Juniper Networks Secure Access Family, Release 5.1R2

Product Description

The Juniper Secure Access Family, Release 5.1R2 includes the following series of appliance models:

- Juniper Networks SA 2000, Release 5.1R2
- Juniper Networks NetScreen-SA 3000 FIPS, Release 5.1R2
- Juniper Networks 4000, Release 5.1R2
- Juniper Networks NetScreen-SA 5000 FIPS, Release 5.1R2
- Juniper Networks SA 6000, Release 5.1R2

The Juniper Secure Access Family Release 5.1R2 acts as a secure application-layer gateway that intermediates all requests between remote computers and internal corporate resources.

All requests from remote computers are encrypted using a secure HTTPS connection.

All unencrypted requests are redirected to HTTPS to ensure the connection is encrypted. Each request is subject to administratively derived access control and authorisation policies, such as dual factor or client side digital certificate administration, before the request is forwarded on to an internal resource.

Users gain authenticated access to authorised resources via an extranet session hosted by the appliance.

From any internet-connected Web server, users can access Web-based enterprise applications, Java applications, file shares and terminal hosts.

Common Criteria Certification – Scope

The scope of the Common Criteria (CC) certification included the following security functionality:

- Security Audit
- Cryptography
- User Data Protection
- Identification and Authentication
- Security Management

- Protection of the Security Function

Common Criteria Certification – Summary

The product has met the requirement of the Common Criteria (CC) evaluation assurance to EAL 2.

DSD Findings - Summary

Because the product employs cryptography, DSD performed a cryptographic evaluation on the product in addition to the Common Criteria certification.

It is possible to configure the SA4000 with encryption algorithms that have not been approved for Australian government use. Therefore, Australian Government users of the SA4000 are reminded that the encryption strength must be set in the Web GUI to allow only key lengths of "168-bits or greater" when configuring the product so that it uses 3DES. For more information regarding DSD Approved Cryptographic Algorithms (DACAs) please see ACSI 33 Chapter 9 on Cryptography.

The product has been evaluated to EAL 2. As such, the SA4000 can be used to transmit:

- UNCLASSIFIED data over networks of any classification
- IN-CONFIDENCE data over networks of any classification
- RESTRICTED data over networks of any classification
- PROTECTED data over networks of any classification
- HIGHLY PROTECTED data over IN-CONFIDENCE networks

It should be noted that information classified CONFIDENTIAL, SECRET or TOP SECRET MUST be encrypted using High Grade Cryptographic Equipment if it is transmitted over a network of lower classification.

Contact

For further information regarding the certification, cryptographic evaluation or compliance with ACSI 33 for the Juniper Networks Secure Access Family, Release 5.1R2, please contact DSD on (02) 62650197 or email assist@dsd.gov.au.

ACSI 33

The advice given in this document is in accordance with ACSI 33 release date September 2006. Australian Government agencies are reminded to check the latest release date of ACSI 33 at www.dsd.gov.au/library/infosec/acsi33.html to investigate if any changes have taken place.

Consumer Guide – Date

This Consumer Guide was issued on 14 May 2007 by DSD.