Cisco IOS/IPSec 12.4(6)T3, 12.4(7) & 12.2(33)

Product Description

Cisco's Internetwork Operating System (IOS) is a software product that runs on proprietary Cisco hardware. A component of this software is the implementation of the IPSec suite of protocols. This allows system administrators to create a Virtual Private Network (VPN) between trusted networks over an untrusted network such as the Internet.

Common Criteria Certification – Scope

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

- IPSec implementation including IKE and ESP.
- Key management in support of the IPSec implementation.
- Packet filtering in support of the IPSec implementation.
- Configuration and management of the IPSec functions, primarily via an interactive Command Line Interface.

Common Criteria Certification – Summary

The product has met the requirements of the CC evaluation assurance level EAL2.

DSD - Cryptographic Verification

In addition to the CC evaluation, DSD verified a subset of the implementations of authentication, encryption and IKE/ISAKMP features available in the IOS, in software and hardware, for the Tunnel Mode of operation using ESP.

The following authentication features were verified:

- the SHA-1 hashing algorithm;
- the MD5 hashing algorithm; and
- truncation of long authentication keys.

The following encryption features were verified:

- 3DES encryption of data packets;
- AES encryption of data packets with key lengths of 128, 192 and 256 bits;
- correct encryption of small and large data packets; and
- truncation of long encryption keys.

The following IKE/ISAKMP features were verified:

- pre-shared keys; and
- RSA encrypted nonces.

Note: In the absence of access to relevant source code, the following could not be verified:

- rejection of short authentication keys; and
- rejection of short encryption keys.

Note: The features excluded from verification testing were:

- the Transport Mode of operation using AH or ESP;
- the Tunnel Mode of operation using AH; and
- IKE/ISAKMP using RSA signatures.

DSD Findings - Summary

As a result of the cryptographic verification process, it was found that (noting DSD's inability to verify the handling of short keys for authentication and encryption) each router correctly implemented SHA-1 and MD5 authentication, 3DES and AES encryption (using multiple key lengths), and IKE/ISAKMP using pre-shared keys and RSA encrypted nonces in software and hardware (where applicable).

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 21 March 2007.