DSD'S CONSUMER GUIDE

NORTEL VPN ROUTER V7.05 AND CLIENT WORKSTATION V7.11

Product Description

The Nortel VPN Router v7.05 is a hardware-based IPsec VPN router with associated software (Client Workstation v7.11) that provides firewall, routing, encryption, authentication and data integrity services. Its main function is to provide remote access to private enterprise networks. Users install Client Workstation software and login through a web-based application. VPN sessions can be established using various tunneling protocols. Only the IPsec protocol is approved for use under Common Criteria. The Nortel VPN Router has the ability to encrypt and authenticate IP traffic between IPsec hosts. Encryption is performed using either 3DES or AES (in FIPS mode).

Common Criteria Certification - Scope

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

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the Security Function
- Trusted Path/Channels

Common Criteria Certification - Summary

The product has met the requirement of the Common Criteria (CC) evaluation assurance to EAL 4+.

DSD Findings - Summary

Because the product employs cryptography, DSD performed a cryptographic evaluation on the product in addition to the Common Criteria certification.

It is possible to configure the Nortel VPN Router with encryption algorithms that have not been approved for Australian government use. Therefore, Australian government users of the Nortel VPN Router are reminded that the encryption options must be configured to allow only 3DES or AES as the choice of symmetric algorithm. SHA-1 should be selected as the hashing algorithm. For more information regarding DSD Approved Cryptographic Algorithms (DACAs) please see the Australian

Government Information and Communications Security Manual (ISM) Chapter 9 on Cryptography.

The product has been evaluated to EAL 4. As such, the Nortel VPN Router can be used to transmit:

- UNCLASSIFIED data over networks of any classification
- IN-CONFIDENCE data over networks of any classification
- RESTRICTED data over networks of any classification
- PROTECTED data over networks of any classification
- HIGHLY PROTECTED data over networks of any classification

It should be noted that information classified CONFIDENTIAL, SECRET or TOP SECRET MUST be encrypted using High Grade Cryptographic Equipment if it is transmitted over a network of lower classification.

Point of Contact

For further information regarding the certification, cryptographic evaluation or compliance with the ISM for the Nortel VPN Router, please contact DSD on (02) 62650197 or email assist@dsd.gov.au

ISM

The advice given in this document is in accordance with ISM release date December 2008. Australian Government agencies are reminded to check the latest release date of ISM at www.dsd.gov.au/library/infosec/ism.html to investigate if any changes have taken place.

Date of this Consumer Guide

This consumer guide was issued by DSD on 12 August 2009.