Juniper Networks Security Appliances: Juniper Networks NetScreen-5GT, 5XT, 25, 50, 204, 208, 500; Juniper Networks NetScreen ISG 1000 and 2000; Juniper Networks NetScreen 5200 and 5400

Product Description

The Juniper Networks evaluated products are integrated security appliances that control traffic flow through a network and operate as the central security hub in a network configuration. The appliances integrate stateful packet inspection firewall, virtual private networking (VPN) and traffic management features. All have hardware-accelerated IPSec encryption and very low latency, allowing them to fit into any network. Installing and managing the appliances is accomplished using a command line interface (CLI).

Each evaluated model consists of hardware and firmware and each runs ScreenOS 5.0.0.r9 in firmware, a Juniper proprietary operating system. The model differences have no effect on the security functions claimed within the Security Target.

The evaluated products generate audit records corresponding to traffic flow, administrator actions and identification and authentication. The evaluated products provide interfaces that allow the administrator to review the audit records, including the ability to search and sort the audit records. Additionally, the evaluated products provide the ability to protect the audit records and limit the loss of records due to storage exhaustion.

The evaluated products enforce an information flow policy that is enforced upon all packets attempting to traverse a Juniper Networks appliance. The policy is configurable by the administrator and is based on the presumed IP source address, destination IP address, protocol, source and destination interface and service. The evaluated products have a packet buffer for temporary storage of packet information. All temporary storage relative to every packet is known, thus ensuring that the product does not reuse any previous packet information. Additionally, the evaluated products provide encryption/decryption capabilities for VPN sessions.

Administrators are the only users of the evaluated products and are forced to be identified and authenticated by the product before they are allowed to invoke any administrator commands.

Security management is provided through the administrator interface. This interface allows an administrator (when properly identified and authenticated) to configure the Juniper Networks appliance. The security management functions are not available to non-administrator users.

The security functions of the evaluated products are protected in two ways. First, untrusted users do not have a direct interface to these functions; they are limited to sending packets to the device. Second, the administrative interface is a separate interface that is not connected to the network and, therefore, not susceptible to many of the general threats on the network such as packet sniffing or attempts to log into a public administrative interface.

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 4.

DSD Findings - Summary

Because the Juniper Network Security Appliances have cryptographic functionality, and furthermore all have the same cryptographic functionality, DSD performed a cryptographic evaluation of the NetScreen 208 in addition to the Common Criteria certification. The DSD evaluation determined that there were no issues with the implementation of the cryptographic functionality contained within the product, however it is possible to configure the Juniper Networks Security Appliances with encryption algorithms that have not been approved for Australian government use. Therefore, Australian government users are reminded that the 3DES or AES encryption algorithms must be chosen when configuring the symmetric encryption aspects of the product. Further to this, when implementing 3DES, users must use either:

- 2 distinct keys in the order key1, key2, key1, or
- 3 distinct keys.

For more information regarding DSD Approved Cryptographic Algorithms (DACAs) please see ACSI 33 Chapter 9 on Cryptography.

The product has been evaluated to EAL 4. As such, the Juniper Networks Security Appliances 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 networks of any classification.

It should be noted that information classified CONFIDENTIAL, SECRET or TOP SECRET must be encrypted using High Grade Cryptographic Equipment if it is to be 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 NetScreen Security Appliances, 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 14th May 2007 by DSD.