Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2009/51

16 Feb 2009

Version 1.0

Amendment Record

Version	Date	Description
0.1	02/02/2009	Internal release.
0.2	09/02/2009	Extended review.
1.0	16/02/2009	Public release.

Executive Summary

1 The Target of Evaluation (TOE) is the Cisco Network Admission Control (NAC) solution including the NAC Appliance, NAC Network Module for Cisco Integrated Services Routers (ISRs), NAC Agent, NAC Profiler, and Cisco Secure Access Control Server (ACS). The TOE is designed to enforce host security policies on all hosts as they attempt to enter the protected network ensuring all hosts comply with corporate security policies before gaining access to the protected network.

2 This report describes the findings of the IT security evaluation of Cisco Systems Inc's Cisco NAC solution, to the Common Criteria (CC) evaluation assurance level EAL2 augmented with ALC_FLR.2. The report concludes that the product has met the target assurance level of EAL2 augmented with ALC_FLR.2 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by CSC and was completed in February 2009.

3 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that users:

a) only use the TOE in its evaluated configuration; and

b) operate the TOE according to the administrator guidance (Refs [3][4][5][6][7][8][9][10][11][12][13]).

4 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

5 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at Ref [1], and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

6 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

7 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Cisco NAC solution, against the requirements of the Common Criteria (CC) evaluation assurance level EAL2 augmented with ALC_FLR.2, and

b) provide a source of detailed security information about the TOE for any interested parties.

8 This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

9 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.5.1 Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Cisco Network Admission Control (NAC) solution including the NAC Appliance, NAC Network Module for Cisco Integrated Services Routers (ISRs), NAC Agent, NAC Profiler, and Cisco Secure Access Control Server (ACS)
Software Version	Cisco NAC Appliance Versions 4.1.6 with patch CSCsv84296, NAC Profiler Collector Release 2.1.8-37, NAC Agent version 4.1.6, NAC Appliance Profiler Release 2.1.8- 37, Cisco Secure ACS for Windows Server version 4.1.4.13
Security Target	Cisco Network Admission Control, Security Target, Revision 1, January 2009
Evaluation Level	EAL2 augmented with ALC_FLR.2
Evaluation Technical Report	Cisco Network Admission Control, Evaluation Technical Report, Version 2.0, 6th February 2009

Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, CCMB- 2006-09-001, September 2006.
Methodology	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2007, version 3.1, Revision 2, CCMB-2007-09-004
Conformance	CC Part 2 extended CC Part 3 conformant, augmented with flaw reporting procedures (ALC.FLR.2). Protection Profile Conformance with U.S. Government Protection Profile Intrusion Detection System Analyzer for Basic Robustness Environments, Version 1.3, dated July 25, 2007.
Sponsor/ Developer	Cisco Systems Inc, 170 West Tasman Dr. San Jose, CA 95134.
Evaluation Facility	CSC Australia Pty Limited's Australasian Information Security Evaluation Facility (AISEF), 15 National Circuit, Barton, ACT 2600, Australia

Chapter 2 - Target of Evaluation

2.1 Overview

10 This chapter contains information about the TOE, including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

11 Cisco NAC is a solution that enables the network infrastructure to enforce security policies on all devices seeking to access network computing resources. Cisco NAC helps ensure that all hosts comply with the latest corporate security policies, such as antivirus, security software, and operating system patch, prior to obtaining normal network access. Vulnerable and noncompliant hosts will be isolated (quarantined) or given limited access until they reach compliance. In addition, Cisco NAC has the ability to perform user authentication at the network level so that only devices with proper user credentials are permitted network access.

2.3 TOE Architecture

12 The TOE is comprised of several major categories of subsystems. These subsystems work together in enforcing the TOE Security Policy (TSP). The major subsystems are as follows:

2.3.1 NAC Manager Subsystems

13 The NAC Manager subsystems provide the following functionality:

- configures and manages the NAC Server subsystem;
- provision of the command line interface (CLI);
- provision of a web console GUI, for a single point of management for the NAC solution (NAC Manager and NAC Servers);
- establishment of secure SSL sessions between the administrative users browser and the NAC;
- Manager and the NAC Manager and other TOE components;
- provision of all necessary cryptographic functions required to establish secure SSH connections;
- management of all administrative and network user requests for local and remote authentication;
- management and configuration of the NAC Servers, device and subnet filtering and vulnerability assessment and remediation;
- management and configuration of the Out-of-Band deployment of Group, Switch, and Port profiles for Out-of-Band deployment, and the Manager's SNMP system;
- management and configuration of users and user roles, traffic control policies;
- management and viewing of NAC Manager Event logs and configuration of SNMP polling and alerting for the NAC Manager;
- configuration of the NAC Manager including:
  i) Clean Access Manager (CAM) SSL certificates;
  ii) Setting system time;
  iii) Creating/restoring the CAM database;
  iv) customising the web login pages for web login users; and
  v) Managing administrative users, groups and privileges.
- storage and retrieval of user information and configuration parameters; and
- provision of SNMPv3 protected communication between the NAC Manager and the Access Switch.

2.3.2 NAC Server Subsystems

14 The NAC Server subsystems provide the following functionality:

- provision of the CLI;
- establishment of secure SSL sessions between the administrative users browser and the NAC;
- Server Web Console;
- provision of all necessary cryptographic functions required to establish secure SSH connections;

- management of all administrative and network user requests for local and remote authentication;
- configuration and implementation of pass-through policies;
- implementation of global and local traffic control policies;
- removal of devices from the Certified Devices list;
- setting the onboard hardware clock manually or using an external NTP server;
- collection of endpoint information for the system that is processed into the database; and
- analysed and presented by the NAC Profiler Server.

2.3.3 NAC Profiler Subsystems

15 The NAC Profiler subsystems provide the following functionality:

- provision of a web console GUI, for management of the NAC Profiler Server;
- provision of the CLI of the NAC Profiler Server;
- establishment of secure SSL sessions between the administrative users browser and the NAC
- Profiler Server and the NAC Profiler Server and NAC Manager;
- establishment of secure SSH sessions between either the administrative users SSH console and the NAC Profiler Server or the NAC Profiler and the NAC Manager;
- management of all administrative and network user requests for local and remote authentication;
- provision of timestamps for the profiler audit data;
- receipt of configuration commands from the web console and Profiler;
- parsing of endpoint data from the NAC server;
- synchronisation of profiler data with the NAC manager;
- analysis of new or modified devices to determine if the device meets an acceptable profile;
- facilitation of encrypted communication between the NAC Profiler and the NAC Server;
- receipt and sending of all information from the other Profiler subsystems; and
- collection and storage of all Auditable events.

2.3.4 NAC Agent Subsystems

16 The NAC Agent subsystems provide the following functionality:

- policy enforcement;
- sends client health report to NAC Server subsystem;
- display of remediation instructions actions that must be taken by the user in order for the machine to be able to pass assessment; and
- temporal vulnerability assessment for client machines.

2.3.5 Switch / Router Subsystems

17 The Switch / Router subsystems provide the following functionality:

- control traffic flows from the un-trusted network through the TOE in the Out-of-Band configuration based on IP based policy;
- maintenance of the run time clock function;
- acceptance of user input and provision of an interface to the command line parser;
- user authentication to router / switch;
- management of user privilege levels;
- enablement SSH to make a secure, encrypted connection to the switch;
- receipt and storage of system event messages for retrieval and review by an authorised administrative user; and
- provision of SNMPv3 protected communication between the NAC Manager TOE component and the Access Switch in Out-Of-Band configurations.

2.3.6 Cisco Secure ACS Subsystems

18 The Secure ACS subsystems provide the following functionality:

- maintenance of user identifiers and passwords;
- RADIUS authentication of network users when the credentials are passed from the NAC Appliance Manager;
- generation of audit log entries; and
- protection of remote administrative sessions.

2.4 Clarification of Scope

19 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.4.1 Evaluated Functionality

20 The TOE provides the following evaluated security functionality:

- **NAC Decisions** - The TOE is able to grant access to the protected network based on the following:
  - i) **Device and User Authentication** – authentication uses the certified devices list within the NAC Manager for device authentication and either the built-in database within the NAC Manager or the Cisco Secure ACS for user authentication;
  - ii) **Posture Assessment** – Tests and Vulnerability scans initiated by the NAC Manager;
  - iii) **Remediation** – forces the connecting host to execute updates before network access is granted; and
  - iv) **Profiling** – allows the TOE to keep track of devices such as printers and FAX machines, not capable of running the NAC agent, thus allowing administrators to understand the types of devices connecting to the network;
- **Audit** - Allows an administrator to view changes in policy, auditing and NAC decisions;
- **Administrator Identification and Authorisation (I&A)** – forces administrators to authenticate prior to gaining access to CLI and Graphical User Interfaces of the NAC Manager;

- **Management** – Provides secure management of the TOE via the NAC Manager CLI (SSH protected) or a GUI over a HTTPS-secured web browser session; and
- **Self Protection** – The NAC appliance provides for isolation at the physical boundary of the TOE ensuring no untrusted processes are permitted on the NAC appliance.

2.4.2 Non-evaluated Functionality

21 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information and Communications Technology Security Manual (ISM) (Ref [2]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

22 The functions and features that have not been included as part of the evaluation are provided below:

- High Availability
- Automated Security Policy Updates
- Authentication Mechanisms:
  i) Kerberos
  ii) NT Lan Manager (NTLM)
  iii) Light Weight Directory Access Protocol (LDAP)
  iv) Active Directory Single Sign On (AD SSO)
  v) Virtual Private Network (VPN) SSO
  vi) NetBIOS SSO
  vii) S/Indent

2.5 Usage

2.5.1 Evaluated Configuration

23 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in these defined evaluated configuration(s). Australian Government users should refer to ISM (Ref [2]) to ensure that configuration(s) meet the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

24 The TOE consists of the following components and applicable versions:

TOE component	**Version**
NAC Appliance Manager. Running on any of the following NAC Appliances 3300 Series platforms:	 Version 4.1.6 with patch CSCsv84296

NAC-3310, NAC-3350, or NAC-3390	
NAC Appliance Server Running on any of the following NAC Appliances 3300 Series platforms: NAC-3310, NAC-3350, or NME-NAC-K9 installed in any of the following Integrated Services Routers (ISRs) running Cisco IOS 12.4(11)T or later: Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3825, or Cisco 3845.	NAC Appliance Server version 4.1.6 (including ActiveX agent to be used when NAC Agent is not available)
NAC Agent software Compatible with Windows Vista, Windows XP, Windows 2000, Windows 98, Windows SE, Windows ME; Mac OS X (10.2, 10.3, 10.4)	Version 4.1.6
Cisco NAC Profiler Server Running on a NAC Appliance 3300 Series 3350 platform (NAC3350-PROF)	2.1.8-37
Cisco NAC Collector Running as an additional component on the NAC Appliance Server 3310 or 3350	2.1.8-37
Cisco Secure ACS	Version 4.1.4.13
Access switch for OOB deployments Running on any of the following. Catalyst 6503 chassis with Supervisor 720, Catalyst 6504 chassis with Supervisor 720, Catalyst 6506 chassis with Supervisor 720, Catalyst 6509 chassis with Supervisor 720, Catalyst 6513 chassis with Supervisor 720, or Catalyst 3750.	65xx running 12.2(33)SXH or 3750 running 12.2(44)SE)

25 The TOE may be deployed in one of three scenarios: In-Band Edge, In-Band Central, or Out-of-Band Central. All three scenarios are included in the evaluated configuration. Scenario deployment configuration requirements are detailed in Security Target (Ref [1]).

2.5.2 Delivery procedures

26 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product.

27 For hardware components; using the packing slip and information on the stickers, the customer must check that the product number and serial numbers on the received hardware match what was ordered. Any discrepancies must be immediately reported to Cisco using the contact information on the packing slip.

28 For Software the customer will access CCO (Cisco Connection Online) to download images. Customers will be prompted for their login and password. To create an account on CCO a user must have a valid support contract with Cisco and access to the contract number. Access control on the CCO site controls what software images a user account is allowed to download. Encryption using SSL protects the software images as they are being downloaded from the Cisco web server to the user's computer.

2.5.3 Determining the Evaluated Configuration

29 To ensure the hardware received is the evaluated product the customer must check the models received against the list of TOE component hardware models at the beginning of the Cisco NAC Appliance Version 4.1 Preparative Procedures Wrapper, Version 8.0, January 2009 document (Ref [3]). This document is made available on the Cisco website for download.

30 In addition to verifying model numbers for hardware components, the software versions must also be verified by the customer recipient. Software versions can be checked by following the "Verification of Image" instruction included in the user guidance.

2.5.4 Product Installation

31 Installation, generation and start up of the TOE such that it is in evaluated configuration is detailed for the consumer in the document Preparative Procedures Wrapper (Ref [3]). This document lists considerations including – but not limited to – User Authentication, In-Band edge, In-Band Central and Out-of-Band configurations.

2.5.5 Documentation

32 It is important that the TOE is used in accordance with guidance documentation in order to ensure the secure usage. The following documentation is available to the consumer for download online at www.cisco.com:

- Preparative Procedures Wrapper for Cisco NAC Appliance Version 4.1(6), Version 8.0, January 2009 (Ref [3]).

This document provides information regarding the key configuration requirements and directs users to the specific user guidance document(s) for each of the TOE components.

The documents below describe the processes and other relevant information for the secure installation and operation of the various components of Cisco NAC. Additionally these documents describe the usage assumptions and details the technical information regarding the TOE's usage (Refs [4][5][6][7][8][9][10][11][12][13]) :

- Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(6), April 08;
- Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(6), April 08;
- User Guide for Cisco Secure Access Control Server, Release 4.1;
- Cisco Network Modules Hardware Installation Guide;
- Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8, August 08;
- Basic Software Configuration Using the Cisco IOS Command-Line Interface, OL-5593-01;
- Basic Software Configuration Using the Setup Command Facility, OL-5992-01;
- Catalyst 6500 Series Switch MSFC Command Reference, OL-5081-03;
- Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide, OL-3999-08;
- Catalyst 3750 Switch Software Configuration Guide, OL-8550-05;

2.5.6 Secure Usage

33 The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

34 The following assumptions were made:

a) The TOE has access to all the IT System resources necessary to perform its functions.

b) The TOE hardware and software critical to security policy enforcement will be protected from unauthorised physical modification.

c) The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorised physical access.

d) There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

e) The authorised administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

f) The TOE can only be accessed by authorised users.

g) The Agent Component will be installed on a physically protected, properly configured IT platform and operated in a secure manner.

35 In addition, the following organisational security policies must be in place:

a) Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to Intruder Detection System (IDS) data and appropriate response actions taken.

b) Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

c) The TOE shall only be managed by authorised users.

d) All data analysed and generated by the TOE shall only be used for authorised purposes.

e) Users of the TOE shall be accountable for their actions within the IDS.

f) Data analysed and generated by the TOE shall be protected from modification.

g) The TOE shall be protected from unauthorised accesses and disruptions of analysis and response activities.

Chapter 3 - Evaluation

3.1 Overview

36 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

37 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [14][15][16]). The methodology used is described in the Common Methodology for Information

Technology Security Evaluation (CEM) (Ref [17]). The evaluation was also carried out in accordance with the operational procedures of the AISEP (Refs [18][19][20][21]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [22]) were also upheld.

3.3 Functional Testing

38 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

39 Whilst not related directly to a specific test; during Installation and Generation of the TOE in preparation to perform testing the evaluators determined that the TOE did not behave as described in the Security Target (Ref [1]). The evaluators identified a software bug in the TOE that resulted in the NAC Manager appliance incorrectly processing encrypted (AuthPriv) SNMPv3 traps. The sponsor subsequently rectified the issue by providing the evaluators with a software patch upgrade (CSCsv84296).

3.4 Penetration Testing

40 The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly available information.

41 Of the vulnerabilities examined, the evaluators deemed that the published attacks were of no impact as they:

- did not violate the TSP;
- required authentication on behalf of the user; and
- were based on earlier Cisco NAC architectures with significant changes to the TOE such that they were of no impact.

As an alternative the evaluators concentrated on the underlying network protocols and supporting infrastructure.

42 The analysis conducted by the evaluators and the subsequent testing indicated that the TOE will resist an attacker with an attack potential of Basic which is consistent with the requirements of an EAL2+ assurance level.

Chapter 4 - Certification

4.1 Overview

43 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

44 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (ETR) (Ref [23]), the ACA certifies the evaluation of Cisco NAC solution performed by the Australasian Information Security Evaluation Facility, CSC.

45 CSC has found that Cisco NAC solution upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL2 augmented with ALC_FLR.2.

46 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

47 EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behaviour.

48 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

49 EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

4.4 Recommendations

50 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref [2]) and New Zealand Government users should consult the GCSB.

51 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3][4][5][6][7][8][9][10][11][12][13]), the ACA also recommends that the administrator follow the Preparative Procedures Wrapper document (Ref

[3]) to ensure an attacker cannot circumvent the isolation mechanisms of the Access Switch.

Annex A - References and Abbreviations

A.1 References

[1] Security Target for Cisco Network Admission Control, Revision 1, January 2009

[2] Australian Government Information and Communications Technology Security Manual (ISM), 2008, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Preparative Procedures Wrapper for Cisco NAC Appliance Version 4.1(6), Version 8.0, January 2009

[4] Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(6), April 08;

[5] Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(6), April 08

[6] User Guide for Cisco Secure Access Control Server, Release 4.1

[7] Cisco Network Modules Hardware Installation Guide

[8] Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8, August 08

[9] Basic Software Configuration Using the Cisco IOS Command-Line Interface, OL-5593-01

[10] Basic Software Configuration Using the Setup Command Facility, OL-5992-01

[11] Catalyst 6500 Series Switch MSFC Command Reference, OL-5081-03

[12] Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide, OL-3999-08

[13] Catalyst 3750 Switch Software Configuration Guide, OL-8550-05

[14] Common Criteria for Information Technology Security Evaluation – Part 1:Introduction and general model, dated September 2006, version 3.1, Revision 1,CCMB-2006-09-001

[15] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2007, version 3.1, Revision 2, CCMB--2007-09-002

[16] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2007, version 3.1, Revision 2, CCMB-2007-09-003

[17] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2007, version 3.1, Revision 2, CCMB-2007-09-004

[18] AISEP Publication No.1, Program Policy, AP1, Version 3.1, September 2006, Australian Certification Authority, (available at www.dsd.gov.au).

[19] AISEP Publication No. 2, Certifier Guidance, AP 2. Version 3.0, 21 February 2006, Australian Certification Authority.

[20] AISEP Publication No.3, Evaluator Guidance, AP3, Version 3.1, September 2006, Australian Certification Authority.

[21] AISEP Publication No. 4, Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September, Australian Certification Authority, (available at www.dsd.gov.au).

[22] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[23] Cisco Network Admission Control, Evaluation Technical Report, Version 2.0, 6th February 2009.

A.2 Abbreviations

ACA	Australasian Certification Authority
ACS	Access Control Server
AD SSO	Active Directory Single Sign On
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CAM	Clean Access Manager
CC	Common Criteria
CCO	Cisco Connection Online
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
I&A	Identification and Authorisation
IDS	Intrusion Detection System
ISM	Australian Government Information and Communications Technology Security Manual
ISR	Integrated Services Routers
LDAP	Light Weight Directory Access Protocol
NAC	Network Admission Control
NTLM	NT Lan Manager
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VPN	Virtual Private Network