



CCT Mark IA Claims Document (ICD)

Juniper Networks Secure Access Family

Secure Access 4000-FIPS & Secure Access 6000-FIPS

Version 5.4R2.1

CCT Mark Certificate Number: 2007/04/0020
Date CCT Mark Awarded: 24 April 2007
CCT Mark Award expires on: 23 April 2009
ICD Issue Date: 24 April 2007

Vendor Address:

Juniper Networks (UK) Limited

Aviator Park

Addlestone

Surrey

KT15 2PG

Telephone Number: 01372 385500

Vendor Website: www.juniper.net

Vendor Email: Thearn@juniper.net

Contents

Contents.....	2
1 Introduction.....	3
1.1 Background.....	3
1.2 Objectives.....	3
1.2.1 ICD Objectives.....	3
1.3 Purpose of Document.....	3
1.4 Structure.....	3
2 Product Description.....	4
2.1 Product Identification.....	4
2.2 Product Overview.....	4
2.2.1 Security Architecture.....	5
2.2.2 Hardware requirements.....	8
2.2.3 Software requirements.....	8
2.2.4 Out of Scope for Claims Testing.....	9
2.3 Usage assumptions.....	10
2.3.1 Assets.....	10
2.3.2 Threat scenario.....	10
3 Security Claims for the IA Product.....	14
3.1 Claims Statements.....	14
3.2 Existing Assurance Certificates.....	18
Annex A Glossary of Terms.....	18
Annex B Marketing Statement.....	21
Annex C System Variables and Boolean Expressions.....	22

1 Introduction

1.1 Background

This document outlines the IA claims made by Juniper Networks Ltd in regard to the suitability of the Secure Access Family for use by the UK Public Sector for remote access solutions. Secure Access has been designed to provide secure remote access to internal network resources across a wide-range of transit networks. Secure Access can provide secure remote access to a variety of resources, such as:

- Corporate file servers
- Web-based enterprise applications
- Intranet pages

1.2 Objectives

1.2.1 ICD Objectives

The objective of this document is to define the assets, threats and controls pertaining to the deployment of a Juniper Secure Access solution with the UK Public Sector. In particular it defines the security claims being made by Juniper Networks on this product.

1.3 Purpose of Document

This document is the ICD for Juniper Networks' Secure Access Family Series of SSL Appliances. This ICD is the baseline document for the CCT Mark claims testing process of Juniper Networks' Secure Access Family Series of SSL Appliances.

1.4 Structure

The structure of this ICD is as follows:

Section 1 contains the introductory material. Section 2 contains the description of functionality of Juniper Networks' Secure Access Family Series of SSL Appliances and all the information related to the security of Juniper Networks' Secure Access Family Series of SSL Appliances. Section 3 details the security functionality claims that are being made.

2 Product Description

2.1 Product Identification

Product Name: Juniper Networks' Secure Access Family

Version: IVEOS 5.4R2.1

Platforms: SA-4000-FIPS and SA-6000-FIPS

The Client operating system/browser combinations to be used in claims testing are shown in the table below:

Product	Client Operating System	Browser
SA-4000-FIPS	Windows XP Professional SP2	Internet Explorer v6.0
	Windows 2000 SP4	Internet Explorer v6.0
	Red Hat Enterprise Server ES4	Firefox 1.5
SA-6000-FIPS	Windows XP Professional SP3	Internet Explorer v6.0
	Windows 2000 SP4	Internet Explorer v6.0
	Red Hat Enterprise Server ES4	Firefox 1.5

2.2 Product Overview

Secure Access acts as a secure application-layer gateway that intermediates all requests between remote computers and internal corporate resources. All requests from remote computers to a Secure Access appliance and from a Secure Access appliance to remote computers are encrypted using SSL/HTTPS 168-bit encryption. All unencrypted requests (e.g. HTTP) are redirected to HTTPS which ensures the connection is encrypted. Each request is subject to administratively defined access control and authorization policies, such as dual-factor or client-side digital certificate authentication, before the request is forwarded to an internal resource. Users gain authenticated access to authorized resources via an extranet session hosted by the appliance. From any Internet-connected Web browser, users can have some level of access to Web-based enterprise applications, Java applications, file shares and terminal hosts depending upon the security policy defined. The SA-6000 appliance is shown in figure 2-1.



Figure 2-1 Juniper SA-6000 Appliance

2.2.1 Security Architecture

With an ISO Common Criteria EAL2 certification for version 5.2R1, Secure Access consists of four major components, detailed in figure 2-2. Together these and other components of the appliance deliver a simple, secure remote access solution within a single machine. The four major components are:

- Content Intermediation Engine
- Protocol Connectors
- Secure Content Server
- System Data Store and Load Balancing System

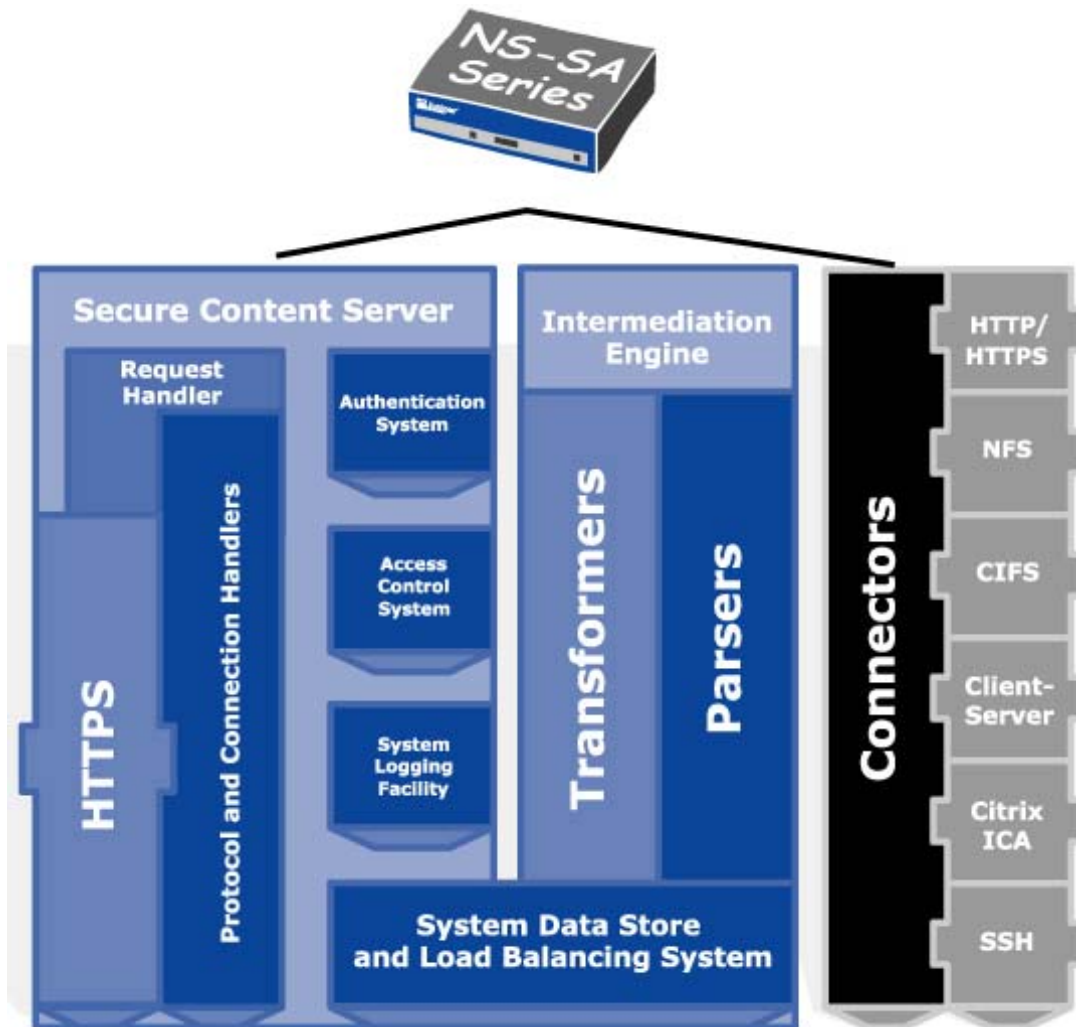


Figure 2.2: SA Architecture

2.2.1.1 Content Intermediation Engine

The Content Intermediation Engine is the core of Secure Access. It consists of:

Parsers - Event-driven components that process resource data streams and decompose them into “chunks” that are manipulated by associated transformers

Transformers - Components that receive the “chunks.” The transformers have the opportunity to modify each chunk in the data stream before writing it out to the Request Handler

Connectors - Components that use protocol adapters to retrieve resource and application data streams, such as documents on file servers, HTML pages on the intranet servers, or messages from an MS Exchange server

Web requests provide the clearest example of the Content Intermediation Engine at work, but generally speaking, support for most content types and application protocols uses a similar approach:

The file sharing application for remote access to Windows shares and NFS volumes uses a backend connector, and the directory and file meta-data is transformed into a Web view of the volume.

The client-server application and messaging application support uses backend connectors to communicate with mail servers, messaging servers, and other servers. These messages are transformed into the secure Web protocols before they are written out to the Request Handler.

The support for Web resources uses a Connector to read HTML and other content streams from an internal HTTP server in addition to a Parser and a Transformer.

2.2.1.2 Protocol Connectors

Each supported content type has an associated protocol connector. These connectors communicate with the content parsers and with the native content servers. For example, the file share connector communicates with MS Windows file servers through the CIFS protocol over TCP and with UNIX file server through NFS over UDP. In order to enforce native access controls, an additional component connects to the MS NT Domain Controller or UNIX NIS server. Juniper supports connectors for many connection types, however only the following will be included in the CCT process

- CIFS
- HTTP/HTTPS
- Windows Terminal Services

2.2.1.3 Secure Content Server

The Secure Content Server provides the core of the security features offered by SA. The Secure Content Server consists of the following components:

- Access Control System
- Authentication System
- Protocol and Connection Handlers
- Request Handler
- System Logging Facility
- Web Server

The Access Control System provides access control enforcement on requests to resources protected by the SA. The Access Control System determines if an authenticated user will be allowed or denied access to a requested resource.

When an authenticated user makes a request to the backend resources available to the role associated with the authenticated user, the appliance evaluates the corresponding resource policies. A resource policy is a set of resource names (such as URLs and hostnames) to which you grant or deny access or other resource-specific actions, such as rewriting and caching. A resource policy serves as the third level of resource access control. While a role may grant access to certain types of access features and resources (such as bookmarks and applications), whether or not a user can access a specific resource is controlled by resource policies. These policies may even specify conditions that, if met, either deny or grant user access to a server share or file. The administrator dynamically sets up user roles and access rules associated with the roles.

The Authentication System provides identification and authentication capabilities for authenticating both administrators and users. The Authentication System performs authentication using authentication realms. However, separate authentication databases are used for administrator and user accounts. An authentication realm is a grouping of authentication resources, including:

- An authentication server, which verifies that the user is who he claims to be. An IVE appliance forwards credentials that a user submits on a sign-in page to an authentication server.
- An authentication policy, which specifies realm security requirements that need to be met before an IVE appliance submits a user's credentials to an authentication server for verification.
- A directory server, which is an LDAP server that provides user and group information to an IVE appliance that the appliance uses to map users to one or more user roles.
- Role mapping rules, which are conditions a user must meet in order for an IVE appliance to map the user to one or more user roles. These conditions are based on either user information returned by the realm's directory server or the user's username.

The Protocol and Connection Handlers provide the necessary protocol negotiations to the end user for the specific protocol being used.

The Request Handler runs within the Secure Access appliance. The Request Handler works with the system software and other components to ensure that content can be projected to authorized users in a secure fashion:

Secure Access uses "cookie trapping." All Web cookies are maintained on the server, and a single session token is transmitted to the Web browser. This feature ensures that no cookie-based session information, stored credentials, or application meta-data leaves the corporate network.

The Secure Access session token expires when the session becomes idle or the user signs out.

HTTP headers with all sensitive content contain the Cache-Control directive “no-cache,” which prevents them from being stored on the client machine in standard browsers.

All form-fields intermediated by the device include the autocomplete=“off” attribute to prevent values from being stored on the client machine.¹

The System Logging Facility provides logging capabilities for recording the access decisions resulting from resource requests initiated by authenticated users. The System Logging Facility also provides logging capabilities for recording the access decisions resulting from the actions performed by authenticated administrators.

The Web Server provides an interface to users for using the SA to access resources protected by the SA, and provides an interface to administrators for managing the SA and its security functions. The Web Server also provides the HTTP protocol that is used for both the user and administrator interfaces to receive/transmit and encrypt/decrypt data to or from the SA.

2.2.1.4 System Data Store

All data stored on the device is encrypted using AES, however, the protection of the AES encryption is outside of the scope of the ICD. Only the Secure Access system software can read the encrypted data store. Further, users and administrators cannot replace arbitrary executable files, and they do not have system-level accounts, so potential attackers cannot employ privilege-elevation attacks against the appliance.

2.2.2 Hardware requirements

There are no specific hardware requirements; the solution being assured is a dedicated appliance. The SA appliance is provided by Juniper Networks as part of the solution. As previously identified, the hardware to be tested is:

Juniper Networks SA 4000 FIPS

Juniper Networks SA 6000 FIPS

2.2.3 Software requirements

2.2.3.1 Server Software

There are no specific server software requirements as the solution being assured is a dedicated appliance running proprietary software. The software is provided by Juniper Networks as part of

¹ These are tags that are embedded in the HTTP code. They are not enforced by the SA, and as such can be over ridden by the user.

the solution. As previously identified, the software to be tested will be version 5.4R2.1 running on the Juniper Networks SA 4000 FIPS and Juniper Networks SA 6000 FIPS platforms.

2.2.3.2 Client Software

The following client supported combinations will be tested as part of the CCT Mark process.

- Windows XP Pro SP2: Internet Explorer 6.0
- Windows 2000 SP4: Internet Explorer 6.0
- Red Hat Linux Enterprise Server 4: Firefox 1.5

2.2.4 Out of Scope for Claims Testing

The following items are out of scope for the claims testing:

2.2.4.1 Client Browsers

- Mac OS X 10.4: Safari 2.0
- Mac OS X 10.3.2: Safari 1.1, Internet Explorer 5.2
- Mac OS X 10.2.8: Safari 1.0
- Mac 9.2: Internet Explorer 5.1.5 and Netscape 4.79
- Fedora Core 5: Firefox 2.0
- Solaris 8: Mozilla 1.4
- Solaris 9: Mozilla 1.4
- Windows Mobile 5.0 based Pocket PC devices: Pocket IE 4.0
- Windows Mobile 2003 based Pocket PCs: Pocket IE 2003
- Treo 650: Palm OS 5.2.1: Blazer 4.0
- Opera browser for Symbian
- iMode client browser for I-Mode capable cell phones and PDAs
- eZweb, openwave client browsers

2.2.4.2 Protocol Connectors

Citrix ICA
IMAP
Lotus Notes
MS MAPI
NFS
POP
SMTP
Socket-dependent Java applets
SSH
Telnet
URL-dependent Java applets

2.2.4.3 SAM/NC

These components will only be tested on Windows Platforms.

2.3 Usage assumptions

2.3.1 Assets

As noted in the introduction, typical assets to be protected by the SA can be defined below, but are not limited to the following.

- Corporate file servers
- Web-based enterprise applications
- Intranet pages

2.3.2 Threat scenario

This should identify the threats to assets which are countered.

- T1 Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to modify the behavior of SA security functions data without being detected.
- T2 An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.
- T3 An unauthorized person may send impermissible information through the SA which results in the exploitation of resources on the internal network.
- T4 An unauthorized person may attempt to bypass the security of the SA so as to access and use security functions and/or non-security functions provided by the SA.
- T5 Because of a flaw in the SA functioning, an unauthorized person may gather residual information from a previous information flow or internal SA data by monitoring the padding of the information flows from the SA.
- T6 An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the SA.
- T7 An unauthorized person may replay valid identification and authentication data obtained while monitoring the SA's network interface to access functions provided by the SA.
- T8 An unauthorized person may read, modify, or destroy security critical SA configuration data.
- T9 The SA may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.
- T10 Human users within the physically secure boundary protecting the SA may attempt to access the SA from some direct connection (e.g., a console port) if the connection is part of the SA.
- T11 There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the SA.
- T12 The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

- T13 Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- T14 The SA does not host public data.
- T15 Authorized administrators may access the SA remotely from the internal and external networks.
- T16 Information can not flow among the internal and external networks unless it passes through the SA.

2.3.2.1 Expected operational environment

This product, as part of an overall solution, will typically be used in the deployment of flexible and mobile working solutions in the Public Sector for networks carrying some types of Restricted data using the existing FIPS 140-2 certification. The precise HMG policy in this area is specified in HMG Infosec Standard No.4 Part 1.

The solution can be used to connect users to applications across the public Internet over broadband networks or for remote users in untrusted locations over the corporate network.

The product can also be used to provide a secure 'front end' access solution to Citrix delivered applications and Microsoft terminal services, however Citrix support is out of scope for the CCTM testing.

It is expected that the product will be part of an overall solution which includes appropriate end device security software like personal firewall and anti-virus and centralised AAA mechanisms.

2.3.2.2 Organisational security policies

This section describes the operating environment for deploying the SA solution. Figure 2-3 details the logical deployment.

2.3.2.2.1 Connectivity

The goal of the SA platform is to provide access to internal resources from out with the organisation's network. Typically this is achieved by leveraging the public Internet as an untrusted transport network.

2.3.2.2.2 Appliance Placement

In general the SA should be deployed behind a firewall device, in a DMZ, with Internet access. The device has two logical interfaces; External Port and Internal port. The External Port is used to terminate user security sessions from the Internet and the Internal port is used for proxied user application sessions. An alternative topological arrangement is permissible; in this situation only the Internal Port is enabled and is used for both user security session termination and user application initiation.

2.3.2.2.3 Firewall Ports

As the principal connection method will be SSL/TLS, the front-end firewall must allow HTTPS protocol (TCP Port 443) traffic to pass through to the SA. If administrators wish to support the automatic re-direction of HTTP requests to the secure port, then TCP Port 80 must also be

allowed. Additionally, if the intention is to utilize the Network Connect access method, then both IP Protocol 50 (Encapsulating Security Protocol – ESP) and UDP 4500 – used for the traversal of NAT devices by IPSec, must be opened on the firewall.

2.3.2.2.4 Local and Remote Management

Management is possible on both Internal and External Ports; the default behaviour is to allow management traffic on the Internal Port and to deny management traffic on the External Port. Management traffic on the External Port can be enabled through administrative configuration. In addition, the SA-6000-FIPS platform provides a dedicated out-of-band management interface.

2.3.2.2.5 Resource Access

Resources can be placed anywhere within the organisation's network providing that the necessary routing and firewall rules are in place to allow connectivity. The organization will therefore require policy to ensure that this is the case. The only exception to this is when deploying the solution in an External/Internal Port mode; in this case the SA will not be able to access resources that are routed through the External Port. This is done to logically separate secure session and user traffic and implies that all resources must be routable through the Internal Port only.

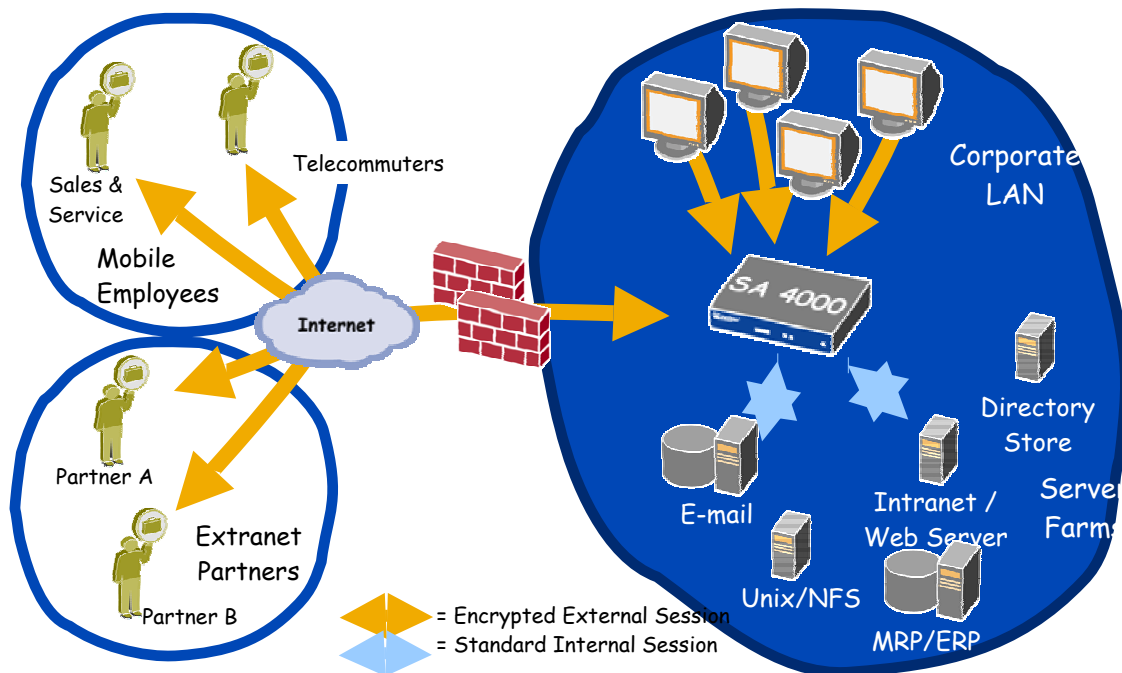


Figure-2-3 SA Typical Deployment Scenario

2.3.2.2.6 Pre-Authentication

As part of the pre-authentication checks possible on the SA, two components are available; Host Checker and Cache Cleaner. Host Checker should be used to verify the compliance to organisation security policy in terms of Personal Firewall, Anti-Virus, Spyware and other such platform checks. If the intention is to allow access from non-managed endpoints, the Cache Cleaner should be deployed to ensure that the machine is left in a known, safe state at the end of the user session.

2.3.2.2.7 User Authentication

The SA is capable of many different types of User Authentication. Best practice in this area would be to deploy the solution with strong, two-factored authentication such as a token system.

2.3.2.2.8 User Authorisation

For User Authorisation, best practice would be to leverage the contents of the organisation's information storage system, giving access to data that can be utilised to confer permissions on user sessions. Typically this is an LDAP directory.

2.3.2.2.9 User Roles

Best practice in this area is to create Roles that are aligned to the resources being offered on a per functional group basis. In this way if a user is to be given access to a resource or group of resources, the user need only be mapped to the role. Role mapping should be based on user group membership and results of the Host Checking process.

2.3.2.2.10 User Resources

Resources should be group together into logical constructs to simplify the process of conferring access to users as per the Role Mapping methods.

2.3.2.3 Security requirements on the environment

The SA should be racked and physically secured in a locked equipment cabinet with the appropriate measures in-place to ensure that no physical interference is possible by unauthorised personnel.

3 Security Claims for the IA Product

3.1 Claims Statements

CS1 – Data Confidentiality, Integrity and Authentication

The SA uses industry-standard TLS to provide security services at the application layer for all user data sessions. The cipher-suite to be tested is

Protocol: TLS
Signature: RSA
Encryption: 3DES-CBC-EDE

While this is the same cipher suite as specified in CESG Manual T, the CCTM accreditation lab setup has not been tested by CESG for compliance against the full requirements in Manual T

CS2 – Pre-Authentication Support

The SA has extensive capabilities to profile an endpoint before permitting a sign-on page. Any of the following criteria can be used by an administrator to determine whether a particular endpoint meets the required security policy.

Sign-in URL
TLS Version and Strength
Source IP Address
User Agent (Browser/OS) Type
Digital Certificate Attributes
Password Length Control
Results for Endpoint Point Security Check – Host Checker/Cache Cleaner
User Session Limits

CS3 – Authentication Options

Users and Administrators are authenticated by the SA through either a local server or via external servers. External server authentication is supported for the following protocols:

Active Directory
NTLM
LDAP
RADIUS
RSA SecurID
PKI
Local

CS4 User Role Definition

The SA provides the administrator with many variables with which to control the process of mapping a user to one or more available roles. Any of the following can be used in the role mapping stage:

Username

- User Attributes
- Certificate Attributes
- LDAP Group Membership
- LDAP OUs
- Custom Boolean Expressions²

CS5 User Role Restrictions

An additional layer of control to the process of assigning user roles is possible by allowing the administrator to restrict access based on the following variables:

- Source IP Address
- User Agent (Browser/OS) Type
- Digital Certificate Attributes
- Results for Endpoint Point Security Check – Host Checker/Cache Cleaner

CS6 – Dynamic Resource-Based Authorisation Policies

The resources that users access, are tied to the Roles assigned to that user. The administrator can further restrict the access to these resources based on the following variables:

- Role
- All Identity Attributes
- Custom Boolean Expressions

CS7 – User Agent Security

To ensure that sensitive information from the Intranet is not left on the host machine, the SA ensures the following are maintained:

- Content is Marked as not Cacheable
- HTML Source Code Cannot be Viewed

CS8 – Client Security Check

The SA deploys a component called Host Checker to profile the endpoint. The results of which can be used as mentioned in CS2, CS4 and CS5. The variables available to the administrator are as follows:

- Anti-Virus Products
- Personal Firewall Products
- Anti-Spyware Products
- Anti-Malware Products
- OS Versions plus Service Pack Level
- Allowable TCP/UDP Ports
- Disallowable TCP/UDP Ports
- Allowable Processes
- Disallowable Processes

² See Annex C for details concerning the system variables that can be utilised and the Boolean logic constructs permissible.

- Allowable Files
- Disallowable Files
- File Version Checking
- MD5 File Hash Checking
- Allowable Registry Entries
- Disallowable Registry Entries
- Registry Version Checking

CS9 – Host Check Remediation

If a user fails any of the checks defined in CS7, the administrator has the option to provide remediation services for that user, allowing them to come back into security policy compliance. The specific options are:

- Display Customisable Instructions to Users
- Evaluate Other Policies (allows for policy chaining)
- Kill Running Processes
- Delete Specific Files

CS 10 – Browser Cache Cleaner

The Cache Cleaner is a downloadable component that ensures that MS IE is left in a known state at the end of the user's session. Specifically the administrator can control the following aspects of IE:

- Disable AutoComplete of web addresses
- Disable AutoComplete of usernames and passwords
- Flush all existing AutoComplete passwords
- Empty Recycle Bin and Recent Documents list at the end of user session
- Clear Browser Cache
- Clear Files and Folders

CS11 – Adaptive Delivery of Host Checker/Cache Cleaner

The Host Checker and Cache Cleaner components can be delivered by either Active-X or Java technology to the endpoint. Active-X is attempted first, if this feature is disabled or not supported on the browser, then the SA will automatically switch to Java. This allows for an adaptive delivery mechanism to be offered to users.

CS12- Intranet Hostname Encoding

As the SA intermediates Intranet web pages, it can be advantageous to encode the actual URLs of these pages for security reasons. The SA can be setup to obfuscate these internal URLs.

CS13- Managing User Sessions

The administrator can forcibly end user sessions. Additionally for those users defined locally, it is possible to disable their accounts in the event of security concerns. This allows administrators to ensure that only fully authorised users can access the system.

CS14- User Session Timeouts

User sessions can be limited through both idle timers and session timers. This feature ensures that an endpoint is not left in a vulnerable situation uncontrolled.

CS15- SecureVirtualWorkspace

Secure Virtual Workspace (SVW) is a client application that creates a logically separate desktop on a PC, within which a secure SA session is contained. The virtual workspace is created within the SA user's real desktop after validating the host integrity of the end user's machine. It provides a secure environment within the user's desktop where only administrator specified programs can run. This feature is supported on Windows 2000 and XP only. The feature can restrict access to the following:

- Restrict Access to Printers
- Restrict Files on Host Machines
- Removable Drives on Host Machine
- Network Shares on Host Machine
- Ability to Switch Between Real and Virtual Desktop
- Ability to Maintain Persistent Session on Host Machine
- Control Panel on Host Machine
- Run Menu on Host Machine
- Registry Editor on Host Machine
- Task Manager on Host Machine
- Command Prompt on Host Machine
- Allowable Application List on Host Machine
- Disallowable Application List on Host Machine

CS16- Secure Application Manager (SAM)

Secure Application Manager is a TLS component that allows particular applications on the host to have their traffic patterns wrapped up securely and intermediated by the SA. SAM can either be downloaded on demand or installed as a standalone application. There are two versions; a Windows component and Java-based component. The Windows version wraps specific applications in TLS whilst the Java version uses a port-forwarding technique to wrap traffic.

CS17- Network Connect (NC)

Network Connect is TLS/IPSec component creating a virtual ethernet interface in the host machine; subsequently assigned an IP address from the SA. This operational mode allows all IP applications to have access to resources as permitted by the administrator from a network perspective – as opposed to an intermediated application perspective. As with SAM, NC can either be downloaded on demand or installed as a standalone application.

NC is adaptive in its transport layer; either TLS or IPSec can be used in a manner transparent to the user. IPSec is the more efficient transport protocol, however it does require the network to pass this type of traffic; firewalls and NAT devices can stop it making connections. For this reason, NC can transparently fall back to TLS, which does not suffer from these problems.

CS18 Logging

The SA provides logging at the following levels:

- System
- User Access
- Admin Access
- User Policy Tracing

User Session Tracing

Packet Capture

Information can be displayed/filtered on screen or sent to external Syslog servers via WELF, W3C or internal methods.

CS19 FIPS Hardware Cryptographic Module

The Hardware Security Module (HSM) must be initialized by employing a Juniper Secure Access FIPS smartcard. The module handles private cryptographic key management and SSL handshakes, simultaneously, ensuring FIPS compliance and off-loading CPU-intensive public key infrastructure (PKI) tasks from the SA to a dedicated module.

3.2 Existing Assurance Certificates

FIPS140-2 Level 3 Compliant nCipher HSM PCI 4000 – Certificate #536

Annex A Glossary of Terms

- AAA Authentication, Authorisation and Accounting. Paradigm for the ability to verify user identity, confer access rights and log usage.
- AES Advanced Encryption Standard. Symmetric encryption algorithm used to ensure data confidentiality
- CBC Cipher-Block Chaining is a mode of cryptographic operation whereby each block of plaintext is XORed with the previous ciphertext block before being encrypted.
- CIFS CIFS defines a standard remote file-system access protocol for use over the Internet, enabling groups of users to work together and share documents across the Internet or within corporate intranets.
- ICA Independent Computing Architecture is a proprietary protocol for an application server system, designed by Citrix Systems. The protocol lays down a specification for passing data between server and clients, but is not bound to any one platform
- CPU A Central Processing Unit CPU, or sometimes simply processor, is the component in a digital computer that interprets computer program instructions and processes data.
- DMZ In computer security, a demilitarized zone (DMZ) or perimeter network is a network area that sits between an organization's internal network and an external network, usually the Internet.
- (3)DES In cryptography, 3DES is a block cipher formed from the Data Encryption Standard (DES) cipher by using it three times.
- EDE Encrypt, Decrypt, Encrypt. Sequence for created ciphertext.
- ESP IPsec (IP Security) is a suite of protocols for securing Internet Protocol (IP) communications by encrypting and/or authenticating each IP packet in a data stream. Encapsulating Security Payload (ESP) provides data confidentiality, payload (message) integrity and authentication.

- FIPS** Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States Federal government for use by all non-military government agencies and by government contractors.
- HTTP** Hypertext Transfer Protocol (HTTP) is a method used to transfer or convey information on the World Wide Web.
- HTTPS** Hypertext Transfer Protocol Secure (HTTPS) refers to the combination of a normal HTTP interaction over an encrypted SSL or TLS transport mechanism.
- HTLM** HyperText Markup Language is the predominant language for the creation of web pages. It provides a means to describe the structure of text-based information in a document.
- HSM** Hardware Security Module. The function of the HSM is to securely generate long term secrets for use in cryptography and usually physically protect the access to and use of those secrets over time.
- IMAP** Internet Message Access Protocol is an application layer Internet protocol that allows a local client to access e-mail on a remote server.
- IE** Internet Explorer. The browser developed by Microsoft Corporation and present in all versions of their Windows operating system.
- ISO** The International Organization for Standardization is an international standard-setting body composed of representatives from national standards bodies.
- IVE** Instant Virtual Extranet. The name coined by Juniper Networks to refer generically to the Secure Access range of products.
- J.E.D.I.** Juniper Endpoint Defence Initiative. A framework and open API developed by Juniper to allow profiling and cleaning of user machines before, during and after a session on the IVE.
- LDAP** Lightweight Directory Access Protocol is a networking protocol for querying and modifying directory services running over the Internet Protocol.
- MS** Microsoft Corporation.
- NFS** Network File System is a protocol which allows a user on a client computer to access files over a network as easily as if attached to its local disks.
- NIC** A Network Interface Controller is a piece of computer hardware designed to allow computers to communicate over a computer network.
- OU** Organisational Unit. A term used in LDAP directories to define a sun-system.
- POP** Local e-mail clients use the Post Office Protocol version 3 (POP3), an application-layer Internet standard protocol, to retrieve e-mail from a remote server over an IP connection.
- PCI** The Peripheral Component Interconnect specifies a computer bus for attaching peripheral devices to a computer motherboard
- RTC** A Real-Time Clock is a computer clock that keeps track of the current time even when the computer is turned off.
- SA** Secure Access. Product name for the Juniper Networks SSL platform
- SHA-1** The SHA (Secure Hash Algorithm) hash function SHA-1 produces a 160-bit digest from a message with a maximum length of $2^{64}-1$ bits.
- SSL** Secure Sockets Layer is a cryptographic protocol which provides secure communications on the Internet for such things as web browsing, e-mail and other data transfers.

- SMTP** Simple Mail Transfer Protocol is the de facto standard for e-mail transmissions across the Internet.
- SSH** Secure SHell is a set of standards and an associated network protocol that allows establishing a secure channel between a local and a remote computer.
- TCP** The Transmission Control Protocol is a connection orientated virtual circuit protocol that is one of the core protocols of the Internet protocol suite.
- TLS** Transport Layer Security is a cryptographic protocol which provides secure communications on the Internet for such things as web browsing, e-mail and other data transfers.
- UDP** The Transmission Control Protocol is a connectionless virtual circuit protocol that is one of the core protocols of the Internet protocol suite.
- URL** Uniform Resource Locator is syntax for global identifiers of network-retrievable documents. More correctly it is a synonym for a Universal Resource Identifier (URI); technically URL is a subset of URI.

Annex B Marketing Statement

The Juniper Secure Access 4000/6000-FIPS appliances can be deployed to provide secure, anywhere, anytime remote access services to public sector employees from a wide variety of end devices and locations. By leveraging the advanced client endpoint assessment features, administrators can provide many levels of differentiated access, consistent with a centralised security policy. Ease of integration into existing AAA environments makes the SA an extremely compelling solution to support Web, Application and Network connectivity for a remote workforce. Following CSIA guidelines and subject to a risk assessment and accreditor approval, the SA4000FIPS and SA6000FIPS, combining FIPS 140-2 Level 3 and the CCT Mark can be used in the Public Sector for networks carrying information up to Restricted data.

Annex C System Variables and Boolean Expressions

1. cacheCleanerStatus

Status of the Cache Cleaner.

Possible values:

1 - cache cleaner is running

0 - cache cleaner is not running

Example:

```
cacheCleanerStatus = 1
```

```
cacheCleanerStatus = 0
```

2. certAttr.

List of attributes from a client-side certificate. certAttr may include the following components of an X.509 Distinguished Name: C, ST, L, O, OU, CN, title, initials, GN, SN, description, UI, or emailAddress.

Use this variable to check that the user has a client-side certificate with the value(s) specified.

Example:

```
certAttr.OU = 'Retail Products Group'
```

3. certAttr.altName.

List of attributes from a client-side certificate. certAttr.altName may include the following components of an X.509 Distinguished Name: directoryName, Email, DNS, URI, ipAddress, and registeredId.

Use this variable to check that the user has a client-side certificate with the value(s) specified.

Example:

```
certAttr.altName.email = "joe@company.com"
```

```
certAttr.altName.directoryName = "cn=joe, ou=company, o=com"
```

```
certAttr.altName.ipAddress = 10.10.0.0/16
```

4. certAttr.serialNumber

Client certificate serial number.

Note that all characters other than [0-9 a-f A-F] are stripped out of a string before comparison with certAttr.serialNumber. Wildcards are not supported.

Example:

```
certAttr.serialNumber = userAttr.certSerial
```

```
certAttr.serialNumber = "6f:05:45:ab"
```

5. certDN

Client certificate subject DN. Wildcard matching is not supported.

Example:

```
certDN = 'cn=John Harding,ou=eng,c=Company'
```

```
certDN = userDN (match the certificate subject DN with the LDAP user DN)
```

```
certDN = userAttr.x509SubjectName
```

```
certDN = ('cn=John Harding,ou=eng,c=Company' or 'cn=Julia Yount,ou=eng,c=Company')
```

6. certDN.<subject-attr>

Any variable from the client certificate subject DN, where subject-attr is the name of the RDN key.

Example:

```
certDN.OU = 'company'
```

```
certDN.emailAddress = 'joe@company.com'
```

```
certDN.ST = 'CA'
```

7. certDNText

Client certificate user DN formatted as a string. Only string comparisons to this value are allowed. Wildcard matching is supported.

Example:

```
certDNText = 'cn=John Harding,ou=eng,c=Company'
```

8. certIssuerDN

Client certificate-issuer subject DN. This variable works like a standard DN attribute such as CertDN. Wild card matching is not supported.

Example:

```
certIssuerDN = 'cn=Company CA,ou=operations,c=Company'
```

```
certIssuerDN = userAttr.x509Issuer
```

```
certIssuerDN = ('ou=eng,c=Company' or 'ou=operations,c=Company')
```

```
certIssuerDN.<issuer-attr>
```

Any variable from the client certificate-issuer subject DN, where issuer-attr is the name of the RDN key.

Example:

```
certIssuerDN.OU = 'company'
```

```
certIssuerDN.DC = ('acme' and 'net')
```

9. certIssuerDNText

Client certificate-issuer subject DN formatted as a string. Only string comparisons to this value are allowed. Wild card matching is supported.

Example:

```
certIssuerDNText = 'cn=Company CA,ou=operations,c=Company'
```

10. defaultNTDomain

If AD/NT authentication is used, then defaultNTDomain contains the Domain value set in the Local authentication server configuration.

Example

```
defaultNTDomain = "CORP"
```

11. group.<group-name>

Group names from the authorization server catalog. The user is a member of the group variables that are true.

Example:

```
group.preferredPartner
group.goldPartner or group.silverPartner
group.employees and time.month = 9
```

12. groups

List of groups as provided by the realm authentication or directory server.

Note: You can enter any character in the groupname, although wildcard characters are not supported.

Example:

```
groups="Sales"
groups="Domain Administrators"
groups= ("Sales" and "Europe")
```

13. hostCheckerPolicy

Host Checker policies that the client has met.

Example:

```
hostCheckerPolicy = ("Norton" or "Sygate")
hostCheckerPolicy = ("Norton" and "firewall check")
```

14. loginHost

Host name or IP address of the browser used to contact the device.

Example:

loginHost = "10.10.10.10"

loginHost = "goldpartner.company.com"

15. loginTime

The time of day at which the user submits his credentials to the device. The time is based on the device's clock.

Example:

loginTime = (8:00AM TO 5:00PM)

loginTime = (08:00 TO 17:00)

16. loginTime.day

The numeric day on which the user submits his credentials to the device, where day is 1-31. The time is based on the device's clock.

Example:

loginTime.day = 3

17. loginTime.dayOfWeek

The day of the week on which the user submits his credentials to the device, where dayOfWeek can be set to [0-6] where 0 = Sunday.

Symbolic values may be used: Sun, Mon, Tue, Wed, Thu, Fri, Sat

Example:

loginTime.dayOfWeek = 6

loginTime.dayOfWeek = Fri

18. loginTime.dayOfYear

The numeric day of the year on which the user submits his credentials to the device, where dayOfYear can be set to [0-365].

Example:

```
loginTime.dayOfYear = 100
```

19. loginTime.month

The month in which the user submits his credentials to the device, where month can be set to [1-12] where 1 = January.

Example:

```
loginTime.month = 4
```

20. loginTime.year

The year in which the user submits his credentials to the device, where year can be set to [1900-2999].

Example:

```
loginTime.year = 2005
```

21. loginURL

URL of the page that the user accessed to sign in to the device. The device gets this value from the Administrator URLs/User URLs column on the Authentication > Sign-in Policies page of the Web console. Note: a star (*) in the sign-in policy URL can be matched by surrounding it with square brackets (['*']) in the expression.

Example:

```
loginURL = "['*']/"
```

```
loginURL = "['*']/partnerLogin"
```

```
loginURL = "partners.company.com/"
```

22. networkIf

The network interface on which the user request is received. Possible values: internal, external, management

Example:

networkIf = internal

networkIf = external

networkIf = management

23. ntomain

If AD/NT authentication is used, then ntomain contains the domain name part of the user name. The ntomain variable is always lower-case.

Example:

ntomain = "corp"

24. ntuser

If AD/NT authentication is used, then ntuser contains the user name part of the user name.

Example:

ntuser = "jsmith"

25. sourceIp

The IP address of the machine on which the user authenticates.

Caveat: In the resource policy, netmask can be specified using the bit number or in the netmask format '255.255.0.0'

Example:

sourceIp = 192.168.10.20

sourceIp = 192.168.10.0/24 (Class A)

sourceIp = 10.11.0.0/16

sourceIp = 10.11.0.0/255.255.0.0

26. time

The time of day at which the role mapping rule or resource policy rule is evaluated. The time of the day can be in 12-hour or 24-hour format.

Example:

time = (9:00AM TO 5:00PM)

time = (09:00 TO 18:00)

time = (Mon TO Fri)

27. time.day

The current day of month, where day is 1-31. The time is based on the device's clock.

Example:

time.day = 3

28. time.dayOfWeek

The day of the week on which the role mapping rule or resource policy rule is evaluated. Numeric values may be used: [0-6] where 0 = Sunday. Symbolic values may be used: Sun, Mon, Tue, Wed, Thu, Fri, Sat

Example:

time.dayOfWeek = 1

time.dayOfWeek = Mon

28. time.dayOfYear

The day of the year on which the role mapping rule or resource policy rule is evaluated. Possible values are: 1-365.

Example:

time.dayOfYear = 100

29. time.month

The month in which the role mapping rule or resource policy rule is evaluated. Possible values are: 1-12

Example:

```
time.month = 9
```

30. time.year

The year in which the role mapping rule or resource policy rule is evaluated, where year can be set to [1900-2999].

Example:

```
time.year = 2005
```

31. user

User name. The user variable will include a domain name if AD/NT authentication is used.

Example:

```
user = 'steve'
```

```
user = 'steve*'
```

```
user = ('steve' or '*jankowski')
```

```
user = 'corp\steve'
```

32. userAgent

The browser's user agent string.

Example:

```
userAgent = '*MSIE*'
```

33. userAttr.<auth-attr>

User attributes retrieved from an LDAP or RADIUS server.

Example:

```
userAttr.division = 'sales'  
userAttr.employeeType = 'contractor'  
userAttr.dept = 'eng'  
userAttr.building = 'MtView[1-3]'
```

34. userDN

The user DN from an LDAP server. If the user is authenticated by the LDAP server, then this DN is from the authentication server; otherwise, the DN comes from the realm's Directory/Attribute server.

Example:

```
userDN = 'cn=John Harding,ou=eng,c=Company'
```

35. userDN.<user-attr>

Any variable from the user DN, where user-attr is the name of the RDN key.

Example:

```
userDN.ou = 'eng'
```

36. userDNText

User DN stored as a string. Only string comparisons to this value are allowed.

Example:

```
userDNText = 'cn=John Harding,ou=eng,c=Company'
```

37. userName

User name excluding domain name. The userName variable will always be just the user name excluding any AD/NT domain name.

Logical Operators

AND

OR

NOT