SECURE COMPUTING CORPORATION – SIDEWINDER VERSION 7.0.0.02

Product Description

Sidewinder is a firewall and access control security platform for the enterprise enabling the implementation of safe and secure extranets for e-business. Sidewinder configured in its operational environment delivers strong security while maintaining performance and scalability. It proves access control of communication and information flow between two or more networks using application-level proxy and packet filtering technology.

The configured Sidewinder provides the highest levels of security by using SecureOS an enhanced UNIX operating system that employs Secure Computing's patented Type Enforcement security technology. Type Enforcement technology protects Sidewinder by separating all processes and services on the firewall.

Sidewinder is a network security gateway that allows an organisation to connect to the Internet while protecting the systems on its internal network from unauthorised users and network attackers. Sidewinder is aware of application-specific protocols and can filter data based on content. It also has packet filter capability to restrict traffic based upon source and destination.

Evaluation Scope

The scope of the Common Criteria evaluation included all functionality except for the following features:

- on-console Administration;
- Virtual Private Network (VPN);
- failover/high availability;
- anti-virus;
- URL filtering;
- mail filtering;
- policy acceleration network cards;
- SSL termination;
- direct login to a Sidewinder via Telnet or SSH;

- firewall policy cloning/one-to-many;
- remote administration from external networks; and
- built-in services (e.g. SSHD).

Common Criteria Certification Summary

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

DSD's Cryptographic Evaluation

Since there was no cryptography within scope of the Common Criteria evaluation DSD did not conduct a cryptographic evaluation.

DSD's Recommendations

For Australian Government users it is recommended that the firewall be configured as per the Target of Evaluation (TOE) for this certification.

This product has been evaluated to EAL4+, and as such, in accordance with ACSI 33, it can be used for connecting:

- IN-CONFIDENCE to UNCLASSIFIED networks;
- RESTRICTED to IN-CONFIDENCE or UNCLASSIFIED networks;
- PROTECTED to HIGHLY-PROTECTED, PROTECTED or IN-CONFIDENCE networks;
- PROTECTED to RESTRICTED or UNCLASSIFIED networks;
- HIGHLY-PROTECTED to HIGHLY-PROTECTED, PROTECTED or IN-CONFIDENCE networks;
- HIGHLY-PROTECTED to RESTRICTED or UNCLASSIFIED when used in conjunction with another EAL4 firewall from a different manufacturer.

For information regarding firewall usage for national security classifications above RESTRCITED refer to blocks 3.10.36-37 of the SECURITY-IN-CONFIDENCE release of ACSI 33.

Point of Contact

For further information regarding the Sidewinder certification 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 2007. Australian Government agencies are reminded to check the latest release of ACSI 33 at www.dsd.gov.au/library/infosec/acsi33.html to investigate if any changes have taken place.

Date of this Consumer Guide

This Consumer Guide was issued by DSD on 21 November 2007.