



CCTM IA CLAIMS DOCUMENT (ICD) Juniper Networks (UK) Limited

Secure Access SA-4500-FIPS/SA-6500-FIPS
IVEOS Version 6.5R1.0

VENDOR DETAILS	TEST LABORATORY DETAILS
Juniper Networks (UK) Limited	SiVenture
Aviator Park Station Road Addlestone Surrey KT15 2PG	Unit 6 Cordwallis Park Clivemont Road Maidenhead Berkshire SL6 7BU
Telephone Number: +44-(0)-137-238-5500	Telephone Number: +44(0)162 865 1366
Email: smckinnon@juniper.net	Email: simon.milford@siventure.com
Website: www.juniper.net	Website: www.siventure.com

CERTIFICATE DETAILS	
CCTM Certificate Number	2009/12/0062
CCTM Awarded on	8 th December 2009
CCTM Award Expires on	7 th December 2010
ICD Issue Date	8 th December 2009

TABLE OF CONTENTS

1	INTRODUCTION.....	3
1.1	Background.....	3
1.2	Objectives	3
1.3	Purpose of Document	3
1.4	Structure.....	3
2	IS PRODUCT/SERVICE DESCRIPTION.....	4
2.1	Product/Service Identification.....	4
2.2	Product/Service Overview.....	4
2.3	Usage assumptions.....	9
3	CCTM CLAIMS FOR THE IS PRODUCT OR SERVICE.....	14
3.1	Claims Statements	14
3.2	Existing assurance certificates.....	17

1 INTRODUCTION

1.1 Background

This document outlines the IA claims made by Juniper Networks in regard to the suitability of the Secure Access (SA) FIPS SSL VPN Appliances for use by the UK Public Sector for secure remote access solutions. Juniper Networks' SA has been designed to provide secure remote access to internal network resources across a wide-range of transit networks. The SA can provide secure remote access through a variety of different methods

Network-based Access

Application-based Access

File-server Access

Web-based enterprise applications

1.2 Objectives

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

1.3 Purpose of Document

1.3.1 This document is the ICD for the Juniper Networks SA FIPS SSL VPN Appliance.

1.3.2 This ICD is the baseline document for the CCTM Claims Test of Juniper Networks SA FIPS SSL VPN Appliance.

1.4 Structure

The structure of this ICD is as follows:

- Section 1 (this section) contains the introductory material.
- Section 2 contains the description of functionality of the Juniper Networks SA FIPS SSL VPN Appliance and all the information related to the security of the Juniper Networks SA FIPS SSL VPN Appliance.
- Section 3 details the security functionality claims that are being made.

2 IS PRODUCT/SERVICE DESCRIPTION

2.1 Product/Service Identification

Product Name: Juniper Networks' Secure Access Family

Version: IVEOS 6.5R1.0

Platforms: SA-4500-FIPS and SA-6500-FIPS

Operating System	Version	Browser	Version
Windows	2000 SP4	IE	6
Windows	2000 SP4	Firefox	3.5
Windows	XP SP3	IE	8
Windows	XP SP3	Firefox	3.5
Windows	Vista SP1	IE	8
Windows	Vista SP1	Firefox	3.5

2.2 Product/Service Overview

The SA acts as a secure application-layer gateway that intermediates all requests between remote computers and internal corporate resources. All requests to and from remote computers to an SA appliance are encrypted using TLS 168-bit encryption. All unencrypted requests (e.g. HTTP) are redirected to HTTPS which ensures the connection is always encrypted. Each request is subject to administratively defined access control and authorisation 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 authorised 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-4500-FIPS and SA-6500-FIPS appliances are shown in figure 2-1.



Figure 2-1 SA FIPS Appliances

2.2.1 Security architecture

The SA 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

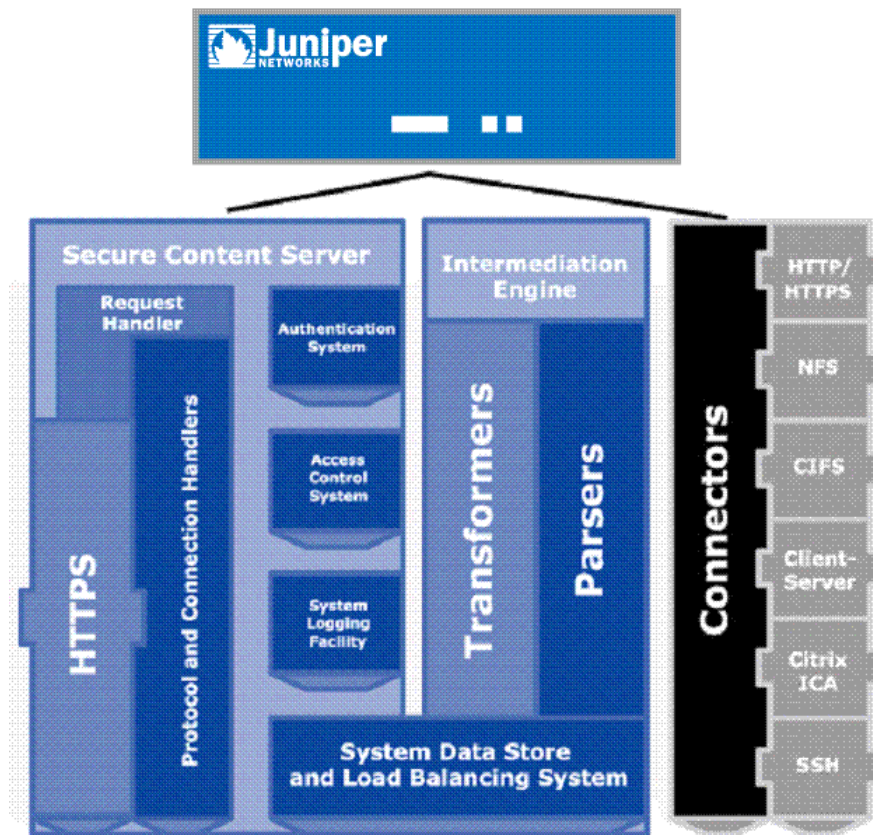


Figure 2-2 Juniper SA Architecture

2.2.1.1 Content Intermediation Engine

The Content Intermediation Engine is the core of SA. 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 a resource available to the role associated with the session, the appliance evaluates the corresponding resource policies. A resource policy is a set of resource names (such as URLs and hostnames) to which access is granted, denied or subject to 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; verifies that the user is who they claim to be. The SA 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 SA appliance submits a user's credentials to an authentication server for verification.

- A directory server; a server that provides user and group information to the SA appliance allowing it to map users to one or more user roles.
- Role mapping rules are conditions a user must meet in order for the SA appliance to map the user's session 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 SA 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:

SA 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 SA 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.

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.

2.2.2 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. To be tested:

- Juniper Networks SA-4500-FIPS
- Juniper Networks SA-6500-FIPS

2.2.3 Software requirements

There are no specific software requirements; the product being assured is a dedicated appliance running proprietary software. The software is provided by Juniper Networks as part of the solution. The software to be tested will be version IVEOS 6.4Rx running on the Juniper Networks SA 4500 FIPS and Juniper Networks SA 6500 FIPS platforms.

2.2.4 Out of Scope

The cryptographic algorithms used in IS Products and Services are not tested under the CCTM Scheme.

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

2.3 Usage assumptions

2.3.1 Assets

Typical assets to be protected by the SA are defined below, but are not limited to the following.

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

2.3.2 Threat Scenario

Threats to assets which are countered are:

- T1 An unauthorised person may send impermissible information through the SA which results in the exploitation of resources on the internal network.

- T2 An unauthorised 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.
- T3 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.
- T4 An unauthorised 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.
- T5 An unauthorised person may replay valid identification and authentication data obtained while monitoring the SA's network interface to access functions provided by the SA.
- T6 An unauthorised person may read, modify, or destroy security critical SA configuration data.
- T7 The SA may be inadvertently configured, used and administered in an insecure manner by either authorised or unauthorised persons.
- T8 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.
- T9 A user may attempt to store and instantiate executables on the SA appliance
- T10 Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- T11 Authorised administrators may attempt to manage the SA remotely from external networks.
- T12 Attempts to flow information among the internal and external networks are possible without passing through the SA.

2.3.2.1 Expected operational environment

This product, as part of an overall solution, will be used in the deployment of flexible and mobile working solutions in the UK Public Sector for networks carrying PROTECT and RESTRICTED data using the existing FIPS 140-2 certification and CESG AST Configuration Guidelines (http://www.cesg.gsi.gov.uk/ia-policy-portfolio/docs/security-procedures/juniper_networks.pdf).

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.

The solution scales from 50 to 10,000 users.

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.

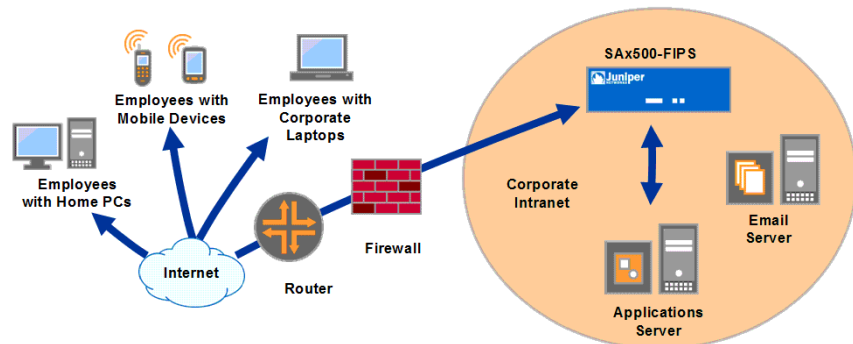


Figure 2-3 Typical Deployment Scenario

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.

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-6500-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.

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 grouped 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 un-authorized personnel.

3 CCTM CLAIMS FOR THE IS PRODUCT OR SERVICE

3.1 Claims Statements

Unique Reference	Claims Statements
CS1 Data Confidentiality, Integrity and Authentication	<p>The SA uses industry-standard TLS to provide security services at the application layer for all user data sessions. The ciphersuites to be used are:</p> <p>Protocol: TLS</p> <p>Signature: RSA</p> <p>Encryption: 3DES-CBC-EDE or AES-256-CBC-SHA</p>
CS2 Pre-Authentication Support	<p>The SA has extensive capabilities to profile an endpoint before permitting a sign-on page. Host Checker and Cache Cleaner results are used by an administrator to determine whether a particular endpoint meets the required security policy. Details of these checks are specified in CS8 and CS10.</p> <p>Results for Endpoint Point Security Check – Host Checker/Cache Cleaner</p>
CS3 Authentication Options	<p>Users and Administrators are authenticated by the SA through either a local server or via external servers. Only the following authentication servers will be tested.</p> <p>SA Local Server</p> <p>Active Directory</p> <p>RSA SecurID</p> <p>ITU-T X.509v3 Digital Certificate</p>
CS4 User Role Definition	<p>The SA controls the process of mapping users to roles through the use of the following variable:</p> <p>Username</p>
CS5 User Role Restrictions	<p>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:</p> <p>Results for Endpoint Point Security Check - Host Checker/Cache Cleaner</p>
CS6 Dynamic Resource-Based Authorisation Policies	<p>The resources that users access are tied to the Roles assigned to that user. The administrator can restrict access to these resources based on the following variable:</p>

	Assigned Role
CS7 User Agent Security	<p>To ensure that sensitive information from the Intranet is not left on the host machine, the SA ensures the following are maintained:</p> <p>Content is Marked as not Cacheable</p>
CS8 Client Security Check	<p>The SA deploys a component called Host Checker to profile the endpoint. The results of which can be used as mentioned in CS2 and CS5. The variables available to the administrator are as follows:</p> <p>Anti-Virus Products</p> <p>Personal Firewall Products</p> <p>Anti-Spyware Products</p> <p>Anti-Malware Products</p> <p>OS Versions plus Service Pack Level</p> <p>Allowable TCP/UDP Ports</p> <p>Disallowable TCP/UDP Ports</p> <p>Allowable Processes</p> <p>Disallowable Processes</p> <p>Allowable Files</p> <p>Disallowable Files</p> <p>File Version Checking</p> <p>MD5 File Hash Checking</p> <p>Allowable Registry Entries</p> <p>Disallowable Registry Entries</p> <p>Registry Version Checking</p> <p>Machine Certificate</p> <p>MAC Address</p>
CS9 Host Check Remediation	<p>If a user fails any of the checks defined in CS8, 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:</p> <p>Display Customisable Instructions to Users</p> <p>Evaluate Other Policies (allows for policy chaining)</p> <p>Kill Running Processes</p> <p>Delete Specific Files</p>
CS10 Browser Cache Cleaner	<p>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</p>

	<p>control the following aspects of IE:</p> <p>Disable AutoComplete of web addresses</p> <p>Disable AutoComplete of usernames and passwords</p> <p>Flush all existing AutoComplete passwords</p> <p>Empty Recycle Bin and Recent Documents list at the end of user session</p> <p>Clear Browser Cache</p> <p>Clear Files and Folders</p>
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 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 a Java-based component. The Windows version captures traffic from specific applications whilst the Java version uses a port-forwarding technique.
CS16 Network Connect (NC)	Network Connect is TLS component that creates a virtual ethernet interface in the host machine. It is then assigned a routable 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. Similar to SAM, NC can either be downloaded on demand or installed as a standalone application.
CS17 FIPS Hardware Cryptographic Module	The Hardware Security Module (HSM). 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. The HSM also handles the bulk data encryption.

3.2 Existing assurance certificates

FIPS-140-2 Level 3 Compliant Hardware Security Module: Cert #1050

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1050.pdf>

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 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.
- HTML 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.
- IPSEC 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.
- 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 SA range of products.
- 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 sub-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 (SA) 4500/6500-FIPS appliances provides secure, mobile, encrypted remote access services to public sector employees from a wide variety of devices and at different Information Assurance Impact Levels (IL) from 1-3. This technology is ideal for local authority mobile and flexible working schemes and for home access to Government Connects through a compliant Code of Connection. By leveraging comprehensive endpoint assessment features, administrators can provide different levels of access consistent with a centralized security policy. Ease of integration into existing systems and applications makes the Juniper SA platforms a very flexible and adaptable solution for most environments. This CCTM certificate covers the use of Juniper SA platforms for security environments up to and including IL2, but the same platforms have been approved by CESG for use at IL3 through specific guidance which is referenced in the ICD.