto maps which are associated to the network interfaces. Neither the VPN Service Module (VPNSM) or IPSec VPN SPA has physical external network interfaces and its internal interfaces must be associated to an “inside” and “outside” VLAN. The supervisor identifies VLAN traffic flows and sends appropriate VLAN packets to the VPNSM or IPSec VPN SPA which performs hardware accelerated IPSec processing on VPN traffic destined for a particular VLAN. The Supervisor 720 software has the responsibility of ensuring VLAN separation is maintained at all times.

In order for the TOE to perform IPSec processing the VPN Service Module (VPNSM) and IPSec VPN SPA must be placed in the path of VPN Traffic. Once either module is installed into the 6500 / 7600 chassis it will view the 6500 / 7600 interfaces and ports as either the inside network (local LAN) or the outside network (outside world). The VPN Service module and IPSec VPN SPA do not contain any external physical ports but have two logical ports that connect the module to the backplane of the chassis. One logical port is assigned as a VPN inside port and the other a VPN outside port. The VPN inside port is used to transfer data to and from the 6500 / 7600 inside ports and the VPN outside port is used to transfer data to and from the 6500 / 7600 outside ports.

Scope and Boundaries

Physical

The routers and switches included within the TOE have two or more network interfaces. When the TOE is in use, at least one of the network interfaces of the internetworking device will be attached to a trusted network, and at least one other interface will be attached to an untrusted network. The TOE configuration will determine how packet flows received on one interface will be transmitted on another. Packet flows that are protected by the IPSec security function of the TOE are received on a trusted network interface and encrypted using IPSec before being transmitted out an untrusted interface.

The contents of Table 1 and Appendix C constitute the TOE physical boundary. Table 1 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.

Table 1 Physical Hardware and Software Included in the Target of Evaluation

Model Family	Models	IPSec Hardware Acceleration Module	Cisco 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-2	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	12.4(11)T3	None
7300	7301	SA-VAM2, SA-VAM2+	12.4(11)T3	None
		VSA	12.4(11)T3	None
6500	6503, 6506, 6509, 6513, all with Supervisor 720	VPNSM or IPSec VPN SPA	12.2(18)SXF10	See Appendix C
7600	7603, 7606, 7609 and 7613, all with Supervisor 720	VPNSM or IPSec VPN SPA	12.2(18)SXF10	See Appendix C

Note 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.

IPSec Hardware Acceleration components offload much of the processor intensive aspects of cryptography, such as encryption, key generation, and compression. All of the devices in the TOE can operate in hardware accelerated mode or software only mode for encryption.

An instance of a TOE also supports remote access clients by supporting VPN connections with VPN clients. When active, the VPN Client helps to provide confidentiality, authenticity, and integrity for traffic transmitted over the untrusted network to the router or switch by its proper implementation of the IPSec policy negotiated with the TOE.

The Cisco IOS contains a collection of features that build on the core components of the system. The following are Cisco IOS features included in the evaluated configuration:

- Advanced Encryption Standard (AES)
- Firewall
- Internet Key Exchange (IKE)
- IPSec
- SSH v2
- VPN
- VLAN
- RIPv2 and OSPF

There are Cisco IOS features that are excluded from the evaluated configuration. These features are disabled. These features are listed below:

- HTTP Server
- EasyVPN
- IEEE 802.11 Wireless Standards
- L2TP
- MPLS
- SNMP
- Syslog
- Telnet
- SSL VPN
- BGP, EIGRP, IGRP, CSPF, and IS-IS

Logical

IPSec

IPSec is an Internet standard developed by the IETF and described in RFCs 2401-2404, 2406-2409 and 2451. It provides network data encryption at the IP packet level to guarantee the confidentiality, authenticity and integrity of IP packets. IPSec only supports IP packets - other network protocols must be encapsulated within IP to be encrypted with IPSec.

Individual IP packets encrypted with IPSec can be detected during transmission, but the IP packet contents (payload) cannot be read. IPSec encrypted packets are forwarded through an IP network in exactly the same manner as normal IP packets, allowing IPSec encrypted packets to be transported across networks and internetworking devices that do not participate in IPSec.

The actual encryption and decryption of IP packets therefore occurs only at devices that are capable of and configured for, IPSec. When an IP packet is transmitted or received by an IPSec-enabled device, it is encrypted or decrypted only if the packet meets criteria defined by the administrator. These criteria are typically described in the form of crypto access control lists.

Internetworking devices such as switches and routers are used to connect networks together to form larger networks. They are therefore logical places in which to implement IPSec to provide confidentiality, authenticity and integrity for packet flows passing from one network to another.

The TOE supports the following IPSec options:

Function	Operation
Authentication between TOE and VPN Peer	IPSec Internet Key Exchange (IKE) with • Pre-Shared Keys, or • Digital Certificates
Confidentiality of Packet Flows	IPSec Encapsulating Security Payload (ESP) with • Triple DES, or • AES Using IPSec Tunnel or Transport Mode
Integrity and Authenticity of Packet Flows	IPSec Encapsulating Security Payload (ESP) with • HMAC Keyed Hash Algorithm, using • SHA-1, or • MD-5 Using IPSec Tunnel or Transport Mode

A more detailed description of the operation of IPSec (based on the standards) can be found in the "Appendix A - IPSec Operation" section on page 59.

Packet Filtering

To enable the TOE to be "self defending" the inbound filtering functions of the IOS operating system are included. This allows (for example) IP packets that are not IPSec to be ignored by the TOE, which is particularly important as the TOE will typically operate with one interface facing a public network.

TOE internetworking devices are deployed at the edges of untrusted networks (such as the Internet) to provide controlled communications between two networks that are physically separated. When a packet flow reaches the TOE stateful packet filtering is applied to the traffic before forwarding it into the remote network. Packet flows arriving at a network interface of the TOE are checked to ensure that they conform with the configured packet filter policy, this may include checking attributes such as the presumed source or destination IP address, the protocol used, the network interface the packet flow was received on, and source or destination UDP/TCP port numbers. Packet flows not matching the configured packet filter policy are dropped.

VLAN Separation

VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical local-area network (LAN) infrastructure into different subnets so that VLAN packets are presented to interfaces within the same VLAN.

The most important requirement of VLANs is the ability to identify which packets belong to which VLANs to ensure packets can only travel to interfaces for which they are authorized.

The VPNSM and IPSec VPN SPA on the Cisco Catalyst 6500 series switches and Cisco 7600 series routers require VLANs to function. When the administrator configures VPNs with the VPNSM or IPSec VPN SPA they attach crypto maps to VLANs (using interface VLANs). The other routers included in the TOE provide the capability to utilize VLANs but are not dependent on them for operation.

Administration

Configuration, management and operation are performed directly from the operating system (IOS) running on the router or switch, using the console and SSH. To ensure that only the authorized administrator can gain secure access to the TOE over a network, the security target specifies that remote management be conducted using SSH or over an IPSec connections to the remote routers.

TOE Security Environment

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any assumptions about the security aspects of the environment and/or of the manner for which the TOE is intended.
- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.

Secure Usage Assumptions

The following assumptions are made in relation to the TOE:

Table 2 Secure Usage Assumptions

Name	Description
A.NoEvil	As the security functions of the TOE can be compromised by an authorized 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. This trusted CA must support 3DES for encryption.
A.PSK	Pre-shared keys are assumed to be securely communicated between disparate administrators.

Threats to Security

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

Threats Addressed by the TOE

The TOE addresses the following threats:

Table 3 Threats Addressed by the TOE

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.

Table 3 Threats Addressed by the TOE

Name	Description
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.

Organizational Security Policies

The following table describes the organizational security policies relevant to the operation of the TOE.

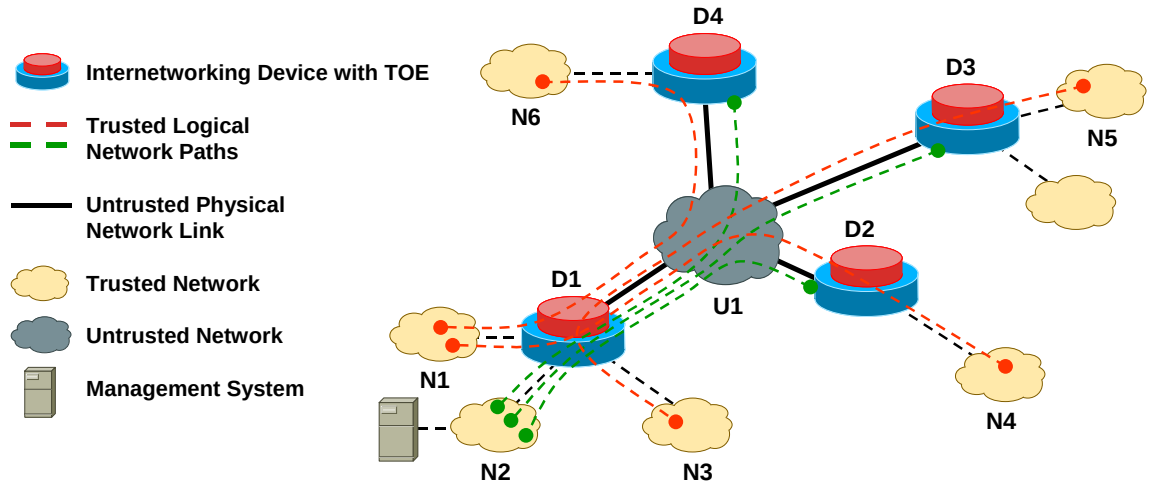
Table 4 Organizational Security Policies

Name	Description
P.Connectivity	The organizational 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.

The organizational security policy, P.Connectivity, is required because it determines how packet flows between trusted networks can be transmitted over an untrusted network. Each instance of the TOE implements a portion of P.Connectivity, which must be matched to, and consistent with, other VPN peers for the TOE security functions to be effective.

For example, in Figure 2, an instance of the TOE, D1, has three trusted networks attached to it (N1, N2, N3).

Figure 2 Organizational Security Policy Example



This example implements the following policy for three trusted network to network packet flows (red) and three secure management packet flows (green) that cross the untrusted network (U1):

Source	Destination	Peer TOE
N1	N6	D4
N1	N5	D3
N3	N4	D2
N2	D2	D2
N2	D3	D3
N2	D4	D4

Notice that in this example, flows are identified solely by the source and destination addresses of IP packets within the flow. As the TOE D1 transmits a packet flow into the untrusted network it encrypts only that traffic which matches the encryption policy, using an encryption key that has been negotiated with the matching peer. Each VPN peer of D1 must have a matching policy implemented to successfully encrypt/decrypt any flow in accordance with P.Connectivity.

The above example demonstrates a single untrusted network interface for each router. Each instance of the TOE is not limited to one untrusted interface and multiple trusted interfaces. The designation of trusted versus untrusted interfaces is specific to the security policy of the organization.

Security Objectives

The security objectives are a high-level statement of the intended response to the security problem. These objectives indicate how the security problem, as characterized in the "TOE Security Environment" section on page 13, is to be addressed.

Security Objectives for the TOE

Table 5 describes security objectives for the TOE.

Table 5 Security Objectives for the TOE

Name	Description
O.Authenticity	The TOE must provide the means for ensuring that a packet flow has been received from a trusted source.
O.Confidentiality	The TOE must protect the confidentiality of packet flows transmitted to/from the TOE over an untrusted network.
O.Integrity	The TOE must ensure that any attempt to corrupt or modify a packet flow transmitted to/from the TOE is detected.
O.Key-Confidentiality	The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt packet flows between instances of the TOE and when kept in short and long-term storage.
O.NoReplay	The TOE must provide a means to detect that a packet flow transmitted to the TOE has not been copied by an eavesdropper and retransmitted to the TOE.
O.Secure-Operation	The TOE must prevent unauthorized changes to its configuration.

Table 5 Security Objectives for the TOE

Name	Description
O.VLAN-Separation	The TOE must provide a means for the logical separation of Virtual LANs to ensure that packets flows are restricted to their authorized Virtual LANs ensuring VLAN separation is achieved.
O.Mediate	The TOE must mediate the flow of all information transmitted to the TOE over an untrusted network.

Security Objectives for the Environment

Table 6 describes objectives for the environment.

Table 6 Security Objectives for the Environment

Name	Description
OE.Policy	Those responsible for the administration of the TOE must provide a policy that specifies **a)** Whether networks connected to the TOE are trusted or untrusted **b)** The packet flows that are to be protected by the TOE, and **c)** The VPN peer that will encrypt/decrypt each packet flow.
OE.Secure-Management	Those responsible for the operation of the TOE must ensure that the TOE environment is physically secure, and management and configuration of the security functions of the TOE are: **a)** Initiated from a management station connected to a trusted network and protected using the security functions of the TOE **b)** Undertaken by trusted staff trained in the secure operation of the TOE **c)** Implemented in conjunction with an evaluated or trusted Certificate Authority (CA), if digital certificates are used for TOE authentication **d)** Configured to interface only to trusted authentication servers. **e)** VLANs are configured and created correctly. **f)** Pre-shared Keys used for configuration in cryptographic maps are securely distributed amongst disparate administrators.
OE.VPN	The VPN external IT entity must be able to encrypt data transmitted to the TOE and decrypt data received from the TOE in accordance with the negotiated IKE/IPSec policy for the established VPN tunnel.

IT Security Requirements

TOE Security Functional Requirements

The TOE functional security requirements are drawn from [CC] Part 2 functional requirement components, with the exception of FTP_RTC.1. FTP_RTC.1 is used to correctly specify the use of a trusted channel for remote administration per CCEVS PD-0108.

Selections are enclosed in [square brackets], assignments are enclosed in [square brackets and underlined], refinements are in **bold** and/or ~~strikethrough~~. Iterations are numbered in sequence as appropriate.

Explicitly stated SFRs are identified by having a label (EXP) meaning 'Explicit Stated SFR for the TOE' after the requirement name for TOE SFRs.

Audit Data Generation (FAU_GEN.1)

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions

b) All auditable events for the [not specified] level of audit;

c) [the events in the Table 7] FAU_GEN.1.1

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 7] FAU_GEN.1.2

Table 7 Auditable Events

Functional Component	Auditable Event	Additional Audit Record Contents
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE.
FIA_UAU.2	Unsuccessful use of the authentication mechanism.	None.
FDP_IFF.1 (1) FDP_IFF.1(2) FDP_IFF.1(3)	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	Changes to the time.	The identity of the administrator performing the operation.
FMT_SMF.1	Use of the management functions	The identity of the administrator performing the operation
FMT_SMR.1	Modifications to the group of users that are part of a role	The identity of the administrator performing the operation

Security Audit Review (FAU_SAR.1)

The TSF shall provide [administrators] with the capability to read [all audit trail data] from the audit records.[FAU_SAR1.1]

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.[FAU_SAR.1.2]

Enforced Proof of Origin (FCO_NRO.2)

The TSF shall enforce the generation of evidence of origin for transmitted [IP packets protected by the IPSec information flow control policy] at all times.[FCO_NRO.2.1]
The TSF shall be able to relate the [IPSec SA peer] of the originator of the information, and the [digital signature] of the information to which the evidence applies.[FCO_NRO.2.2]
The TSF shall provide a capability to verify the evidence of origin of information to [the receiving SA peer] given [the successful establishment of an IPSec SA with the transmitting SA peer].[FCO_NRO.2.3]

Cryptographic Key Generation (FCS_CKM.1) (1) RSA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [512, 1024 bits] that meet the following: [PKCS #1].[FCS_CKM.1.1(1)]

Cryptographic Key Generation (FCS_CKM.1) (2) Diffie-Hellman

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Diffie-Hellman key agreement] and specified cryptographic key sizes [768 bit, 1024 bit, and 1536 bit] that meet the following: [PKCS #3].[FCS_CKM.1.1(2)]

Cryptographic Key Destruction (FCS_CKM.4)

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite] that meets the following: [no standard].[FCS_CKM.4.1]

Cryptographic Operation (FCS_COP.1(1)) – Encryption

The TSF shall perform [bulk encryption and decryption] in accordance with a specified cryptographic algorithms [3DES, AES] and cryptographic key sizes [168 bit, 256 bit] that meet the following: [FIPS 46-3 , FIPS 197].[FCS_COP.1.1(1)]

Cryptographic Operation (FCS_COP.1(2)) – Signing

The TSF shall perform [digital signing and signature verification] in accordance with a specified cryptographic algorithm [SHA-1, MD5] and cryptographic key sizes [160 bit, 128 bit] that meet the following: [RFC 2404, RFC 2403].[FCS_COP.1.1(2)]

Cryptographic Operation (FCS_COP.1(3)) – Remote Administration

The TSF shall perform [encryption of remote authorized administrator sessions] in accordance with a specified cryptographic algorithm: [Triple Data Encryption Standard (DES) as specified in FIPS PUB 46-3 and implementing any mode of operation specified in FIPS PUB 46-3 with Keying Option 1 (K1, K2, K3 are independent keys)] and cryptographic key sizes [that are 192 binary digits in length] that meet the following: [FIPS PUB 46-3 with Keying Option 1 and FIPS PUB 140-1 (Level 1)]. [FCS_COP.1.1(3)]

Cryptographic Operation (FCS_COP.1(4)) – SCEP signing

The TSF shall perform [digital signing and signature verification] in accordance with a specified cryptographic algorithm [MD5 with RSA Encryption] and cryptographic key sizes [128, 512, or 1024 bits] that meet the following: [PKCS#1, PKCS#7].[FCS_COP.1.1(4)]

Cryptographic Operation (FCS_COP.1(5)) – SCEP encryption

The TSF shall perform [encryption/decryption] in accordance with a specified cryptographic algorithm [3DES] and cryptographic key sizes [168 bits] that meet the following: [FIPS 46-3].[FCS_COP.1.1(5)]

Subset Information Flow Control (FDP_IFC.1(1)) - IPSec

The TSF shall enforce the [IPSec information flow control SFP] on [

Subject: IP network devices

Information: IP packets

Operations: encrypt, decrypt or ignore][FDP_IFC.1.1(1)]

Subset Information Flow Control (FDP_IFC.1(2)) - VLAN

The TSF shall enforce the [VLAN information flow control SFP] on [

Subject: physical network interfaces

Information: IP packets

Operations: permit or deny layer two communication] [FDP_IFC.1.1(2)]

Subset Information Flow Control (FDP_IFC.1(3)) – Packet Filter

The TSF shall enforce the [packet filter information flow control SFP] on [

Subject: IP network devices

Information: IP packet

Operations: permit or deny][FDP_IFC.1.1(3)]

Simple Security Attributes (FDP_IFF.1(1)) - IPSec

The TSF shall enforce the [IPSec information flow control SFP] based on the following types of subject and information security attributes: [

Subject Security Attributes

- Presumed address;

Information Security Attributes

- Receiving/transmitting interface;
- Source/destination IP address;
- Source/destination port number;
- transport layer protocol;
- IPSec Security Association].[FDP_IFF.1.1 (1)]

The TSF shall permit an information flow between ~~a~~ controlled subject**s** ~~and~~ **of** controlled information via a controlled operation if the following rules hold: [

- if one subject can authenticate another subject through the establishment of an IPSec Security Association based on VPN security attributes established by the authorised administrator
-]. [FDP_IFF.1.2(1)]

The TSF shall enforce ~~the~~ [the following additional rules:

- incoming IPSec-encapsulated traffic shall be decrypted per FCS_COP.1(1) and verified in accordance with FDP_UCT.1 and FDP_UIT.1, based on VPN security attributes defined in crypto access control list established by the authorised administrator for the security association

- outgoing traffic shall be encrypted per FCS_COP.1.(1) using IKE/IPSec in accordance with FDP_UCT.1 and FDP_UIT.1, based on VPN security attributes defined in crypto access control list established by the authorised administrator for the security association and tunnelled to the VPN peer corresponding to the destination address]. FDP_IFF.1.3(1)

The TSF shall provide the following [inbound packet filtering based on access control lists to filter on presumed source/destination IP address, protocol, interface and source/destination port number as configured by the administrator and defined by rules specified in FDP_IFF.1(3).] FDP_IFF.1.4(1)

The TSF shall explicitly authorize an information flow based on the following rules: [none]. FDP_IFF.1.5(1)
The TSF shall explicitly deny an information flow based on the following rules: [the administrator-configured explicit "deny" rules based on the above Information Security Attributes]. FDP_IFF.1.6(1)

Simple Security Attributes (FDP_IFF.1(2)) - VLAN

The TSF shall enforce the [VLAN information flow control SFP] based on the following types of subject and information security attributes: [

Subject Security Attributes:

- Receiving/transmitting VLAN interface

Information Security Attributes:

- VLAN ID in Packet Header] FDP_IFF.1.1 (2)

The TSF shall permit an information flow between ~~a~~ controlled subject**s** ~~and~~ **of** controlled information via a controlled operation if the following rules hold: [if the VLAN interfaces (subjects) are configured to be in the same VLAN] FDP_IFF.1.2(2)

The TSF shall enforce the [information flow so that only packets contain a matching VLAN ID in the header will be forwarded to the appropriate VLAN interfaces] FDP_IFF.1.3(2)

The TSF shall provide the following [modification of VLAN ID after information flow has been permitted via FDP_IFF.1(1) or FDP_IFF.1(3)] FDP_IFF.1.4(2)

The TSF shall explicitly authorize an information flow based on the following rules: [none]. FDP_IFF.1.5(2)

The TSF shall explicitly deny an information flow based on the following rules: [packets associated with a VLAN will not be forwarded to VLAN interfaces (subjects) not configured to be in that VLAN] FDP_IFF.1.6(2).

Simple Security Attributes (FDP_IFF.1(3)) – Packet Filter

The TSF shall enforce the [packet filter Information Flow Control SFP] based on the following types of subject and information security attributes: [

Subject Security Attributes

- Presumed address

Information Security Attributes

- presumed address of source subject
- presumed address of destination subject
- transport layer protocol (TCP or UDP)
- network layer protocol (Internet Protocol number 0 to 255 or defined name: eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, or pim)
- TOE interface on which traffic arrives and departs.] FDP_IFF.1.1 (3)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:[

a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:

- the packet's source and destination address, protocol (IP/TCP/UDP) and port are specifically permitted by the information flow security policy rules
- the presumed address of the source subject, in the information, translates to an internal network address
- and the presumed address of the destination subject, in the information, translates to an address on another connected network

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- the packet's source and destination address, protocol (IP/TCP/UDP) and port are specifically permitted by the information flow security policy rules
- the presumed address of the source subject, in the information, translates to an external network address
- and the presumed address of the destination subject, in the information, translates to an address on another connected network.] FDP_IFF.1.2(3)

The TSF shall enforce the [none]. FDP_IFF.1.3(3)

The TSF shall provide the following [none]. FDP_IFF.1.4(3)

The TSF shall explicitly authorize an information flow based on the following rules: [none]. FDP_IFF.1.5(3)

The TSF shall explicitly deny an information flow based on the following rules: [

a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network.] FDP_IFF.1.6(3)

Basic Data Exchange Confidentiality (FDP_UCT.1(1))

The TSF shall enforce the [IPSec information flow control SFP] to be able to [transmit **and** receive] ~~objects~~ **IP packets** in a manner protected from unauthorized disclosure.FDP_UCT.1.1(1)

Data Exchange Integrity (FDP_UIT.1(1))

The TSF shall enforce the [IPSec information flow control SFP] to be able to [transmit **and** receive] ~~user data~~ **IP packets** in a manner protected from [modification, insertion **and** replay] errors.FDP_UIT.1.1(1)
The TSF shall be able to determine on receipt of ~~user data~~ **IP packets**, whether [modification, insertion **and** replay] has occurred. FDP_UIT.1.2(1)

User Authentication Before Any Action (FIA_UAU.2)

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.[FIA_UAU.2.1]

Multiple Authentication Mechanisms (FIA_UAU.5(1))

The TSF shall provide [password based, signature, and certificate based mechanisms] to support user authentication.[FIA_UAU.5.1(1)]

The TSF shall authenticate any user's claimed identity according to the [following rules:

- Reusable password based authentication mechanism shall be used for authorised administrators to access the TOE such that successful authentication must be achieved before allowing any other TSF mediated actions on behalf of that user.
- IKE-based authentication mechanism shall be used for external IT entities for site-to-site and remote client VPN connections such that successful authentication must be achieved before allowing any other TSF mediated actions on behalf of that user
- Reusable password for IKE extended authentication (XAUTH) shall be used for remote client VPN connections such that successful authentication must be achieved before allowing any other TSF mediated actions on behalf of that user]. [FIA_UAU.5.2(1)]

User Identification Before Any Action (FIA_UID.2)

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user. [FIA_UID.2.1]

Management of Security Functions Behavior (FMT_MOF.1)

The TSF shall restrict the ability to [determine the behavior of, disable, enable, **and** modify the behavior of] the functions [:

- that implement the IPSec information flow control SFP
- that implement the VLAN information flow control SFP
- that implement the packet filter information flow control SFP
- use of an external authentication server] to [administrators]. [FMT_MOF.1.1]

Management of Security Attributes (FMT_MSA.1(1))

The TSF shall enforce the [IPSec information flow control SFP] to restrict the ability to [query, modify**,** delete, and define] the security attributes [VPN policy settings in crypto maps, VPN configuration attributes and crypto map client authentication list] to [administrator.][FMT_MSA.1.1(1)]

Management of Security Attributes (FMT_MSA.1(2))

The TSF shall enforce the [VLAN information flow control SFP] to restrict the ability to [query, modify **and** delete] the security attributes [VLAN policy settings] to [administrator.][FMT_MSA.1.1(2)]

Management of Security Attributes (FMT_MSA.1(3))

The TSF shall enforce the [packet filter information flow control SFP] to restrict the ability to [query, modify **and** delete] the security attributes [information security attributes values within packet filtering rules] to [administrator.][FMT_MSA.1.1(3)]

Secure Security Attributes (FMT_MSA.2)

The TSF shall ensure that only secure values are acceptable for security attributes.[FMT_MSA.2.1]

Static Attribute Initialization (FMT_MSA.3(1))

The TSF shall enforce the [IPSec information flow control SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.[FMT_MSA.3.1(1)]

The TSF shall allow the [administrator] to specify alternative initial values to override the default values when an object or information is created. [FMT_MSA.3.2(1)]

Static Attribute Initialization (FMT_MSA.3(2))

The TSF shall enforce the [VLAN information flow control SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.[FMT_MSA.3.1(2)]

The TSF shall allow the [administrator] to specify alternative initial values to override the default values when an object or information is created. [FMT_MSA.3.2(2)]

Static Attribute Initialization (FMT_MSA.3(3))

The TSF shall enforce the [packet filter information flow control SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.[FMT_MSA.3.1(3)]

The TSF shall allow the [administrator] to specify alternative initial values to override the default values when an object or information is created. [FMT_MSA.3.2(3)]

Management of TSF Data (FMT_MTD.1(1))

The TSF shall restrict the ability to [delete, [generate and view]] the [IPSec Pre-Shared Keys] to [administrators]. [FMT_MTD.1.1(1)]

Management of TSF Data (FMT_MTD.1(2))

The TSF shall restrict the ability to [query, modify, delete **and** clear] the [TSF configuration] to [administrator].[FMT_MTD.1.1(2)]

Specification of Management Functions (FMT_SMF.1)

The TSF shall be capable of performing the following security management functions: [

- disable, enable, and modify the behavior of the functions that implement the IPSec, VLAN, and packet filtering information flow control SFPs
- disable, enable, and modify the behavior of the functions for use of an external authentication server
- query, modify, define, and delete VPN policy settings, VPN configuration attributes and crypto map client authentication list
- query, modify and delete VLAN policy settings
- query, modify and delete information security attributes values within packet filtering rules
- delete, generate, and view IPSec pre-shared keys
- verify TSF data and executable code
- specify alternative initial values to override the default values of security attributes for IPSec information flow control SFP, VLAN information flow control SFP, and packet filtering information flow control SFP
- query, modify, delete, and clear the TSF configuration].[FMT_SMF.1.1]

Security Roles (FMT_SMR.1)

The TSF shall maintain the roles: [VPN Client user and administrator]. [FMT_SMR.1.1]
The TSF shall be able to associate **human** users with **VPN Client user, administrator and privileged** roles.[FMT_SMR.1.2]

Application Note The VPN Client user role does not have access to the administrative functions or interfaces to the TOE.

Non-bypassability of the TSP (FPT_RVM.1)

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. FPT_RVM.1.1

TSF Domain Separation (FPT_SEP.1)

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.FPT_SEP.1.1

The TSF shall enforce separation between the security domains of subjects in the TSC.FPT_SEP.1.2

Reliable Time Stamps (FPT_STM.1)

The TSF shall be able to provide reliable time stamps for its own use. FPT_STM.1.1

Abstract Machine Testing (FPT_AMT.1)

The TSF shall run a suite of tests [during initial start-up] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.FPT_AMT.1.1

TSF Testing (FPT_TST.1)

The TSF shall run a suite of self tests [during initial start-up] to demonstrate the correct operation of [the TSF]. FPT_TST.1.1

The TSF shall provide authorised users with the capability to verify the integrity of [TSF data]. FPT_TST.1.2

The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.FPT_TST.1.3

TOE Session Establishment (FTA_TSE.1)

The TSF shall be able to deny session establishment based on [access control list specifying a combination of source/destination IP address and source/destination TCP/UDP port number].FTA_TSE.1.1

Inter-TSF Trusted Channel (FTP_ITC.1(1))

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.FTP_ITC.1.1(1)

The TSF shall permit [the TSF **or** the remote IT trusted product] to initiate communication via the trusted channel.FTP_ITC.1.2(1)

The TSF shall initiate communication via the trusted channel for [IPSec VPN traffic].FTP_ITC.1.3(1)

Inter-TSF Trusted Channel (FTP_ITC.1(2))

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.FTP_ITC.1.1(2)
The TSF shall permit [the TSF] to initiate communication via the trusted channel.FTP_ITC.1.2(2)
The TSF shall initiate communication via the trusted channel for [external authentication services].FTP_ITC.1.3(2)

Application Note The TOE can be configured to use local authentication mechanisms or use authentication services provided by an external authentication server. The use of an external authentication server is optional in all TOE configurations, and not required for any TOE configuration. The TOE shall be responsible for correctly invoking the external authentication mechanism, and for taking the correct actions based on authentication decisions. In keeping with industry practice the choice of authentication server is not mandated by this ST.

Remote Administration Trusted Channel (FTP_RTC.1) (EXP)

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.[FTP_RTC.1.1]

The TSF shall permit the remote IT trusted product to initiate communication via the trusted channel.[FTP_RTC.1.2]

The TSF shall use a trusted channel for the following functions: secure remote administration.[FTP_RTC.1.3]

Application Note Secure remote administration is provide by SSH.

Security Requirements for the IT Environment

The following functional requirements are met by the VPN peer .

Basic Data Exchange Confidentiality (FDP_UCT.1(2))

The **IT environment** shall enforce the [IPSec information flow control SFP] to be able to [transmit **and** receive] ~~objects~~ **IP packets** in a manner protected from unauthorized disclosure.[FDP_UCT.1.1(2)]

Data Exchange Integrity (FDP_UIT.1(2))

The **IT environment** shall enforce the [IPSec information flow control SFP] to be able to [transmit **and** receive] ~~user data~~ **IP packets** in a manner protected from [modification, insertion **and** replay] errors.[FDP_UIT.1.1(2)]

The **IT environment** shall be able to determine on receipt of ~~user data~~ **IP packets**, whether [modification, insertion **and** replay] has occurred. [FDP_UIT.1.2(2)]

Inter-TSF Trusted Channel (FTP_ITC.1(3))

The **IT environment** shall provide a communication channel between itself and **the TSF** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.[FTP_ITC.1.1(3)]

The **IT environment** shall permit [the TSF **or** the remote IT trusted product] to initiate communication via the trusted channel.[FTP_ITC.1.2(3)]

The **IT environment** shall initiate communication via the trusted channel for [IPSec VPN traffic].[FTP_ITC.1.3(3)]

TOE Security Assurance Requirements

The TOE meets all the EAL4 assurance requirements as defined in CC Part 3 augmented with ALC_FLR.1 (Basic Flaw Remediation). They are summarized by Assurance Class in Table 8.

Table 8 Assurance Requirements: EAL4 Augmented

Assurance Class	Assurance Components
ACM	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2
ADO	ADO_DEL.2 ADO_IGS.1
ADV	ADV_FSP.2 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 ADV_RCR.1 ADV_SPM.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1 ALC_LCD.1 ALC_TAT.1, ALC_FLR.1
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_MSU.2 AVA_SOF.1 AVA_VLA.2

TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

IT Security Functions

This section presents the security functions performed by the TOE and provides a mapping between the identified security functions and the Security Functional Requirements that it must satisfy. This ST claims compliance with the external standards for DES, 3DES, SHA-1 and MD-5 for the definition of the encryption algorithms as indicated in FCS_COP.1(1), FCS_COP.1(2), and FCS_COP.1(3). For the IPSEC.1, IPSEC.2 and REMOTE.1 Security Functions described below, the encryption was not analyzed or tested to conform to cryptographic standards as part of this evaluation. The cryptography used in the TOE has been FIPS certified as indicated in Appendix B, FIPS Conformance.

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.

If the crypto map entry is tagged as **ipsec-manual**, IPSec is triggered. If no SA exists that IPSec can use to protect this traffic to the peer, the traffic is dropped. In this case, the SAs are installed via the configuration, without the intervention of IKE. If the SAs did not exist, IPSec did not have all of the necessary pieces configured.

Once established, the set of SAs (outbound, to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the 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 costly 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) support for a manageable, scalable IPSec implementation
- 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 user name 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 user name and password entries into the local user name 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 (labelled 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:

- 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
- The granularity of the flow to be protected by a set of SAs

- How to identify the peer TOE that will decrypt the packet flow
- The interface(s) that are enabled for IPSec using the parameters specified above
- What IPSec SA should be applied to the packet flow (by selecting from a list of one or more transform sets)
- 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 modelled in the IPSec Information Flow SFP.

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, interface, 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 - ACL Options" section on page 66 for more information on all of the ACL options.

VLAN Management

The TOE controls the logical connections between combinations of internal Virtual Local Area Networks (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 modelled in the VLAN Information Flow SFP.

On the Cisco Catalyst 6500 Series switch or Cisco 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.

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 authorised 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 user name 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 can be configured to use the local authentication mechanism or an external authentication server for local or remote administration and VPN Client user authentication. The use of an external authentication server is optional for all TOE configurations, and not required for any TOE configuration.

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 authorised 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.

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. The cryptography used in the TOE has been FIPS certified as indicated in Appendix B, FIPS Conformance.

KEYMGT.1 - Key Management

The TOE generates secure RSA public/private keys (128, 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.

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.

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 authorised administrators. The TOE complies with IPSec protocol (RFCs 2401-2404, 2406-2410) 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 user name/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 authorised 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.

Table 9 Mapping Summary Specifications to Functional Requirements

TSS Reference	IT Security Function	Functional Component	Functional Requirement
IPSEC.1	IPSec Internet Key Exchange (IKE)	FCS_CKM.1(2)	Cryptographic key generation (Diffie Hellman)
		FCS_CKM.4	Cryptographic key destruction
		FTP_ITC.1(1)	Inter-TSF trusted channel
		FMT_MSA.2	Secure security attributes
		FCS_COP.1 (2)	Cryptographic operation (Signing)
		FMT_MTD.1(1)	Management of TSF Data
		FTP_ITC.1(2)	Inter-TSF trusted channel
		FIA_UAU.5(1)	Multiple authentication mechanisms
		FIA_UAU.2	User authentication before any action
		FIA_UID.2	User identification before any action
		FMT_MSA.1(1)	Management of security attributes
IPSEC.2	IPSec Encapsulating Security Payload (ESP)	FCO_NRO.2	Enforced proof of origin
		FCS_COP.1 (1)	Cryptographic operation (Encryption)
		FDP_UCT.1(1)	Basic data exchange confidentiality
		FDP_UIT.1 (1)	Data exchange integrity
		FTP_ITC.1(1)	Inter-TSF trusted channel
		FMT_MSA.2	Secure security attributes
		FMT_MSA.1()	Management of security attributes
IPSEC.3	Cryptographic Maps	FDP_IFC.1(1)	Subset information flow control (IPSec)
		FDP_IFF.1(1)	Simple security attributes (IPSec)
		FTP_ITC.1(1)	Inter-TSF trusted channel
		FMT_MSA.1(1)	Management of security attributes
PACKETFILTER.1	Packet Filtering	FTA_TSE.1	TOE session establishment
		FDP_IFF.1(1)	Simple security attributes (IPSec)
		FDP_IFC.1(1)	Subset information flow control (IPSec)
		FDP_IFF.1(3)	Simple security attributes (packet filter)
		FDP_IFC.1(3)	Subset information flow control (packet filter)
		FTP_RVM.1	Non-bypassability of the TSP
		FMT_MSA.1(3)	Management of security attributes

Table 9 Mapping Summary Specifications to Functional Requirements (continued)

TSS Reference	IT Security Function	Functional Component	Functional Requirement
VLAN.1	VLAN Processing	FDP_IFC.1(2)	Subset information flow control (VLAN)
		FDP_IFF.1(2)	Simple security attributes (VLAN)
		FMT_MSA.1(2)	Management of security attributes
CONFIG.1	System Messages	FAU_GEN.1	Audit data generation
		FAU_SAR.1	Security audit review
		FMT_SMF.1	Specification of Management Functions
CONFIG.2	Management Interfaces	FIA_UAU.2	User authentication before any action
		FIA_UAU.5(1)	Multiple authentication mechanisms
		FIA_UID.2	User identification before any action
		FMT_SMR.1	Security roles
		FMT_MOF.1	Management of security functions behavior
		FMT_MSA.1(1)	Management of security attributes
		FMT_MSA.1(2)	Management of security attributes
		FMT_MSA.1(3)	Management of security attributes
		FMT_MSA.2	Secure security attributes
		FMT_MSA.3(1)	Static attribute initialization
		FMT_MSA.3(2)	Static attribute initialization
		FMT_MSA.3(3)	Static attribute initialization
		FMT_MTD.1(2)	Management of TSF data
		FPT_AMT.1	Abstract machine testing
		FPT_TST.1	TSF testing
		FMT_SMF.1	Specification of Management Functions
		FMT_MTD.1(1)	Management of TSF data
		FTP_ITC.1(2)	Inter-TSF trusted channel
CONFIG.3	Management of Time	FPT_STM.1	Reliable time stamps
KEYMGT.1	Key Management	FCS_CKM.1 (1)	Cryptographic key generation
		FCS_CKM.4	Cryptographic key destruction
		FCS_COP.1(4)	SCEP signing
		FCS_COP.1(5)	SCEP encryption
		FMT_MSA.2	Secure security attributes

Table 9 Mapping Summary Specifications to Functional Requirements (continued)

TSS Reference	IT Security Function	Functional Component	Functional Requirement
REMOTE.1	Remote Management	FCS_COP.1(3)	Cryptographic Operation (encryption)
		FIA_UAU.5(1)	Multiple authentication mechanisms
		FIA_UID.2	User identification before any action
		FMT_MSA.2	Secure security attributes
		FTP_RTC.1	Remote administration trusted channel
PROTECT.1	Self Protection	FTP_SEP.1	TSF domain separation

Assurance Measures

The purpose of this section is to show that the identified assurance measures are appropriate to meet the assurance requirements by mapping the identified assurance measures onto the assurance requirements.

The Assurance Measures that demonstrate the correct implementation of the Security Functions of the TOE are as follows:

- User Guidance (UG) Documentation
- Functional Specification (FSP) Document
- Security Policy Model (SPM) Document
- High Level Design (HLD) Document
- Low Level Design (LLD) Documentation
- Configuration Management Plan (CMP) Document
- Analysis of Testing (ATE) Document
- Security Functional Analysis (SFA) Document
- Vulnerability Assessment (VA) Document

Table 10 demonstrates that the identified assurance measures completely meet the assurance requirements by showing that all requirements are mapped to an assurance measure.

Table 10 Mapping of Assurance Measures to Assurance Requirements

CC Assurance Component		Assurance Measure
ACM_AUT.1	Partial CM automation	Configuration Management Plan
ACM_CAP.4	Generation support and acceptance procedures	Configuration Management Plan
ACM_SCP.2	Problem tracking CM coverage	Configuration Management Plan
ADO_DEL.2	Detection of modification	Configuration Management Plan
ADO_IGS.1	Installation, generation, and start-up procedures	User Guidance
ADV_FSP.2	Fully defined external interfaces	Functional Specification User Guidance

Table 10 Mapping of Assurance Measures to Assurance Requirements (continued)

CC Assurance Component		Assurance Measure
ADV_HLD.2	Security enforcing high-level design	High Level Design
ADV_IMP.1	Subset of the implementation of the TSF	Low Level Design
ADV_LLD.1	Descriptive low-level design	Low Level Design
ADV_RCR.1	Informal correspondence demonstration	Functional Specification High Level Design Low Level Design
ADV_SPM.1	Informal TOE security policy model	Security Policy Model
AGD_ADM.1	Administrator guidance	User Guidance
AGD_USR.1	User guidance	User Guidance
ALC_DVS.1	Identification of security measures	Configuration Management Plan
ALC_FLR.1	Basic Flaw Remediation	Configuration Management Plan
ALC_LCD.1	Developer defined life-cycle model	Configuration Management Plan
ALC_TAT.1	Well-defined development tools	Configuration Management Plan
ATE_COV.2	Analysis of coverage	Analysis of Testing
ATE_DPT.1	Testing: high-level design	Analysis of Testing
ATE_FUN.1	Functional testing	Analysis of Testing
ATE_IND.2	Independent testing - sample	Analysis of Testing, TOE
AVA_MSU.2	Validation of analysis	Security Functional Analysis
AVA_SOF.1	Strength of TOE security function evaluation	Security Functional Analysis
AVA_VLA.2	Independent vulnerability analysis	Vulnerability Assessment

The assurance measures documents have been specifically written to address the assurance requirements and are structured as follows:

User Guidance (UG)

- Provides TOE users and administrators with procedural information on installation, configuration and management of the TOE (AGD_USR.1) (AGD_ADM.1)
- Describes procedures for the installation, generation, and start-up of the TOE (ADO_IGS.1)
- Detailed syntax information on the external interfaces used for such interaction with the TOE (ADV_FSP.2)

Functional Specification (FSP)

- Describes the security functionality of the TOE (ADV_FSP.2)
- Defines the external interfaces to the TOE (ADV_FSP.2)
- Demonstrates correspondence with the ST (ADV_RCR.1)

Security Policy Model (SPM)

- Describes the security policy implemented by the TOE (ADV_SPM.1)

High Level Design (HLD)

- Describes the relationship between TOE sub-systems, their interfaces and the sequence of events in response to stimulus at those interfaces. (ADV_HLD.2)
- Demonstrates correspondence with the FSP (ADV_RCR.1)

Low Level Design (LLD)

- Describes the TOE sub-systems, their interfaces and the sequence of events in response to stimulus at those interfaces (ADV_LLD.1)
- A source code representation of the TOE. (ADV_IMP.1)
- Demonstrates correspondence with the HLD (ADV_RCR.1)

Configuration Management Plan (CMP)

- Describes the development life-cycle model (ALC_LCD.1)
- Describes the security measures for the development site (ALC_DVS.1)
- Describes the development tools (ALC_TAT.1)
- Describes the CM model (ACM_AUT.1) and how problem tracking is undertaken (ACM_SCP.2)
- Describes the delivery procedures and how they provide for the detection of modification (ADO_DEL.2)
- Description of TOE generation and acceptance procedures (ACM_CAP.4)
- Description of Flaw Remediation procedures (ALC_FLR.1)

Analysis of Testing (ATE)

- Describes the testing undertaken of the TOE and the implementation of the functionality specified in the ST and the design documentation (ATE_DPT.1)
- Describes coverage of the testing (ATE_COV.2)
- Describes the testing of security functionality (ATE_FUN.1)
- The TOE will be provided to the evaluators (ATE_IND.2)

Security Functional Analysis (SFA)

- Describes vulnerability analysis undertaken (AVA_MSU.2)
- Strength of TOE security function evaluation (AVA_SOF.1)

Vulnerability Assessment (VA)

- Identifies potential vulnerabilities in the TOE and provides a rationale as to why they are not exploitable in the intended environment for the TOE (AVA_VLA.2).

PP Claims

This Security Target was not written to conform to any Protection Profile.

Rationale

Security Objectives Rationale

The purpose of this rationale is to demonstrate that the identified security objectives are:

- suitable, they are sufficient to address the security needs
- necessary, and there are no redundant security objectives

All Assumptions, Policies and Threats Addressed

Table 11 Cross Reference Objectives to Threats/Assumptions/Policies

Objective / Policy/ Threat/ Assumption	O.Authenticity	O.Confidentiality	O.Integrity	O.Key-Confidentiality	O.NoReplay	O.Secure-Operation	O.VLAN-Separation	O.Mediate	OE.Policy	OE.VPN	OE.Secure-Management
T.Attack						√					√
T.Untrusted-Path	√	√	√	√	√					√	
T.VLAN-Hopping							√				√
T.Mediate								√			
A.PhySec											√
A.PSK											√
A.NoEvil											√
A.Training											√
A.Trusted-CA											√
P.Connectivity									√		√

Sufficiency of Security Objectives

The following arguments are provided to demonstrate the sufficiency of the Security Objectives outlined above:

Table 12 Sufficiency of Security Objectives (1)

Policies	Objectives
P.CONNECTIVITY Rules for Data Flows	The objectives (OE.Policy, OE.Secure-Management) will provide complete coverage as: OE.Policy states that those responsible for the administration of the TOE will be provided with a policy that specifies: 1. whether the networks which are connected to the TOE are trusted or untrusted 2. which packet flows are to be protected by the TOE 3. the peer TOE to be associated with each data flow OE.Secure-Management states that those responsible for the operation of the TOE will ensure that management and configuration functions of the security functions of the TOE are: 1. initiated from a management station connected to a trusted network and protected using the security functions of the TOE

Table 13 Sufficiency of Security Objectives (2)

Threat	Objectives
T.ATTACK Unauthorized access	The objectives (O.Secure-Operation, OE.Secure-Management) will provide an effective countermeasure as: • The TOE will be correctly configured in accordance with a security policy which will prevent bypass of the TSF; • The TSP can only be altered by a trusted administrator from a secure management station.
T.UNTRUSTED-PATH Secure transmission of packet flows	The objectives (O.Authenticity, O.Confidentiality, O.Integrity, O.Key-Confidentiality, O.NoReplay, OE.VPN) will provide an effective countermeasure as: • O.Authenticity ensures that packet flows are received/transmitted from/to known, trusted sources; • O.Confidentiality ensures that the confidentiality of packet flows is maintained during transmission; • O.Integrity ensures that a packet flow cannot be modified without being detected by the TOE; • O.Key-Confidentiality ensures that cryptographic keys cannot be captured and used to decrypt packet flows; • O.NoReplay ensures that a packet flow transmitted to the TOE has not been copied by an eavesdropper and retransmitted to the TOE. • OE.VPN requires the VPN peer to be able to protect the confidentiality and integrity of the packet flows by properly enforcing the negotiated IPSec policy with the TOE.

Table 13 Sufficiency of Security Objectives (2) (continued)

Threat	Objectives
T.VLAN-Hopping VLAN crosses another VLAN	The objectives O.VLAN-Separation and OE.Secure-Management will provide an effective countermeasure as • The TOE will be correctly configured in accordance with a security policy which will ensure VLAN separation; • Management and configuration of the security functions of the TOE are undertaken by trusted staff trained in the secure operation of the TOE.
T.Mediate Impermissible flow	The objective O.Mediate will provide an effective countermeasure to ensure all traffic to the TOE is mediated before allowing information flow.

Table 14 Sufficiency of Security Objectives (3)

Assumption	Objectives
A.PHYSEC TOE will be kept in a physically secure environment.	The objective (OE.Secure-Management) upholds the assumption as: • The TOE will be maintained in a location, which is physically secure.
A.PSK Pre-shared keys are assumed to be securely communicated between disparate administrators.	The objective (OE.Secure-Management) upholds the assumption as: • Pre-shared Keys used for configuration in cryptographic maps are securely distributed amongst disparate administrators.
A.NOEVIL Administrators assumed to be non-hostile and trusted to perform their duties correctly.	The objective (OE.Secure-Management) upholds the assumption as: • Those responsible for the operation of the TOE must ensure that management and configuration of the security functions of the TOE are undertaken by trusted staff trained in the secure operation of the TOE.
A.TRAINING Administrators of the TOE have received training.	The objective (OE.Secure-Management) upholds the assumption as: • Management and configuration of the security functions of the TOE are undertaken by trusted staff trained in the secure operation of the TOE
A.TRUSTED-CA Digital Certificates are issued from an evaluated/trusted Certificate Authority.	The objective (OE.Secure-Management) upholds the assumption as: • Management and configuration of the security functions of the TOE are implemented in conjunction with an evaluated or trusted Certificate Authority (CA), if digital certificates are used for TOE authentication.

Security Requirements Rationale

The purpose of this section is to show that the identified security requirements (Section 5) are *suitable* to meet the security objectives (Security Objectives , page 16). The following tables show that each security requirement (and SFRs in particular) is *necessary,* that is, each security objective is addressed by at least one security requirement, and vice versa.

Functional Security Requirements Rationale

Table 15 Functional Component to Security Objective Mapping

Objective / Requirement	O.Authenticity	O.Confidentiality	O.Integrity	O.Key-Confidentiality	O.NoReplay	O.VLAN-Separation	O.Mediate	O.Secure-Operation
FAU_GEN.1								√
FAU_SAR.1								√
FCO_NRO.2	√				√			
FCS_CKM.1 (1)				√				
FCS_CKM.1 (2)				√				
FCS_CKM.4				√				
FCS_COP.1(1)		√						
FCS_COP.1(2)	√		√					
FCS_COP.1(3)								√
FCS_COP.1(4)								√
FCS_COP.1(5)								√
FDP_IFC.1(1)	√	√	√	√	√			
FDP_IFC.1(2)						√		
FDP_IFC.1(3)							√	
FDP_IFF.1(1)	√	√	√	√	√			
FDP_IFF.1(2)						√		
FDP_IFF.1(3)							√	
FDP_UCT.1(1)		√						
FDP_UIT.1(1)			√					
FIA_UAU.2								√
FIA_UAU.5(1)								√
FIA_UID.2	√				√			√
FMT_MOF.1								√
FMT_MSA.1(1)								√

Table 15 Functional Component to Security Objective Mapping (continued)

Objective / Requirement	O.Authenticity	O.Confidentiality	O.Integrity	O.Key-Confidentiality	O.NoReplay	O.VLAN-Separation	O.Mediate	O.Secure-Operation
FMT_MSA.1(2)								√
FMT_MSA.1(3)								√
FMT_MSA.2	√	√	√	√				√
FMT_MSA.3(1)								√
FMT_MSA.3(2)								√
FMT_MSA.3(3)								√
FMT_MTD.1(2)								√
FMT_MTD.1(1)				√				
FMT_SMF.1								√
FMT_SMR.1								√
FPT_AMT.1								√
FPT_RVM.1								√
FPT_SEP.1								√
FPT_STM.1								√
FPT_TST.1								√
FTA_TSE.1								√
FTP_ITC.1(1)	√	√	√	√	√			
FTP_ITC.1(2)	√							√
FTP_RTC.1								√

Table 16 SFR Sufficiency SFR Dependency Rationale

Objective	Requirement
O.AUTHENTICITY Ensure packet flows have been received from a trusted source.	The SFRs [FCO_NRO.2, FIA_UID.2, FCS_COP.1(2), FMT_MSA.2, FDP_IFC.1(1), FDP_IFF.1(1), FTP_ITC.1(1), FTP_ITC.1(2)] are sufficient to satisfy the objective because: • Packet flows received by the TOE must have been digitally signed using the FCO_NRO.2 SFR with key material associated with an identified (FIA_UID.2) remote trusted IT product. • The FCS_COP.1(2) SFR ensures that the received transmission is digitally signed and therefore its authenticity can be established cryptographically. FMT_MSA.2 ensures cryptographic values used are valid. • The information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1(1) SFR • The FDP_IFF.1(1) SFR is used to identify which IPSec peer is authenticating which packet flow, and which packet flow is to be authenticated for transmission to a remote IPSec peer. • The FTP_ITC.1(1) SFR establishes a trust relationship with a remote TOE instance (e.g.. another instance of the TOE) to establish network-network VPN. • The FTP_ITC.1(2) SFR establishes a trust relationship with an external authentication server to authenticate users if configured by the administrator.
O.CONFIDENTIALITY Protect the confidentiality of packet flows transmitted to/from the TOE over an untrusted network.	The SFRs [FCS_COP.1(1), FMT_MSA.2, FDP_UCT.1(1), FDP_IFC.1(1), FDP_IFF.1(1), FTP_ITC.1(1)] are sufficient to satisfy the objective because: • The FCS_COP.1(1) SFR ensures the confidentiality of transmissions through strong encryption. FMT_MSA.2 ensures cryptographic values used are valid. • The FDP_UCT.1(1) SFR provides confidentiality for packet flows received by, or transmitted from, the TOE using key material associated with an identified IPSec peer • The information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1(1) SFR • The FDP_IFF.1(1) SFR is used to identify which IPSec peer is providing confidentiality for which packet flow, and which packet flow is to be protected when transmitted to a remote IPSec peer • The FTP_ITC.1(1) SFR establishes a trust relationship with a VPN peer to establish a IPSec VPN tunnel.
O.INTEGRITY Any attempt to corrupt or modify a packet flow transmitted to/from the TOE is detected.	The SFRs [FCS_COP.1(2), FMT_MSA.2, FDP_UIT.1(1), FDP_IFC.1(1), FDP_IFF.1(1), FTP_ITC.1(1)] are sufficient to satisfy the objective because: • The FCS_COP.1(2) SFR ensures that the received transmission is digitally signed and therefore its integrity can be established cryptographically. FMT_MSA.2 ensures cryptographic values used are valid. • The FDP_UIT.1(1) SFR provides integrity for packet flows received by, or transmitted from, the TOE using key material associated with an identified remote IPSec peer • The information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1(1) SFR • The FDP_IFF.1(1) SFR is used to identify which IPSec peer is providing integrity verification for which packet flow, and which packet flow is to be protected when transmitted to a remote IPSec peer • The FTP_ITC.1(1) SFR establishes a trust relationship with a VPN peer to establish a IPSec VPN tunnel

Table 16 SFR Sufficiency SFR Dependency Rationale (continued)

Objective	Requirement
O.KEY-CONFIDENTIALITY Provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt packet flows between instances of the TOE and when kept in short and long-term storage.	The SFRs [FCS_CKM.1 (1), FCS_CKM.1 (2), FCS_CKM.4, FMT_MSA.2, FDP_IFC.1(1), FDP_IFF.1(1), FTP_ITC.1(1), FMT_MTD.1(1)] are sufficient to satisfy the objective: • The FCS_CKM.1 (1) SFRs ensures that key generation is robust • FCS_CKM.4 SFR ensures that keys can be safely destroyed • The FCS_CKM.1 (2), SFR ensures that the establishment of the trust relationship and the key agreement operations are cryptographically sound • Cryptographic keys generated are checked to ensure they are secure (FMT_MSA.2) • The information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1(1) SFR • The FDP_IFF.1(1) SFR is used to identify which IPSec peer is providing integrity verification for which packet flow, and which packet flow is to be protected when transmitted to a remote IPSec peer • The FTP_ITC.1(1) SFR establishes a trust relationship with a VPN peer to establish a IPSec VPN tunnel • The FTP_MTD.1(1) ensures that Pre-Shared Key entry and deletion is only allowed by the administrator
O.NOREPLAY Provide a means to detect if an eavesdropper has copied a packet flow and retransmitting it to the TOE.	The SFRs [FCO_NRO.2, FIA_UID.2, FDP_IFC.1(1), FDP_IFF.1(1), FTP_ITC.1(1)] are sufficient to satisfy the objective because: • The FTP_ITC.1(1) SFR establishes a trust relationship with a remote TOE instance to establish network-network VPN • Packet flows received by the TOE are marked using the FCO_NRO.2 SFR with a sequence number that is uniquely associated with a remote IPSec peer. FIA_UID.2 supports the need to identify the remote IPSec peer. • The information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1(1) SFR • The FDP_IFF.1(1) SFR is used to identify which IPSec peer is providing integrity verification for which packet flow, and which packet flow is to be protected when transmitted to a remote IPSec peer
O.SECURE-OPERATION Prevent Unauthorized changes to TOE configuration.	The SFRs [FTA_TSE.1, FIA_UAU.2, FIA_UAU.5(1), FIA_UID.2, FAU_GEN.1, FAU_SAR.1, FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.2, FMT_MSA.3(1), FMT_MSA.3(2), FMT_MSA.3(3), FMT_SMF.1, FMT_SMR.1, FMT_MTD.1(2), FPT_RVM.1, FPT_SEP.1, FPT_STM.1, FPT_AMT.1, FPT_TST.1, FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5), FTP_RTC.1, FTP_ITC.1(2] are sufficient to satisfy the objective because: • The TSF can reject Unauthorized session establishments by applying access control lists to deny session establishment, supported by FTA_TSE.1; • The FIA_UAU family supports the requirement for multiple user authentication mechanisms before any actions are carried out on the TSF and FTP_ITC.1(2) supports the optional use of an external authentication server; • The FIA_UID family supports the requirement to identify the user before any actions are taken on that user's behalf; • The requirements for recording the occurrence of security relevant events that take place under TSF control and the identification of the level of auditing are provided by FAU_GEN.1, and the ability for authorised users to review this audit information is provided by FAU_SAR.1; • Authorised users' control over the management of the security attributes is allowed by the FMT_MSA family;

Table 16 SFR Sufficiency SFR Dependency Rationale (continued)

Objective	Requirement
O.SECURE-OPERATION Prevent Unauthorized changes to TOE configuration.	• The requirement to restrict the ability to determine the behaviour of, disable, enable and modify the IPSec, VLAN, and packet filtering information flow control SFPs and use of an external authentication service satisfied by FMT_MOF.1; • Authorized users' control over the management of the securityattributes is allowed by the FMT_MSA family; • Control over the assignment of the administrator role and VPN Client User role to different users is provided by the FMT_SMR.1 family. No user will be able to assume the role of administrator without explicitly requesting and being authenticated as having permission. Users will not be able to assume administrator role unless they have first assumed the administrator role. VPN clients will not be allowed to establish an IPSec connection unless being authenticating as having permission; • FMT_SMF.1 describes the security functions available to the administrators that can be used to ensure the secure operation of the TOE. • The requirement to restrict the ability to query, modify, delete and clear the TSF configuration to administrators is provided by FMT_MTD.1(2); • The requirement for reliable time-stamps is satisfied by FPT_STM.1; • The requirement for the self-testing of the abstract machine upon which the security functions rely is satisfied by FPT_AMT.1.; • The requirement for self-testing upon startup to verify the proper operation of the TSF code is satisfied by FPT_TST.1 • FCS_COP.1(3) describes the encryption capability provided by SSH • FCS_COP.1(4) describes the signing capability of SCEP. • FCS_COP.1(5) describes the encryption capability of SCEP. • FTP_RTC.1 ensures that the remote administration is through a protected channel • FPT_RVM.1 ensures that the TSF is always invoked from initial start-up and is nonbypassable; • FPT_SEP.1 ensures that the TSF has a domain of execution that is separate and cannot be violated by Unauthorized users. This component also ensures that the domains of execution for the various processes are isolated and cannot be violated by Unauthorized users.
O.VLAN-Separation Provide a means for the logical separation of Virtual LANs to ensure that packets flows are restricted to their authorised Virtual LANs ensuring VLAN separation is achieved.	The SFRs FDP_IFC.1(2) and FDP_IFF.1(2) are sufficient to satisfy the objective because: • The VLAN traffic information control SFP and the scope of control of the policies that form the identified VLAN traffic information flow control portion of the TSP are identified and defined by the FDP_IFC.1(2) SFR. • The FDP_IFF.1(2) SFR is used to identify which VPN is providing integrity verification for which packet flow, and which packet flow is to be protected when transmitted to an IPSec compatible entity and modifies the VLAN Tag to ensure that VLAN traffic can only be sent to VLANs with the corresponding VLAN ID.
O.Mediate The TOE must mediate the flow of all information transmitted to the TOE over an untrusted network.	The SFRs [FDP_IFC.1(3), FDP_IFF.1(3)] are sufficient to satisfy the objective because: • The packet filter information flow control SFP and the scope of control of the policy that form the identified information flow control portion of the TSP are identified and defined by the FDP_IFC.1(3) SFR; and • The FDP_IFF.1(3) SFR is used to identify which packet flows are to be mediated.

Table 17 shows that the security target has satisfied SFR's with dependencies.

Table 17 SFR Dependency Rationale

Requirement	Dependencies
FAU_GEN.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1
FCO_NRO.2	FIA_UID.2
FCS_CKM.1(1)	FCS_COP.1(1), FCS_CKM.4, FMT_MSA.2
FCS_CKM.1(2)	FCS_COP.1(2) , FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	FCS_CKM.1(1), FCS_CKM.1(2), FMT_MSA.2
FCS_COP.1(1)	FCS_CKM.1(1), FCS_CKM.4, FMT_MSA.2
FCS_COP.1(2)	FCS_CKM.1(2), FCS_CKM.4, FMT_MSA.2
FCS_COP.1(3)	FCS_CKM.1(1), FCS_CKM.4, FMT_MSA.2
FCS_COP.1(4)	FCS_CKM.1(1), FCS_CKM.4, FMT_MSA.2
FCS_COP.1(5)	FCS_CKM.1(1), FCS_CKM.4, FMT_MSA.2
FDP_IFC.1(1)	FDP_IFF.1(1)
FDP_IFC.1(2)	FDP_IFF.1(2)
FDP_IFC.1(3)	FDP_IFF.1(3)
FDP_IFF.1(1)	FDP_IFC.1(1), FMT_MSA.3(1)
FDP_IFF.1(2)	FDP_IFC.1(2), FMT_MSA.3(2)
FDP_IFF.1(3)	FDP_IFC.1(3), FMT_MSA.3(3)
FDP_UCT.1(1)	FTP_ITC.1(1), FDP_IFC.1(1)
FDP_UIT.1(1)	FDP_IFC.1(1), FTP_ITC.1(1)
FIA_UAU.2	FIA_UID.2
FIA_UAU.5(1)	N/A
FIA_UID.2	N/A
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1(1)	FDP_IFC.1(1), FMT_SMR.1, FMT_SMF.1
FMT_MSA.1(2)	FDP_IFC.1(2), FMT_SMR.1, FMT_SMF.1
FMT_MSA.1(3)	FDP_IFC.1(3), FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	ADV_SPM.1, FDP_IFC.1, FMT_MSA.1, FMT_SMR.1
FMT_MSA.3(1)	FMT_MSA.1(1), FMT_SMR.1
FMT_MSA.3(2)	FMT_MSA.1(2), FMT_SMR.1
FMT_MSA.3(3)	FMT_MSA.1(3), FMT_SMR.1
FMT_MTD.1 (1,2)	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	N/A
FMT_SMR.1	FIA_UID.2
FPT_AMT.1	N/A
FPT_RVM.1	N/A
FPT_SEP.1	N/A

Table 17 SFR Dependency Rationale (continued)

Requirement	Dependencies
FPT_STM.1	N/A
FPT_TST.1	FPT_AMT.1
FTA_TSE.1	N/A
FTP_ITC.1(1)	N/A
FTP_ITC.1(2)	N/A
FTP_RTC.1	N/A

All functional component dependencies are met, as shown in Table 17. According to the CC, FDP_IFC.1 (or FDP_ACC.1) and FMT_MSA.1, is required as a dependency for FMT_MSA.2. FMT_MSA.2 is included in this ST as a result of including cryptographic requirements and not information flow (or access control) requirements. This ST does include three information flow policies and their associated requirements so the dependencies are technically met. However, this requirement should only be relevant to attributes associated with cryptographic operations.

Assurance Security Requirements Rationale

This section shows how the minimum strength of function level for the ST is consistent with the security objectives for the TOE. This ST claims SOF-basic for the strength of function level of the TOE, as

- the TOE is assumed to be physically secure (A.PhySec) and administered by trusted and non-hostile (A.NoEvil) staff with appropriate training (A.Training), and
- the AVA_VLA.2 assurance component, required for EAL4, is considered to be suitable for SOF-basic.

The TOE is intended to be used in environments in which users require a moderate to high level of assured security when connecting trusted networks via untrusted networks (such as the Internet), without incurring additional security-specific engineering costs. CC Part 3 suggests CC EAL4 as suitable in these circumstances. EAL 4 is augmented by ALC_FLR.1 to help ensure that the customers can report the flaws and the flaws can be systematically corrected.

Mutually Supportive Security Requirements

The purpose of this rationale is to show that the IT security requirements (and the SFRs in particular) are complete and internally consistent by demonstrating that they are mutually supportive and provide an “integrated and effective whole”.

Dependency helps in showing mutual support because if SFR-A is dependent on SFR-B then by definition, SFR-B is supportive of SFR-A. Table 17 shows the dependencies of the Security Functional Requirements.

This ST is targeting a standard EAL 4 assurance package and so the dependency and mutual support of the assurance requirements is self-evident as the EAL is taken from the CC.

Primary and Supporting SFRs

The objectives of the TOE, and the associated SFRs, can be separated into two groups:

1. Those that provide confidentiality, authenticity and integrity for packet flows transmitted and received by the TOE using IPSec (O.Authenticity, O.Confidentiality, O.Integrity, O.Key-Confidentiality, O.VLAN-Separation, O.Mediate, and O.NoReplay). These represent the PRIMARY security enforcing objectives of the TOE, and the associated primary SFRs are listed on the left of Table 18.
2. Those that ensure the TOE can be securely configured, operated and managed (O.Secure-Operation). This is a SUPPORTING objective, and the associated supporting SFRs are listed on the right of Table 18: Primary and supporting SFRs.

The supporting SFRs provide the ability to securely configure, operate and manage the primary SFRs. Therefore, the primary objectives (to protect packet flows) are indirectly provided by the supporting SFR's. Thus, the supporting SFRs provide mutual support for the primary SFRs, as the supporting SFRs help defend the primary SFRs against attacks aimed at defeating the primary SFRs by gaining access to the configuration, operation and management functions of the TOE.

Table 18 Primary and Supporting SFRs

Primary SFRs	Supporting SFRs
FCO_NRO.2, FCS_CKM.1(1) FCS_CKM.1(2), FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFC.1(3), FDP_IFF.1(1), FDP_IFF.1(2), FDP_IFF.1(3), FDP_UCT.1(1), FDP_UIT.1(1), FTP_ITC.1(1), FTP_RTC.1	FAU_GEN.1, FAU_SAR.1, FCS_COP.1(4), FCS_COP.1(5), FIA_UAU.2, FIA_UAU.5(1), FIA_UID.2, FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.2, FMT_MSA.3(1), FMT_MSA.3(2), FMT_MSA.3(3), FMT_MTD.1(1), FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1, FPT_AMT.1, FPT_RVM.1, FPT_SEP.1, FPT_STM.1, FPT_TST.1, FTA_TSE.1, FTP_ITC.1(2)

Help Prevent Bypassing of Other SFRs

FIA_UID.2 and FIA_UAU.2 support other functions that allow the user access to the assets by restricting the actions the user can take before being authorised. FIA_UAU.5(1) provides the authentication mechanisms to restrict the actions of the user.

The management functions FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MTD.1(1), and FMT_MTD.1(2) support all other SFRs by restricting the ability to change certain management functions to authorised users, ensuring other users cannot circumvent these SFRs.

FMT_MSA.2, FMT_MSA.3(1), FMT_MSA.3(2), and FMT_MSA.3(3) limit the acceptable values for secure data, protecting the SFRs dependent on those values from being bypassed.

FPT_AMT.1 and FPT_TST.1 provides for start up and user initiated testing to ensure the security functions are operational, thus preventing their bypass.

FPT_RVM.1 ensures that the TSF is always invoked and succeed before allowing other mediated actions to occur.

Help Prevent Tampering of Other SFRs

The cryptographic functions FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), and FCS_COP.1(3) provide for the secure generation, handling, destruction and operation of keys, and therefore support those SFRs that may rely on the use of those keys.

FDP_UIT.1(1) supports all other SFRs that deal with data by maintaining data integrity.

FDP_UCT.1(1) supports all other SFR's that deal with data by maintaining data confidentiality.

FIA_UID.2 and FIA_UAU.2 support other functions that allow the user access to the assets by restricting the actions the user can take before being authorised. FIA_UAU.5(1) provides the authentication mechanisms to restrict the actions of the user.FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MTD.1(1), FMT_MTD.1(2), and FMT_SMF.1 support all other SFRs by identifying management functions and restricting the ability to change certain management functions to authorised users, ensuring other users cannot tamper with these SFRs.

FMT_MSA.2, FMT_MSA.3(1), FMT_MSA.3(2), and FMT_MSA.3(3) limit the acceptable values for secure data, protecting the SFRs dependent on those values from being tampered with.

FPT_AMT.1 and FPT_TST.1 provides for start up and user initiated testing to ensure the security functions are operational, thus checking for tampering.

FPT_SEP.1 provides a separation of information streams traversing the TOE ensuring that the TSF has a domain of execution that is separate and cannot be violated by Unauthorized users.

Help Prevent De-activation of Other SFRs

The Information Flow Control policies detailed in FDP_IFF.1 (1), FDP_IFF.1 (2), and FDP_IFF.1 (3) along with the primary SFR's identified in Table 18: Primary and supporting SFRs, provide for rigorous control of allowed data flow, preventing Unauthorized deactivation of SFRs.

FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MTD.1(1), FMT_MTD.1(2), and FMT_SMF.1 support all other SFRs by identifying management functions and restricting the ability to change certain management functions to authorised users, ensuring other users cannot de-activate these SFRs.

FMT_MSA.2 FMT_MSA.3(1), FMT_MSA.3(2), and FMT_MSA.3(3) limit the acceptable values for secure data, protecting the SFRs dependent on those values from being de-activated.

FPT_AMT.1 and FPT_TST.1 provides for start up and user initiated testing to ensure the security functions are operational, thus checking for de-activation.

FIA_UID.2 and FIA_UAU.2 support other functions that allow the user access to the assets by restricting the actions the user can take before being authorized.

FTA_TSE.1 supports other functions by allowing the TOE to block the establishment of a user session.

Enable Detection of Misconfiguration or Attack of Other SFRs

FAU_GEN.1 and FAU_SAR.1 support other functions by providing logging functions that allow misconfiguration and attacks to be detected.

FPT_AMT.1 supports other functions by providing a reliable timestamp for logging messages.

Strength of Function Claims

It is not appropriate to make a Strength of Function claim for cryptographic algorithms as it is outside the scope of the Common Criteria, so the developers can make no claim of strength for the cryptographic algorithms. This addresses the explicit strength of function claims for the FCS class of SFR's, and also applies to the IT Security Functions IPSEC.1, IPSEC.2, and KEYMGT.1.

For SFR FIA_UAU.5(1) the strength of function claim is SOF-basic. A strength of function claim of SOF-basic is also made for IT Security Function IPSEC.1 (Xauth) and CONFIG.2.

Rationale for Security Functional Requirements of the IT Environment

Except for OE.VPN and OE.Secure-Management item d), all of the security objectives for the environment are met by non-IT measures.

The following rationale is provided to support security functional requirements that are met within the TOE environment.

FDP_UIT.1(2), FDP_UIT.1(2), FTP_ITC.1(3)

These requirements correspond to the TOE requirements FDP_UIT.1(1), FDP_UIT.1(1), FTP_ITC.1(1) and ensure the VPN peer provides a corresponding VPN security policy with the TOE to protect the IPSec VPN tunnel. These components trace back to and aids in meeting the following objective: OE.VPN.

Rationale for Explicitly Stated SFRs for the TOE

FTP_RTC.1 was created to correctly specify the TOE's use of a protected channel for remote administration. Per PD-0108, an explicit SFR based on FTP_ITC.1 is specified.

TOE Summary Specification Rationale

This section demonstrates the suitability of the security functions defined in section 6.1 of meeting the TOE's Security Functional Requirements identified in Section 5.1 and that the security functional requirements are completely and accurately met by the TOE's Security Functions identified in the IT Security Functions Section 6.1.

Table 19 demonstrates the correspondence between the Security Functions and the TOE Security Functional Requirements. With the demonstration of correspondence given below and the descriptions of the security functions given in Section 6.1 on how the security functions are providing the functionality to meet the security functional requirements this provides the evidence of suitability of the security functions in meeting the security functional requirements stated in Section 5.1.

The mutually supportive nature of the IT security functions can be derived from the mutually support of the SFRs (demonstrated in Section 8.2), as each of the security functions can be mapped to one or more SFRs, as demonstrated in Table 19: SFR to TSF Cross-Reference.

Suitability of TOE Security Functions to Meet Security Requirements

Table 19 SFR to TSF Cross-Reference

SFR \ TSF	IPSEC.1	IPSEC.2	IPSEC.3	PACKETFILTER.1	VLAN.1	CONFIG.1	CONFIG.2	CONFIG.3	KEYMGT.1	REMOTE.1	PROTECT.1
FAU_GEN.1						√					
FAU_SAR.1						√					
FCO_NRO.2		√									

Table 19 SFR to TSF Cross-Reference (continued)

SFR \ TSF	IPSEC.1	IPSEC.2	IPSEC.3	PACKETFILTER.1	VLAN.1	CONFIG.1	CONFIG.2	CONFIG.3	KEYMGT.1	REMOTE.1	PROTECT.1
FCS_CKM.1 (1)									√		
FCS_CKM.1 (2)	√										
FCS_CKM.4	√								√		
FCS_COP.1(1)		√									
FCS_COP.1(2)	√										
FCS_COP.1(3)										√	
FCS_COP.1(4)									√		
FCS_COP.1(5)									√		
FDP_IFC.1(1)			√	√							
FDP_IFC.1(2)					√						
FDP_IFC.1(3)				√							
FDP_IFF.1(1)			√	√							
FDP_IFF.1(2)					√						
FDP_IFF.1(3)				√							
FDP_UCT.1		√									
FDP_UIT.1		√									
FIA_UAU.2	√						√				
FIA_UAU.5(1)	√						√			√	
FIA_UID.2	√						√			√	
FMT_MOF.1							√				
FMT_MSA.1(1)	√	√	√				√				
FMT_MSA.1(2)					√		√				
FMT_MSA.1(3)				√			√				
FMT_MSA.2	√	√					√		√	√	
FMT_MSA.3(1)							√				
FMT_MSA.3(2)							√				

Table 19 SFR to TSF Cross-Reference (continued)

SFR \ TSF	IPSEC.1	IPSEC.2	IPSEC.3	PACKETFILTER.1	VLAN.1	CONFIG.1	CONFIG.2	CONFIG.3	KEYMGT.1	REMOTE.1	PROTECT.1
FMT_MSA.3(3)							√				
FMT_MTD.1(1)	√						√				
FMT_MTD.1(2)							√				
FMT_SMF.1						√	√				
FMT_SMR.1							√				
FPT_AMT.1							√				
FPT_RVM.1				√							
FPT_SEP.1											√
FPT_STM.1								√			
FPT_TST.1							√				
FTA_TSE.1				√							
FTP_ITC.1(1)	√	√	√								
FTP_ITC.1(2)	√						√				
FTP_RTC.1										√	

FIA_GEN.1

The SF CONFIG.1 satisfies this requirement by generating audit logs in accordance with the requirement.

FAU_SAR.1

The SF CONFIG.1 satisfies this requirement by enabling the ability for authorised users to review the audit logs.

FCO_NRO.2

The SF IPSEC.2 satisfies this requirement by supplying digital signatures on transmitted packets, with which proof of origin cannot be repudiated.

FCS_CKM.1 (1)

The SF KEYMGT.1 satisfies this requirement by providing a mechanism for generating 512 and 1024-bit RSA keys.

FCS_CKM.1 (2)

The SF IPSEC.1 satisfies this requirement by implementing the Diffie Hellman key agreement algorithm, to establish a shared secret over an unsecure communications channel. Diffie-Hellman is used within IKE to establish session keys. 768-bit (the default), 1024-bit, and 1536-bit Diffie-Hellman groups are supported.

FCS_CKM.4

The SF KEYMGT.1 and SF IPSEC.1 satisfies this requirement by supplying a mechanism for overwriting (destroying) cryptographic keys.

FCS_COP.1 (1)

The SF IPSEC.2 satisfies this requirement by providing a mechanism by which data within transmitted packets can be encrypted and decrypted.

FCS_COP.1 (2)

The SF IPSEC.1 satisfies this requirement by providing a mechanism by which transmitted packets can be digitally signed, and digital signatures can be verified.

FCS_COP.1 (3)

The SF REMOTE.1 satisfies this requirement by providing a mechanism by which remote administration packets can be encrypted and decrypted using SSH.

FCS_COP.1(4)

The SF KEYMGT.1 satisfies this requirement by providing the cryptographic mechanism for signing that supports the retrieval of digital certificates from a Certificate Authority (CA) using the Simple Certificate Enrollment Protocol (SCEP)l.

FCS_COP.1(5)

The SF KEYMGT.1 satisfies this requirement by providing the cryptographic mechanism for encryption/ decryption that supports the retrieval of digital certificates from a Certificate Authority (CA) using the Simple Certificate Enrollment Protocol (SCEP)

FDP_IFC.1(1)

The SF IPSEC.3 and SF PACKETFILTER.1 satisfy this requirement by examining each packet flow and applying the IPSec and packet filter information flow control policy to it.

FDP_IFC.1(2)

The SF VLAN.1 satisfies this requirement by examining each packet flow and applying the VLAN information flow control policy to it.

FDP_IFC.1(3)

The SF PACKETFILTER.1 satisfies this requirement by examining each packet flow and applying the packet filter information flow control policy to it.

FDP_IFF.1(1)

The SF IPSEC.3 and SF PACKETFILTER.1 satisfy this requirement by implementing the cryptographic maps function, which permits or deny a packet flow based on its source and destination IP address, and the packet filter function which is applied to router / switch interfaces to implements the information flow control SFP which defines the rules for packet filtering.

FDP_IFF.1(2)

The SF VLAN.1 satisfies this requirement by permitting or denying the packet flows based on the information found in the packet header and the applying the VLAN information flow control SFP which defines the rules for packet filtering.

FDP_IFF.1(3)

The SF PACKETFILTER.1 satisfies this requirement by permitting or denying the packet flows based on the information found in the packet header and the applying the packet filter information flow control SFP which defines the rules for packet filtering.

FDP_UCT.1(1)

The SF IPSEC.2 satisfies this requirement by providing ESP which encrypts an IP datagram providing confidentiality.

FDP_UIT.1(1)

The SF IPSEC.2 satisfies this requirement by providing ESP which signs an IP datagram providing integrity.

FIA_UAU.2

The SF CONFIG.2 satisfies this requirement by requiring users to undergo authentication before access to its management interfaces is granted. The SF IPSEC.1 satisfies this requirement by requiring device authentication and user authentication (for VPN clients) before the IPSec SA can be negotiated to establish a VPN connection.

FIA_UAU.5(1)

The SF CONFIG.2 satisfies this requirement by requiring a username and password for user authentication. The SF CONFIG.2 requires just an “enable” password for administrator authentication. SF REMOTE.1 satisfies this requirement by requiring the remote administrator to authenticate themselves as part of SSH. The SF IPSEC.1 satisfies this requirement by requiring device authentication and user authentication (for VPN clients) before the IPSec SA can be negotiated to establish a VPN connection.

FIA_UID.2

The SF CONFIG.2 satisfies this requirement by requiring users to undergo identification before access to its management interfaces is granted. SF REMOTE.1 satisfies this requirement by requiring the remote administrator to identify themselves as part of SSH. The SF IPSEC.1 satisfies this requirement by requiring device identification and user identification (for VPN clients) as part of authentication before the IPSec SA can be negotiated to establish a VPN connection.

FMT_MOF.1

The SF CONFIG.2 satisfies this requirement by allowing only the administrator the right to manage the functions that implement the IPSec, VLAN, and packet filtering information flow control SFPs and to optionally configure the use an external authentication server

FMT_MSA.1(1)

The SF CONFIG.2 satisfies this requirement by allowing only the administrator the right to manage the configuration (IPSec policy settings, IPSec configuration attributes and identity credentials) that implements the IPSec information flow control SFP. SF IPSEC.1, SF IPSEC.2, and SF IPSEC.3 implements the IPSec information flow control SFP based on the configuration parameters set by the administrator.

FMT_MSA.1(2)

The SF CONFIG.2 satisfies this requirement by allowing only the administrator the right to manage the configuration (VLAN policy settings) that implements the VLAN information flow control SFP. SF VLAN.1 implements the VLAN information flow control SFP based on the configuration parameters set by the administrator.

FMT_MSA.1(3)

The SF CONFIG.2 satisfies this requirement by allowing only the administrator the right to manage the configuration (packet filtering rules) that implements the packet filter information flow control SFP. SF PACKETFILTER.1 implements the packet filter information flow control SFP based on the configuration parameters set by the administrator.

FMT_MSA.2

The SFs IPSEC.1, IPSEC.2, KEYMGT.1, and REMOTE.1 satisfy this requirement by implementing the various cryptographic standards and RFCs to ensuring that only appropriate secure cryptographic attributes are used. SF CONFIG.2 ensures all cryptographic attributes provided by the authenticated administrator are valid.

FMT_MSA.3(1)

The SF CONFIG.2 satisfies this requirement by ensuring that restrictive default values are allocated to security attributes for the IPSec Information Flow Control SFP, and allowing the administrator to alter the values from the default.

FMT_MSA.3(2)

The SF CONFIG.2 satisfies this requirement by ensuring that restrictive default values are allocated to security attributes for the VLAN Information Flow Control SFP, and allowing the administrator to alter the values from the default.

FMT_MSA.3(3)

The SF CONFIG.2 satisfies this requirement by ensuring that restrictive default values are allocated to security attributes for the packet filter Information Flow Control SFP, and allowing the administrator to alter the values from the default.

FMT_MTD.1(2)

The SF CONFIG.2 satisfies this requirement by only allowing the administrator to alter the TSF configuration.

FMT_MTD.1(1)

The SF CONFIG.2 satisfies this requirement by only allowing the administrator to alter the Pre-Shared Keys. The Pre-Shared Keys are used by IPSEC.1 during the IKE negotiation.

FMT_SMF.1

The SFs CONFIG.1 and CONFIG.2 satisfy this requirement by listing the security functions for which administrators have the ability to access.

FMT_SMR.1

The SF CONFIG.2 satisfies this requirement by maintaining administrator and administrator roles and ensuring that a user is authenticated as an administrator before allowing them to authenticate as a administrator by using the “enable” password. The SF CONFIG.2 satisfies this requirement by maintaining VPN Client user role ensuring that a VPN Client user is authenticated before establishing a VPN connection.

FPT_AMT.1

The SF CONFIG.2 satisfies this requirement by initiating a suite of tests upon startup to ensure proper operation of the underlying abstract machine which underlies the TOE.

FPT_RVM.1

The SF PACKETFILTER.1 satisfies this requirement by ensuring that security enforcing functions are invoked and succeed before allowing any other mediated action to occur.

FPT_SEP.1

The SF PROTECT.1 satisfies this requirement by providing a separation of information streams traversing the TOE. All traffic arriving at a TOE interface is mediated by the TSF by the IPSec, VLAN, and Packet Filtering information flow policies. The domains of execution for the various processes are isolated and separated and cannot be violated by unauthorized users.

FPT_STM.1

The SF CONFIG.3 satisfies this requirement by monitoring the network time and using the timestamp in audit records.

FPT_TST.1

The SF CONFIG.2 satisfies this requirement by initiating a suite of tests upon startup to ensure proper operation of the TOE functions.

FTA_TSE.1

The SF PACKETFILTER.1 satisfies this requirement by examining each packet and discarding those which do not match the access control list it holds.

FTP_ITC.1(1)

The SFs IPSEC.1, IPSEC.2 and IPSEC.3 satisfy this requirement by authenticating IPSec peers using pre-shared keys, RSA keys or digital certificates and establishing a trusted channel (called Security Associations) for the communication of information with assured identification of end-points; using ESP on IP datagrams to provide confidentiality, authentication, integrity and non-repudiation of sender; and maintaining a cryptographic map or crypto profile which ensures that packet flow source, destination and transmission parameters are controlled.

FTP_ITC.1(2)

The SF IPSEC.1 and CONFIG.2 satisfy this requirement by requiring the remote VPN Client user to undergo authentication before a VPN tunnel is established or requiring the administrator to authenticate before performing any TSF-mediated actions. This requirement ensures that the TOE uses a trusted source external authentication server to provide authentication services if configured by the administrator.

FTP_RTC.1

The SF REMOTE.1 satisfies this requirement by ensuring a protected channel is provided for remote administration. This SF requires the use of SSH.

Appendix A - IPSec Operation

IPSec Standards

IPSec combines trusted security technologies into a complete system that provides confidentiality, integrity, and authenticity of IP packets.

These technologies include:

- Diffie-Hellman key exchange for deriving key material between SA peers
- Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties and avoid man-in-the-middle attacks
- Bulk encryption algorithms, such as 3DES and AES, for encrypting the data
- Keyed hash algorithms, such as HMAC, combined with traditional hash algorithms such as MD5 or SHA for providing packet authentication
- Digital certificates signed by a certificate authority to act as digital ID cards

IPSec itself is broken into two parts:

- The IP Security Protocol proper, which defines the information to add to an IP packet to enable confidentiality, integrity, and authenticity controls as well as defining how to encrypt the packet data. The TOE uses the IPSec Encapsulating Security Payload (ESP) in IPSec Tunnel mode.
- Internet Key Exchange (IKE), which negotiates the security association between two entities and exchanges key material. It is not necessary to use IKE, but manually configuring security associations is a difficult and manually intensive process. IKE should be used in most real-world applications to enable large-scale secure communications.

Figure 3 IPSec Tunnel Mode

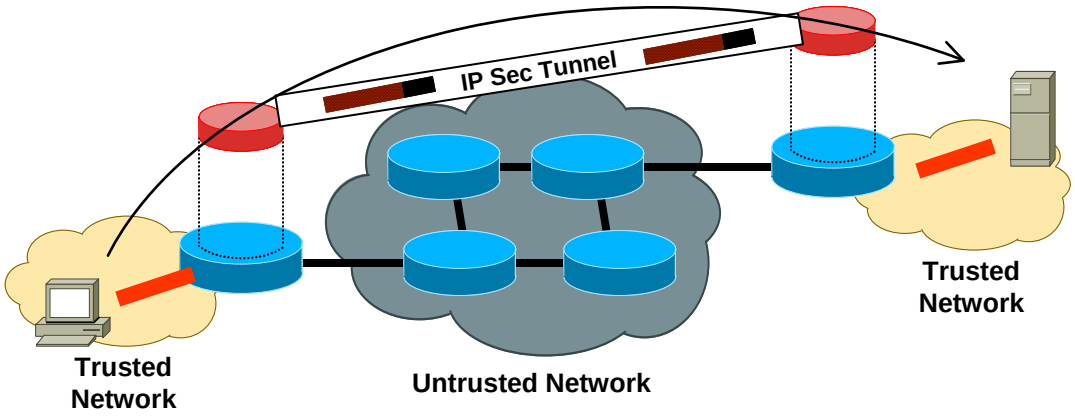
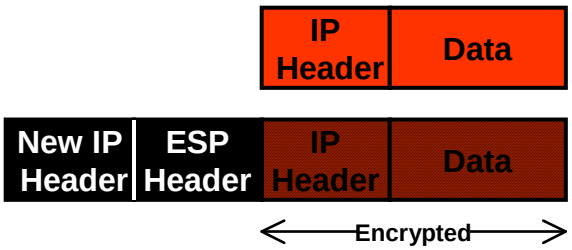


Figure 4 IPSec Encapsulating Security Payload



IPSec Security Associations

IPSec provides many options for performing network encryption and authentication. The TOE requires encryption, integrity and authentication. When the security service is determined, the two communicating nodes must determine exactly which algorithms to use (the TOE uses 3DES or AES for encryption; and SHA-1 for integrity). After deciding on the algorithms, the two devices must share session keys. The security association is the method that IPSec uses to track all the particulars concerning a given IPSec communication session. A Security Association (SA) is a relationship between two or more IPSec devices that describes how the entities will use security services to communicate securely.

An IPSec security association is unidirectional, meaning that for each pair of communicating IPSec devices there are at least two security connections - one from A to B and one from B to A. The security association is uniquely identified by a randomly chosen unique number called the security parameter index (SPI) and the destination IP address of the destination. When a system sends a packet that requires IPSec protection, it looks up the security association in its database, applies the specified processing, and then inserts the SPI from the security association into the IPSec header. When the IPSec peer receives the packet, it looks up the security association in its database by destination address and SPI and then processes the packet as required.

A special bi-directional SA, known as the IKE SA is used to establish and manage all IPSec SA's.

IPSec Operation

Authentication

IKE creates an authenticated, secure tunnel between two IPSec entities (e.g.. the TOE) called the IKE SA, which is then used to negotiate the security associations for IPSec used to protect the packet flow. This process requires that the two entities authenticate themselves to each other and establish shared keys. IKE supports multiple authentication methods. The two entities must agree on a common authentication protocol through a negotiation process. The following mechanisms are supported in the TOE:

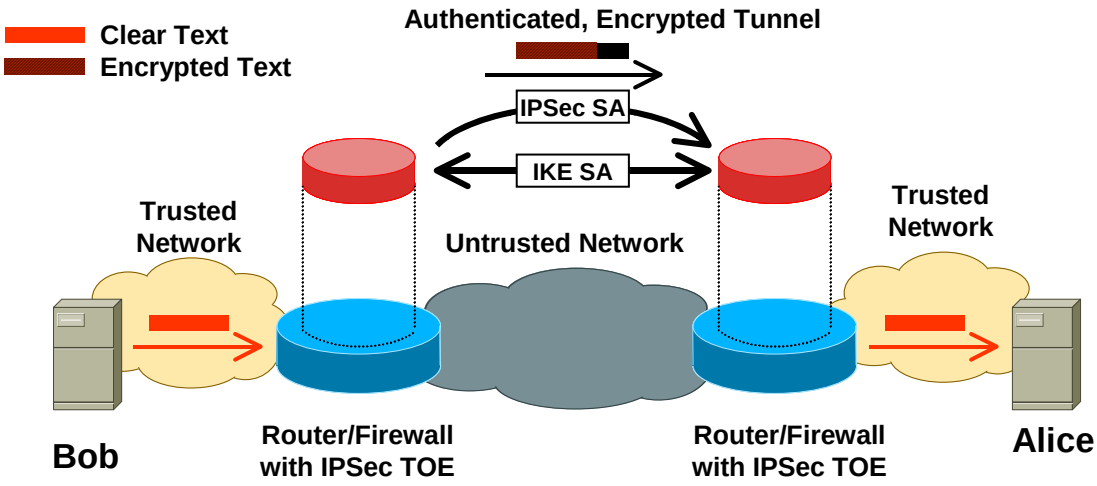
- Pre-shared key - The same key is pre-installed on each device. IKE peers authenticate each other by computing and sending a keyed hash of data that includes the preshared key. If the receiving peer is able to independently create the same hash using its preshared key, it knows that both parties must share the same secret, thus authenticating the other party
- Public key cryptography -Each party generates a pseudo-random number (a nonce) and encrypts it in the other party's public key. The ability for each party to compute a keyed hash containing the other peer's nonce, decrypted with the local private key as well as other publicly and privately available information, authenticates the parties to each other. This system provides for deniable transactions. That is, either side of the exchange can plausibly deny that it took part in the exchange. Currently only the RSA public key algorithm is supported
- Digital signature -Each device digitally signs a set of data and sends it to the other party. This method is similar to the previous one, except that it provides nonrepudiation. Currently both the RSA public key algorithm and the digital signature standard (DSS) are supported.

Key Exchange

Both parties must have a shared session key in order to encrypt the IKE tunnel. The Diffie-Hellman protocol is used to agree on a common session key. The exchange is authenticated as described above to guard against "man-in-the-middle" attacks.

These two steps, authentication and key exchange, create the IKE SA, a secure tunnel between the two devices. One side of the tunnel offers a set of algorithms, and the other side must then accept one of the offers or reject the entire connection. When the two sides have agreed on which algorithms to use, they must derive key material to use for IPSec with Authentication Headers (AH), ESP (Encapsulating Security Payload), or both together (the TOE uses ESP only). IPSec uses a different shared key than IKE. The IPSec shared key can be derived by using Diffie-Hellman again to ensure perfect forward secrecy, or by refreshing the shared secret derived from the original Diffie-Hellman exchange that generated the IKE SA by hashing it with pseudo-random numbers (nonces). The first method provides greater security but is slower. After this is complete, the IPSec SA is established and the packet flow is passed over the IPSec SA.

Figure 5 IPSec and IKE Operation



For example, in Figure 5, Bob is trying to securely communicate with Alice. Bob sends his data (IP packets) toward Alice. When Bob's internetworking device sees the packet, it checks its security policy and realizes that the packet should be encrypted. The preconfigured security policy also says that Alice's internetworking device will be the other endpoint of the IPSec tunnel.

Bob's internetworking device looks to see if it has an existing IPSec SA with Alice's internetworking device. If not, then it negotiates one using IKE. If the two internetworking devices already share an IKE SA, the IPSec SA can be quickly and immediately generated. If they do not share an IKE SA, one must first be created before negotiation of the IPSec SAs. As part of this process, the two internetworking devices exchange authentication credentials, e.g. digital certificates. A certificate authority that both Bob and Alice's internetworking devices trust must sign the certificates beforehand.

When the IKE session becomes active, the two internetworking devices can negotiate the IPSec SA. When the IPSec SA is set up, both internetworking devices will have agreed on an encryption algorithm (for example, 3DES) and an authentication algorithm (for example, SHA), and have a shared session key. Now, Bob's internetworking device can encrypt Bob's IP packet, place it into a new IPSec packet and send it to Alice's internetworking device. When Alice's internetworking device receives the IPSec packet, it looks up the IPSec SA, properly processes and unpacks the original datagram, and forwards it over to Alice. Note that this process is transparent to both Alice and Bob.

Appendix B - FIPS Conformance

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.

IOS-IPSec TOE Router Model	TOE IPSEC Hardware Acceleration Module	FIPS Certification Number	Pending Certification
c871	On Board	707	
c876	On Board	707	
c877	On Board	707	

IOS-IPSec TOE Router Model	TOE IPSEC Hardware Acceleration Module	FIPS Certification Number	Pending Certification
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		

IOS-IPSec TOE Router Model	TOE IPSEC Hardware Acceleration Module	FIPS Certification Number	Pending Certification
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		

Appendix C - 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, SEP, 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-X6704-10GE	X			
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	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-X6148A-45AF	X	X		

Name / Description	Ethernet	802.3af	Transceiver	XENPAK, SEP, or GBIC Line Card
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	

Cisco Catalyst 6500 and Cisco 7600 Modules Specifically Excluded from the TOE

- 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 / Cisco Catalyst 6500 Series WebVPN Services Module
- Cisco 7600 Series / Cisco Catalyst 6500 Series Anomaly Guard Module
- Cisco 7600 Series / Cisco Catalyst 6500 Series Traffic Anomaly Detector Module

Appendix D - ACL Options

Table 20 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.

Table 20 ACL Options Specifically tested for Common Criteria

ACL Option	Description
deny | permit	Denies or permits access if the conditions are matched.
Protocol	Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **nos**, **ospf**, **pim**, **tcp**, or **udp**, or 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 1's 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 1's 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 21 desribes additional options available for use with an access control list, but were not specifically tested for Common Criteria.

Table 21 ACL Options 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.

Table 21 ACL Options Not Specifically Tested for Common Criteria (continued)

ACL Option	Description
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.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html