Cisco IOS/Firewall v12.3(14)T & v12.4(4)T

Product Description

Cisco's Internetwork Operating System (IOS) is a software product that runs on proprietary Cisco hardware. This specific implementation of the IOS operates in the capacity of a firewall. Firewall functionality in a router is used to provide controlled and audited access to services between networks by permitting or denying the flow of IP traffic. Firewall options supported by Cisco routers include packet filtering, auditing and administration functions.

Common Criteria Certification – Scope

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

- Packet filtering functions.
- Searching and sorting of audit logs.
- Administration of firewall functions.
- Remote administration of the Cisco IOS via a SSH connection.

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

- Remote administration of the Cisco IOS router via SNMP, HTTP or Telnet.

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 of the Cisco IOS there was no need to conduct a cryptographic verification. SSH is considered a DSD Approved Cryptographic Protocol (DACP) and as long as it uses 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 Findings - Summary

For Australian Government users it is recommended that the Cisco IOS/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 an originating network of classification to a destination network of classification:

- IN-CONFIDENCE to UNCLASSIFIED or public domain networks;
- RESTRICTED to IN-CONFIDENCE, UNCLASSIFIED or public domain networks; and
- PROTECTED to national security above RESTRICTED, HIGHLY PROTECTED, PROTECTED, RESTRICTED, IN-CONFIDENCE, UNCLASSIFIED or public domain networks.

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 on 16 April 2007, by DSD.