CA Layer 7

SecureSpan SOA Gateway v8.0

Security Target

May 2014

LAYER 7
TECHNOLOGIES
a CA Technologies company

Document prepared by

CSC

BUSINESS SOLUTIONS
TECHNOLOGY
OUTSOURCING

Document History

Version	Date	Author	Description
1.0	29 January 2013	L Turner	Initial release for evaluation.
1.1	12 April 2013	L Turner	Update to address EDR001.
1.2	11 December 2013	L Turner	Update to address validator comments and re-branding.
1.3	13 December 2013	L Turner	Update FAU_SEL and add build numbers.
1.4	5 March 2014	L Turner	Update to address validator sync session comments.
1.5	14 April 2014	L Turner	Update to address validator comments – scope revised.
1.6	15 May 2014	L Turner	Update to address lab observations.
1.7	28 May 2014	L Turner	Release for publication.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Overview

1 The SecureSpan SOA Gateway is an enterprise security management solution that provides centralized management and access control over web services and related resources. The Gateway is designed to protect web services and mediate communications between Service Oriented Architecture (SOA) clients and endpoints residing in different identity, security, or middleware domains.

2 This Security Target (ST) defines the SecureSpan SOA Gateway v8.0 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

3 For a precise statement of the scope of incorporated security features, refer to section 2.3.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	CA Layer 7 SecureSpan SOA Gateway v8.0
Security Target	CA Layer 7 SecureSpan SOA Gateway v8.0 Security Target, v1.7

1.3 Conformance Claims

4 This ST supports the following conformance claims:

a) CC version 3.1 Release 3, July 2009

b) CC Part 2 extended

c) CC Part 3 conformant

d) Standard Protection Profile for Enterprise Security Management Policy Management, v1.4, 23 May 2012 (ESM Policy Manager PP)

e) Standard Protection Profile for Enterprise Security Management Access Control, v2.0, 22 February 2012 (ESM Access Control PP)

1.4 Terminology

Table 2: Terminology

Term	Definition
CA	Certificate Authority
CC	Common Criteria
DMZ	Demilitarized Zone
EAL	Evaluation Assurance Level
ESM	Enterprise Security Management

Term	Definition
FTP	File Transfer Protocol
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICAP	Internet Content Adaptation Protocol
Identity Provider	A user database (internal or external) within the context of the TOE.
JDBC	Java Database Connectivity
JMS	Java Message Service
LDAP	Lightweight Directory Access Protocol
MQ Native	Refers to MQ Native Queues that can be used by the Layer 7 Gateway to natively communicate with IBM WebSphere MQ message-oriented middleware.
NTP	Network Time Protocol
PKI	Public Key Infrastructure
PP	Protection Profile
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol. SOAP defines the message format used in web services requests.
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSF	TOE Security Functions
TOE	Target of Evaluation
UDDI	Universal Description, Discovery and Integration
URL	Universal Resource Locator
WSDL	Web Services Description Language
WS-Security	WS-Security (Web Services Security) is an extension to SOAP

Term	Definition
	to apply security to web services. The protocol specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats, such as SAML, Kerberos, and X.509. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security.
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language

2 TOE Description

2.1 Type and Usage

5 The TOE is an enterprise security management solution that provides centralized management and access control over SOAP web services. The TOE controls how SOAP web services are exposed to and accessed by external client applications.

6 The TOE is comprised of two main components for policy definition and policy consumption as follows:

a) **Policy Manager.** A GUI application that provides the user with the primary administrative interface to the Gateway. The Policy Manager is used to construct policies and administer the TOE.

b) **Gateway.** One or more hardware or virtual appliances that enforce policy assertions to control web services. Basic configuration is performed using the Gateway Configuration Utility – a menu based Command Line Interface (CLI). The Gateway consumes policies defined by the Policy Manager which also provides the primary administrative interface.

7 The Gateway interfaces with client-side applications that require communication with web services. Client systems send message requests intended for the web service to the Gateway. The Gateway then functions as a client-side proxy, enforcing access control decisions and applying necessary requirements such as identities, protocols, headers, and/or transformations to the message as required by the policy in use. Policies modified through the Policy Manager are automatically applied in real time by the Gateway to ensure that all subsequent messages conform to the updated policy.

8 In a typical network, the Gateway resides in the demilitarized zone (DMZ), shielding downstream services as it enforces policy assertions on incoming and outgoing messages. A typical TOE deployment is depicted in Figure 1.

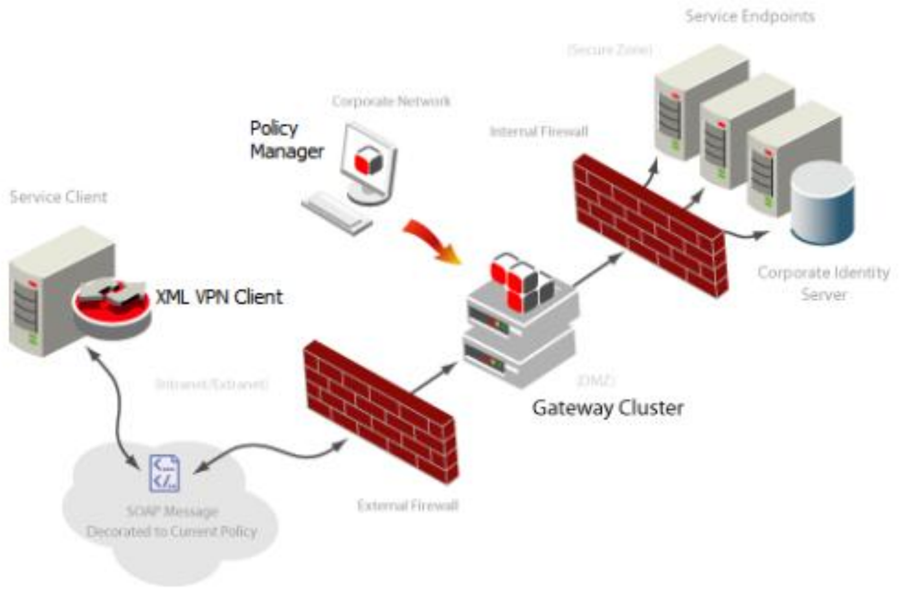

Figure 1: TOE deployment scenario

9 Figure 1 shows the following non-TOE components:

a) **Service client.** An external IT entity that accesses web services via the Gateway. Service clients do not log into the TOE.

b) **SecureSpan XML VPN Client.** A Layer 7 software product optionally deployed on the client side to enable secure and optimized communication between the Gateway and service clients.

c) **Firewalls.** Corporate firewalls providing traditional perimeter security.

d) **Service endpoints.** An internal IT entity that provides SOAP web services via the Gateway.

e) **Corporate identity server.** An internal IT entity that provides identity services – such as an LDAP directory.

2.2 Architecture

10 Endpoints and clients that communicate via the Gateway are Hypertext Transfer Protocol (HTTP), Java Message Service (JMS), File Transfer Protocol (FTP) or raw Transmission Control Protocol (TCP) socket accessible applications. Clients access the Gateway via a Universal Resource Locator (URL) queue or socket that is compatible with one of the above protocols. The Gateway functions as a reverse proxy for service requests and should be the single web service traffic enforcement point in a network.

11 Figure 2 below illustrates the architectural layers and deployment options of the Gateway component of the TOE –Standalone Gateway (dark blue), Basic Cluster Gateway (yellow), Extended Gateway Cluster (green excluding the load balancer), Each layer in Figure 2 below is described in the following sections. Figure 2 uses the abbreviation SSG to refer to the SecureSpan SOA Gateway. Figure 2 is not intended to illustrate TOE scope (refer to sections 2.5 and 2.6). The Policy Manager is not shown.

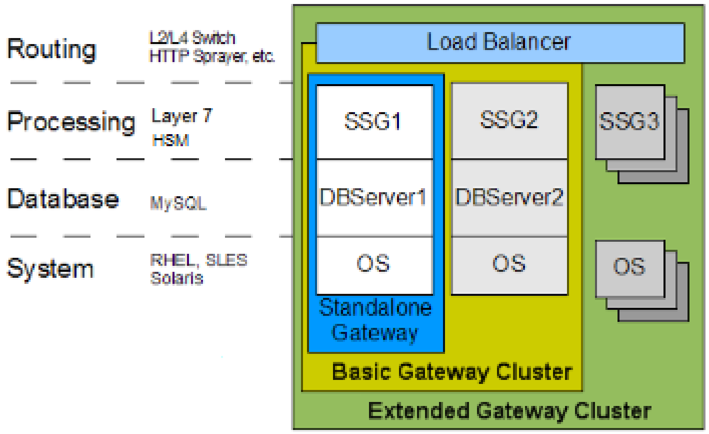

Figure 2: Gateway architecture

2.2.1 Routing Layer

12 External to the TOE, the Routing Layer represents an industry-standard load balancer configured to provide TCP-level load balancing and failover. It is not required for a standalone Gateway.

2.2.2 Processing Layer

13 The Processing Layer represents the Gateway's core runtime component. When a request message is received, the Gateway executes a service resolution process that attempts to identify the targeted destination service. When a published service is resolved, the Gateway executes the Policy Manager-configured policy for the service. If the policy assertions succeed, then the request is routed; if one or more policy assertions fail, then the request is either denied with a SOAP fault or the connection is dropped. In a Gateway cluster, systems that are installed with this runtime component are referred to as "Processing Nodes".

14 The Processing Layer may also involve the following components:

a) **Identity providers.** The Gateway uses identity providers to authenticate and identify users and groups when authenticating messages and administrative access. The Gateway can use its built-in identity provider (called the Internal Identity Provider or the Federated Identity Provider in an identity bridging scenario) or interface directly with any LDAP-based identity provider. **Note:** LDAP is not supported in the evaluated configuration.

b) **Trust store.** The Gateway maintains a trust store of certificates that do not belong to it but that are trusted and used for one or more vital security functions, such as signing client certificates. Certificates are imported into the Gateway trust store via the Policy Manager. The Gateway can be configured to perform revocation checking for certificates through Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP).

c) **UDDI.** The Gateway supports publishing of web services by using the Web Services Description Language (WSDL) located in a Universal Description, Discovery and Integration (UDDI) registry. **Note:** UDDI is not supported in the evaluated configuration.

d) **Logging and auditing functionality.** The Gateway provides several logging and auditing features, allowing users to monitor the activity and health of the Gateway, and the ongoing success or failure of service policy resolution. Auditing is provided for all system events, and is configurable for individual service policies. All audit records can be viewed through the Policy Manager. Gateway logging is performed during runtime, and those logs can also be viewed through the Policy Manager. The Manager also features a Dashboard that allows administrators to monitor activity through the Gateway in real-time.

e) **Hardware Security Module (HSM)** Optional hardware module for cryptographic operations. See section 2.3.2 below.

2.2.3 Database Layer

15 The Gateway stores policies, processing audits, Internal Identity Provider, keystore, configuration details and other information in a MySQL database. In a typical configuration this database will reside on the same physical system as a Processing Node, although in rare circumstances it may reside on a separate system.

16 In a Gateway cluster, systems that are installed with the database component are referred to as "Database Nodes". There will typically be two replicated Database Nodes in a cluster: Primary and Secondary. The Processing Nodes are configured to

communicate with one of the Database Nodes (normally the Primary) and then fail over to the Secondary Database Node should the Primary become unavailable.

2.2.4 System Layer

17 The System Layer represents the Operating System (Red Hat Enterprise Linux), Java Virtual Machine (Sun JDK) and hardware / virtual platform.

2.3 Evaluated Configuration

18 The following sections describe the high-level configuration of the TOE. Assurance gained from evaluation is only applicable to the configurations and components that are identified within. Detailed guidance for establishing the evaluated configuration is provided in the *CA Layer 7 SecureSpan SOA Gateway v8.0 Secure Installation Guide*.

2.3.1 Architecture

19 The evaluated configuration of the TOE reflects the following architectural decisions:

a) **Routing Layer.** The presence of a load balancer is determined by whether the TOE is deployed in a standalone or cluster configuration. Both standalone and cluster Gateway deployments are included in the evaluated configuration. The load balancer is not part of the TOE.

b) **Processing Layer**

   i) **Identity providers.** The evaluated configuration supports the Internal Identity Provider and Federated Identity Providers with an X.509 credential source. LDAP-based identity providers, Federated Identity Providers with SAML credential source and custom identity assertions are excluded from the evaluated configuration. The Internal Identity Provider is part of the TOE, Federated Identity Providers require an identity server to be present in the environment. In the evaluated configuration, TOE administrative users may only authenticate against the Internal Identity Provider.

   ii) **Trust store.** The Gateway is configured to perform revocation checking for certificates using either CRL or OCSP. The trust store is part of the TOE.

   iii) **UDDI**. UDDI functionality is not within the scope of the TOE.

   iv) **Logging and auditing.** The evaluated configuration includes logging to the internal database and/or an external Syslog server. The internal database is part of the TOE.

   v) **Hardware Security Module (HSM)** Optional hardware module for cryptographic operations. See section 2.3.2 below. HSMs are not part of the TOE but may be used in the evaluated configuration.

c) **Database Layer.** The MySQL database may reside on a Processing Node or Database node. The database is part of the TOE.

d) **System Layer.** In the evaluated configuration, the Gateway component of the TOE may be deployed on a hardware or virtual appliance however the hardware and virtualization layers are not part of the TOE.

2.3.2 Keystore & Cryptographic Operations

20 The TOE requires a keystore which may be implemented in a number of ways. The TOE does not provide its own internal cryptographic functionality but relies on third party software libraries or hardware modules to perform cryptographic operations for the TOE. Software cryptographic libraries are shipped with the TOE. All of the options below are included in the evaluated configuration (the cryptographic functions are provided by FIPS-140 validated modules):

i) **Software / internal DB.** This is a software keystore that is built into every Gateway database. Cryptographic operations provided by RSA BSAFE Crypto-J Toolkit (CMVP Certificate No. 1786).

ii) **PCI HSM.** Optional Thales nCipher nShield PCI HSM (CMVP Certificate No. 1742).

iii) **Network HSM.** Optional network-attached HSMs: SafeNet Luna SA (FIPS Certificate No. 1856/1857) or nCipher nShield (CMVP Certificate No. 1742).

iv) **Policy manager software cryptographic module.** Policy manager cryptographic operations are provided by RSA BSAFE Crypto-J Toolkit (CMVP Certificate No. 1786).

21 The evaluated configuration assumes that the TOE is configured to be in FIPS mode (*security.fips.enabled* – refer to the Miscellaneous Cluster Properties section of the *Policy Manager User Manual*).

2.3.3 Management

22 The SOA Gateway can be managed in by a number of different interfaces / applications. Only the Policy Manager application and Gateway Configuration Utility are included in the evaluated configuration.

23 The Policy Manager web interface and Enterprise Security Manager application are excluded from the evaluated configuration.

2.4 Security Functions

24 The following sections describe the security functions provided by the TOE (refer to section 6 for additional detail on each security function).

2.4.1 Access Control Policy Definition

25 The Policy Manager allows the TOE administrator to define detailed policies to enforce robust access control over web services. The following policy assertions are covered by the evaluation:

a) **Access control assertions.** The following subset of access control assertions are evaluated:

i) **Authenticate User or Group.** Require specified users and/or groups to be authenticated against a selected identity provider. Applies the credentials collected by a ‘require’ assertion listed below to authenticate a user or group specified in this ‘authenticate’ assertion.

ii) **Authenticate against Identity Provider.** Requires provided client credentials to be successfully authenticated against a selected identity provider. Applies the credentials collected by the ‘require’ assertions to be authenticated.

iii) **Require HTTP Basic** (**Note:** should be used in conjunction with Require SSL or TLS). Require that incoming requests to contain HTTP basic authentication credentials.

iv) **Require SAML Token Profile.** Requires incoming requests to contain a SAML (Security Assertions Markup Language) token. **Note:** The evaluated configuration defined in the *Secure Installation Guide* specifies a limited set of SAML attributes that may be used.

v) **Require SSL or TLS Transport with Client Authentication.** Requires clients to connect via SSL or TLS and optionally to provide a valid / trusted X.509 certificate.
Note: This assertion appears in two different assertion palettes:

- When accessed from the Access Control palette, this assertion is labeled "Require SSL or TLS Transport with Client Authentication" and has the Require Client Certificate Authentication check box selected by default.
- When accessed from the Transport Layer Security palette, this assertion is labeled "Require SSL or TLS Transport" and does not have the Require Client Certificate Authentication check box selected by default.

vi) **Require WS-Security Signature Credentials.** Requires that the web service target message includes an X.509 client certificate and has at least one element signed by that client certificate's private key as a proof of possession.
Note: The evaluated configuration defined in the *Secure Installation Guide* specifies a limited set of attributes that may be used with this assertion – multiple signatures are not supported.

b) **Service availability assertions.** The following subset of service availability assertions are evaluated:

i) **Limit Availability to Time/Days.** Enables restricting service access by a time and/or day interval. When the Gateway receives a request for the service, it will check the time and/or day restrictions before allowing the message to proceed.

ii) **Restrict Access to IP Address Range.** Enables restricting service access based on the IP address of the requesting service client.

c) **Policy logic assertions.** The following subset of policy logic assertions are evaluated in support of access control:

i) **All Assertions Must Evaluate to True.** All associated assertions must evaluate to true to achieve a ‘success outcome’.

ii) **At Least One Assertion Must Evaluate to True.** At least one associated assertion must evaluate to true to achieve a ‘success outcome’.

26 The Policy Manager can detect inconsistencies in the application of policies so that policies are unambiguously defined.

27 The Policy Manager uniquely identifies the policies it creates so that it can be used to determine what policies are being implemented by remote products.

2.4.2 Access Control Policy Enforcement

28 The Gateway enforces the policies defined by the Policy Manager. The Gateway inspects messages sent between service clients (request messages) and service endpoints (response messages) to evaluate and enforce compliance with the defined policies.

2.4.3 Policy Security

29 Communication between the Policy Manager and the Gateway is protected from disclosure and modification. A trusted channel is established to identify and authenticate each end point using TLS client / server authentication.

30 The Gateway validates the integrity of the policy data it receives and rejects any invalid or replayed data. The Gateway generates evidence of receipt of policies.

31 The TOE protects the integrity of policy, identity, credential, attribute, and other security information obtained from other trusted IT entities.

2.4.4 System Monitoring

32 The TOE provides the ability to keep an audit/log trail to provide administrative insight into system management and operation, including identifying what policies are being defined and enforced. The TOE is capable of sending audit/log information to an external trusted entity.

33 The following policy assertions are used in support of system monitoring:

a) **Audit Message in Policy.** Enables auditing of messages within a policy. It records events pertaining to the processing of a policy— e.g. assertion violations.

b) **Add Audit Detail.** Allows the definition of a custom message that can enhance the context of an audit message.

c) **Customize SOAP Fault Response.** Allows customization of the SOAP fault response on a policy-by-policy basis.

2.4.5 Robust Administrative Access

34 Administrative access to the TOE requires authentication and is governed by role based access control. The TOE protects against attacker attempts to illicitly authenticate using repeated guesses and enforces an administrator define password policy. The TOE displays a banner a login.

2.4.6 Continuity of Enforcement

35 The Gateway will continue policy enforcement in the event of a loss of connectivity with the Policy Manager.

2.5 Physical Scope

36 The TOE consists of the following components:

a) **Policy Manager (v8.0, Build: 4582).** The application software running on supported non-TOE operating systems.

b) **Gateway (v8.0, Build: 4582).** The software including operating system, Java Virtual Machine (JDK 7u40) and database executing on supported non-TOE hardware and virtual appliances. Firmware executing on the appliance hardware is excluded from the physical boundary.

37 The various TOE form factors are marketed as (Policy Manager software included):

a) **CA Layer 7 SecureSpan SOA Gateway Appliance.** Gateway ships on hardware.

b) **CA Layer 7 SecureSpan SOA Gateway Soft Appliance.** Gateway ships as a virtual appliance (ssg-appliance-8.0-5).

c) **CA Layer 7 SecureSpan SOA Gateway Software.** Gateway ships as software only for installation on client hardware (ssg-8.0-5).

2.5.1 Guidance Documents

38 The TOE includes the following guidance documents:

a) CA Layer 7 SecureSpan SOA Gateway v8.0 Installation and Maintenance Manual (Appliance Edition)

b) CA Layer 7 SecureSpan SOA Gateway v8.0 Secure Installation Guide
Note: This is the Common Criteria specific guidance document.

c) CA Layer 7 SecureSpan SOA Gateway v8.0 Policy Manager User Manual

d) CA Layer 7 SecureSpan SOA Gateway v8.0 Policy Authoring User Manual

2.5.2 Non-TOE Components

39 The Gateway appliance is available on the following platforms:

a) **Hardware appliance.** Oracle X4170 M3 Server or equivalent.

b) **Virtual appliance.** VMWare Workstation/ESXi/vSphere.

40 The Policy Manager application runs on the following Operating Systems, Java Virtual Machine and supporting hardware:

a) Red Hat Enterprise Linux 4 or later

b) Fedora Core 10 or later

c) Ubuntu 9 or later

d) SUSE Linux 10 or later

e) Microsoft Windows XP, 7 or Server 2008

f) Java Virtual Machine: JRE 7u40

41 The TOE operates with the following components in the environment:

a) **Federated Identity components.** When using a Federated Identity Provider, the following components must be present in the environment:

i) **Certificate Authority.** CA capable of signing X.509 certificates for use by service clients.

b) **Audit server.** The TOE can utilize Syslog servers to store audit records.

c) **Time server.** The TOE can utilize a Network Time Protocol (NTP) server to synchronize its system clock with a central time source.

d) **PKI server.** The TOE can make use of Public Key Infrastructure (PKI) related servers for X.509 certificate import, verification and revocation checking.

e) **Email server.** The TOE can periodically poll a POP or IMAP email server for SOAP messages to process.

f) **Hardware Security Module.** The TOE can utilize third-party HSMs for the keystore (see section 2.3.2 for supported HSMs).

g) **SecureSpan XML VPN Client.** A Layer 7 software product optionally deployed on the client side to enable secure and optimized communication between the Gateway and service clients. **Note:** This client has not been evaluated.

h) **Service clients.** IT entities that access web services via the Gateway. Service clients do not log into the TOE.

i) **Service endpoints.** IT entities that provide SOAP web services via the Gateway.

2.6 Logical Scope

2.6.1 Evaluated Features

42 The logical scope of the TOE comprises the security functions defined in section 2.4 based on the evaluated configuration specified in section 2.3.

43 Administrators should configure the TOE according to the *CA Layer 7 SecureSpan SOA Gateway v8.0 Secure Installation Guide* to establish the Common Criteria evaluated configuration.

2.6.2 Unevaluated Features

44 The following security related features have not been evaluated:

a) Gateway Appliance Firewall (IP Tables)

b) UDDI Registries

c) Policy Manager Audit Alerts

d) Security Zones

e) SFTP Polling Listeners

f) Working with SiteMinder

g) Use the Gateway as an HTTP Proxy

h) Salesforce Integration

i) Windows Domain Login

j) Gateway Backup and Restore

k) Gateway Patch Management

l) Mediation of access to non-SOAP web services

m) Authentication performed by Identity Providers – the evaluation ensures that the result of the authentication is enforced but does not evaluate the authentication itself as this can be performed by a variety of third party providers. In addition, the evaluated configuration does not include use of the following Identity Providers:

   i) LDAP Identity Providers

   ii) Federated Identity Provider using SAML credential source

n) Global Policy Fragments

2.6.3 Scope of Evaluated Policy Assertions

45 The core functionality of the SecureSpan SOA Gateway is its ability to define and enforce policies for web services. To achieve this, the SecureSpan SOA Gateway utilizes a policy assertion language. All available policy assertions are defined in the *Policy Authoring User Manual.* Not all policies are related to access control or security – in order to clarify the relationship between policy assertions and the scope of evaluation, the following table classifies each policy assertion as one of the following:

a) **Enforcing.** Assertions that enforce the TOE security policy and are the focus of this evaluation.

b) **Unevaluated Functional.** Assertions that facilitate product functionality and may be present in the evaluated configuration but that do not interfere with the security functions of the TOE. Such assertions have not been evaluated.

c) **Unevaluated Security.** Assertions that are security related but have not been evaluated.

Table 3: Scope of evaluated policy assertions

Assertion	**Enforcing**	**Unevaluated Functional**	**Unevaluated Security**
Access Control Assertions			
Authenticate User or Group Assertion	X		
Authenticate Against Identity Provider Assertion	X		
Require HTTP Basic Credentials Assertion	X		
Require SAML Token Profile Assertion	X		
Require SSL or TLS Transport Assertion with Client Authentication (same as Transport Layer Security assertion: Require SSL or TLS Transport Assertion)	X		
Authenticate Against SiteMinder Assertion			X
Authorize via SiteMinder Assertion			X
Check Protected Resource Against SiteMinder Assertion			X
Exchange Credentials using WS-Trust Assertion			X
Extract Attributes from Certificate Assertion			X
Extract Attributes for Authenticated User Assertion			X

Assertion	**Enforcing**	**Unevaluated Functional**	**Unevaluated Security**
Perform JDBC Query Assertion			X
Query LDAP Assertion			X
Require Encrypted Username Token Profile Credentials Assertion			X
Require FTP Credentials Assertion			X
Require HTTP Cookie Assertion			X
Require Remote Domain Identity Assertion			X
Require NTLM Authentication Credentials Assertion			X
Require SSH Credentials Assertion			X
Require Windows Integrated Authentication Credentials Assertion			X
Require WS-Secure Conversation Assertion			X
Require WS-Security Kerberos Token Profile Credentials Assertion			X
Require WS-Security Password Digest Credentials Assertion			X
Require WS-Security Signature Credentials Assertion	X		
Require WS-Security UsernameToken Profile Credentials Assertion			X
Require XPath Credentials Assertion			X
Retrieve Credentials from Context Variable Assertion			X
Retrieve Kerberos Authentication Credentials Assertion			X
Retrieve SAML Browser Artifact Assertion			X
Use WS-Federation Credential Assertion			X
Transport Layer Security Assertions			
Require SSL or TLS Transport (same as Access Control assertion: Require SSL or TLS Transport Assertion with Client Authentication)	X		
XML Security Assertions			X
Message Validation / Transformation Assertions		X	

Assertion	**Enforcing**	**Unevaluated Functional**	**Unevaluated Security**
Message Routing Assertions			
Add Header Assertion		X	
Configure Message Streaming Assertion		X	
Copy Request Message to Response Assertion		X	
Execute Salesforce Operation		X	
Return Template Response to Requestor Assertion		X	
Route via FTP(S) Assertion – Configured with FTP		X	
Route via FTP(S) Assertion – Configured with FTPS			X
Route via HTTP(S) Assertion – Configured with HTTP		X	
Route via HTTP(S) Assertion – Configured with HTTPS			X
Route via JMS Assertion		X	
Route via MQ Native Assertion		X	
Route via Raw TCP Assertion		X	
Route via SecureSpan Bridge Assertion			X
Route via SSH2 Assertion			X
Service Availability Assertions			
Limit Availability to Time/Days Assertion	X		
Restrict Access to IP Address Range Assertion	X		
Apply Rate Limit Assertion		X	
Apply Throughput Quota Assertion		X	
Look Up in Cache Assertion		X	
Query Rate Limit Assertion		X	
Query Throughput Quota Assertion		X	

Assertion	Enforcing	Unevaluated Functional	Unevaluated Security
Resolve Service Assertion		X	
Store to Cache Assertion		X	
Logging, Auditing, and Alerts Assertions			
Add Audit Detail Assertion	X		
Audit Messages in Policy Assertion	X		
Capture Identity of Requestor Assertion		X	
Customize Error Response Assertion		X	
Customize SOAP Fault Response Assertion	X		
Send Email Alert Assertion			X
Send SNMP Trap Assertion		X	
Policy Logic Assertions			
Add Comment to Policy Assertion		X	
All Assertions Must Evaluate to True Assertion	X		
At Least One Assertion Must Evaluate to True Assertion	X		
Compare Expression Assertion			X
Continue Processing Assertion			X
Create Routing Strategy Assertion			X
Execute Routing Strategy Assertion			X
Export Variables from Fragment Assertion			X
Generate UUID Assertion			X
Include Policy Fragment Assertion			X
Join Variable Assertion			X
Look Up Context Variable			X

Assertion	**Enforcing**	**Unevaluated Functional**	**Unevaluated Security**
Look Up Item by Value Assertion			X
Look Up Item by Index Position Assertion			X
Manipulate Multivalued Variable Assertion			X
Map Value Assertion			X
Process Routing Strategy Result Assertion			X
Run All Assertions Concurrently Assertion			X
Run Assertions for Each Item Assertion			X
Set Context Variable Assertion			X
Split Variable Assertion			X
Stop Processing Assertion			X
Threat Protection Assertions			X
Internal Assertions		X	
Custom Assertions			X

3 Security Problem Definition

3.1 Threats

46 Table 4 identifies the threats drawn from the ESM Policy Manager PP.

Table 4: Threats (ESM Policy Manager PP)

Identifier	**Description**
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.CONDTRADICT	A careless administrator may create a policy that contains contradictory rules for access control enforcement.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FORGE	A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product.
T.UNAUTH	A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly utilize the TOE's management functions.
T.WEAKPOL	A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate robust access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.
T.WEAKIA	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.

47 Table 5 identifies the threats drawn from the ESM Access Control PP.

Table 5: Threats (ESM Access Control PP)

Identifier	**Description**
T.DISABLE	A malicious user or careless user may suspend or terminate the TOE's operation, thus making it unable to enforce its access controls upon the environment or TOE-protected data.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FALSIFY	A malicious user can falsify the TOE's identity, giving the Policy Management product false assurance that the TOE is enforcing a policy.
T.FORGE	A malicious user may create a false policy and send it to the TOE to

Identifier	Description
	consume, adversely altering its behavior.
T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.NOROUTE	A malicious or careless user may cause the TOE to lose connection to the source of its enforcement policies, adversely affecting access control behaviors.
T.OFLOWS	A malicious user may attempt to provide incorrect Policy Management data to the TOE in order to alter its access control policy enforcement behavior.
T.UNAUTH	A malicious or careless user may access an object in the Operational Environment that causes disclosure of sensitive data or adversely affects the behavior of a system.

3.2 Organizational Security Policies

48 Table 6 identifies the Organizational Security Policies (OSPs) drawn from the ESM Policy Manager PP.

Table 6: OSPs (ESM Policy Manager PP)

Identifier	Description
P.BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

49 Table 7 identifies the OSPs drawn from the ESM Access Control PP.

Table 7: OSPs (ESM Access Control PP)

Identifier	Description
P.UPDATEPOL	The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.

3.3 Assumptions

50 Table 8 identifies the assumptions drawn from the ESM Policy Manager PP.

Table 8: Assumptions (ESM Policy Manager PP)

Identifier	Description
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.USERID	The TOE will receive identity data from the Operational Environment.

Identifier	Description
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.

51 Table 9 identifies the assumptions drawn from the ESM Access Control PP.

Table 9: Assumptions (ESM Access Control PP)

Identifier	Description
A.AUDIT	A protected repository will exist in the Operational Environment to which audit data can be written.
A.POLICY*	The TOE will receive policy data from the Operational Environment.
A.USERID	The TOE will receive validated identity data from the Operational Environment.
A.TIMESTAMP	The TOE will receive a reliable timestamp from the Operational Environment.
A.INSTAL	There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.

52 ***Note:** The assumption A.POLICY is included for PP conformance; however, it is addressed by the requirements of the ESM Policy Manager PP – see security objective O.POLICY. The Policy Manager provides policy data.

4 Security Objectives

4.1 Objectives for the Operational Environment

53 Table 10 identifies the objectives for the operational environment drawn from the ESM Policy Manager PP.

Table 10: Operational environment objectives (ESM Policy Manager PP)

Identifier	Description
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.
OE.AUDIT	The Operational Environment will provide a remote location for storage of audit data.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a secure manner.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PROTECT*	One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.
OE.USERID	The Operational Environment must be able to identify a user requesting access to the TOE.

54 ***Note:** OE.PROTECT is included for PP conformance; however, it is addressed by the requirements of the ESM Access Control PP. The Gateway performs the ESM Access Control functions.

55 Table 11 identifies the objectives for the operational environment drawn from the ESM Access Control PP.

Table 11: Operational environment objectives (ESM Access Control PP)

Identifier	Description
OE.AUDIT	The Operational Environment will provide a remote location for storage of audit data.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
OE.POLICY*	The Operational Environment will provide a policy that the TOE will enforce.
OE.PROTECT	The Operational Environment will protect the TOE from unauthorized modifications and access to its functions and data.

Identifier	Description
OE.USERID	The Operational Environment must be able to identify the user and convey validation of this to the TOE.
OE.TIME	The Operational Environment must provide a reliable timestamp to the TOE.

56 ***Note:** The environmental objective OE.POLICY is included for PP conformance; however, it is addressed by the requirements of the ESM Policy Manager PP – see security objective O.POLICY. The Policy Manager provides policy data.

4.2 Objectives for the TOE

57 Table 12 identifies the security objectives for the TOE drawn from the ESM Policy Manager PP.

Table 12: Security objectives (ESM Policy Manager PP)

Identifier	Description
O.ACCESSID	The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.
O.AUDIT	The TOE will provide measures for generating security relevant events that will detect access attempts to TOE-protected resources by users.
O.AUTH	The TOE will provide a mechanism to examine human and IT entity user identity data received from the Operational Environment and determine the extent to which the claimed identity should be able to perform TSF management functions.
O.BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.CONSISTENT	The TSF will provide a mechanism to identify and rectify contradictory policy data.
O.DISTRIB	The TOE will provide the ability to distribute policies to trusted IT products using secure channels.
O.MANAGE	The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.
O.EAVES	The TOE will either leverage a third-party cryptographic suite or contain the ability to utilize cryptographic algorithms to secure the communication channels to and from itself.
O.INTEGRITY	The TOE will contain the ability to assert the integrity of policy data.
O.POLICY	The TOE will provide the ability to generate policies that are sufficiently detailed to satisfy the Data Protection requirements for one or more technology types in the Standard Protection Profile for Enterprise Security Management Access Control.

Identifier	Description
O.ROBUST	The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
O.SELFID	The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.

58 Table 13 identifies the security objectives for the TOE drawn from the ESM Policy Manager PP.

Table 13: Security objectives (ESM Access Control PP)

Identifier	Description
O.MONITOR	The TOE will monitor the behavior of itself for anomalous activity (e.g., provide measures for generating security relevant events that will detect access attempts to TOE-protected resources by users).
O.DATAPROT	The TOE will protect data from unauthorized modification by enforcing an access control policy produced by a Policy Management product.
O.INTEGRITY	The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components using secure hash algorithms in hashing and keyed message authentication modes.
O.RESILIENT	If the TOE mediates actions performed by a user against resources on an operating system, the system administrator or user shall not be allowed to perform an operation in the Operational Environment that would disable or otherwise modify the behavior of the TOE.
O.MAINTAIN	The TOE will be capable of maintaining policy enforcement if disconnected from the Policy Management product.
O.OFLOWS	The TOE will be able to recognize and discard invalid or malicious input provided by users.
O.SELFID	The TOE will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival.
O.MNGRID	The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.

5 Security Requirements

5.1 Conventions

59 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

5.2 Extended Components Definition

60 Table 14 identifies the extended components which are incorporated into this ST. All extended components are reproduced directly from the Protection Profiles to which this ST claims conformance and therefore no further definition is provided in this document.

Table 14: Extended Components

Component	Title	Source
ESM_ACD.1	Access Control Policy Definition	ESM Policy Manager PP
ESM_ACT.1	Access Control Policy Transmission	ESM Policy Manager PP
ESM_ATD.1	Object Attribute Definition	ESM Policy Manager PP
ESM_ATD.2	Subject Attribute Definition	ESM Policy Manager PP
FAU_SEL_EXT.1	External Selective Audit	ESM Policy Manager PP
FAU_STG_EXT.1	External Audit Trail Storage	ESM Policy Manager PP ESM Access Control PP
FMT_MOF_EXT.1	External Management of Functions Behavior	ESM Policy Manager PP
FMT_MSA_EXT.5	Consistent Security Attributes	ESM Policy Manager PP
FTA_SSL_EXT.1	TSF-initiated session locking	ESM Policy Manager PP
FPT_FLS_EXT.1	Failure of Communications	ESM Access Control PP

5.3 Functional Requirements

Table 15: Summary of SFRs

Requirement	Title	Source
ESM_ACD.1	Access Control Policy Definition	ESM Policy Manager PP
ESM_ACT.1	Access Control Policy Transmission	ESM Policy Manager PP
ESM_ATD.1	Object attribute definition	ESM Policy Manager PP
ESM_ATD.2	Subject attribute definition	ESM Policy Manager PP
FAU_GEN.1	Audit Data Generation	ESM Policy Manager PP ESM Access Control PP
FAU_SEL.1	Selective Audit	ESM Access Control PP
FAU_STG.1	Protected Audit Trail Storage (Local Storage)	ESM Access Control PP
FAU_SEL_EXT.1	External Selective Audit	ESM Policy Manager PP
FAU_STG_EXT.1	External Audit Trail Storage	ESM Policy Manager PP ESM Access Control PP
FCO_NRR.2	Enforced Proof of Receipt	ESM Access Control PP
FDP_ACC.1	Access Control Policy	ESM Access Control PP
FDP_ACF.1	Access Control Functions	ESM Access Control PP
FIA_AFL.1	Authentication Failure Handling	ESM Policy Manager PP
FIA_SOS.1	Verification of Secrets	ESM Policy Manager PP
FIA_UAU.2	User Authentication Before Any Action	ESM Policy Manager PP
FIA_UID.2	User Identification Before Any Action	ESM Policy Manager PP
FIA_USB.1	User-Subject Binding	ESM Policy Manager PP
FMT_MOF.1(1)	Management of Functions Behavior	ESM Access Control PP
FMT_MOF.1(2)	Management of Functions Behavior	ESM Access Control PP
FMT_MOF_EXT.1	External Management of Functions Behavior	ESM Policy Manager PP
FMT_MSA.1(1)	Management of Security Attributes (internal attributes)	ESM Policy Manager PP

Requirement	Title	Source
FMT_MSA.1(2)	Management of Security Attributes (external attributes)	ESM Policy Manager PP ESM Access Control PP
FMT_MSA.3	Static Attribute Initialization	ESM Policy Manager PP ESM Access Control PP
FMT_MSA_EXT.5	Consistent Security Attributes	ESM Policy Manager PP
FMT_SMF.1	Specification of Management Functions	ESM Policy Manager PP ESM Access Control PP
FMT_SMR.1	Security Management Roles	ESM Policy Manager PP ESM Access Control PP
FPT_FLS_EXT.1	Failure of Communications	ESM Access Control PP
FPT_RPL.1	Replay Detection	ESM Access Control PP
FPT_STM.1	Reliable Time Stamps	ESM Policy Manager PP
FRU_FLT.1	Degraded Fault Tolerance	ESM Access Control PP
FTA_SSL_EXT.1	TSF-initiated Session Locking and Termination	ESM Policy Manager PP
FTA_SSL.4	User-initiated termination	ESM Policy Manager PP ESM Access Control PP
FTA_TAB.1	TOE Access Banner	ESM Policy Manager PP
FTP_ITC.1(1)	Inter-TSF Trusted Channel (prevention of disclosure)	ESM Policy Manager PP ESM Access Control PP
FTP_ITC.1(2)	Inter-TSF Trusted Channel (detection of modification)	ESM Policy Manager PP ESM Access Control PP
FTP_TRP.1	Trusted Path	ESM Policy Manager PP

5.3.1 Enterprise Security Management (ESM)

ESM_ACD.1 Access Control Policy Definition

Hierarchical to: No other components.

ESM_ACD.1.1 The TSF shall provide the ability to define access control policies for consumption by one or more compatible Access Control products.

ESM_ACD.1.2 Access control policies defined by the TSF must be capable of containing the following:

a) Subjects:
   - *Service Clients (Source: Identity Provider)* and

b) Objects:
   - *SOAP Web Services (Source: TOE Published Services)*; and

c) Operations:
   - *Service Request (Source: Service Client)*

d) Attributes:
   - *Access Control assertion attributes:*
     - *Authentication Credentials (Source: Service Client via Service Request)*
     - *User/Group (Source: Identity Provider)*
   - *Service Availability assertion attributes:*
     - *Context attributes – time or day (Source: the Gateway)*
     - *Source IP address (Source: Service Client via Service Request)*

ESM_ACD.1.3 The TSF shall associate unique identifying information with each policy.

Dependencies: No dependencies

Application Note: The Policy Manager defines access control policies for consumption by the Gateway.

ESM_ACT.1 Access Control Policy Transmission

Hierarchical to: No other components.

ESM_ACT.1.1 The TSF shall transmit policies to compatible and authorized Access Control products under the following circumstances: immediately following creation of a new or updated policy, *no other circumstances*.

Dependencies: ESM_ACD.1 Access control policy definition

ESM_ATD.1 Object attribute definition

Hierarchical to: No other components.

ESM_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual objects:

- Object: SOAP *Web Services:*
  - Attributes: *Associated policy assertions*

ESM_ATD.1.2 The TSF shall be able to associate security attributes with individual objects.

Dependencies: No dependencies.

ESM_ATD.2 Subject attribute definition

Hierarchical to: No other components.

ESM_ATD.2.1 The TSF shall maintain the following list of security attributes belonging to individual subjects:

- Subject: *Service Clients*
  - Attributes: *Authentication Credentials, User/Group*

ESM_ATD.2.2 The TSF shall be able to associate security attributes with individual subjects.

Dependencies: No dependencies.

5.3.2 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions; *and*

b) All auditable events identified in Table 16 for the not specified level of audit; and

c) *No additional events.*

FAU_GEN.1.2 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 (if applicable), and 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 16*.

Dependencies: FPT_STM.1 Reliable time stamps

Table 16: Auditable events

Component	Event	Additional Information
ESM_ACD.1	Creation or modification of policy	Unique policy identifier
ESM_ACT.1	Transmission of policy to Access Control products	Destination of policy
ESM_ATD.1	Definition of object attributes.	Identification of the attribute defined.

Component	Event	Additional Information
ESM_ATD.1	Association of attributes with objects.	Identification of the object and the attribute.
ESM_ATD.2	Definition of subject attributes.	Identification of the attribute defined.
ESM_ATD.2	Association of attributes with subjects.	Identification of the subject and the attribute.
FAU_SEL.1	All modifications to audit configuration	None
FAU_SEL_EXT.1	All modifications to audit configuration	None
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
FCO_NRR.2	The invocation of the non-repudiation service	Identification of the information, the destination, and a copy of the evidence provided
FDP_ACC.1	Any changes to the enforced policy or policies	Identification of Policy Management product making the change
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP	Subject identity, object identity, requested operation
FIA_AFL.1	The reaching of an unsuccessful authentication attempt threshold, the actions taken when the threshold is reached, and any actions taken to restore the normal state.	Action taken when threshold is reached
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret	None
FIA_SOS.1	Identification of any changes to the defined quality metrics	The change made to the quality metric
FIA_UAU.2	All use of the authentication mechanism	None
FIA_UID.2	All use of the identification mechanism	Provided user identity

Component	Event	Additional Information
FIA_USB.1	Successful and unsuccessful binding of user attributes to a subject	None
FMT_MOF.1	All modifications to TSF behavior	None
FMT_MSA.1	All modifications of security attributes	None
FMT_MSA.3	All modifications of the initial values of security attributes	Attribute modified, modified value
FMT_SMF.1	Use of the management functions	Management function performed
FMT_SMR.1	Modifications to the members of the management roles	None
FPT_FLS_EXT.1	Failure of communication between the TOE and Policy Management product	Identity of the Policy Management product, Reason for the failure
FPT_RPL.1	Detection of replay	Action to be taken based on the specific actions
FTP_ITC.1(1)	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_ITC.1(2)	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available

FAU_SEL.1 Selective Audit

Hierarchical to: No other components.

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) event type; and

b) *no additional attributes.*

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

Application Note: The selective audit capability is exercised by the Policy Manager, not by a user directly accessing the Gateway.

FAU_SEL_EXT.1 External selective audit

Hierarchical to: No other components.

FAU_SEL_EXT.1.1 The TSF shall be able to select the set of events to be audited by an ESM Access Control product from the set of all auditable events based on the following attributes:

a) event type; and

b) *no additional attributes.*

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

Application Note: The external selective audit capability is exercised by the Policy Manager, not by a user directly accessing the Gateway.

FAU_STG.1 Protected Audit Trail Storage (Local Storage)

Hierarchical to: No other components.

FAU_STG.1.1 The TSF shall protect *200 mb* locally stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG_EXT.1 External audit trail storage

Hierarchical to: No other components.

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to *a Syslog server and/or TOE-internal storage*.

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

a) protects the stored audit records in the TOE-internal audit trail from unauthorised deletion; and

b) prevent unauthorised modifications to the stored audit records in the TOE-internal audit trail.

Dependencies: FAU_GEN.1 Audit data generation
FTP_ITC.1 Inter-TSF Trusted Channel

5.3.3 Class FCO: Communication

FCO_NRR.2 Enforced proof of receipt

Hierarchical to: FCO_NRR.1 Selective proof of receipt

FCO_NRR.2.1 The TSF shall enforce the generation of evidence of receipt for received *policies* at all times.

FCO_NRR.2.2 The TSF shall be able to relate the *software name, version*, *node, time, policy update message, user, source IP* of the originator of the information, and the *stored internal data identifying allowable Policy Management products* of the information to which the evidence applies.

FCO_NRR.2.3 The TSF shall provide a capability to verify the evidence of receipt of information to *the Policy Management product* given *30 seconds*.

Dependencies: FIA_UID.1 Timing of identification

5.3.4 FCS: Cryptographic Support

61 The TOE utilizes third-party cryptographic suites and therefore does not claim any of the optional cryptographic SFRs per guidance at Annex C.4 of the ESM Policy Manager PP and Annex C.3 of the Access Control PP.

5.3.5 Class FDP: User Data Protection

FDP_ACC.1 Access Control Policy

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the *access control Security Function Policy (SFP)* on

- Subjects: *Service Clients (on behalf of users)*
- Objects: SOAP *Web Services*; and
- Operations: *Service Request*

Dependencies: FDP_ACF.1 Security attribute based access control

Application note: The Gateway enforces the access control SFP.

FDP_ACF.1 Access Control Functions

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the *access control SFP* to objects based on the following: *all operations between users and objects based upon the attributes defined in ESM_ACD.1*.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *rules received from the Policy Manager.*

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *no additional rules*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *if a requested object is not explicitly allowed by policy, then the access to the requested object is denied by default*.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

5.3.6 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within *a range of 1 and 20* unsuccessful authentication attempts occur related to *login at the Policy Manager*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall *lock the account for an administrator defined period of time*.

Dependencies: FIA_UAU.1 Timing of authentication

Application note: This requirement relates only to the Policy Manager component of the TOE as the SFR is drawn from the ESM Policy Manager PP.

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet the following:

a) For password-based authentication, the following rules apply:

1. Passwords shall be able to be composed of a subset of the following character sets: *all printable ASCII characters* that include the following values *26 uppercase letters, 26 lowercase letters, 10 numbers, and 10 special characters "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"*. ; and

2. Minimum password length shall settable by an administrator, and support passwords of 16 characters or greater; and

3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and

4. Passwords shall have a maximum lifetime, configurable by an administrator; and

5. New passwords must contain a minimum of an administrator-specified number of character changes from the previous password; and

6. Passwords must not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based authentication, the following rules apply:

1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2-20.

Dependencies: No dependencies.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: *username*, *role*.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

- *The TSF determines the username from the credentials presented for authentication.*
- *The TSF associates the role with the corresponding username*

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *Once a user’s session is established, the security attributes associated with a subject acting on behalf of a user cannot be changed for the duration of that user’s session.*

Dependencies: FIA_ATD.1 User attribute definition

Application note: This requirement refers to TOE administrative users.

5.3.7 Class FMT: Security Management

FMT_MOF.1(1) Management of Functions Behavior

Hierarchical to: No other components.

FMT_MOF.1.1(1) The TSF shall restrict the ability to query the behavior of, modify the behaviour of the functions: *audited events, repository for remote audit storage, Access Control SFP, policy being implemented by the TSF, Access Control SFP behavior to enforce in the event of communications outage*, *no other functions* to *an authorized and compatible Policy Management product.*

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF.1(2) Management of Functions Behavior

Hierarchical to: No other components.

FMT_MOF.1.1(2) The TSF shall restrict the ability to query the behaviour of the functions: *policy being implemented by the TSF*, *no other functions* to *an authorized and compatible Enterprise Security Management product.*

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF_EXT.1 External management of functions behavior

Hierarchical to: No other components.

FMT_MOF_EXT.1.1 The TSF shall restrict the ability to query the behavior of, modify the functions of Access Control products*: audited events, repository for remote audit storage, Access Control SFP, policy version being implemented, Access Control SFP behavior to enforce in the event of communications outage*, *Gateway configuration* to **the roles** *Administrator (query and modify), Operator (query only)*.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Application note: The TOE supports numerous roles (refer to Table 17) of which the Administrator and Operator are the superset.

FMT_MSA.1(1) Management of security attributes (internal attributes)

Hierarchical to: No other components.

FMT_MSA.1.1(1) The TSF shall restrict the ability to *perform the operations in Table 17 on* the security attributes *listed in Table 17* to *the roles in Table 17*.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1(2) Management of security attributes (external attributes)

FMT_MSA.1.1(2) The TSF shall restrict the ability to *perform the operations in Table 17 on* the security attributes *listed in Table 17* to *the roles in Table 17*.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

Table 17: Roles and permissions

Role	Operations	Attributes
Administrator	Any	Policy Manager – All
Operator	Read	Policy Manager – All
ssgconfig	Any	Gateway Configuration Utility - All
root	Any	Gateway Configuration Utility - All Privileged Shell (CLI) - All
Gateway Maintenance	Create, read, and update	FTP Audit Archiver (used to back up the audit logs on the Gateway via FTP to a specified host)
Invoke Audit Viewer Policy	Read	Audit events
Manage [name] Folder	Read, update, and delete	Policies within a defined folder
Manage [name] Identity Provider	Read, update, and delete	Identity Provider (with a defined name)
Manage[name] Policy	Read, update, and delete	Named Policy
Manage [name] Service	Delete, view, update	Web Service Assertions for web service policies
Manage Administrative Accounts Configuration	Create, read, and update	Cluster properties applicable to administrative account configuration: logon.maxAllowableAttempts logon.lockoutTime logon.sessionExpiry logon.inactivityPeriod.

Role	Operations	Attributes
Manage Certificates	Create, read, update, and delete	Trusted certificates Policies for revocation checking
Manage Cluster Properties	Create, read, update, and delete	Cluster status information
Manage Internal Users and Groups	Create, read, update, and delete	Users Groups (used to organize users as a time-saving tool)
Manage Listen Ports	Create, read, update, and delete	Gateway listen ports (both HTTP(S) and FTP(S))
Manage Log Sinks	Create, read, update, and delete	Log sinks (manage where audit records should be sent)
	Read	Folders Identity Providers Listen ports Log files Policies Services Users
Manage Password Policies	Read and update	Password policy
Manage Private Keys	Create, read, update, and delete	Private keys Default SSL key Default CA key
Manage Secure Passwords	Read, create, update, and delete	Stored passwords
Manage UDDI Registries	Create, read, update, and delete	UDDI registries **Note:** UDDI not within scope of the TOE. This role is listed for completeness.
Manage Web Services	Publish, edit, delete	Web Service
	Read	Existing Users
	Edit	Global Policy Assertions for web service policies

Role	Operations	Attributes
Publish External Identity Providers	Create	External Identity Provider
Publish Web Services	Publish	Web Service
Search Users and Groups	Read	Users and Groups
View [name] Folder	Read	Policies within a defined folder
View [name] Log Sink	Read	Audit events
View Audit Records	Read	Audit events

Note: For additional detail related to roles and terms above, refer to the *Predefined Roles and Permissions* section of the *Policy Manager User Manual*.

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the *access control SFP* to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *Administrator* to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA_EXT.5 Consistent security attributes

Hierarchical to: No other components.

FMT_MSA_EXT.5.1 The TSF shall identify the following internal inconsistencies within a policy prior to distribution: *incorrect assertion order, syntax errors and unfulfilled dependencies*.

FMT_MSA_EXT.5.2 The TSF shall take the following action when an inconsistency is detected: issue a prompt for an administrator to manually resolve the inconsistency.

Dependencies: FMT_MOF_EXT.1 External Management of Functions Behavior

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: *activities listed in Table 18 and Gateway configuration*.

Dependencies: No dependencies.

Table 18: Management Functions within the TOE

Requirement	Management Activities
ESM_ACD.1	Creation of policies
ESM_ACT.1	Transmission of policies
ESM_ATD.1	Definition of object attributes. Association of attributes with objects.
ESM_ATD.2	Definition of subject attributes. Association of attributes with subjects.
FAU_SEL_EXT.1	Configuration of auditable events for defined external entities
FAU_STG_EXT.1	Configuration of external audit storage location
FIA_AFL.1	Configuration of authentication failure threshold value, configuration of actions to take when threshold is reached, execution of restoration to normal state following threshold action
FIA_SOS.1	Management of the metric used to verify secrets
FIA_UAU.2	Management of authentication data for both interactive users and authorized IT entities
FIA_UID.2	Management of user identities for both interactive users and authorized IT entities
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes
FMT_MOF_EXT.1	Configuration of the behavior of other ESM products
FMT_MSA.1	Management of sets of subjects that can interact with security attributes, Management of rules by which security attributes inherit specified values
FMT_MSA.3	Managing the subjects that can specify initial values, Managing the permissive or restrictive setting of default values for a given access control SFP, Management of rules by which security attributes inherit specified values
FMT_SMR.1	Management of the users that belong to a particular role
FTA_TAB.1	Maintenance of the banner
FTP_ITC.1(1)	Configuration of actions that require trusted channel
FTP_ITC.1(2)	Configuration of actions that require trusted channel

Requirement	Management Activities
FTP_TRP.1	Configuration of actions that require trusted path

FMT_SMR.1 Security Management Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles *defined in* Table 17.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of Authentication

5.3.8 Class FPT: Protection of the TSF

FPT_FLS_EXT.1 Failure of Communications

Hierarchical to: No other components.

FPT_FLS_EXT.1.1 The TSF shall maintain policy enforcement in the following manner when the communication between the TSF and the Policy Management product encounters a failure state: enforce the last policy received.

Dependencies: No dependencies.

FPT_RPL.1 Replay Detection

Hierarchical to: No other components.

FPT_RPL.1.1 The TSF shall detect replay for the following entities: *TLS protected data*.

FPT_RPL.1.2 The TSF shall perform *reject the data* when replay is detected.

Dependencies: No dependencies.

FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.

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

Dependencies: No dependencies

Application note: The TOE can use NTP to synchronize its internal clock with a time server.

5.3.9 Class FRU: Resource Utilization

FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components.

FRU_FLT.1.1 The TSF shall ensure the operation of *enforcing the most recent policy* when the following failures occur: *failure of communications with the Policy Management product after an outage*.

Dependencies: FPT_FLS.1 Failure with preservation of secure state

5.3.10 Class FTA: TOE Access

FTA_TAB.1 TOE access banner

Hierarchical to: No other components.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

Dependencies: No dependencies.

Application note: This is only relevant to the Policy Manager interface.

FTA_SSL_EXT.1 TSF-initiated session locking

Hierarchical to: No other components

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions,

- terminate the session

after an Authorized Administrator specified time period of inactivity.

Dependencies: No dependencies

Application note: This requirement is only applicable to the Policy Manager.

FTA_SSL.4 User-initiated termination

Hierarchical to: No other components

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator’s own interactive session.

Dependencies: No dependencies

5.3.11 Class FTP: Trusted Paths/Channels

FTP_ITC.1(1) Inter-TSF trusted channel (Prevention of Disclosure)

Hierarchical to: No other components.

FTP_ITC.1.1(1) The TSF shall **use *TLS in conjunction with the ciphersuites specified at section 6.7* to** provide a trusted communication channel between itself and authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure.

FTP_ITC.1.2(1) The TSF shall permit the TSF **or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3(1) The TSF shall initiate communication via the trusted channel for transfer of policy data, **and for the following functions when configured by the administrator:**

- *service client connections*
- *Syslog server communication*

Dependencies: No dependencies.

FTP_ITC.1(2) Inter-TSF trusted channel (Detection of Modification)

Hierarchical to: No other components.

FTP_ITC.1.1(2) The TSF shall **use *TLS in conjunction with the ciphersuites specified at section 6.7*** ~~**to provide**~~ **in providing** a trusted communication channel between itself and authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and detection of the modification of data.

FTP_ITC.1.2(2) The TSF shall permit the TSF **or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3(2) The TSF shall initiate communication via the trusted channel for transfer of policy data, **and for the following functions when configured by the administrator:**

- *service client connections*
- *Syslog server communication*

Dependencies: No dependencies.

Application note: Use of TLS for service client connections is optional based on the configuration specified by the administrator. This is achieved via use of the ‘Require SSL or TLS Transport Assertion’.

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

FTP_TRP.1.1 The TSF shall **leverage third-party cryptographic suites** to provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification and disclosure.

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication, execution of management functions.

Dependencies: No dependencies.

5.4 Assurance Requirements

62 The TOE security assurance requirements, summarized in Table 19, are drawn from the claimed Protection Profiles.

Table 19: Assurance Requirements

Assurance Class	Components	Description
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Tests	ATE_IND.1	Independent Testing - conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM Coverage

6 TOE Summary Specification

6.1 Access Control Policy Definition

Related SFRs:	ESM_ACD.1, ESM_ATD.1, ESM_ATD.2, FMT_MSA.1(2), FMT_MSA.3, FMT_MSA_EXT.5, FMT_SMF.1

63 This security function refers to the access control policy definition capabilities of the Policy Manager. The Policy Manager is used to configure and define access control policies for the Layer 7 SecureSpan SOA Gateway (i.e. the Gateway is the compatible access control product). A summary of the policy definition capability is provided below however an entire manual – the *Policy Authoring User Manual* – is dedicated to this topic and should be referenced for detailed information.

64 A policy defines restrictions for the consumption of a published Gateway-protected service. At the highest layer of abstraction, the attributes used in policy definition are as defined in ESM_ACD.1. Details for included policy assertions are provided in sections 6.1.1, 6.1.2 and 6.1.3 below.

65 In the Policy Manager, a service policy includes assertions that determine the authentication method, identity credentials, transport method, and routing method for the web service. The specific types of assertions, their relative location, and the other assertions determine the properties and validity of a policy. During processing, the Gateway scans each policy assertion from top to bottom, assigning a 'succeed' or 'fail' outcome to each.

66 Policies are constructed in a ‘policy development window’ by moving assertions and policy fragments (template groups of assertions) into a meaningful tree structure resulting in ‘1st level’ and ‘child’ assertions. There are two special assertions used to refine policy logic:

a) **At least one assertion must evaluate to true folder.** Each child assertion placed in this folder is processed until an assertion succeeds. At this point, processing of the folder stops and the "At least one" folder is assigned a successful outcome. However if all assertions in the folder fail, then the "At least one" assertion is assigned a failure outcome.

b) **All assertions must evaluate to true folder.** Each child assertion placed in this folder is processed until an assertion fails. At this point, processing of the folder stops and the "All assertions" folder is assigned a failure outcome. However if all assertions in the folder succeed, then the "All assertions" folder is assigned a successful outcome.

67 The TOE restricts the ability to manage security attributes in accordance with Table 17 and provides the management capabilities defined in the *Policy Authoring User Manual* and the *Installation and Maintenance Manual (Appliance Edition)*.

68 Policy values are restrictive by default – access to objects is denied unless the administrator defines a policy to enable access.

69 Policy consistency checking is performed by the Policy Validator within the Policy Manager. The Policy Validator detects syntax error, unfulfilled dependencies and incorrect ordering of assertions. The administrator is notified when an error is detected. The Policy Validator is not configurable.

6.1.1 Access Control Assertions

70 The following subset of assertions are evaluated:

a) **Authenticate User or Group.** Require specified users and/or groups to be authenticated against a selected identity provider. Applies the credentials collected by a ‘require’ assertion listed below to authenticate a user or group specified in this ‘authenticate’ assertion. Refer to *Authenticate User or Group Assertion* section of the *Policy Authoring User Manual* for a list of related attributes and behavior.

b) **Authenticate against Identity Provider.** Requires provided client credentials to be successfully authenticated against a selected identity provider. Applies the credentials collected by the ‘require’ assertions to be authenticated. Refer to *Authenticate against Identity Provider Assertion* section of the *Policy Authoring User Manual* for a list of related attributes and behavior. In the evaluated configuration (specified by the *Secure Installation Guide*), the following Identity Providers are supported:

   i) Internal

   ii) Federated with X.509 credentials

c) **Require HTTP Basic** (**Note:** should be used in conjunction with Require SSL or TLS). Require that incoming requests to contain HTTP basic authentication credentials. Refer to *Require HTTP Basic Credentials Assertion* section of the *Policy Authoring User Manual* for a list of related attributes and behavior.

d) **Require SAML Token Profile.** Requires incoming requests to contain a SAML token. Refer to *Require SAML Token Profile Assertion* section of the *Policy Authoring User Manual* for a list of related attributes and behavior. In the evaluated configuration (specified by the *Secure Installation Guide*), the allowable attributes are as follows:

   i) **SAML Version.** SAML v2

   ii) **SAML Statement Type.** Authentication

   iii) **Authentication Methods.** Password, Password Protected Transport, SSL/TLS Client Certificate authentication, X.509 Public Key, XML Digital Signature

   iv) **Authorization Statement.** Not applicable

   v) **Attribute Statement.** Not applicable

   vi) **Subject Confirmation.** Sender Vouches (SV) or Holder-of-Key (HOK)

   vii) **Name Identifier.** Any

   viii) **Conditions.** Check Assertion Validity Period.

e) **Require SSL or TLS Transport with Client Authentication.** Requires clients to connect via SSL or TLS and to provide a valid / trusted X.509 certificate. Refer to *Require SSL or TLS Transport Assertion* section of the *Policy Authoring User Manual* for a list of related attributes and behavior.
Note: This assertion appears in two different assertion palettes:

   i) When accessed from the Access Control palette, this assertion is labeled "Require SSL or TLS Transport with Client Authentication" and has the Require Client Certificate Authentication check box selected by default.

   ii) When access from the Transport Layer Security palette, this assertion is labeled "Require SSL or TLS Transport" and does not have the Require Client Certificate Authentication check box selected by default.

f) **Require WS-Security Signature Credentials.** Requires that the web service target message includes an X.509 client certificate and has at least one element signed by that client certificate's private key as a proof of possession. Refer to *Require WS-Security Signature Credentials Assertion* section of the *Policy Authoring User Manual* for a list of related attributes and behavior. In the evaluated configuration (specified by the *Secure Installation Guide*), the allowable attributes are as follows:

   i) **Allow multiple signatures.** Disabled / unchecked

   ii) **Signature element variable.** Any

   iii) **Signature reference element variable.** Any

6.1.2 Service Availability Assertions

71 The following subset of service availability assertions are evaluated:

a) **Limit Availability to Time/Days.** Enables restricting service access by a time and/or day interval. When the Gateway receives a request for the service, it will check the time and/or day restrictions before allowing the message to proceed. Refer to *Limit Availability to Time/Days Assertion* section of the *Policy Authoring User Manual* for a list of related attributes and behavior.

b) **Restrict Access to IP Address Range.** Enables restricting service access based on the IP address of the requesting service client. Refer to *Restrict Access to IP Address Range Assertion* section of the *Policy Authoring User Manual* for a list of related attributes and behavior.

6.1.3 Policy Logic Assertions

72 The following subset of policy logic assertions are evaluated in support of the above assertions:

a) **All Assertions Must Evaluate to True.** The "All assertions must evaluate to true" assertion is a folder that organizes and defines the processing conditions for the assertions that it contains and for the overall policy. When assertions are grouped into one of these folders, each successive child assertion is processed until all assertions succeed, yielding a success outcome for the folder. Processing in this assertion folder will stop when the first child assertion fails, yielding a fail outcome for the folder. Refer to *All Assertions Must Evaluate to True Assertion* section of the *Policy Authoring User Manual* for a list of related attributes and behavior.

b) **At Least One Assertion Must Evaluate to True.** The "At least one assertion must evaluate to true" assertion is a folder that organizes and defines the processing conditions for the assertions that it contains and for the overall policy. When assertions are grouped into one of these folders in the policy window, each successive child assertion is processed until a single assertion succeeds, yielding a success outcome for the folder. If all child assertions in the folder fail, then the overall folder fails. Refer to *At Least One Assertion Must Evaluate to True Assertion* section of the *Policy Authoring User Manual* for a list of related attributes and behavior.

6.2 Access Control Policy Enforcement

Related SFRs:	FDP_ACC.1, FDP_ACF.1, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF_EXT.1, FMT_MSA.1(2), FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FTA_SSL.4

73 The Gateway enforces polices defined by the Policy Manager (see section 6.1 for policy types). In the evaluated configuration, the Gateway may only consume policies from the Layer 7 SecureSpan Policy Manager although it is compatible with other means as described in section 2.3.3. The Gateway authenticates the Policy Manager using TLS endpoint authentication (refer to section 6.7 for TLS details).

74 The Gateway performs the following message processing for a typical policy:

a) Service request arrives.

b) Request is run through the WS-Security processor:

   i) Encrypted sections are decrypted and WS-Security Signatures are verified. The sign and/or encrypt order is chosen by the sender (in the evaluated configuration, only signature verification is applicable when SAML envelope signatures are in use).

   ii) Default security header can be optionally removed before routing

c) Request is run through the policy assertions in linear order

d) Response is run through the WS-Security decorator:

   i) Default security header is created

   ii) Signatures specified by the policy are applied (only applicable for SAML envelope signatures)

   iii) Encryption specified by the policy is performed (not applicable in the evaluated configuration).

e) Response is sent back to the client.

75 All first level assertions in a policy (including first level "At least" and "All assertions" folders) must succeed in order for the overall policy to succeed. When the policy succeeds, the service requestor receives a response message. If the policy fails, the service requestor receives an error message.

76 Initial Gateway configuration is performed using the Gateway Configuration Utility, described in Chapter 3 of the *Installation and Maintenance Manual (Appliance Edition).* Subsequent to initial setup, configuration in performed by the Policy Manager.

77 The Gateway Configuration Utility recognizes only the ssgconfig and root roles. The TOE restricts the ability to manage security attributes in accordance with Table 17.

78 Policy values are restrictive by default – access to objects is denied unless the administrator defines a policy to enable access.

79 A user may terminate their own interactive session at the Gateway Configuration Utility.

6.3 Policy Security

Related SFRs:	ESM_ACT.1, FIA_UID.2, FIA_UAU.2, FTP_ITC.1(1), FTP_ITC.1(2), FTP_TRP.1, FPT_RPL.1, FCO_NRR.2, FIA_SOS.1

80 The Policy Manager transmits policies to the Gateway immediately after creation. A trusted channel (TLS) is established between the Policy Manager and the Gateway to protect the transmission of policy data. TLS provides replay detection and will reject the replayed packets and generate an audit event when detection occurs. TLS also provides certificate based mutual authentication between the Policy Manager and the Gateway.

81 Access to the Policy Manager and the Gateway requires user identification and authentication (username & password) as described in section 6.5.

82 The Policy Manager is a thick client Java application executed on a general purpose operating system. Remote access to the Policy Manager application is not supported. The Gateway Configuration Utility may be accessed locally or remotely. Remote access is secured using SSH (refer to section 6.7 for detail).

83 The TOE relies on FIPS validated third-party cryptographic modules for both TLS and SSH as identified in section 2.3.2. Refer to section 6.7 for TLS and SSH details.

84 The Gateway generates an audit record when a policy is received from the Policy Manager, providing proof of receipt. Refer to *Gateway Confirmation of Policy Versions* section of the *Security Installation Guide* for the contents and formatting of the receipt / audit record. The Policy Manager is used to view generated audit records. As documented above, the Policy Manager and Gateway are mutually authenticated using TLS certificates. The 'node' field of the receipt identifies the name of the Gateway to which the policy was applied.

6.4 System Monitoring

Related SFRs:	FAU_GEN.1, FAU_SEL.1, FAU_SEL_EXT.1, FAU_STG.1, FAU_STG_EXT.1, FPT_STM.1

85 The TOE generates the audit events identified in Table 16 (a full list of TOE audit message codes is provided in Appendix F of the *Policy Manager User Manual*). The TOE may store logs in an internal database or an external Syslog server. Communication with the Syslog server may be secured using TLS (refer to section 6.7 for detail).

86 Authorized users may view audit events via the Policy Manager. The set of events to be audited may be filtered based on event type. Event type is based on Severity Level (INFO, WARNING, SEVERE) with allowable selections being as follows: Selectable is INFO and WARNING | Non-Selectable is SEVERE (i.e. SEVERE is always logged). Additional details are provided in the *Overriding the Audit Level* section of the *Policy Manager User Manual.*

87 Audit logs cannot be modified via the Policy Manager. The Administrator may delete audit events that are more than 7 days old. Audit events are recorded until a predefined percentage of the database hard disk space is consumed. Once the threshold is reached, all message processing ceases until the log size drops below the threshold. The threshold is defined in the *audit.archiverShutdownThreshold* cluster property and is 90% by default.

88 Additional detail regarding the audit functionality is provided in the *Gateway Audit Events* section of the *Policy Manager User Manual*.

89 Detail regarding the local system logs on the Gateway appliance is available at the following sections of the *Installation and Maintenance Manual (Appliance Addition)*:

a) *Viewing Logs on the Gateway Appliance*

b) *Configuring the Gateway Logging Functionality*

90 By default, these local system logs consist of 10 log files of 20 MB each, which are used and rolled over as they fill up.

91 The TOE uses an internal clock provided by the underlying hardware platform to maintain time. If configured, the TOE can synchronize the internal clock with an NTP server. For configuration details, refer to *Configuring System Settings* of the *Installation and Maintenance Manual (Appliance Addition)*.

92 When configured in accordance with the *Security Installation Guide,* the following policy assertions are used in support of system monitoring:

a) **Audit Message in Policy.** Enables auditing of messages within a policy. It records events pertaining to the processing of a policy— e.g. assertion violations. Refer to the *Audit Messages in Policy Assertion* section of the *Policy Authoring User Manual* for a list of related attributes and behavior.

b) **Add Audit Detail.** Allows the definition of a custom message that can enhance the context of an audit message. Refer to the *Add Audit Detail Assertion* section of the *Policy Authoring User Manual* for a list of related attributes and behavior.

c) **Customize SOAP Fault Response.** Allows customization of the SOAP fault response on a policy-by-policy basis. Refer to the *Customize SOAP Fault Response Assertion* section of the *Policy Authoring User Manual* for a list of related attributes and behavior.

6.5 Robust Administrative Access

Related SFRs:	FIA_AFL.1, FIA_SOS.1, FTA_SSL_EXT.1, FTA_SSL.4, FIA_UAU.2, FIA_UID.2, FIA_USB.1, FMT_MSA.1(1), FMT_SMR.1, FTP_TRP.1, FTA_TAB.1

93 Access to the TOE can be achieved via the Policy Manager application or the Gateway Configuration Utility. Users must authenticate prior to being granted access. Users may authenticate via username and password.

94 The TOE administrative user database may be:

a) **Internal.** User details are maintained on an internal TOE database (refer to the *Internal Identity Provider Users and Groups* section of the *Policy Manager User Manual*).

95 The TOE determines the username from the credentials presented at authentication and associates the defined role with the corresponding username. The TOE maintains the roles and associated access permissions defined in Table 17. For configuration details refer to the *Managing Roles* section of the *Policy Manager User Manual.*

96 The TOE detects when an administrator defined threshold of unsuccessful authentication attempts has occurred (default 5) and locks the associated account for a configurable period of time (default 20 minutes). For configuration details refer to the *Managing Administrative User Account Policy* section of the *Policy Manager User Manual.*

97 The TOE allows specification of a password policy in accordance with FIA_SOS.1 and terminates inactive local sessions at the Policy Manager after an administrator defined period of inactivity. Users may also terminate their own session. For configuration details refer to *Managing Password Policy* section of the *Policy Manager User Manual*.

98 The Policy Manager is a thick client Java application executed on a general purpose operating system. Remote access to the Policy Manager application is not supported. The Gateway Configuration Utility may be accessed locally or remotely. Remote access is secured using SSH (refer to section 6.7 for SSH details).

99 The TOE displays an administrator defined banner at logon to the Policy Manager. For configuration details, refer to the *Administrative Account Cluster Properties* section of the *Policy Manager User Manual*.

6.6 Continuity of Enforcement

Related SFRs: FPT_FLS_EXT.1, FRU_FLT.1

100 The Gateway continues policy enforcement in the event of a loss of connectivity with the Policy Manager by enforcing the last policy received. Continuous connectivity with the Policy Manager is not expected or required.

6.7 TLS and SSH Details

101 This section provides additional detail regarding the TOE’s implementation of TLS and SSH. All Gateway cryptographic operations for TLS and SSH are performed by the RSA BSAFE Crypto-J Toolkit unless a HSM is installed in which case the HSM will provide Gateway cryptographic functions (see section 2.3.2 for supported HSMs). All Policy Manager cryptographic operations for TLS are performed by the RSA BSAFE Crypto-J Toolkit .

6.7.1 TLS

102 The TOE makes use of TLS in the following ways:

a) Between service clients and the Gateway – in this case the TOE is a TLS server.

b) Between the Policy Manager and the Gateway – in this case the TOE is both a TLS client (Policy Manager) and TLS server (Gateway).

c) Between the Gateway and a Syslog server – in this case the TOE is a TLS client.

103 The TLS implementation has the following characteristics when configured in accordance with the *Secure Installation Guide*:

a) TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346) and TLS 1.2 (RFC 5246) are supported without extensions.

b) Client authentication is supported (i.e. if configured the client must submit a trusted certificate to the server).

c) When acting as either client or server, the TOE is configure to negotiate the following ciphersuites in the following order of preference, if a listed ciphersuite is not supported by the other party then the connection will be refused:

i) TLS_RSA_WITH_AES_256_CBC_SHA

ii) TLS_RSA_WITH_AES_128_CBC_SHA

6.7.2 SSH

104 The TOE makes use of SSH to secure remote administrator access to the Gateway.

105 The SSH implementation has the following characteristics when configured in accordance with the *Secure Installation Guide* :

a) The TOE implements SSHv2

b) Password authentication is supported

c) The TOE supports the following SSH encryption algorithms:

i) AES-CBC-256

   ii) AES-CBC-192

   iii) AES-CBC-128

   iv) 3DES-CBC

d) In FIPS mode the TOE supports the following SSH data integrity algorithms:

   i) HMAC-SHA1-96

   ii) HMAC-SHA1

e) The TOE is configured to negotiate the above algorithms in order of preference. If a connecting client does not support the listed algorithms the connection will be refused.

7 Rationale

7.1 Conformance Claim Rationale

106 The following rationale is presented with regard to the PP conformance claims:

a) **TOE type.** As identified in section 2.1, the TOE is an enterprise security management solution that provides centralized management and access control over web services. The Policy Manager is consistent with the TOE type identified by the ESM Policy Manager PP and the Gateway is consistent with the TOE type identified in the ESM Access Control PP.

b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are identical to those of the ESM Policy Manager PP and the ESM Access Control PP**.**

c) **Security objectives.** As shown in section 4, the security objectives are identical to those of the ESM Policy Manager PP and the ESM Access Control PP.

d) **Security requirements.** Section 5 of this ST defines the claimed security requirements. SARs have been reproduced directly from the claimed PPs. There were a number of duplicate SFRs included in both the ESM Policy Manager PP and the ESM Access Control PP. Table 20 below describes how this duplication has been addressed. In addition, the claimed PPs included a number of optional SFRs, Table 21 below describes how these have been addressed. No additional requirements have been specified.

107 The conformance of this ST to both the ESM Policy Manager PP and the ESM Access Control PP is consistent with the PP application notes presented in section 6.1.1 of each document, which states: *'The ESM PPs represent a family of related Protection Profiles written to encompass the variable capabilities of ESM products. For an ST that claims conformance to multiple PPs within the ESM PP family, it is recommended that the ST author clarify how the ESM components relate to one another through usage of application notes. This will assist the reader in determining how the parts of the product that are to be evaluated correspond with the CC's notion of different ESM capabilities*.'

Table 20: Duplicate SFRs

Requirement	How the duplication of SFRs is handled in the ST
FAU_GEN.1	Same base requirement in both PPs. SFR specified once in the ST and events combined in Table 16.
FAU_STG_EXT.1	SFR from the ESM Policy Manager PP included in the ST as it is a superset of the SFR defined by the ESM Access Control PP.
FCS_CKM.1 (optional)	Same requirement in both PPs. Not claimed (optional).
FCS_CKM_EXT.4 (optional)	Same requirement in both PPs. Not claimed (optional).
FCS_COP.1(1) (optional)	Same requirement in both PPs. Not claimed (optional).

Requirement	How the duplication of SFRs is handled in the ST
FCS_COP.1(2) (optional)	Same requirement in both PPs. Not claimed (optional).
FCS_COP.1(3) (optional)	Same requirement in both PPs. Not claimed (optional).
FCS_COP.1(4) (optional)	Same requirement in both PPs. Not claimed (optional).
FCS_RBG_EXT.1 (optional)	Same requirement in both PPs. Not claimed (optional).
FMT_MSA.1	FMT_MSA.1(2) from the ESM Policy Manager PP covers the required functionality that is defined by FMT_MSA.1 of the ESM Access Control PP.
FMT_MSA.3	FMT_MSA.3 from the ESM Policy Manager PP covers the required functionality that is defined by FMT_MSA.1 of the ESM Access Control PP.
FMT_MSA.3	Same requirement in both PPs. SFR specified once in the ST.
FMT_SMF.1	Same base requirement in both PPs. SFR specified once in the ST and management functions combined in Table 18.
FMT_SMR.1	Same requirement in both PPs. SFR specified once in the ST.
FTA_SSL_EXT.1	Same requirement in both PPs. SFR specified once in the ST.
FTA_SSL.3	Same requirement in both PPs. SFR specified once in the ST.
FTA_SSL.4	Same requirement in both PPs. SFR specified once in the ST.
FTA_TSE.1	Not claimed (optional).
FTP_ITC.1(1)	Same requirement in both PPs. SFR specified once in the ST.
FTP_ITC.1(2)	Same requirement in both PPs. SFR specified once in the ST.

Table 21: Optional SFRs

Requirement	Source	Rationale
ESM_ATD.1	ESM Policy Manager PP	Included
ESM_ATD.2	ESM Policy Manager PP	Included

Requirement	Source	Rationale
ESM_DSC.1	ESM Access Control PP	Not included. Per ESM Access Control PP section C.1.5, this SFR is relevant to Data Loss Prevention or similar TOEs that require automated discovery and inventory of objects. In the TOE, objects (Web Services) are manually added by the administrator.
FCS_CKM.1	ESM Policy Manager PP	Not included. The TOE utilizes third-party cryptographic suites and therefore does not claim any of the optional cryptographic SFRs per guidance at Annex C.4 of the ESM Policy Manager PP and Annex C.3 of the Access Control PP.
FCS_CKM.1	ESM Access Control PP	
FCS_CKM_EXT.4	ESM Policy Manager PP	
FCS_CKM_EXT.4	ESM Access Control PP	
FCS_COP.1(1)	ESM Policy Manager PP	
FCS_COP.1(1)	ESM Access Control PP	
FCS_COP.1(2)	ESM Policy Manager PP	
FCS_COP.1(2)	ESM Access Control PP	
FCS_COP.1(3)	ESM Policy Manager PP	
FCS_COP.1(3)	ESM Access Control PP	
FCS_COP.1(4)	ESM Policy Manager PP	
FCS_COP.1(4)	ESM Access Control PP	
FCS_RBG_EXT.1	ESM Policy Manager PP	
FPT_FLS.1	ESM Access Control PP	Not included. Per ESM Access Control PP sections 4.4 and C.2.2, this SFR is relevant to systems that require continued enforcement mechanisms to counter the threat of disablement by users, such as host based access control systems. The TOE is not a host based system.
FPT_STM.1	ESM Policy Manager PP	Included
FTA_SSL_EXT.1	ESM Policy Manager PP	Included
FTA_SSL_EXT.1	ESM Access Control PP	Not included. Timeout not enforced for local Gateway CLI sessions.

Requirement	Source	Rationale
FTA_SSL.3	ESM Policy Manager PP ESM Access Control PP	Not included. No remote access to the Policy Manager. Timeout period not configurable for the Gateway.
FTA_SSL.4	ESM Policy Manager PP ESM Access Control PP	Included
FTA_TSE.1	ESM Policy Manager PP ESM Access Control PP	Not included. Not required.

7.2 Security Objectives Rationale

108 All security objectives are drawn directly from the ESM Policy Manager PP and the ESM Access Control PP. A conformance rationale is presented at section 7.1.

7.3 Security Requirements Rationale

109 Security requirements are drawn directly from the ESM Policy Manager PP and the ESM Access Control PP. A conformance rationale is presented at section 7.1. An unfulfilled dependencies rationale is presented in section 6.1.9 of the ESM Policy Manager PP.

7.4 TOE Summary Specification Rationale

110 Table 22 provides a coverage mapping showing that all SFRs are mapped to the security functions described in the TSS.

Table 22: Map of SFRs to TSS Security Functions

SFR	Access Control Policy Definition	Access Control Policy Enforcement	Policy Security	System Monitoring	Robust Administrative Access	Continuity of Enforcement
ESM_ACD.1	X					
ESM_ACT.1			X			
ESM_ATD.1	X					
ESM_ATD.2	X					
FAU_GEN.1				X		

SFR	Access Control Policy Definition	Access Control Policy Enforcement	Policy Security	System Monitoring	Robust Administrative Access	Continuity of Enforcement
FAU_SEL.1				X		
FAU_STG.1				X		
FAU_SEL_EXT.1				X		
FAU_STG_EXT.1				X		
FCO_NRR.2			X			
FDP_ACC.1		X				
FDP_ACF.1		X				
FIA_AFL.1					X	
FIA_SOS.1			X		X	
FIA_UAU.2			X		X	
FIA_UID.2			X		X	
FIA_USB.1					X	
FMT_MOF.1(1)		X				
FMT_MOF.1(2)		X				
FMT_MOF_EXT.1		X				
FMT_MSA.1(1)					X	
FMT_MSA.1(2)	X	X				
FMT_MSA.3	X	X				
FMT_MSA_EXT.5	X					
FMT_SMF.1	X	X				
FMT_SMR.1		X			X	
FPT_FLS_EXT.1						X

SFR	Access Control Policy Definition	Access Control Policy Enforcement	Policy Security	System Monitoring	Robust Administrative Access	Continuity of Enforcement
FPT_RPL.1			X			
FPT_STM.1				X		
FRU_FLT.1						X
FTA_SSL_EXT.1					X	
FTA_SSL.4		X			X	
FTA_TAB.1					X	
FTP_ITC.1(1)			X			
FTP_ITC.1(2)			X			
FTP_TRP.1			X		X	

Annex A: Assurance Activities

Annex A.1: ESM Policy Manager PP Assurance Activities

#	Source	Requirement	Assurance Family
1.	ESM_ACD.1	The evaluator must do the following: • Verify that the ST identifies compatible Access Control products • Verify that the ST describes the scope and granularity of the entities that define policies (subjects, objects, operations, attributes) • Review STs for the compatible Access Control products and verify that there is correspondence between the policies the TOE is capable of creating and the policies the Access Control products are capable of consuming	ASE
2.	ESM_ACD.1	Verify that the design documentation indicates how policies are identified	ADV_FSP
3.	ESM_ACD.1	The evaluator will test this capability by using the TOE to create a policy that utilizes the full range of subjects, objects, operations, and attributes and sending it to a compatible Access Control product for consumption. The evaluator will then perform actions that are mediated by the Access Control product in order to confirm that the policy was applied appropriately. The evaluator will also verify that a policy identifier is associated with a transmitted policy by querying the policy that is being implemented by the Access Control product.	ATE_IND
4.	ESM_ACT.1	The evaluator shall review the operational guidance to determine how to create and update policies, and the circumstances under which new or updated policies are transmitted to consuming ESM products (and how those circumstances are managed, if applicable). The evaluator shall obtain a compatible Access Control product, and following the procedures in the operational guidance for both the Policy Manager and the Access Control product, create a new policy and ensure that the new policy defined in the Policy Manager is transmitted and installed successfully in the Access Control product, in accordance with the circumstances defined in the SFR. In other words, (a) if the selection is completed to transmit after creation of a new policy, then the evaluator shall create the new policy and ensure that, after a reasonable window for transmission, the new policy is installed; (b) if the selection is completed to transmit periodically, the evaluator shall create the new policy, wait until the periodic period has passed, and then confirm that the new policy is present in the Access Control component; or (c) if the section is completed to transmit upon the request of a compatible Secure Configuration Management component, the evaluator shall create the policy, use the Secure Configuration Management component to request transmission, and the confirm that the Access Control component has received and installed the policy. If the ST author has specified “other circumstances”, then a similar test shall be executed to confirm transmission under those circumstances. The evaluator shall then make a change to the previously created policy, and	AGD_OPE ATE_IND

#	Source	Requirement	Assurance Family
		then repeat the previous procedure to ensure that the updated policy is transmitted to the Access Control component in accordance with the SFR-specified circumstances. Lastly, as updating a policy encompasses deletion of a policy, the evaluator shall repeat the process a third time, this time deleting the policy to ensure it is removed as an active policy from the Access Control component. Note: This testing will likely be performed in conjunction with the testing of ESM_ACD.1.	
5.	FAU_GEN.1	The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides description of the content of each type of audit record. Each audit record format type must be covered, and must include a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN 1.2, and the additional information specified in Table 16. The evaluator shall review the operational guidance, and any available interface documentation, in order to determine the administrative interfaces (including subcommands, scripts, and configuration files) that permit configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken to do this. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements. Using this list, the evaluation shall confirm that each security relevant administrative interface has a corresponding audit event that records the information appropriate for the event.	AGD_OPE ADV_FSP
6.	FAU_GEN.1	The evaluator shall test the TOE's audit function by having the TOE generate audit records for all events that are defined in the ST and/or have been identified in the previous two activities. The evaluator should then check the audit repository defined by the ST, operational guidance, or developmental evidence (if available) in order to determine that the audit records were written to the repository and contain the attributes as defined by the ST. This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an incorrect authentication secret is entered, then audit records will be expected to be generated as a result of testing identification and authentication. The evaluator shall also check to ensure that the content of the logs are consistent with the activity performed on the TOE. For example, if a test is performed such that a policy is defined, the corresponding audit record should correctly indicate the definition of policy.	ATE_IND
7.	FAU_SEL_EXT.1	The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events, and shall confirm that it contains all of the selections identified in the Security Target.	AGD_OPE
	FAU_SEL_EXT.1	The evaluator shall test this capability by configuring a compatible Access Control product to have:	ATE_IND

#	Source	Requirement	Assurance Family
		• All selectable auditable events enabled • All selectable auditable events disabled • Some selectable auditable events enabled For each of these configurations, the evaluator shall perform all selectable auditable events and determine by review of the audit data that in each configuration, only the enabled events are recorded by the Access Control product.	
8.	FAU_STG_ EXT.1	The evaluator shall check the operational and preparatory guidance in order to determine that they describe how to configure and use an external repository for audit storage. The evaluator shall also check the operational guidance in order to determine that a discussion on the interface to this repository is provided, including how the connection to it is established, how data is passed to it, and what happens when a connection to the repository is lost and subsequently re-established.	AGD_OPE
9.	FAU_STG_ EXT.1	The evaluator shall test this function by configuring this capability, performing auditable events, and verifying that the local audit storage and external audit storage contain identical data. The evaluator shall also make the connection to the external audit storage unavailable, perform audited events on the TOE, re-establish the connection, and observe that the external audit trail storage is synchronized with the local storage. Similar to the testing for FAU_GEN.1, this testing can be done in conjunction with the exercise of other functionality. Finally, since the requirement specifically calls for the audit records to be transmitted over the trusted channel established by FTP_ITC.1, verification of that requirement is sufficient to demonstrate this part of this one.	ATE_IND
10.	FIA_AFL.1	The evaluator shall check the operational guidance to verify that a discussion on authentication failure handling is present and consistent with the representation in the Security Target.	AGD_OPE
11.	FIA_AFL.1	The evaluator shall test this capability by using the authentication function of the TSF to deliberately enter incorrect credentials. The evaluator should observe that the proper action occurs after a sufficient number of incorrect authentication attempts. The evaluator should also use the TSF to reconfigure the threshold value in a manner consistent with operational guidance to verify that it can be changed.	ATE_IND
12.	FIA_SOS.1	The evaluator shall examine the ST and operational guidance in order to identify whether password or non password based authentication is used: a. For password based authentication, the evaluator shall identify that all password composition, configuration, and aging requirements specified in the ST are discussed in the TSS and AGD and test these capabilities one at a time (for example: set minimum password length to 6, observe that a 7 character password and a 16 character password are both accepted, then change the minimum length to 8, observe that a 7 character password is rejected but that a 16 character password is accepted) b. For non-password based authentication, the evaluator shall perform a basic strength of function analysis to determine the solution space of the	ASE_TSS AGD_OPE ATE_IND

#	Source	Requirement	Assurance Family
		authentication mechanism and the frequency with which password attempts can be made. For example, if the authentication is a 4-digit PIN that can be attempted once an hour, this requirement would not pass. If the strength of the authentication mechanism can't be determined by strength of function metrics at face value (for example, if a biometric authentication mechanism is being used), the vendor should provide some evidence of the strength of function.	
13.	FIA_UAU.2	The evaluator shall check the operational guidance in order to determine how the TOE determines whether a interactive user requesting access to it has been authenticated and how the TOE validates authentication credentials or identity assertions that it receives. The evaluator shall test this capability by accessing the TOE without having provided valid authentication information and observe that access to the TSF is subsequently denied. This SFR also applies to authorized IT entities exchanging information with the TOE (such as authorized access control components). To address this, the evaluator shall review operational guidance and the TSS to determine the mechanism used to authorize communication with IT entities, and shall configure that mechanism to permit at least one IT entity to communicate with the TOE. The evaluator shall then attempt communication with that IT entity to ensure it successfully is authenticated and identified. The evaluator shall also attempt communications with unidentified or unauthenticated entities to ensure that such connections are not successful.	AGD_OPE ATE_IND
14.	FIA_UID.2	This functionality—for both interactive users and authorized IT entities--is verified concurrently with FIA_UAU.2.	ATE_IND
15.	FIA_USB.1	The evaluator shall check the operational guidance in order to verify that it describes the mechanism by which external data sources are invoked and mapped to user data that is controlled by the TSF.	AGD_OPE
16.	FIA_USB.1	The evaluator shall test this capability by configuring the TSF to accept user information from external sources as defined by the ST. The evaluator shall then perform authentication activities using these methods and validate that authentication is successful in each instance. Based on the defined privileges assigned to each of the subjects, the evaluator shall then perform various management tests in order to determine that the user authorizations are consistent with their externally-defined attributes and the configuration of the TSF's access control policy. For example, if a user who is defined in an LDAP repository belongs to a certain group and the TSF is configured such that members of that group only have read-only access to policy information, the evaluator shall authenticate to the TSF as that user and verify that as a subject under the control of the TSF that they do not have write access to policy information. This verifies that the aspects of the user's identity data that are pertinent to how the TSF treats the user are appropriately taken from external sources and utilized in order to determine what the user is able to do.	ATE_IND
17.	FMT_MOF_EXT.1.1	The evaluator shall test this capability by deploying the TOE in an environment where there is an Access Control component that is able to communicate with it. The evaluator must configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator must use the Policy Management product to modify the behavior of the functions specified in the requirement above. For	ATE_IND

#	Source	Requirement	Assurance Family
		each function, the evaluator must verify that the modification applied appropriately by using the Policy Management product to query the behavior for and after the modification. The evaluator must also perform activities that cause the TOE to react in a manner that the modification prescribes. These actions include, for each function, the following activities: - Audited events: perform an event that was previously audited (or not audited) prior to the modification of the function's behavior and observe that the audit repository now logs (or doesn't log) this event based on the modified behavior - Repository for remote audit storage: observe that audited events are written to a particular repository, modify the repository to which the TOE should write audited events, perform auditable events, and observe that they are no longer written to the original repository - Access Control SFP: perform an action that is allowed (or disallowed) by the current Access Control SFP, modify the implemented SFP such that that action is now disallowed (or allowed), perform the same action, and observe that the authorization differs from the original iteration of the SFP. - Policy being implemented by the TSF: perform an action that is allowed (or disallowed) by a specific access control policy, provide a TSF policy that now disallows (or allows) that action, perform the same action, and observe that the authorization differs from the original iteration of the FSP. - Access Control SFP behavior to implement in the event of communications outage: perform an action that is handled in a certain manner in the event of a communications outage (if applicable), re-establish communications between the TOE and the Policy Management product, change the SFP behavior that the TOE should implement in the event of a communications outage, sever the connection between the TOE and the Policy Management product, perform the same action that was originally performed, and observe that the modified way of handling the action is correctly applied. Once this has been done, the evaluator shall reconfigure the TOE and Policy Management product such that the Policy Management product is no longer authorized to configure the TOE. The evaluator shall then attempt to use the Policy Management product to configure the TOE and observe that it is either disallowed or that the option is not even present.	
18.	FMT_MSA.1 (1)	The evaluator shall review the ST and operational guidance to determine that it describes how the TSF maintains its own access control internally (i.e. "if I'm an administrator on the PM TOE, how do I say who my users are, what AC products they can control, and to what extent can they control those AC products").	ASE_TSS AGD_OPE
19.	FMT_MSA.1 (1)	The evaluator shall perform testing to confirm that described behaviors exhibit the documented semantics (i.e. set up a new user, give them privileges, log in and see that those privileges were granted, change some attributes that will affect their privileges, log back in and see that those privileges have been changed). The evaluator shall also review the ST and operational guidance to determine how the TOE is associated with ESM Access Control products. The evaluator	ATE_IND

#	Source	Requirement	Assurance Family
		shall verify how the TOE discovers AC products in the operational environment and how it is recognized as the valid controller of those products. The evaluator shall confirm this behavior with testing. One approach to doing this is to place the TOE and two compatible AC products on the same network. The evaluator shall follow the documented configuration steps such that one of the AC products is associated with the TOE. The evaluator shall then confirm that they now have the ability to manage only that AC product. The evaluator shall capture traffic and replaying it against the other AC product and confirm that it has no effect. The evaluator shall review the ST and operational guidance to determine if there are any other defined internal security attributes. If there are, the evaluator shall verify that they can be configured in the manner specified by the evidence, and that their configuration has the effect defined in the evidence.	
20.	FMT_MSA.1 (2)	The evaluator shall review the ST in order to determine that it specifies the operations that can be managed by the TSF. For example, the TSF must have the ability to create policies. The data that can comprise these policies should be defined in the ST.	ASE_TSS
21.	FMT_MSA.1 (2)	The evaluator shall then check the operational guidance in order to determine that it defines a set of managed attributes consistent with the ST and the TSF mechanisms by which these attributes can be manipulated.	AGD_OPE
22.	FMT_MSA.1 (2)	The evaluator shall test this capability by performing, for each defined attribute and operation, an operation on the TSF that manipulates the attribute. They should also verify that the mechanism of session establishment is defined so that it’s understood how permissions to operate the TSF come to be assigned to users who provide a collection of external identification and authentication information to it.	ATE_IND
23.	FMT_MSA.3	The evaluator shall review the operational guidance in order to determine that it defines what the default values are for managed attributes.	AGD_OPE
24.	FMT_MSA.3	The evaluator shall test this capability by performing activities against the TSF that involve the instantiation of new security attributes and verifying that the default values are consistent with the description in the guidance and that they can collectively be described in the manner defined by the ST.	ATE_IND
25.	FMT_MSA_ EXT.5	The evaluator shall review the operational guidance in order to determine that it explains what potential contradictions in policy data may exist. For example, a policy could potentially contain two rules that permit and forbid the same subject from accessing the same object. Alternatively, the TOE may define an unambiguous hierarchy that makes it impossible for contradictions to occur.	AGD_OPE
26.	FMT_MSA_ EXT.5	The evaluator shall test this capability by defining policies that contain the contradictions indicated in the operational guidance and observing if the TSF responds by detecting the contradictions and reacting in the manner prescribed in the ST. If the TSF behaves in a manner that prevents contradictions from occurring, the evaluator shall review the operational guidance in order to determine if the mechanism for preventing contradictions is described and if this feature is communicated to administrators. This feature should be tested in	ATE_IND

#	Source	Requirement	Assurance Family
		conjunction with a compatible Access Control product; in other words, if the TOE has a mechanism that prevents contradictions (for example, if a deny rule always supersedes an allow rule), then correct enforcement of such a policy by a compatible Access Control product is both a sufficient and a necessary condition for demonstrating the effectiveness of this mechanism.	
27.	FMT_SMF.1	The evaluator shall check the operational guidance in order to determine that it defines all of the management functions that can be performed against the TSF, how to perform them, and what they accomplish.	AGD_OPE
28.	FMT_SMF.1	The evaluator shall test this capability by accessing the TOE and verifying that all of the defined management functions exist, that they can be performed in the prescribed manner, and that they and accomplish the documented capability.	ATE_IND
29.	FMT_SMR.1	The evaluator shall review the ST and operational guidance to determine the roles that are defined for the TOE. The evaluator shall use the TOE to associate different users with different roles. This may be tested concurrently with other requirements if being assigned to a role impacts how the user interacts with the TSF. For example, the TSF's internal access control mechanisms may grant different levels of authority to users who have different roles (only the super user can create new users, an auditor can only view policies and not change them, etc.), and so the effects of changing the user's role attribute would already have been tested by FMT_MSA.1(1).	AGD_OPE ATE_IND
30.	FPT_STM.1	The evaluation team must determine through the evaluation of operational guidance how the TOE initializes and initiates the clock. The evaluation team must then follow those instructions to set the clock to a known value, and observe that the clock monotomically increments in a reliable fashion (comparison to a reference timepiece is sufficient). Through its exercise of other TOE functions, the evaluation team must confirm that the value of the timestamp is used appropriately.	AGD_OPE ATE_IND
31.	FTA_TAB.1	The evaluator shall review the operational guidance to determine how the TOE banner is displayed and configured. If the banner is not displayed by default, the evaluator shall configure the TOE in accordance with the operational guidance in order to enable its display. The evaluator shall then attempt to access the TOE and verify that a TOE banner exists. If applicable, the evaluator will also attempt to utilize the functionality to modify the TOE access banner as per the standards defined in FMT_SMF.1 and verify that the TOE access banner is appropriately updated.	AGD_OPE ATE_IND
32.	FTA_SSL_EXT.1.1	The evaluator follows the operational guidance to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that re-authentication is needed when trying to unlock the session.	AGD_OPE ATE_IND
33.	FTA_SSL.3	The evaluator follows the operational guidance to configure several different values for the inactivity time period referenced in the component; these shall consist at least of the minimum and maximum allowed values as specified in	AGD_OPE ATE_IND

#	Source	Requirement	Assurance Family
		the operational guidance, as well as one other value. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.	
34.	FTA_SSL.4	The evaluator shall perform the following tests: • Test 1: The evaluator initiates an interactive local session with the TOE. The evaluator then follows the operational guidance to exit or log off the session and observes that the session has been terminated. • Test 2: The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the operational guidance to exit or log off the session and observes that the session has been terminated.	ATE_IND
35.	FTP_ITC.1(1)	The evaluator shall check the operational guidance in order to determine the mechanism by which secure communications are enabled. The evaluator shall also check the TSS, operational guidance, and other provided evidence to determine the means by which secure communications are facilitated. Based on this, the following analysis will be required: • If cryptography is internal to the TOE, the evaluator shall verify that the product has been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national standard for the nation in which the evaluation is being conducted. • If cryptography is provided by the Operational Environment, the evaluator shall review the operational guidance, ST, and any available design documentation to see how cryptography is utilized and to verify that the functions used have been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national standard for the nation in which the evaluation is being conducted.	AGD_OPE ASE_TSS
36.	FTP_ITC.1(1)	The evaluator shall test this capability by enabling secure communications on the TOE and placing a packet sniffer on the local network. They shall then use the TOE to perform actions that require communications to all trusted IT products with which it communicates and observe the captured packet traffic that is directed to or from the TOE to ensure that their contents are obfuscated.	ATE_IND
37.	FTP_ITC.1(2)	The evaluator shall check the operational guidance in order to determine the mechanism by which secure communications are enabled. The evaluator shall also check the TSS, operational guidance, and other available evidence to determine the means by which secure communications are facilitated. Based on this, the following analysis will be required: • If cryptography is internal to the TOE, the evaluator shall verify that the product has been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national standard for the nation in which the evaluation is being conducted. • If cryptography is provided by the Operational Environment, the evaluator shall review the operational guidance, ST, and any available design documentation to see how cryptography is utilized and to verify that the functions used have been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national	AGD_OPE ASE_TSS

#	Source	Requirement	Assurance Family
		standard for the nation in which the evaluation is being conducted.	
38.	FTP_ITC.1(2)	The evaluator shall test this capability by enabling secure communications on the TOE and placing a packet sniffer on the local network. They shall then use the TOE to perform actions that require communications to all trusted IT products with which it communicates and observe the captured packet traffic that is directed to or from the TOE to ensure that their contents are obfuscated.	ATE_IND
39.	FTP_TRP.1	The evaluator shall check the operational guidance to verify that it discusses the methods by which users will interact with the TOE such as a web application via HTTPS. The evaluator shall check the operational guidance to determine if it discusses the mechanism by which a trusted path to the TOE is established and what environmental components (if any) the TSF relies on to assist in this establishment.	AGD_OPE
40.	FTP_TRP.1	The evaluator shall test this capability in a similar manner to the assurance activities for FTP_ITC.1. If data transmitted between the user and the TOE is obfuscated, the trusted path can be assumed to have been established.	ATE_IND

Annex A.2: ESM Access Control PP Assurance Activities

#	Source	Requirement	Assurance Family
1.	FAU_GEN.1	As per ESM Policy Manager PP assurance activity, in addition: This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an access request is denied by a policy specified in FDP_ACF.1, then audit records will be expected to be generated as a result of testing the policy's effectiveness. The evaluator shall also check to ensure that the content of the logs are consistent with the activity performed on the TOE. For example, if a test is performed such that an access request is denied by policy, the corresponding audit record should correctly indicate the failure.	ATE_IND
2.	FAU_SEL.1	The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events, and shall confirm that it contains all of the selections identified in the Security Target.	AGD_OPE
3.	FAU_SEL.1	The evaluator shall test this capability by using a compatible Policy Management product to configure the TOE in the following manners: - All selectable auditable events enabled - All selectable auditable events disabled - Some selectable auditable events enabled For each of these configurations, the evaluator shall perform all selectable auditable events and determine by review of the audit data that in each configuration, only the enabled events are recorded.	ATE_IND

#	Source	Requirement	Assurance Family
4.	FAU_STG.1	The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. The evaluator shall also examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.	ASE_TSS
5.	FAU_STG_ EXT.1	The evaluator shall examine the administrative guidance to ensure it instructs the administrator how to establish communication with the audit server. The guidance must instruct how this channel is established in a secure manner (e.g., IPsec, TLS). .	AGD_OPE
6.	FAU_STG_ EXT.1	The evaluator shall test the administrative guidance by establishing a link to the audit server, and confirming that the audit records generated have been transmitted to that server. Note that this will need to be done in order to perform the assurance activities prescribed under FAU_GEN.1	ATE_IND
7.	FCO_NRR.2	The evaluator shall check the development evidence in order to determine how the TOE confirms evidence of received policy data back to the Policy Management product that originally sent it that policy data. This should include the contents and formatting of the receipt such that the data that it contains is verifiable.	ASE_TSS
8.	FCO_NRR.2	The evaluator shall test this capability by configuring an environment such that the TOE is allowed to accept a policy from a certain source, sending it a policy from that source, observing that the policy is subsequently consumed, and that an accurate receipt is transmitted back to the Policy Management product within the time interval specified in the ST. The evaluator confirms accuracy by using the Policy Management product to view the receipt and ensure that its contents are consistent with known data.	ATE_IND
9.	FDP_ACC.1 FDP_ACF.1	The evaluator shall check the ST and operational guidance in order to verify that the TOE is capable of mediating the activities that are defined.	ASE_TSS AGD_OPE
10.	FDP_ACC.1 FDP_ACF.1	The evaluator shall then use an authorized and compatible Policy Management product to define policies that contain rules for mediating these activities. For each subject/object/operation/attribute combination, the evaluator shall execute at least one positive and one negative test in order to show that the TSF is capable of appropriately mediating these activities. For example, the policy may define a rule that allows one user to visit a certain URL and another that forbids a different user from visiting the same URL. Once this policy is implemented, the evaluator will access a system as each of these users and observe that the ability to visit the specified URL is appropriately allowed or denied. Additionally, for each conditional attribute (such as a time of day restriction) that is supported, the evaluator will devise a positive and negative test that proves that the conditional attribute affects whether or not the requested operation is allowed. This activity is then repeated for each other	ATE_IND

#	Source	Requirement	Assurance Family
		subject/object/operation/attribute tuple.	
11.	FMT_MOF.1 (1)	The evaluator shall test this capability by deploying the TOE in an environment where there is a Policy Management product that is able to communicate with it. The evaluator must configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator must use the Policy Management product to modify the behavior of the functions specified in the requirement above. For each function, the evaluator must verify that the modification applied appropriately by using the Policy Management product to query the behavior for and after the modification. The evaluator must also perform activities that cause the TOE to react in a manner that the modification prescribes. These actions include, for each function, the following activities: - Audited events: perform an event that was previously audited (or not audited) prior to the modification of the function's behavior and observe that the audit repository now logs (or doesn't log) this event based on the modified behavior - Repository for remote audit storage: observe that audited events are written to a particular repository, modify the repository to which the TOE should write audited events, perform auditable events, and observe that they are no longer written to the original repository - Access Control SFP: perform an action that is allowed (or disallowed) by the current Access Control SFP, modify the implemented SFP such that that action is now disallowed (or allowed), perform the same action, and observe that the authorization differs from the original iteration of the SFP. - Policy being implemented by the TSF: perform an action that is allowed (or disallowed) by a specific access control policy, provide a TSF policy that now disallows (or allows) that action, perform the same action, and observe that the authorization differs from the original iteration of the FSP. - Access Control SFP behavior to implement in the event of communications outage: perform an action that is handled in a certain manner in the event of a communications outage (if applicable), re-establish communications between the TOE and the Policy Management product, change the SFP behavior that the TOE should implement in the event of a communications outage, sever the connection between the TOE and the Policy Management product, perform the same action that was originally performed, and observe that the modified way of handling the action is correctly applied. Once this has been done, the evaluator shall reconfigure the TOE and Policy Management product such that the Policy Management product is no longer authorized to configure the TOE. The evaluator shall then attempt to use the Policy Management product to configure the TOE and observe that it is either disallowed or that the option is not even present.	ATE_IND
12.	FMT_MOF.1 (2)	The evaluator shall test this capability by deploying the TOE in an environment where there is a Policy Management product that is able to communicate with it. The evaluator must configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator must use the Policy Management product to	ATE_IND

#	Source	Requirement	Assurance Family
		query the policy being implemented by the TOE. Once this has been done, the evaluator shall reconfigure the TOE and Policy Management product such that the Policy Management product is no longer authorized to configure the TOE. The evaluator shall then attempt to use the Policy Management product to configure the TOE and observe that it is either disallowed or that the option is not even present.	
13.	FMT_MSA.1	The evaluator shall review the TSS and the guidance documentation to confirm that the indicated attributes are maintained by the TOE. The evaluation shall also confirm that the documentation indicates that the ability to perform the indicated operations are restricted to the identified roles (which is anticipated a function provided by components compliant with the ESM Policy Definition PP).	ASE_TSS AGD_OPE
14.	FMT_MSA.1	The evaluator shall use the associated Policy Definition product to confirm each identified operation against the indicated attributes may be performed, and that the TOE interfaces do not provide the ability for any other roles to perform operations against the indicated attributes.	ATE_IND
15.	FMT_MSA.3	The evaluator shall review the TSS and the guidance documentation to confirm that they describe how restrictive default values are put into place (for example, access control policies should operate in deny-by-default mode so that the absence of an access control rule doesn’t fail to restrict an operation) by the TOE.	ASE_TSS AGD_OPE
16.	FMT_MSA.3	The evaluator shall use the associated Policy Definition product to confirm that for each identified security attribute and restrictive initial state, the TOE implements the correct restrictive value.	ATE_IND
17.	FMT_SMF.1	The evaluator shall check the TOE summary specification in order to determine what Policy Management and Secure Configuration Management product(s) are compatible with the TOE. The evaluator shall deploy the TOE in a configuration with these compatible products and use these products to perform the functions defined in the Security Target and operational guidance. For each advertised management function in the ST and operational guidance, the evaluator shall use the Policy Management product to execute this management function. Then, for each management function, the evaluator shall attempt this behavior and verify that the behavior observed is consistent with the expectations of the management function executed.	ATE_IND
18.	FMT_SMR.1	The evaluator shall review the TSS and the guidance documentation to confirm that they describe how management authority is delegated via one or more roles, and how an authorized Policy Definition product is associated with those roles.	ASE_TSS AGD_OPE
19.	FMT_SMR.1	The evaluator shall use the associated Policy Definition product to connect to the TOE and confirm that it is operating in the assigned role. The evaluation shall also confirm that a user or other external entity that has not been authorized for the indicated role cannot assume the indicated role.	ATE_IND
20.	FPT_FLS_EXT.1	The evaluator shall check the operational guidance (and developmental evidence, if available) in order to determine that it discusses how the TOE is	AGD_OPE

#	Source	Requirement	Assurance Family
		deployed in relation to other ESM products. This is done so that the evaluator can determine the expected behavior if the TOE is unable to interact with its accompanying Policy Management product.	
21.	FPT_FLS_EXT.1	The evaluator shall test this capability by terminating the product that distributes policy to the TOE and also by severing the network connection between the TOE and this product if applicable. The evaluator will then interact with the TOE while these communications are suspended in order to determine that the behavior it exhibits in this state is consistent with the expected behavior.	ATE_IND
22.	FPT_RPL.1.1	The evaluator shall check the administrative guidance and TSS (and developmental evidence, if available) in order to determine that it describes the method by which the TSF detects replayed data. For example, it may provide a certificate or other value that can be validated by the TSF to verify that the policy is consistent with some anticipated schema. Alternatively, the TOE may utilize a protocol such as SSL for transmitting data that immunizes it from replay threats.	ASE_TSS AGS_OPE
23.	FPT_RPL.1.1	The evaluator shall test this capability by running a packet sniffer application (such as Wireshark) on the local network with the TOE, sending a valid policy to it, and observing the packets that comprise this policy. The evaluator can then take these packets and re-transmit them to the TOE. Once this has been done, the evaluator shall execute an appropriate subset of User Data Protection testing with the expectation that the policy enforced will be the first policy transmitted. If the expected results are met, the TOE is sufficiently resilient to rudimentary policy forgery.	ATE_IND
24.	FRU_FLTS.1	The evaluator shall test this capability by severing the network connection between the TOE and the Policy Management product, defining an updated policy, and re-establishing the connection will determine if the TOE appropriately receives the new policy data within the time interval specified in FCO_NRR.2.3. The evaluator shall devise a scenario such that the old policy allows a specific action and that the new policy denies that same action. The evaluator shall then perform that action, observe that it is allowed, sever connection with the Policy Management product, define the new policy during that outage, re-establish the connection, wait for the interval defined by FCO_NRR.2.3, perform the same action again, and observe that it is no longer allowed.	ATE_IND