Cisco PIX Security Appliances 515/515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520 and 5540, Version 1.0

Product Description

The Cisco PIX Security Appliance and the Cisco ASA Adaptive Security Appliance are stateful packet filtering firewalls. A stateful packet filtering firewall controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connectionless IP packets against a set of rules specified by the firewall's authorised administrator. This header information includes source and destination host (IP) address, source and destination port numbers, and the transport service application protocol (TSAP) held within the data filed of the IP packet. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. The stateful firewall remembers the state of the connection from information gleaned from prior packets flowing on the connection and uses it to regulate current packets. The packet will be denied if the security policy is violated.

Common Criteria Certification - scope

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

- Security management to enable, disable, or modify the behaviour of the TOE.
- Security auditing.
- Information flow control between interfaces of the firewall.
- Identification and authentication of administrators.
- Provision of a secure multitasking environment with residual information protection and assured invocation of security functions.
- Provision of accurate data and time information.

Areas that were specifically out of scope for this certification were:

- RIP,
- SNMP,
- ASDM,
- DHCP Server, and
- Virtual private Networks

Common Criteria Certification – summary

The product has met the requirements of the CC evaluation assurance level EAL4.

DSD's Cryptographic Verification

As this product uses SSH for remote administration functions there was no need to conduct a cryptographic verification. SSH is considered a DSD Approved Cryptographic Protocol (DACP) and as long as used with a DSD Approved Cryptographic Algorithm (DACA) it is approved for use. In this case both 192-bit 3DES and 128-bit AES are available for use with SSH.

DSD's Recommendations

For Australian Government users it is recommended that the Cisco firewall be configured as per the Target of Evaluation (TOE) for this certification. Use of SSH for remote administration purposes should be configured in accordance with ACSI 33.

This product has been evaluated to EAL4+, and as such, in accordance with ACSI 33, it can be used for connecting networks of classifications of:

- IN-CONFIDENCE to UNCLASSIFIED or public domain networks;
- RESTRICTED to IN-CONFIDENCE, UNCLASSIFIED or public domain networks;
- PROTECTED to any national or non-national security classified network or public domain networks;
- HIGHLY-PROTECTED to any national or non-national security classified network above RESTRICTED or IN-CONFIDENCE; and
- HIGHLY-PROTECTED to UNCLASSIFIED or public domain when used in conjunction with another EAL4 firewall from a different manufacturer.

For information regarding firewall usage for national security classifications above RESTRCITED refer to block 3.10.32 of the SECURITY-IN-CONFIDENCE release of ACSI 33.

Contact

For further information regarding the certification of these products, or compliance with ACSI 33, please contact DSD on (02) 6265 0197 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 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 by DSD on 18 July 2007.