



CCTM TEST REPORT SUMMARY

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: +46 (0)462 765 100 | Telephone Number: +44 (0)1628 651 384 |

| | |
|---|-------------------------------|
| Test Report Summary Reference Number | <insert here> |
| Test Report Summary Version Number | 1-0 |
| Test Report Summary Date | 8 th December 2009 |
| CCTM Certificate Number | 2009/12/0062 |

Reproduction is authorised provided the document is copied in its entirety

Further details about the claims tested are included in [ICD] - published on the CCTM website (www.cctmark.gov.uk).

1 EXECUTIVE SUMMARY

1.1 Scope of IS Product Claims Tests

The Juniper Networks' Secure Access (SA) 4500 and 6500 FIPS SSL VPN Appliances have been designed to provide secure remote access to internal network resources across a wide-range of transit networks. The SA acts as a secure application-layer gateway that intermediates all requests between remote computers and internal corporate resources. For further details, see sections 2.1 and 2.2 of [ICD].

1.2 Test Results

The CCTM Claims Testing of the Juniper Network's Secure Access SA-4500 FIPS/SA-6500 FIPS version 6.5R1.0 by SiVenture concluded that the security functionality claims made within the IA Claims Document [ICD] are valid.

1.3 Observations and Recommendations

CS10 in Section 3.1 of [ICD] claims one function of the Cache Cleaner component is to delete specified files and sub-folders from an endpoint during their session (or after their session has ended). One constraint is that the Cache Cleaner is unable to delete any files stored on the root drive (C:*.*) of a PC running Microsoft Windows Vista (as its operating system). However, all files stored in sub-directories of the root drive can be deleted. This caveat is only applicable to the Vista operating system and is due to the way Vista implements administrator privileges for files on the root directory.

2 CCTM TEST OVERVIEW

2.1 Introduction

This Test Report documents the results of the CCTM Claims Tests of the IS Product as detailed in [ICD].

2.2 Scope of IS Product Claims Tests

Sections 2.1-2.2 of [ICD] describe the scope of the IS Product to be Claims Tested. The Test Laboratory confirmed this to be accurate for the IS Product tested.

Sections 2.2 and 2.3 of [ICD] summarise the security features, environmental assumptions, expected operational environment, operational security issues and threats, and platforms.

Section 2.2.4 of [ICD] details the security features of the Juniper Networks' SA-4500 FIPS/SA-6500 FIPS IVEOS 6.5R1.0 SSL VPN Appliances that are out of scope and hence are not tested under the CCTM Scheme. In particular, the cryptographic algorithms used in IS Products and Services are not tested under the CCTM Scheme.

The Test Laboratory performed tests based on the CCTM Claims made in Section 3.1 of [ICD] for the IS product. The Claims Tests were only performed with the IS Product running on the platform combinations and IT environment detailed in Section 2.4. The platforms themselves were not tested under the CCTM Scheme.

2.3 Location and Date of Tests

Details of the location[s] where the Test Laboratory conducted Claims Testing and where witness testing was undertaken can be found in [ICD].

The start and end dates of Claims Testing were as follows:

- Juniper Networks (UK) Limited: 2nd, 3rd and 5th November.
- SiVenture: 9th -11th and 17th November.

2.4 Platform Configuration

The platforms supported by the IS Product and used in the Claims Tests are detailed below:

Product: Juniper Networks' Secure Access Family

Version: IVEOS 6.5R1.0

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

Platforms for client devices:

| 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 |

2.5 Test Configuration

The test configuration comprised the product running on the platform combinations detailed below:

| Claim Reference | Platforms (IVEOS 6.5R1.0) | Operating System / browsers (see Section 2.6 for combinations) |
|-----------------|------------------------------|---|
| Installation | SA-4500 / SA-6500 | Not applicable |
| CS1 | SA-4500 / SA-6500 | IE and Firefox on all operating systems |
| CS2 | SA-4500 / SA-6500 | IE and Firefox on all operating systems |
| CS3 | SA-4500 / SA-6500 | IE8 on Vista |
| CS4 | SA-4500 / SA-6500 | IE8 on Vista |
| CS5 | SA-4500 / SA-6500 | IE8 on Vista |
| CS6 | SA-4500 / SA-6500 | IE8 on Vista |
| CS7 | SA-4500 / SA-6500 | IE and Firefox on all operating systems |
| CS8 | SA-4500 / SA-6500 | IE and Firefox on all operating systems |
| CS9 | SA-4500 / SA-6500 | IE and Firefox on all operating systems |
| CS10 | SA-4500 / SA-6500 | IE on all operating systems |
| CS11 | SA-4500 / SA-6500 | IE and Firefox on all operating systems |
| CS12 | SA-4500 / SA-6500 | IE8 on Vista |
| CS13 | SA-4500 / SA-6500 | IE8 on XP, Vista |
| CS14 | SA-4500 / SA-6500 | IE8 on Vista |
| CS15 | SA-4500 / SA-6500 | IE and Firefox on all operating systems |
| CS16 | SA-4500 / SA-6500 | IE and Firefox on all operating systems |
| CS17 | SA-4500 / SA-6500 | Not applicable |

2.6 Test Method

The Juniper Networks' SA-4500 FIPS/SA-6500 FIPS IVEOS 6.5R1.0 SSL VPN Appliances were tested using the Test Method [TLG and TM] against the security claims made in the [ICD].

3 EASE OF USE

The installation of the IS Product was as described in [QSG].

Administrators should note that the Juniper Networks' SA-4500 FIPS/SA-6500 FIPS IVEOS 6.5R1.0 SSL VPN Appliances are extremely flexible devices that can be configured to suit many secure operating environments. It is therefore necessary for the Administrators of this device to understand all possible configuration options when implementing this device on their Network. Administrators can find all the relevant configuration information in [AG] and as context sensitive help when using the administration interface. Juniper Networks also provides extensive support for these products.

4 QUALITY OF USER AND ADMINISTRATION DOCUMENTATION

The guidance documentation is detailed in [AG] and [QSG]. It is supplied with the IS Product or may be downloaded from the Vendor's website: www.juniper.net.

The [QSG] is a short (12 page) Quick Start Guide that details the installation process. The [AG] is a comprehensive (1078 pages) Administration Guide that details all the functionality of the IS Product and how it is configured and managed, including advice on policy, strategy and deployment.

5 RESISTANCE TO PUBLICLY KNOWN VULNERABILITIES

A search for publicly known vulnerabilities on a sample of security websites failed to yield any known weakness in the security of the IS Product. In addition, searches failed to find any publicly known vulnerabilities in the underlying platform for which patches were not available. None of these were relevant to the test configuration. The security websites surveyed were:

<http://www.cve.mitre.org>

<http://www.us-cert.gov>

<http://www.securityfocus.com>

<http://www.nvd.nist.gov>

6 VALIDATION OF EXISTING ASSURANCE CERTIFICATES

The Test Laboratory confirms that the existing assurance certificate specified in [ICD] has been validated for the exact version of the IS Product that has been Claims Tested. The certificate [Cert] was correctly stated in [ICD].

7 DISCLAIMERS

CCTM Claims Testing is not a guarantee of freedom from security vulnerabilities. There remains a probability that exploitable security vulnerabilities may exist in the IS Product/Service, or the IT environment supporting the IS Product/Service.

This Test Report Summary serves solely to summarise the results of testing carried out for the CCTM Scheme and is not an endorsement or otherwise of the IS Product/Service.

8 ABBREVIATIONS

The key IS Product abbreviations used within this Test Report are listed below. Generic CCTM Scheme abbreviations used within this report are defined in the Scheme Description [DES].

| Term | Meaning |
|----------|---|
| AES | Advanced Encryption Standard. |
| CBC | Cipher-Block Chaining |
| (3)DES | Data Encryption Standard |
| EDE | Encrypt, Decrypt, Encrypt (sequence for created ciphertext) |
| ESP | Encapsulating Security Payload |
| FIPS | Federal Information Processing Standards |
| HTML | HyperText Markup Language |
| HSM | Hardware Security Module |
| IE | Internet Explorer |
| oNCP/NCP | Junipers' (optimised) Network Communication Protocol |
| SA | Secure Access |
| SHA | Secure Hash Algorithm |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| VPN | Virtual Private Network |

9 REFERENCES

- [AG] Juniper Networks Secure Access Administration Guide, Part Number 65A063009 Release 6.5, August 2009;
- [Cert] FIPS-140-2 Level 3 Compliant Hardware Security Module: Cert #1050, <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1050.pdf>;
- [ICD] CCTM IA Claims Document (ICD), version 27, November 2009;
- [QSG] Juniper Networks Secure Access, Quick Start Guide for Secure Access 2500, 4500 and 6500, Part Number 530-023034 Revision 02, January 2009;
- [TLG] CCTM Scheme Test Laboratory Guide, Issue 3.0.0, March 2009;
- [TM] CCTM Generic Claims Test Method ([TLG] Appendix B) and Specialist Testing method ([TLG] Appendix G), Issue 3.0.0, March 2009;