CISCO IOS/IPSEC 12.4(11)T3, 12.4(15)T5 & 12.2(18)SXF10

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; and
- Configuration and management of the IPSec functions, primarily via an interactive Command Line Interface (CLI). Event logging facilities with reliable timestamps are also provided.

Common Criteria Certification - Summary

The product has met the requirements of the CC evaluation assurance level EAL4+ (augmented with ALC_FLR.1 – Basic Flaw Remediation). The CC evaluation covers the following IOS versions:

- 12.4(11)T3
- 12.2(18)SXF10

However, 12.4(11)T3 has subsequently been withdrawn and Cisco have replaced this with 12.4(15)T5 for the same hardware platforms. The DSD Cryptographic Evaluation included 12.4(15)T5 as part of this evaluation however this version has not undergone Common Criteria evaluation.

DSD - Cryptographic Evaluation

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

The authentication features verified were:

- the HMAC-SHA1 hashing algorithm,
- correct handling of small and large data packets, and
- truncation of long authentication keys.

The encryption features verified were:

- 3DES encryption of data packets with a key length of 168 bits,
- 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 IKE/ISAKMP features verified were:

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

Note: the features that were excluded from the verification activities were:

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

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

- rejection of short authentication keys;
- rejection of short encryption keys; and
- correct implementation of 3DES with 112 bit key lengths.

DSD Findings - Summary

As a result of the cryptographic verification process undertaken, it was found that each router correctly implemented HMAC-SHA1 authentication, 3DES (168 bit) and AES (128, 192 and 256 bit key lengths) encryption, manual keying and IKE/ISAKMP using pre-shared keys and RSA encrypted nonces using both software and hardware cryptographic engines (where applicable).

DSD Findings - 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 meet the ISM;
- if using IKE/ISAKMP, utilising Main Mode of operation only and disabling Aggressive Mode and XAUTH support;
- if using manual keying the key lengths specified must be of the appropriate length and in the case of 3DES with manual keying the key length must be 168 bit (equivalent to 192 bits of key material)
- HMAC-SHA1 as per hashing algorithms that meet the ISM;
- key generation using modulus sizes of 1024 bits or larger as per the ISM;
- a Diffie-Hellman Group with modulus size of 1024 bits or larger as per the ISM; and
- a maximum Security Association lifetime of 4 hours (14400 seconds).

This product has been evaluated to EAL 4 with a DSD Cryptographic Evaluation, and as such, in accordance with the ISM, it can be used to reduce transit encryption requirements of data of the following classifications:

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

Point of Contact

For further information regarding the certification of these products or compliance with the ISM please contact DSD on (02) 6265 0197 or email assist@dsd.gov.au.

ISM

The advice given in this document is in accordance with ACSI 33 release date September 2007. Australian Government agencies are reminded to 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 24 August 2009.