Cisco Firewall Services Module (FWSM) version 3.1 (4) for Cisco Catalyst 6500 switches and Cisco 7600 routers

Product Description

The Cisco FWSM is a stateful packet filtering firewall. 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.

In addition to IP header information, the Cisco FWSM mediates information flows on the basis of other information, such as the direction (incoming or outgoing) of the packet on any given firewall network interface. For connection-oriented transport services, the firewall either permits connections and subsequent packets for the connection or denies the connection and subsequent packets associated with the connection.

Common Criteria Certification – Scope

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

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

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

- Routing Information Protocol (RIP),
- Simple Network Management Protocol (SNMP),
- Dynamic Host Control Protocol (DHCP) Server, and
- Virtual Private Networks.

Common Criteria Certification – Summary

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

DSD - 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 AES are available for use with SSH.

DSD Recommendations

For Australian Government users the following cryptographic configuration is recommended:

- Tunnel Mode of operation using ESP;
- 3DES or AES as per DSD Approved Cryptographic Algorithms that meets ACSI 33;
- if using IKE/ISAKMP, disabling aggressive mode of operation and XAUTH support;
- HMAC-SHA1 or HMAC-MD5 as per hashing algorithms that meet ACSI 33;
- key generation using modulus sizes of 1024 bits or larger as per ACSI 33;
- a Diffie-Hellman Group with modulus size of 1024 bits or larger as per ACSI 33; and
- a maximum Security Association lifetime of 4 hours (14400 seconds).

This product has been evaluated to EAL2, and as such, in accordance with ACSI 33, it can be used for the transit of encrypted information of classification:

- IN-CONFIDENCE over an UNCLASSIFIED network;
- RESTRICTED over UNCLASSIFIED, IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED networks;
- PROTECTED over UNCLASSIFIED or IN-CONFIDENCE networks; and
- HIGHLY PROTECTED over IN-CONFIDENCE or PROTECTED.

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 periodically check the latest release of ACSI 33 at www.dsd.gov.au/library/infosec/acsi33.html.

Consumer Guide – Date

This Consumer Guide was issued by DSD on 05 September 2007.