Cisco Network Admission Control Security Target

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco Network Admission Control solutions. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

April 2009
Version: 2.0

Table of Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

List of Tables

List of Figures

Security Target Introduction

This Chapter presents Security Target (ST) identification information, an overview of the ST, Target of Evaluation (TOE) identification, an overview of the TOE, and an in-depth description of the TOE including a description of the security features provided by the TOE and the physical components of the TOE. An ST contains the information technology (IT) security requirements of an identified TOE and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. The Security Target contains the following sections:

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 4.

ST and TOE Identification

This section provides information needed to identify and control this ST and its TOE. This ST targets Evaluation Assurance Level EAL2 augmented with ALC_FLR.2. This ST also is compliant with the U.S. Government Protection Profile Intrusion Detection System Analyzer for Basic Robustness Environments, Version 1.3, dated July 25, 2007.

Table 1 ST and TOE Identification

ST Title	Cisco Network Admission Control Security Target
ST Version	Revision 2.0
Publication Date	April 2009
Vendor and ST Author	Cisco Systems
TOE Identification	Cisco Network Admission Control (NAC) solution including the NAC Appliance, NAC Appliance network module for Cisco Integrated Services Routers (ISRs), NAC Agent, NAC Profiler, and Cisco Secure ACS
TOE Software Version	Cisco NAC Appliance Versions 4.5.1, NAC Profiler Collector Release 2.1.8-37, NAC Agent version 4.5.1, NAC Appliance Profiler Release 2.1.8-37, Cisco Secure ACS for Windows Server version 4.1.4.13
Security Target Evaluation Status	Final
Keywords	IDS, Analyzer, Network Security

TOE Overview

Cisco® Network Admission Control (NAC) is a solution that enables the network infrastructure to enforce security policies on all devices seeking to access network computing resources. 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.

Note that throughout the ST the term NAC Appliance will be used to refer to the 3300 series hardware and software package. If the actual physical appliances are intended, a name such as the 3300 Series appliance platforms will be used.

TOE Product Type

The Cisco NAC TOE is a network-based admission control solution that allows organizations to enforce their host security policies on all hosts as they enter the interior of the network, regardless of their access method, ownership, device type, application set, or operating system. 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 credentials are permitted network access.

Required Non-TOE Hardware/ Software/ Firmware (IT Environment Dependencies)

The TOE requires Internet Explorer Web browser (Microsoft Internet Explorer 6.0 or higher) to be used by administrators of the TOE to communicate with the TOE's administrative web interfaces.

The TOE relies on the Windows and Mac Operating Systems for the Agent to operate and for some protection, including cryptography. The Agent relies on the host Windows or Mac OS for protection of the software application files and processes running. The Agent also relies on the host OS for crypto libraries for establishing SSL communications back to the NAC Server. The specific versions of Windows and Mac OS's that are included in the evaluation are listed under the "Annex A: Cisco NAC Agent System Requirements" section on page 76 of this document.

The TOE relies on the Windows Server Operating System (Windows 2000 and 2003) for the Cisco Secure ACS to operate and for some protection, including cryptography. The Agent relies on the host Windows Server OS for protection of the software application files and processes running.

The TOE in In-Band Central and Out-of-Band deployments relies on a router if the TOE is configured as layer-3 adjacent.

The TOE in In-Band Central and Out-of-Band deployments relies on a central switch to perform VLAN separation and processing of traffic.

The TOE also supports devices in the environment with no ability to run the agent or a web browser, such as IP Phones, printers, etc.

TOE Description

This section provides an overview of the Cisco NAC Target of Evaluation (TOE). This section also defines the physical and logical boundaries of the TOE and describes the evaluated configuration of the TOE.

Overview

The Cisco NAC protects corporate assets and applies an organization's security policy to users and their devices consistently. It addresses the pressing security concerns arising from a mobile workforce, increased business interactions, usage of personal devices, attacks from the inside and stringent compliance requirements.

A primary advantage of this solution is enabling user authentication at the network and physical layer, and then using that information to grant network access based on the user's identity and characteristics of the device. For example, all guest users receive only limited Internet access and internal access. Cisco NAC can leverage existing security technologies, such as antivirus, antispam, and operating system updaters to ensure that the user machines are current with the latest patches. Cisco NAC can also collaborate with the network infrastructure to identify, assess and authorize users according to the compliance status of the user's PC.

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. In-Band refers to scenarios where the NAC Server is deployed in-line between the connecting hosts and the internal network. Out-of-Band refers to scenarios where the NAC Server is not in-line but is deployed off of the central switch. Edge refers to scenarios where the NAC Server sits on the edge of the network between an access switch and a central deployment switch. Central refers to scenarios where the NAC Server is centrally located off of the central deployment switch in the network.

Additionally, the TOE is deployed in either layer 2 mode or layer 3 mode. Both modes of operation are included in the evaluated configuration. In Layer 2 mode, users are Layer 2-adjacent to the Cisco NAC Appliance Server. In Layer 3 mode, users are multiple Layer 3 hops away from the Cisco NAC Appliance Server.

The In-Band Central and Out-of-Band Central deployment scenarios run either in Layer 2 or Layer 3 mode with respect to the NAC Server (In-Band Edge deployments do not run in Layer 3 mode since the Cisco NAC Appliance Server is Layer 2 adjacent to the network and does not require routers to route traffic to it). Layer 2 mode indicates that all clients in the auth VLAN are Layer 2 adjacent to the NAC Server (i.e. they are in the same IP subnet as the NAC Server and the NAC Server can see real MAC addresses of all clients). Layer 3 mode indicates that all clients are one or more routed Layer 3 hops away from the NAC Server (i.e. client traffic must pass through one or more routers to reach the NAC Server). Layer 3 also includes layer 2 adjacency checks, and requires use of either the NAC Agent or an ActiveX or Java applet with web login for the NAC Appliance to learn the client's real MAC address.

In cases where Layer 3 mode is deployed, out-of-band (IT environment) traffic control methods are required to implement the traffic controls on the auth VLAN. In this scenario either policy-based routing (PBR) or access control lists (ACLs) can be used to restrict traffic. PBR works by forcing defined traffic to follow a set path through the network to the NAC Server, and it overrides the existing route if that traffic is detected. ACLs work by filtering traffic based on rules, and would be configured on the Layer 3 device closest to the connecting clients. PBR and ACLs can be used in the same network, for example ACLs could be placed on the devices closest to the clients, and the next hops could have the PBR policy implemented.

The TOE may be configured to handle Layer 2 and Layer 3 mode configurations, as follows:

A. Layer 2 mode — When the NAC Application Server is operating in Layer 2 mode it is acting as a L2 bridge similar to the way an inline IPS device looks. In this configuration, the NAC Appliance Server does not have an externally visible IP address.

B. Layer 3 mode – In L3 mode, the NAC Application Server is acting as a router and routes packets from the outside to inside interface which are on two different networks.

The In-Band Edge, In-Band Central, and Out-of-Band Central deployment scenarios are described in detail below.

The NAC includes several TOE components, some of which are not applicable in all of the scenarios listed above. See the following table for how the required components break up based on these three scenarios. The components listed are required for both Layer 2 and Layer 3 modes unless otherwise noted in the table. Note that (ENV) indicates that the component is part of the environment:

Table 2 NAC Components

Component	In-Band Edge	In-Band Central	Out-of-Band Central
Cisco NAC Appliance Manager	Required	Required	Required
Cisco NAC Appliance Server	Required (can be NME[1])	Required (can be NME)	Required
NAC Profiler (Server and Collector)	N/A	N/A	Required
Central deployment switch (ENV)	N/A for security enforcement	Required	Required
Cisco Catalyst access switch	N/A, can be any switch	N/A, can be any switch	Required
Cisco NAC Agent (Software/ ActiveX)	Required	Required	Required
Cisco Router – base for NME	Required, if NME used	Required, if NME used	N/A
Router (ENV)	N/A	Required, if layer-3 adjacent[2]	Required, if layer-3 adjacent
Cisco Secure ACS	Required	Required	Required

1. The NAC Server can be deployed as a stand-alone appliance or as a network module (NME) in a Cisco router.
2. Indicates scenarios where routing happens between the connecting host and the NAC Server. See below for complete definition.

These components are described in more detail in the subsections below.

The stages of NAC include authentication, posture assessment, and remediation. Authentication is the process of verifying that the device and user attempting to connect are who they say they are. Posture assessment involves confirmation that the device meets the policies that were defined for controlling

access to the network, including vulnerability scans. Remediation is the process of displaying to the user the open issues from posture assessment (if any) and quarantining or blocking traffic from that device until those issues are resolved.

Table 3 TOE Component Descriptions

TOE Component	Description
NAC Appliance Manager	The NAC Appliance Manager, also referred to as the NAC Manager, is the administration server. It allows for central management and monitoring of the deployment of NAC Appliance Servers and NAC Agents. It provides a centralized Web-based or CLI interface for NAC posture and remediation management, NAC monitoring, and reporting, NAC Server communication, NAC Agent distribution, and for NAC In-Band or Out-of-Band scenarios. It also provides authentication server management and access/switch management. Note that references to the Clean Access Manager (CAM) throughout the documentation refer to this NAC Appliance Manager. The NAC Manager includes a local database for identification and authentication purposes. This is a PostgreSQL database, and SHA hashing is used to protect the stored credentials.
NAC Appliance Server	The NAC Appliance Server, also referred to as the NAC Server, is the policy enforcer, between the untrusted and trusted networks. NAC Appliance Server's job is to enforce the security policies created in the NAC Appliance Manager. The NAC Server is implemented at the network level to provide a guest/unmanaged captive portal, authentication services and posture remediation services. It also provides identity access control for NAC In-Band. The NAC Server can run on either the NAC 3300 series appliances or as a network module (NME) in Cisco Integrated Services Routers. Note that references to the Clean Access Server (CAS) throughout the documentation refer to this NAC Appliance Server.
Cisco NAC Agent	The Cisco NAC Agent, also referred to as the Clean Access Agent or Software Agent, is a Cisco-provided, free software program that resides on client PCs. Its purpose is to gather information about the user and device on which it is installed. It runs on a variety of endpoint machines (Windows, Mac) and is provisioned over the web. The agent functionality can also be met by an ActiveX version of the agent that is downloaded from the NAC Server. Both the Software Agent and the ActiveX agent provide the same security functionality. They are client-side components that facilitate user authentication and deliver deep inspection of a device's security profile by analyzing registry settings, services, and applications.
NAC Profiler and Collector	The Cisco NAC Profiler system enables you to automatically discover, categorize, and monitor endpoints for which use of the NAC Agent does not apply (such as printers, IP phones, fax machines). The NAC Profiler has two components: the Cisco NAC Profiler Server and the Cisco NAC Profiler Collector. The Cisco NAC Profiler Collector is a software-based service that can be enabled on a NAC-3310 or NAC-3350 NAC Server. The Cisco NAC Profiler Server, also referred to as the Profiler Server, manages the Cisco NAC Profiler Collector component enabled on each NAC Appliance Server.

Table 3 TOE Component Descriptions (continued)

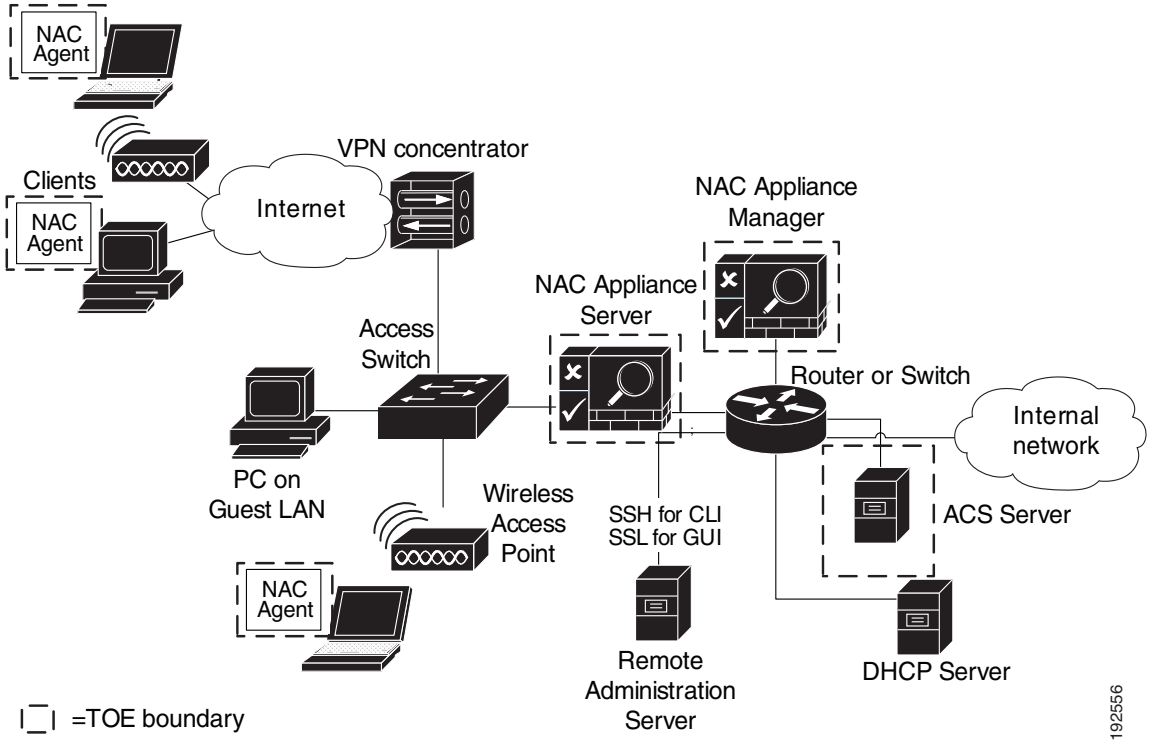
TOE Component	Description
Cisco Switch (Access Switch)	Out-of-band deployments of the TOE require a Cisco access switch for connectivity and enforcement of NAC decisions. This switch can be filled by one of the following: • the Catalyst 6500s running IOS version 12.2(33)SXH: – Catalyst 6503 chassis with 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 the Catalyst 3750 running IOS version 12.2(44)SE.
Cisco Router (Base for NAC Server NME)	The Cisco NAC Server on the NME requires a base Cisco Integrated Services Router (ISR). The supported ISRs are the Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3825, or Cisco 3845. The host router provides power to the network module as well as access to the NME's CLI through the router CLI. The network module provides its own operating system, management, and timestamps.
Cisco Secure ACS for Windows Server version 4.1.4.13	Cisco Secure ACS is a highly scalable, high-performance access control server that operates as a centralized RADIUS server. This component is used for authenticating users attempting to connect to the network.

In-Band Edge Deployment Solution

The NAC In-Band Edge Deployment, also referred to as NAC IB Edge, is illustrated in Figure 1 below. In NAC IB Edge, the NAC Servers are inline with user traffic—before, during, and after authentication, posture assessment, and remediation. The NAC Server is used to securely control authenticated and

unauthenticated user traffic by managing traffic policies based on protocol/port/device or subnet, using time based sessions. NAC IB is ideal for shared media ports, guest environments, VPN or wireless networks, and non-Cisco network infrastructure.

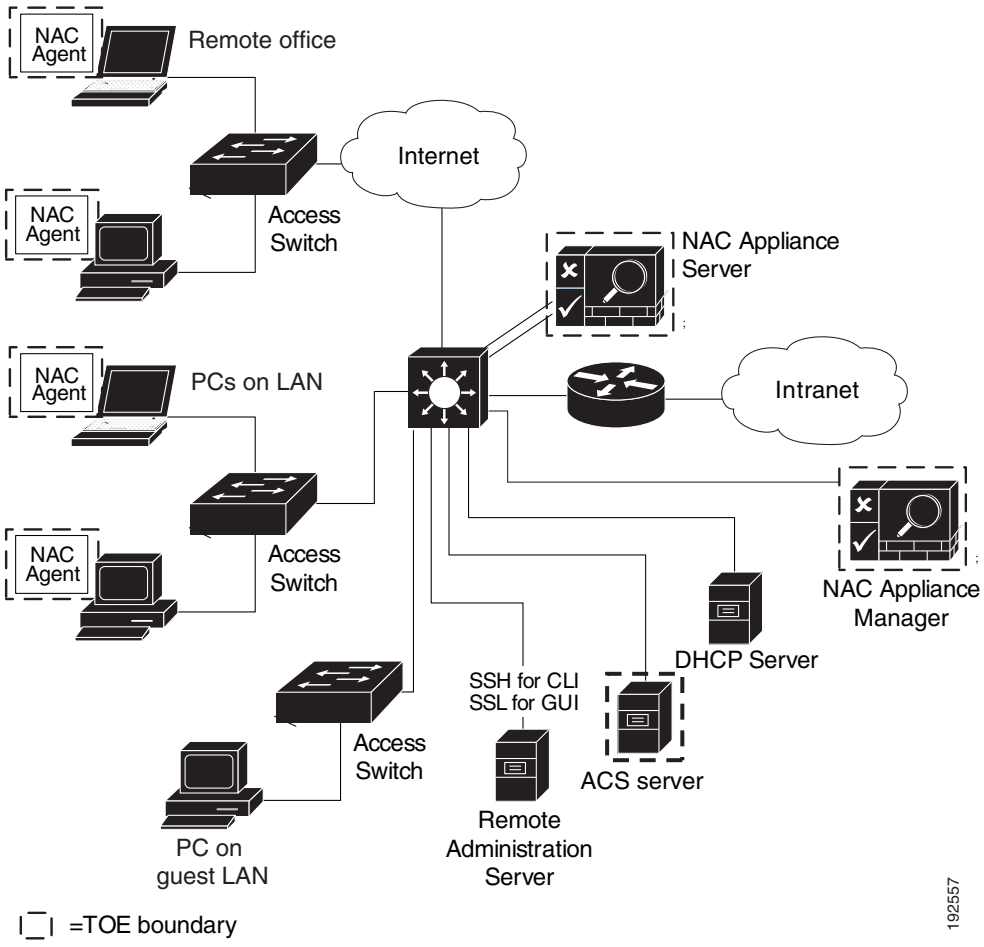
Figure 1 In-Band Edge Deployment Scenario



In-Band Central Deployment Solution

The NAC In-Band Central Deployment, also referred to as NAC IB Central, is illustrated in Figure 2 below. In NAC IB Central, the NAC Servers are logically inline with user traffic—before, during, and after authentication, posture assessment, and remediation. The NAC Server is used to securely control authenticated and unauthenticated user traffic by managing traffic policies based on protocol/port/device or subnet, using time based sessions.

Figure 2 In-Band Central Deployment Scenario



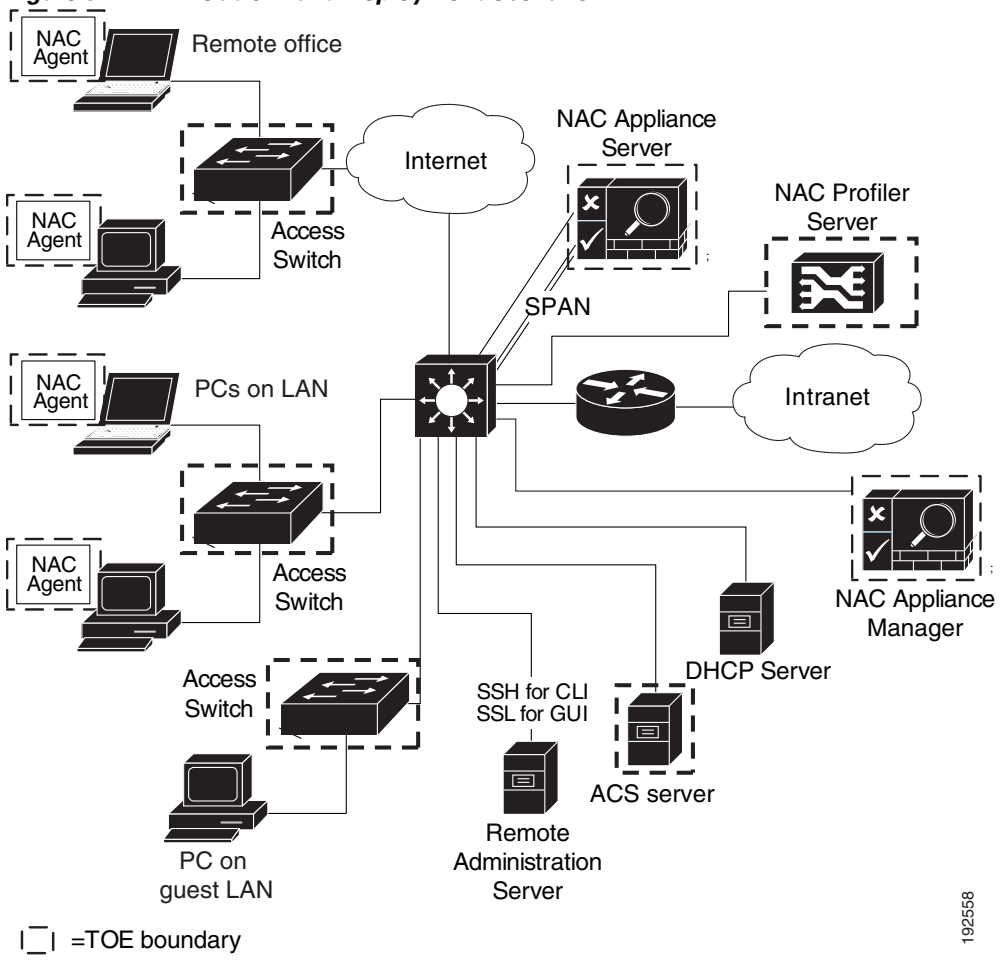
Out-of-Band Deployment Solution

The NAC Out-of-Band Deployment, also referred to as NAC OOB, is illustrated in Figure 3 below. In NAC OOB, the NAC Server is logically inline with user traffic only during the process of authentication, posture assessment, and remediation. Once the user has successfully authenticated and the device is determined to comply with policy, its traffic then bypasses the NAC Server and traverses the switch port directly. In the meantime, the NAC Manager provides port- or role-level control by assigning switch ports via SNMP (version 3) to quarantine VLANs, assigning users to specific roles that map to specific VLANs, and providing a time-based session timeout per role. NAC OOB is ideal for high-throughput, highly routed environments such as LANs and works only in modes where networks are directly connected to the supported Cisco switch or router.

All NAC OOB solutions have the following two VLAN types: authentication and access. The authentication (auth) VLAN is used when a device first connects to the switch. While part of this VLAN, the device is always logically in-line with the NAC Server, and all client traffic is forced to pass through the server. Client authentication, posture assessment, and remediation are all performed in this VLAN just as they are in In-Band deployments. The access VLAN is used once the authentication and certification of the device are completed. The NAC Manager sends an SNMP write command (SNMP

v3) to the switch and transfers the device's port to the access VLAN. At this point, the client's traffic no longer flows through the NAC Server. Multiple access VLANs can be included for different roles and privileges.

Figure 3 Out-of-Band Deployment Scenario



NAC Profiler

Cisco NAC Profiler enables network administrators to efficiently deploy and manage Network Admission Control (NAC) in enterprise networks of varying scale and complexity by identifying, locating and determining the capabilities of all attached network endpoints, regardless of device type, in order to ensure and maintain appropriate network access. Cisco NAC Profiler is an agentless system that discovers, catalogs, and profiles all endpoints connected to a network.

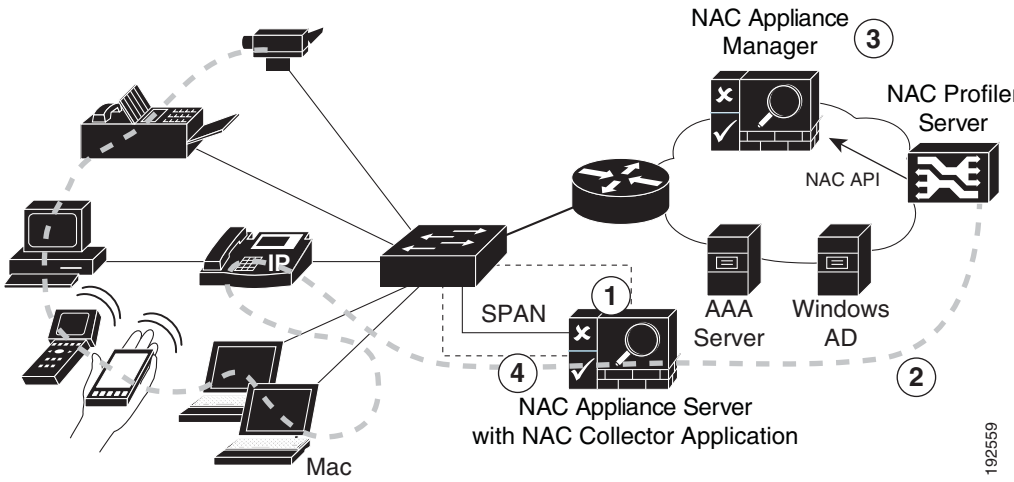
Typically, devices such as printers, FAX machines, IP telephones and Uninterruptible Power Supplies are not capable of running a NAC client. This means that in the deployment of NAC, special purpose devices such as these do not have an agent available, nor do they provide a means by which a user can manually intervene through a browser. In this case, the ports connecting these endpoints must either be provisioned to circumvent the NAC system (e.g., placed on a special VLAN) or alternatively, the NAC system configured to recognize these devices via their unique hardware address in order to provide them access without direct participation in the admission control protocol. This typically requires that the NAC system be made aware of these endpoints by MAC address so that they can be admitted based on

that credential alone with no further interaction with the NAC system. In the case of Cisco NAC Appliance, non-NAC devices such as these are accommodated via the Device Filters list of the Clean Access Manager.

Cisco NAC Profiler provides Endpoint Profiling and Behavior Monitoring functions to allow administrators to thoroughly understand the types of devices connecting to the network, their location and their abilities relative to the state of the port on which they currently reside. The NAC Profiler functions follow this progression (as outlined in Figure 4, below):

1. NAC Collector Application collects the relevant data (including Netflow information, SNMP, DHCP, or traffic mirrored over SPAN) and consolidates the information to send to the NAC Profiler Server
2. NAC Profiler Server aggregates all of the information from the Collectors and maintains a database of all network-attached endpoints (e.g. phones, printers, badge readers, modalities, etc.)
3. NAC Profiler Server continuously maintains the Filters List via the NAC API and provisions the appropriate access decisions (allow, deny, check, "role", or ignore)
4. NAC Collector Application continuously monitors behavior of profiled devices (to detect spoofing) and updates Profiler Server

Figure 4 NAC Profiler Progression



The NAC Profiler is not compatible with the NME version of the NAC Server and therefore will not be included in the In-Band Configurations of this TOE.

Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the NAC. The NAC TOE is comprised of the following:

Table 4 Physical Scope of the TOE

TOE Component	Details
NAC Appliance Manager version 4.5.1	Running on any of the following NAC Appliances 3300 Series platforms: • NAC-3310, • NAC-3350, or • NAC-3390
NAC Appliance Server version 4.5.1 (including ActiveX agent to be used when NAC Agent is not available)	Running on any of the following NAC Appliances 3300 Series platforms or modules: • 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[3]
NAC Agent software version 4.5.1	For any of the following Operating Systems: • Windows Vista, Windows XP, Windows 2000, Windows 98, Windows SE, Windows ME; • Mac OS X (10.2, 10.3, 10.4)[4]
Cisco NAC Profiler Server	Running on a NAC Appliance 3300 Series 3350 platform (NAC3350-PROF)
Cisco NAC Collector	Running as an additional component on the NAC Appliance Server 3310 or 3350.
Cisco Secure ACS	Cisco Secure ACS for Windows Server version 4.1.4.13
Access switch for OOB deployments	65xx running 12.2(33)SXH or 3750 running 12.2(44)SE)

[3]The NME is only compatible with In-Band NAC scenarios.

[4] For exact OS versions supported, see Annex A: Cisco NAC Agent System Requirements, page 76 of this document.

The TOE includes all the hardware and software that are delivered with the above listed NAC 3300 series appliances in both NAC Manager and NAC Server mode. The hardware is a dedicated appliance running a hardened Linux kernel (version 2.6.11-1.1369_FC4smp). No third-party software can be installed. The

TOE also includes the hardware and software for the NAC Appliance network module (NME-NAC-K9), and the router hardware or software in which it is installed. The NAC network module runs the same hardened Linux kernel and software version as the 3300 series appliances.

The TOE includes the NAC Agent software, but not the hardware or OS software on which it is installed.

Data Included in the TOE Physical Boundary

The following sections identify the data included in the TOE's physical boundary.

TSF Data

TSF data in the TOE includes the security policies used during authentication and posture assessment and the data gathered by the NAC Server and Client to determine whether connecting devices have access to the network and what level of access they have. Administrators may add and modify policies according to the desired scenarios to allow the appropriate admission to the network. Policies created or modified by an administrator of the TOE are considered TSF data. Profiler data gathered is considered TSF data. Results of decisions made on network admission based on the data gathered are considered TSF data. The roles and authentication credentials of devices connecting to the network are considered TSF data. TSF data includes audit records generated by the TOE during the course of execution.

User Data

User data on the TOE are roles (the authorizations a user has), user password (authentication data), and user identifier. This is also considered Analyzer Data for this TOE. As the network devices will either bypass or unknowingly continue to flow through the NAC after certification (authentication, posture assessment, and remediation) no additional user data is kept on the TOE.

Security Attributes

The security attributes of the TOE are roles (the authorizations a user has), user password (authentication data), and user identifier.

The TOE also maintains SNMPv3 credentials for communication with the access switch.

Logical Scope of the TOE

The TOE is comprised of a device and user authentication, posture assessment, and remediation solution, along with self-protection of these functions, audit capabilities, administrator identification and authentication, and management capabilities. These functions are described in more detail in the subsections below.

NAC Decisions

NAC decisions are made based on Device and User Authentication, Posture Assessment, Remediation, and Profiling. These decisions result in the connecting device either being allowed access to the internal network or not being allowed access to the internal network.

Device and User Authentication

The device and user attempting to connect to the network must authenticate to the NAC Appliance in order to access the network. This 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. The outcome of the authentication is association of that device and user with a login role.

Posture Assessment

Posture Assessment is the second key functionality of the NAC. It is accomplished via tests and vulnerability scans initiated by the NAC Manager, as described in the detailed progressions above.

Remediation

Remediation is the third and final key functionality of the NAC prior to granting access to the network. It involves forcing the connecting host to execute updates in order to meet the defined security policy, as described in the detailed progressions above.

Profiling

For devices such as printers, FAX machines, IP telephones and Uninterruptible Power Supplies, that are not capable of running a NAC Agent (or a web browser to support the ActiveX client) the TOE is capable of using the NAC Profiler to keep tabs on these endpoints by MAC address so that they can be admitted based on that credential alone with no further interaction with the NAC system. Cisco NAC Profiler provides Endpoint Profiling and Behavior Monitoring functions (defined further in Profiling, page 47) to allow administrators to thoroughly understand the types of devices connecting to the network, their location and their abilities relative to the state of the port on which they currently reside.

Audit

Auditing is provided and stored on the NAC Manager on Administrator authentication, changes to policies, changes to auditing, and the NAC decisions. Auditing is provided on the NAC Profiler for Administrator authentication. Auditing is also provided on the NME host router and access switch.

Administrator Identification and Authentication

The administrators of the NAC Manager, NAC Server, Cisco Secure ACS and Profiler are forced to authenticate prior to being allowed access to either the Command Line Interface (CLI) or the graphical user interface (GUI). The same is true for the administrators of the base router needed by the NME and the access switch required for out-of-band deployments.

Management

Management of the NAC is done through the NAC Manager CLI (SSH protected) or a GUI over an HTTPS-secured web browser session. Both methods allow for device management, switch management, user management (including creation of user roles and access policies), monitoring, and administration tasks (including administrative user management). The NAC Server (both in Server and Module form) has a separate CLI (SSH protected), a local GUI over an HTTPS-secured web browser session, and also can be managed through the NAC Manager GUI, to configure its network settings, managing SSL certificates, managing time, updating local admin passwords, monitoring active VPN clients, and

viewing logs. The Cisco NAC Profiler Server is configured and managed via its own HTTPS-secured web console interface, which is where the NAC Profiler Collector is managed from as well. The Cisco Secure ACS is also configured and managed via its own HTTPS-secured web console interface.

Self-Protection

The NAC Manager and Server (whether on the 3300 series appliance or the network module) each maintain a security domain for their own use. The security domain is all the hardware and software that makes up the NAC Appliance. The NAC appliance provides for isolation at the physical boundary of the TOE component. For this reason the whole NAC Manager and Server are each an isolated security domain. The administrative interface is protected by authentication and by physical controls. SSH is used to secure connections to the CLI. The Administrative GUI is accessed over an HTTPS connection, so data passing between it and a web browser is protected. The NAC Appliance is a dedicated piece of hardware, with no general purpose operating system or programming interface. No untrusted processes are permitted on the NAC Appliance. Because the whole NAC Appliance is a separate physical domain and a dedicated platform solely supporting its own processes and the fact that it controls and mediates access to its interfaces, it provides a security domain for the TSF that is protected from interference and tampering.

The NAC Profiler Server is its own security domain, like the other NAC Appliances. The appliance provides for isolation at the physical boundary of the TOE component. The Cisco NAC Profiler Server is configured and managed via its own web console interface or CLI.

The Cisco NAC Agent, as a software implementation, is dependent up on the IT environment. The client software of the Agent may operate on either Mac or Windows. The following section will detail the security capability support of the hosting IT Environments that the Agent needs to maintain secure operation of the TSF present in its software. The Agent uses crypto libraries from Windows and Mac to do SSL connections to the NAC Server. When the agent runs posture checks it can check specific credentials from the required applications on the host to ensure that it is getting data from legitimate sources.

The Cisco Secure ACS, as a software implementation, is dependent up on the IT environment. The Cisco Secure ACS software may operate on either Windows 2000 Server or Windows 2003 Server. The following section will detail the security capability support of the hosting IT Environments that the Cisco Secure ACS needs to maintain secure operation of the TSF present in its software. The Cisco Secure ACS uses crypto libraries from Windows to do SSH and SSL connections with administrators attempting to remotely administer the Cisco Secure ACS.

The Cisco switch and router are stand-alone hardware devices with single domains of execution. The chassis vary in the number of slots they provide, but this difference does not affect the security functionality claimed by the TOE. They also provide their own identification and authentication mechanisms for self-protection.

TOE Evaluated Configurations

The TOE's In-Band Edge evaluated configuration requires:

Table 5 In-Band Edge

Hardware	Software
One Cisco NAC 3300 Series 3310, 3350, or 3390	Cisco NAC Appliance version 4.5.1
One or more Cisco NAC 3300 Series 3310, 3350, or NAC Network Modules (NME-NAC-K9);	Cisco NAC Appliance version 4.5.1
If the NME is used: one Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3825, or Cisco 3845.	Cisco IOS 12.4(11)T or later
	Cisco Secure ACS for Windows Server version 4.1.4.13
	One or more Cisco NAC Software Agents version 4.5.1 or ActiveX Agents (included with NAC Appliance version 4.5.1).

The TOE's In-Band Central evaluated configuration requires:

Table 6 In-Band Central

Hardware	Software
One Cisco NAC 3300 Series 3310, 3350, or 3390	Cisco NAC Appliance version 4.5.1
One or more Cisco NAC 3300 Series 3310, 3350, or NAC Network Modules (NME-NAC-K9);	Cisco NAC Appliance version 4.5.1
If the NME is used: one Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3825, or Cisco 3845.	Cisco IOS 12.4(11)T or later
	Cisco Secure ACS for Windows Server version 4.1.4.13
	One or more Cisco NAC Software Agents version 4.5.1 or ActiveX Agents (included with NAC Appliance version 4.5.1).

The TOE's Out-of-Band evaluated configuration requires:

Table 7 Out-of-Band

Hardware	Software
One Cisco NAC 3300 Series 3310, 3350, or 3390	Cisco NAC Appliance version 4.5.1
One or more Cisco NAC 3300 Series 3310 or 3350	Cisco NAC Appliance version 4.5.1
One Cisco NAC 3350 Profiler Server	Cisco NAC Profiler Release 2.1.8-37;
One 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 one Catalyst 3750;	IOS 12.2(33)SXH or 12.2(44)SE
	Cisco Secure ACS for Windows Server version 4.1.4.13
	One or more Cisco NAC Software Agents version 4.5.1 or ActiveX Agents (included with NAC Appliance ver. 4.5.1).

And all configurations require one or more of the browsers, switches, and OS/platforms specified in the IT Environment dependency section above.

Excluded Functionality

The following features and functionality are excluded from the TOE evaluated configuration:

- High Availability
- Automated Security Policy Updates
- Authentication Mechanisms:
  - Kerberos
  - NTLM
  - LDAP
  - AD SSO
  - VPN SSO
  - Netbios SSO
  - S/Ident

Conformance Claims

Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1.

The TOE and ST are EAL2 Part 3 conformant.

The TOE and ST are CC Part 2 extended

Protection Profile Conformance

This ST claims compliance to the U.S. Government Protection Profile Intrusion Detection System Analyzer for Basic Robustness Environments, Version 1.3, dated July 25, 2007

Protection Profile Refinements

The Protection Profile contained errors where requirements and policies were not included in mappings or justifications. These issues were remedied in this Security Target.

The Protection Profile also mapped three new environmental objectives (OE.TIME, OE.AUDIT_PROTECTION, and OE.AUDIT_SORT) to SFRs on the TOE, which is not possible. In this ST the affected SFRs were iterated on the IT environment so that the objectives could be properly traced.

Protection Profile Additions

The following objectives were added to the IT environment: OE.PROTCT and OE.VLAN.

The following requirements were added to the set of SFRs on the TOE: FCS_COP.1(1) through (8), FCS_CKM.1(1) through (3), FCS_CKM.4, FDP_IFC.1(1), FDP_IFF.1(1), FIA_UAU.2, FIA_UID.2 FIA_UAU.5(1), FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FPT_ITT.1, and IDS_COL.1.

The following requirements were added to the set of SFRs on the IT environment: FAU_SAR.3(2), FAU_STG.2(2), FCS_COP.1(9), FDP_IFC.1(2), FDP_IFF.1(2), FIA_UAU.5(2), FPT_STM.1(2).

Protection Profile Conformance Claim Rationale

TOE Appropriateness

The NAC TOE provides all of the Intrusion Detection functionality at a level of security commiserate with that identified in the U.S. Government Protection Profile Intrusion Detection System Analyzer for Basic Robustness Environments.

TOE Security Problem Definition Consistency

The U.S. Government Protection Profile Intrusion Detection System Analyzer for Basic Robustness Environments contains the following Assumptions, Threats, and Organizational Security Policies:

A. Assumptions:

1. A. ACCESS
2. A.PROTCT
3. A.LOCATE
4. A.MANAGE
5. A.NOEVIL
6. A.NOTRST

B. Threats:

1. T.COMINT
2. T.COMDIS
3. T.LOSSOF
4. T.NOHALT
5. T.PRIVIL
6. T.IMPCON
7. T.IMPCON
8. T.FALACT
9. T.FALREC
10. T.FALASC

C. Organizations Security Policies:

1. P.ANALYZ
2. P.DETECT
3. P.MANAGE
4. P.ACCESS
5. P.ACCACT
6. P.INTGTY
7. P. PROTCT

The Assumptions, Threats, and Organization Security Policies included in the Security Target are identical to the ones specified in the Protection Profile with two exceptions, as follows:

A. The Security Target contains the additional assumption, A.HOST. This assumption is included in the Security Target to address the to address the need for the TOE agents to be properly installed on the host Operating System.

B. The Security Target contains the additional threat, T.BYPASS. This threat is included in the Security Target to address the TOE's ability to protect from unauthorized access to the TOE protected network.

Statement of Security Objectives Consistency

The U.S. Government Protection Profile Intrusion Detection System Analyzer for Basic Robustness Environments contains the following Security Objectives:

A. O.PROTCT

B. O.IDACTS

C. O.RESPON
D. O.EADMIN
E. O.ACCESS
F. O.IDAUTH
G. O.OFLOWS
H. O.AUDITS
I. O.INTEGR
J. O.EXPORT
K. OE.TIME
L. OE.AUDIT_PROTECTION
M. OE.AUDIT_SORT
N. OE.INSTAL
O. OE. PHYCAL
P. OE.CREDEN
Q. OE.PERSON
R. OE.INTROP

The Security Objectives included in the Security Target are identical to the ones specified in the Protection Profile with four exceptions, as follows:

A. The Security Target contains the additional Security Objective, O.COLLECT. This Security Objective is included in the Security Target to address the TOEs ability to collect information related to intrusions.
B. The Security Target contains the additional Security Objective, OE.PROTCT. This Security Objective is included in the Security Target to address the cryptography required in the IT Environment.
C. The Security Target contains the additional Security Objective, OE.VLAN. This Security Objective is included in the Security Target to address the VLAN management services provided by the IT environment.

Statement of Security Requirements Consistency

The U.S. Government Protection Profile Intrusion Detection System Analyzer for Basic Robustness Environments contains the following Security Functional Requirements:

A. TOE SFRs
    1. FAU_GEN.1
    2. FAU_SAR.1
    3. FAU_SAR.2
    4. FAU_SAR.3
    5. FAU_SEL.1
    6. FAU_SEL.1
    7. FAU_STG.2
    8. FAU_STG.4

9. FIA_UAU.1
10. FIA_ATD.1
11. FIA_UID.1
12. FMT_MOF.1
13. FMT_MTD.1
14. FMT_SMR.1
15. FPT_ITA.1
16. FPT_ITC.1
17. FPT_ITI.1
18. FPT_STM.1
19. IDS_ANL.1
20. IDS_RCT.1
21. IDS_RDR.1
22. IDS_STG.1
23. IDS_STG.2

B. IT Environment SFRs

1. N/A

The Security Functional Requirements specified in the Security Target are identical to the ones specified in the Protection Profile with the following exceptions:

A. FCS_COP.1(1) through (8) TOE SFRs were added to specify the TOE's SSL, SSH, SNMP, RADIUS, and other cryptographic capabilities.

B. FCS_CKM.1(1) through (3) TOE SFRs were added to specify the TOE's SSL, SSH, SNMP, and other cryptographic capabilities.

C. FCS_CKM.4 TOE SFR was added to specify the cryptographic key destruction provided by the TOE

D. FDP_IFC.1(1) TOE SFR was added to specify the TOEs ability to prevent access to protected network resources until the machine attempting to access protected network resources meets the specified criteria.

E. FDP_IFF.1(1) TOE SFR was added to specify the TOEs ability to prevent access to protected network resources until the machine attempting to access protected network resources meets the specified criteria.

F. FIA_UAU.2 TOE SFR was added to specify the TOE administrator authentication.

G. FIA_UAU.5(1) TOE SFR was added to specify the TOE administrator authentication.

H. FIA_AFL.1 TOE SFR was added to specify the TOE administrator authentication.

I. FIA_UID.2 TOE SFR was added to specify the TOE administrator identification.

J. FMT_MSA.1 TOE SFR was added to specify the TOE management functionality.

K. FMT_MSA.2 TOE SFR was added to specify the TOE management functionality.

L. FMT_MSA.3 TOE SFR was added to specify the TOE management functionality.

M. FMT_SMF.1 TOE SFR was added to specify the TOE management functionality.

N. FPT_ITT.1 TOE SFR was added to specify the TOEs ability to protect data while it is being transferred between TOE components.

O. IDS_COL.1 TOE SFR was added to specify the TOEs capability to collect intrusion related data.

P. FAU_SAR.3(2) IT Environment SFR was added to specify the optional use of environmentally provided audit capabilities.

Q. FAU_STG.2(2) IT Environment SFR was added to specify the optional use of environmentally provided audit capabilities.

R. FCS_COP.1(9) IT Environment SFR was added to specify the SSL capabilities of the NAC Agent and Cisco Secure ACS host Operating System.

S. FDP_IFC.1(2) IT Environment SFR was added to specify the VLAN handling requirements of the TOE environment.

T. FDP_IFF.1(2) IT Environment SFR was added to specify the VLAN handling requirements of the TOE environment.

U. FPT_STM.1(2) IT Environment SFR was added to specify the optional use of environmentally provided time stamps.

Security Problem Definition

This chapter identifies the following:

A. Significant assumptions about the TOE's operational environment.

B. IT related threats to the organization countered by the TOE.

C. Environmental threats requiring controls to provide sufficient protection.

D. Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name. Policies are identified as P.policy with "policy" specifying a unique name.

Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's IT environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 8 TOE Assumptions

Assumption Name	Assumption Definition
A.ACCESS	The TOE has access to all the IT System resources necessary to perform its functions.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

Table 8 TOE Assumptions (continued)

Assumption Name	Assumption Definition
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.
A.HOST	The Agent Component will be installed on a physically protected, properly configured IT platform and operated in a secure manner.

Threats

Table 9 lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is unsophisticated.

Table 9 Threats

Threat Name	Threat Definition
T.COMINT	An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE.
T.NOHALT	An unauthorized person may attempt to compromise the continuity of the TOEs analysis functionality by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.IMPCON	The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T. FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.BYPASS	Traffic may bypass the TOE due to incorrect network configuration.

Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 10: Organizational Security Policies identifies the organizational security policies.

Table 10 Organizational Security Policies

Policy Name	Policy Definition
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
P.DETECT	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.
P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data analyzed and generated by the TOE shall only be used for authorized purposes.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.INTGTY	Data analyzed and generated by the TOE shall be protected from modification.
P. PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of analysis and response activities.

Security Objectives

This Chapter identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

- This document identifies objectives of the TOE as O.*objective* with *objective* specifying a unique name. Objectives that apply to the IT environment are designated as OE.*objective* with *objective* specifying a unique name.

Security Objectives for the TOE

Table 11: Security Objectives for the TOE identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 11 Security Objectives for the TOE

TOE Security Objective Name	TOE Security Objective Definition
O. PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDACTS	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond appropriately to analytical conclusions.

Table 11 Security Objectives for the TOE (continued)

TOE Security Objective Name	TOE Security Objective Definition
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and Analyzer data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses and use of the Analyzer functions.
O.INTEGR	The TOE must ensure the integrity of all audit and Analyzer data.
O. EXPORT	When the TOE makes its Analyzer data available to other IDS components, the TOE will ensure the confidentiality of the Analyzer data.
O.COLLECT	The TOE must collect data that might indicate an intrusion.

Security Objectives for the Environment

The assumptions identified in Assumptions, page 26, are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Only OE.PROTCT is IT in nature. Table 12: Security Objectives for the Environment identifies the security objectives for the environment.

Table 12 Security Objectives for the Environment

IT Environment Security Objective Name	IT Environment Security Objective Definition
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.AUDIT_SORT	The IT Environment will provide the capability to sort the audit information.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE. PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the Analyzer.

Table 12 Security Objectives for the Environment (continued)

IT Environment Security Objective Name	IT Environment Security Objective Definition
OE.INTROP	The TOE is interoperable with the IT System it monitors and other IDS components within its IDS.
OE.PROTCT	The host platforms in the IT environment must protect itself from unauthorized modifications and access to its functions and data and support the required SSL/TLS versions for correct SSL implementation.
OE.VLAN	The IT environment must be able to properly route traffic to the TOE using VLAN information.

Security Requirements

This section identifies the Security Functional Requirements for the TOE and for the IT Environment. The Security Functional Requirements included in this section are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1* and all National Information Assurance Partnership (NIAP) and international interpretations with the exception of the items listed below with the text (EXP) in the title, which were derived from the Intrusion Detection System Analyzer Protection Profile or explicitly created.

Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

Conventions that were used in the PP and were carried into this ST (and in some places corrected) to show the changes from the CC part 2 version of requirements:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text and strikethroughs, if necessary;
- Selection: Indicated with underlined text;

Conventions that are used in this Security Target to show actions taken above and beyond the PP follow the same conventions above but put the value in square brackets [*Assignment_value*].

Explicitly stated SFRs are identified by having a label ‘(EXP)’ after the requirement name for TOE SFRs.

TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in Table 13 are described in more detail in the following subsections.

Table 13 TOE Security Functional Requirements

Functional Component	
Security Functional Requirements Directly Drawn from CC Part 2	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3(1)	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.2(1)	Guarantees of audit data availability
FAU_STG.4	Prevention of audit data loss
FCS_COP.1(1) through (8)	Cryptographic operation
FCS_CKM.1(1) through (3)	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FDP_IFC.1(1)	Subset Information Flow Control
FDP_IFF.1(1)	Simple security attributes
FIA_UAU.1	Timing of authentication
FIA_UAU.2	User authentication before any action
FIA_UAU.5(1)	Multiple authentication mechanisms
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UID.1	Timing of identification
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_ITA.1	Inter-TSF availability within a defined availability metric
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITI.1	Inter-TSF detection of modification
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_STM.1(1)	Reliable time stamps

Table 13 TOE Security Functional Requirements (continued)

Functional Component	
Extended Security Functional Requirements	
IDS_ANL.1	Analyzer analysis
IDS_RCT.1	Analyzer react
IDS_RDR.1	Restricted data review
IDS_STG.1	Guarantee of analyzer data availability
IDS_STG.2	Prevention of Analyzer data loss
IDS_COL.1	Collection of Data

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

A. Start-up and shutdown of the audit functions;

B. All auditable events for the basic level of audit; and

C. *Access to the Analyzer and access to the TOE and Analyzer data.*

Application Note: The auditable events for the basic level of auditing are included in Table 14 Auditable Events.

Table 14 Auditable Events

Component	Event	Details
FAU_GEN.1	Start- up and shutdown of audit functions	
FAU_GEN.1	Access to Analyzer	
FAU_GEN.1	Access to the TOE Analyzer data	**Object ID, Requested access**
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FIA_UAU.1	All use of the authentication mechanism	**User identity, location**
FIA_UAU.2	All use of the authentication mechanism	**User identity, outcome**
FIA_UID.1	All use of the user identification mechanism	**User identity, location**
FIA_UID.2	All use of the authentication mechanism	**User identity, outcome**
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	**User identity**

Table 14 Auditable Events (continued)

Component	Event	Details
FCS_CKM.1	Success and failure of creation of cryptographic keys for remote administration.	
FIA_UAU.5(1)	Host authentication	**Host identity**
FDP_IFF.1(1), FDP_IFC.1(1)	Posture Assessment, Reaction	
FDP_IFF.1(1), FDP_IFC.1(1)	Profiling on NAC Manager	
FDP_IFF.1(1), FDP_IFC.1(1)	Profiling on NAC Profiler	

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

A. Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

B. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **the additional information specified in the Details column of [Table 14:] *Auditable Events*.**

FAU SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [*authorized NAC Server administrator, authorized Analyzer administrator, Profiler Administrator, Router Administrator, Switch Administrator*] with the capability to read [*information as displayed in Table 15*] from the audit records.

Table 15 Audit Review by Role

Role	Audit Information Available
Authorized NAC Server Administrator	All audit information on the NAC Server
Authorized Analyzer Administrator	All audit information on the NAC Manager
Profiler Administrator	All audit information on the NAC Profiler Server
Router Administrator	All audit information on the NME base router.
ACS Administrator	All audit information on the Cisco Secure ACS.
Switch Administrator	All audit information on the access switch.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 (1) Selectable Audit Review

FAU_SAR.3.1(1) The TSF shall provide the ability to perform sorting of audit data based on *date and time, subject identity, type of event, and success or failure or related event.*

FAU_SEL.1 Selective Audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

A. event type;

B. *[no other attributes].*

FAU_STG.2 (1) Guarantees of Audit Data Availability

FAU _STG.2.1(1) The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2(1) The TSF shall be able to detect unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.2.3(1) The TSF shall ensure that [*the most recent, limited by available storage space*] audit records will be maintained when the following conditions occur: [audit storage exhaustion].

FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and *send an alarm* if the audit trail is full.

FCS_COP.1 (1) Cryptographic Operation – Remote Administration (SSH and SSL)

FCS_COP.1.1(1) The TSF shall perform [*encryption of remote authorized administrator sessions*] in accordance with a specified cryptographic algorithm: [*RC2, RC4, IDEA, Data Encryption, or Triple Data Encryption Standard (3DES)*] and cryptographic key sizes [*that are 64 or 128, or 192 binary digits in length]* that meet the following: *[RC2: RFC 2268, RC4: N/A, IDEA: N/A, DES: FIPS PUB 46-3, 3DES: FIPS PUB 46-3 with Keying Option 1]*.

FCS_COP.1 (2) Cryptographic Operation – Agent Communication (SSL)

FCS_COP.1.1(2) The TSF shall perform [*Agent Communications*] in accordance with a specified cryptographic algorithm: [*RC2, RC4, IDEA, Data Encryption, or Triple Data Encryption Standard (3DES)*] and cryptographic key sizes [*that are 64 or 128, or 192 binary digits in length*] that meet the following: [*RC2: RFC 2268, RC4: N/A, IDEA: N/A, DES: FIPS PUB 46-3, 3DES: FIPS PUB 46-3 with Keying Option 1*].

Application Note: This requirement is split between the TOE and IT environment. The environment initiates the SSL session, but the TOE maintains the SSL certificate and enforces the strength of the algorithm.

FCS_COP.1 (3) Cryptographic Operation – Inter-TOE Communication (SSL)

FCS_COP.1.1(3) The TSF shall perform [*inter-TOE communication*] in accordance with a specified cryptographic algorithm: [*RC2, RC4, IDEA, Data Encryption, or Triple Data Encryption Standard (3DES)*] and cryptographic key sizes [*that are 64 or 128, or 192 binary digits in length*] that meet the following: [*RC2: RFC 2268, RC4: N/A, IDEA: N/A, DES: FIPS PUB 46-3, 3DES: FIPS PUB 46-3 with Keying Option 1*].

FCS_COP.1 (4) Cryptographic Operation – SNMPv3

FCS_COP.1.1(4) The TSF shall perform [*data encryption and decryption*] in accordance with a specified cryptographic algorithm: [*DES in Cipher Block Chaining (CBC) mode (CBC-DES)*] and cryptographic key sizes [*that are 64 binary digits in length*] that meet the following: [*FIPS PUB 46-3, ANSI X9.52, FIPS PUB 140-2 (Level 1)*].

FCS_COP.1 (5) Cryptographic Operation – SNMPv3 hash

FCS_COP.1.1(5) The TSF shall perform [*secure hash (message digest) authentication*] in accordance with a specified cryptographic algorithm: [*MD5 or SHA in HMAC mode (HMAC-MD5 or HMAC-SHA)*] and cryptographic key sizes [*that are 128 binary digits in length for MD5 or a message digest that is 160 binary digits in length for SHA*] that meet the following: [*RFC2104(HMAC), ANSI X9.71(HMAC), FIPS PUB 198(HMAC), RFC1321(MD5), FIPS PUB 180-2(SHA)*].

FCS_COP.1 (6) Cryptographic Operation – RADIUS

FCS_COP.1.1(6) The TSF shall perform [*secure hash (message digest)*] in accordance with a specified cryptographic algorithm: [*MD5*] and cryptographic key sizes [*128-bit hash value*] that meet the following: [*RFC 1321*].

FCS_COP.1 (7) Cryptographic Operation – NAC Profiler – NAC Manager (SSH)

FCS_COP.1.1(7) The TSF shall perform [*encryption of NAC Profiler – NAC Manager communication*] in accordance with a specified cryptographic algorithm: [*RC2, RC4, IDEA, Data Encryption, or Triple Data Encryption Standard (3DES)*] and cryptographic key sizes [*that are 64 or 128, or 192 binary digits in length*] that meet the following: [*RC2: RFC 2268, RC4: N/A, IDEA: N/A, DES: FIPS PUB 46-3, 3DES: FIPS PUB 46-3 with Keying Option 1*].

FCS_COP.1 (8) Cryptographic Operation – NAC Profiler – NAC Server

FCS_COP.1.1(8) The TSF shall perform [*encryption of NAC Profiler – NAC Server communication*] in accordance with a specified cryptographic algorithm: [*AES or Blowfish*] and cryptographic key sizes [*that are 256 bits (AES) or 448 bits (Blowfish)*] that meet the following: [*AES: FIPS 197, Blowfish: N/A*].

FCS_CKM.1 (1) Cryptographic Key Generation – Remote Administration, Agent Communication, and Inter-TOE Communication

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*RSA*] and specified cryptographic key sizes [*between 1024 and 2048 bits*] that meet the following: [*PKCS #1*].

FCS_CKM.1 (2) Cryptographic Key Generation – SNMPv3

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*as defined in the SNMPv3 standard RFC3414*] and specified cryptographic key sizes [*that are 64 binary digits in length*] that meet the following: [*generation and exchange of session keys as defined in the SNMPv3 standard RFC3414*].

FCS_CKM.1 (3) Cryptographic Key Generation – NAC Profiler – NAC Manager Communication

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*SHA-1 hash*] and specified cryptographic key sizes [*that are either 256 bits or 448 bits*] that meet the following: [*AES (256 bit) or Blowfish (448 bit)*].

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwrite*] that meets the following: [*no standard*].

FDP_IFC.1 (1) Subset Information Flow Control

FDP_IFC.1.1(1) The TSF shall enforce the [*NAC SFP*] on [:

A. *subjects: hosts attempting access to the internal network post-authentication, assessment, and remediation;*

B. *information: network traffic*

C. *operation: pass, block, or quarantine information through the TSF on behalf of the connecting IT entity;.*

FDP_IFF.1 (1) Simple Security Attributes

FDP_IFF.1.1(1) The TSF shall enforce the [*NAC SFP*] based on the following types of subject and information security attributes: [

A. *subject attributes: identification and authentication credentials provided by subject, state of subject's machine with regards to vulnerability scan, registry settings on subject machine, role assigned to subject by NAC Manager;*

B. *information attributes: presumed MAC address of source subject, presumed IP address of source subject, presumed IP source port number, IP destination port number*].

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*unauthenticated external entities may be allowed admission to the network through the TOE if:*

- *They successfully authenticate;*
- *Their machine passes the NAC SFP posture assessment; and*
- *They have no issues that are not addressed during remediation*

Or

- *if the NAC Profiler identifies them as a host that is unable to access the NAC authentication and posture assessment mechanisms; and*
- *their network behavior matches the expected profile*

Or

- *a traffic policy is configured to allow access by an unauthenticated user*].

FDP_IFF.1.3(1) The TSF shall enforce the [*none*].

FDP_IFF.1.4(1) The TSF shall explicitly authorize an information flow based on the following rules: [

- *All traffic shall be copied through the TOE via a SPAN port to the NAC Server.*
- *DHCP requests are allowed through the TOE during authentication*].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules: [*none*].

FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when a *settable, non-zero number* of unsuccessful authentication attempts occur related to *external IT products attempting to authenticate*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *prevent the offending external IT product from successfully authenticating until an authorized administrator takes some action to make authentication possible for the external IT product in question.*

FIA_UAU.1 Timing of Authentication – Users

FIA_UAU.1.1 The TSF shall allow [*only the actions configured (in Traffic policies) for the unauthenticated user*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 User Authentication Before Any Action – Administrators

FIA_UAU.2.1 The TSF shall require each [~~user~~ **administrator**] to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that [~~user~~ **administrator**].

FIA_UAU.5 (1) Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide [*the following authentication mechanisms:*

A. *Reusable username and password for SNMP authentication;*

B. *Reusable username and password for local and remote administration of the switch, router, or NAC components;*

C. *Reusable username and password, plus MAC address for the local NAC Manager host database;*

D. *Reusable RADIUS credentials for the Cisco Secure ACS]*

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **following: [**

A. *if the user is attempting to access the TOE through SNMP, the SNMP authentication shall be used with access only granted after successful authentication*

B. *if the user is attempting to locally or remotely administer the switch, router, or any NAC component, username and password verification shall be used. Only after successful authentication will the user be allowed to administer the TOE*

C. *if a user is attempting to gain access to the protected network and local NAC Manager authentication is used, username, password and MAC address verification shall be used. Only after successful verification will the user be allowed to access to the TOE protected network*

D. *if a user is attempting to gain access to the protected network and the Cisco Secure ACS is used for authentication, RADIUS authentication shall be used. Only after successful RADIUS authentication will the user be allowed to access to the TOE protected network***].**

FIA ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

A. *User identity;*

B. *Authentication data;*

C. *Authorizations; and*

D. *[Group].*

FIA_UID.1 Timing of Identification – Users

FIA_UID.1.1 The TSF shall allow [*only the actions configured (in Traffic policies) for the unauthenticated user*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2 User Identification before any Action - Administrators

FIA_UID.2.1 The TSF shall require each [~~user~~ **administrator**] to identify itself before allowing any other TSF-mediated actions on behalf of that [~~user~~ **administrator**].

FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the functions *of analysis and reaction to authorized Analyzer administrators*.

FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [*NAC SFP*] to restrict the ability to [modify] the security attributes [*roles of users, actions based on scan results, and required registry settings on subject machine*] to [*authorized Analyzer administrators*].

FMT_MSA.2 Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [*cryptographic keys*] **per the key generation techniques specified in FCS_CKM.1(1), FCS_CKM.1(2), and FCS_CKM.1(3).**

FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [*NAC SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*authorized Analyzer administrator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query *and add Analyzer data, query audit data, and shall restrict the ability to query and modify all other TOE data to [authorized Analyzer administrator, authorized NAC Server administrator, Profiler Administrator, Router Administrator, and Switch Administrator as indicated in Table 16, below].*

Table 16 NAC TSF Management

Role	TSF Privileges
Authorized NAC Server Administrator	Query and modify all TOE data on the NAC Server
Authorized Analyzer Administrator	Query and add analyzer data on the NAC Manager. Query audit data on the NAC Manager. Query and modify all TOE data on the NAC Manager.
Profiler Administrator	Query and modify all TOE data on the NAC Profiler Server
Router Administrator	Query and modify all TOE data on the NME base router.
ACS Administrator	Query and modify all TOE data on the Cisco Secure ACS.
Switch Administrator	Query and modify all TOE data on the access switch.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:[

A. *the ability to modify behavior of System data collection, analysis and reaction; and*

B. *the ability to query and add System and audit data; and*

C. *the ability to query and modify all other TOE data.*].

FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the **following** roles: *authorized [**NAC Server**] administrator, authorized Analyzer administrators, and [Profiler Administrator, Router Administrator, ACS Administrator, Switch Administrator, SNMP user and user*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

FPT_ITA.1 Inter-TSF Availability within a Defined Availability Metric

FPT_ITA.1.1 The TSF shall ensure the availability of *audit and Analyser data* provided to a remote trusted IT product within [*60 seconds*] given the following conditions [*use of Internet Explorer and a routable connection to the TOE from the workstation hosting the Internet Explorer being used to connect to the TOE*].

FPT_ITC.1 Inter-TSF Confidentiality During Transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

FPT_ITI.1 Inter-TSF Detection of Modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [*all incorrect Message Authentication Code (MAC)*].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [*drop network packet and request resend for those packets with incorrect MACs*] if modifications are detected.

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from [disclosure] when it is transmitted between separate parts of the TOE.

FPT_STM.1 (1) Reliable Time Stamps

FPT_STM.1.1(1) The TSF shall be able to provide reliable time stamps for its own use.

Extended Security Functional Requirements

Extended Components Definition

This Security Target contains several Security Functional Requirements that are not drawn from existing CC part 2 Security Function Requirements.

A family of IDS requirements was included in this ST drawn from the Intrusion Detection System Analyzer Protection Profile, version 1.2, dated April 27, 2005. The PP stated rational for the explicitly stated requirements is:

“A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.”

The explicitly stated requirements included in this ST from the Intrusion Detection System Analyzer Protection Profile are:

A. IDS_ANL.1 – Analyzer analysis

B. IDS_RCT.1 – Analyzer react

C. IDS_RDR.1 – Restricted Data Review

D. IDS_STG.1 - Guarantee of Analyzer Data Availability

E. IDS_STG.2 - Prevention of Analyzer Data Loss

The family of IDS requirements also includes one additional extended Security Functional Requirement not drawn from the Intrusion Detection System Analyzer Protection Profile, IDS_COL.1 – Collection of Data. This Security Functional Requirements was included in the Security Target to instantiate the data collection associated with TOEs intrusion detection functionality. This SFR was included neither in the Intrusion Detection System Analyzer Protection Profile nor the CC part 2.

The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

The identification structure of each Security Functional Requirement is modeled after the Security Functional Requirements included in CC part 2. The identification structure includes the following,

A. Class – All extended SFRs included in this ST are part of the IDS class of requirements

B. Family – The extended SFR families include ANL, RCT, RDR, STG, and COL

C. Component – All extended SFRs are at a component level 1 with the exception of IDS_STG.2, which, is at component level 2

IDS_ANL.1 Analyzer Analysis (EXP)

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all IDS data received:

A. [signature, statistical]; and

B. [*none*].

IDS_ANL.1.2 The TSF shall record within each analytical result at least the following information:

A. Date and time of the result, type of result, identification of data source; and

B. [*No other security relevant information about the result*].

IDS_RCT.1 Analyzer React (EXP)

IDS_RCT.1.1 The TSF shall send an alarm to [*the audit log*] and take [*the action to inform the user of the necessary updates and block or quarantine the device's traffic*] when an intrusion is detected.

IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1 The Analyzer shall provide [*the authorized Analyzer administrator*] with the capability to read [*all information*] from the Analyzer data.

IDS_RDR.1.2 The Analyzer shall provide the Analyzer data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The Analyzer shall prohibit all users read access to the Analyzer data, except those users that have been granted explicit read-access.

IDS_STG.1 Guarantee of Analyzer Data Availability (EXP)

IDS_STG.1.1 The Analyzer shall protect the stored Analyzer data from unauthorized deletion.

IDS_ STG.1.2 The Analyzer shall protect the stored Analyzer data from modification.

IDS_ STG.1.3 The Analyzer shall ensure that [*the most recent, limited by available storage space*] Analyzer data will be maintained when the following conditions occur: [Analyzer data storage exhaustion].

IDS_STG.2 Prevention of Analyzer Data Loss (EXP)

IDS_STG.2.1 The Analyzer shall [overwrite the oldest stored Analyzer data] and send an alarm if the storage capacity has been reached.

IDS_COL.1 Collection of Data (EXP)

IDS_COL.1.1 The TSF shall be able to collect the following information from the devices attempting to connect to the network: [*registry settings, detected known vulnerabilities*].

Component Definition:

IDS_COL.1.1 The TSF shall be able to collect the following information from the devices attempting to connect to the network: [*Assignment: List of information collected from devices attempting to access the protected network*].

Assignment: This assignment should be completed with a list of information collected from devices that are attempting to connect to the TOE protected network.

IT Environment Security Functional Requirements

This section identifies the Security Functional Requirements for the IT environment. The SFRs on the IT environment defined in this section are from requirements in Part 2 of the CC. Table 17 outlines the requirements and their dependencies.

Table 17 IT Environment Security Functional Requirements

Functional Component		Dependencies
FAU_SAR.3(2)	Selectable audit review	FAU_SAR.1
FAU_STG.2(2)	Guarantees of audit data availability	FAU_GEN.1
FCS_COP.1(9)	Cryptographic operation	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2
FDP_IFC.1(2)	Subset Information Flow Control	FDP_IFF.1
FDP_IFF.1(2)	Simple security attributes	FDP_IFC.1 FMT_MSA.3
FPT_STM.1(2)	Reliable time stamps	No Dependencies

FAU_SAR.3 (2) Selectable Audit Review – Agent Host OS

FAU_SAR.3.1(2) The ~~TSF~~ **IT Environment** shall provide the ability to perform sorting of audit data based on *date and time, subject identity, type of event, and success or failure or related event*.

FAU_STG.2 (2) Guarantees of Audit Data Availability – Agent Host OS

FAU _STG.2.1(2) The ~~TSF~~ **IT Environment** shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2(2) The ~~TSF~~ **IT Environment** shall be able to detect unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.2.3(2) The ~~TSF~~ **IT Environment** shall ensure that [*the most recent, limited by available storage space*] audit records will be maintained when the following conditions occur: [audit storage exhaustion].

FCS_COP.1 (9) Cryptographic Operation – Remote Administrator Sessions (SSL)

FCS_COP.1.1(9) The ~~TSF~~ **IT Environment** shall perform [*encryption of remote authorized administrator sessions*] in accordance with a specified cryptographic algorithm: [*RC2, RC4, IDEA, Data Encryption, or Triple Data Encryption Standard (3DES)*] and cryptographic key sizes [*that are 64 or 128, or 192 binary digits in length*] that meet the following: [*RC2: RFC 2268, RC4: N/A, IDEA: N/A, DES: FIPS PUB 46-3, 3DES: FIPS PUB 46-3 with Keying Option 1*].

Application Note: This requirement is split between the TOE and IT environment. The environment initiates the SSL session, but the TOE maintains the SSL certificate and enforces the strength of the algorithm.

FDP_IFC.1 (2) Subset Information Flow Control – VLAN

FDP_IFC.1.1(2) The ~~TSF~~ **IT Environment** shall enforce the [*VLAN information flow control SFP*] on [:

A. *subjects: physical network interfaces;*

B. *information: IP packets;*

C. *operation: permit or deny layer two communication;*]

FDP_IFF.1 (2) Simple Security Attributes – VLAN

FDP_IFF.1.1(2) The ~~TSF~~ **IT Environment** shall enforce the [*VLAN information flow control SFP*] based on the following types of subject and information security attributes: [

A. *security subject attributes: Receiving/transmitting VLAN interface;*

B. *security information attributes: VLAN ID in Packet Header*].

FDP_IFF.1.2(2) The ~~TSF~~ **IT Environment** shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[*if the VLAN interfaces (subjects) are configured to be in the same VLAN*].

FDP_IFF.1.3(2) The ~~TSF~~ **IT Environment** shall enforce the [*information flow so that only packets contain a matching VLAN ID in the header will be forwarded to the appropriate VLAN interfaces*].

FDP_IFF.1.4(2) The ~~TSF~~ **IT Environment** shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5(2) The ~~TSF~~ **IT Environment** shall explicitly deny an information flow based on the following rules:

[*packets associated with a VLAN will not be forwarded to VLAN interfaces (subjects) not configured to be in that VLAN*].

Application Note: These (VLAN) iterations of FDP_IFC.1 and FDP_IFF.1 apply to the In-Band Central and Out-of-Band deployments of the TOE.

FPT_STM.1 (2) Reliable Time Stamps

FPT_STM.1.1(2) The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for its own use.

TOE Security Assurance Requirements

The TOE security assurance requirements summarized in Table 18: TOE Assurance Requirements are drawn from CC Part 3 and identify the management and evaluative activities required to address the threats and policies identified in the Security Objectives section of this ST. This ST complies with assurance level EAL2 augmented with ALC_FLR.2.

Table 18 TOE Assurance Requirements

Assurance Class	Assurance Components
Development	Architectural Design with domain separation and non-bypassability (ADV_ARC.1) Security-enforcing Functional Specification (ADV_FSP.2) Basic design (ADV_TDS. 1)
Guidance documents	Operational user guidance (AGD_OPE. 1) Preparative User guidance (AGD_PRE. 1)
Life Cycle Support	Use of a CM system (ALC_CMC.2) Parts of the TOE CM coverage (ALC_CMS.2) Delivery procedures (ALC_DEL.1) Flaw reporting procedures (ALC_FLR.2)
Tests	Evidence of coverage (ATE_COV. 1) Functional testing (ATE_FUN. 1) Independent testing - conformance (ATE_IND.2)
Vulnerability Assessment	Vulnerability analysis (AVA_VAN. 2)

TOE Summary Specification

This chapter identifies and describes the security functions implemented by the TOE and the assurance measures applied to ensure their correct implementation.

TOE Security Functions

NAC Decisions

The TOE's NAC Decisions Security Functionality provides for the network admission decisions and access control to the network. In addition to the three phases defined from "Device and User Authentication" section on page 18 through "Remediation" section on page 18, the TOE provides traffic filtering. Traffic policies may grant access to specific resources for users assuming the unauthenticated role. For in-band deployments this is provided by the NAC Appliance, which includes three types of traffic policies:

- IP-based policies—IP-based policies are fine-grained and flexible and can stop traffic in any number of ways. IP-based policies are intended for any role and allow you to specify IP protocol numbers as well as source and destination port numbers. For example, you can create an IP-based policy to pass through IPSec traffic to a particular host while denying all other traffic.
- Host-based policies—Host-based policies are less flexible than IP-based policies, but have the advantage of allowing traffic policies to be specified by host name or domain name when a host has multiple or dynamic IP addresses. Host-based policies are intended to facilitate traffic policy configuration primarily for Clean Access Agent Temporary and quarantine roles and should be used for cases where the IP address for a host is continuously changing or if a host name can resolve to multiple IPs.
- Layer 2 Ethernet traffic policies—To support data transfer or similar operations originating at the Layer 2 level, Cisco Clean Access Layer 2 Ethernet traffic control policies enable you to allow or deny Layer 2 Ethernet traffic through the CAS based on the type of traffic. Network Frames except for IP, ARP, and RARP frames constitute standard Layer 2 traffic.

In-Band Central deployments enforce the three types of traffic policies defined above, but rely on the central switch (within the IT environment) to provide vlan security so that traffic passes through the NAC Server.

For out-of-band deployments the traffic filtering functionality is provided by access lists on the access switch (which is part of the TOE) and vlan security on the central switch. On the access switch the IP-based policies noted above are supported.

In addition, in out-of-band and in-band central deployments, if layer 3 adjacency is used, either PBR or ACLs are used on Layer 3 devices in the IT environment for traffic engineering to forward user traffic to the NAC Server. PBR works by forcing defined traffic to follow a set path through the network to the NAC Server, and it overrides the existing route if that traffic is detected. ACLs work by filtering traffic based on rules, and would be configured on the Layer 3 device closest to the connecting clients. This is not required in Layer 2 modes of deployment.

NAC decisions are based on either successful completion of Host Authentication, Posture Assessment, and Remediation or passing Profiling checks and requirements.

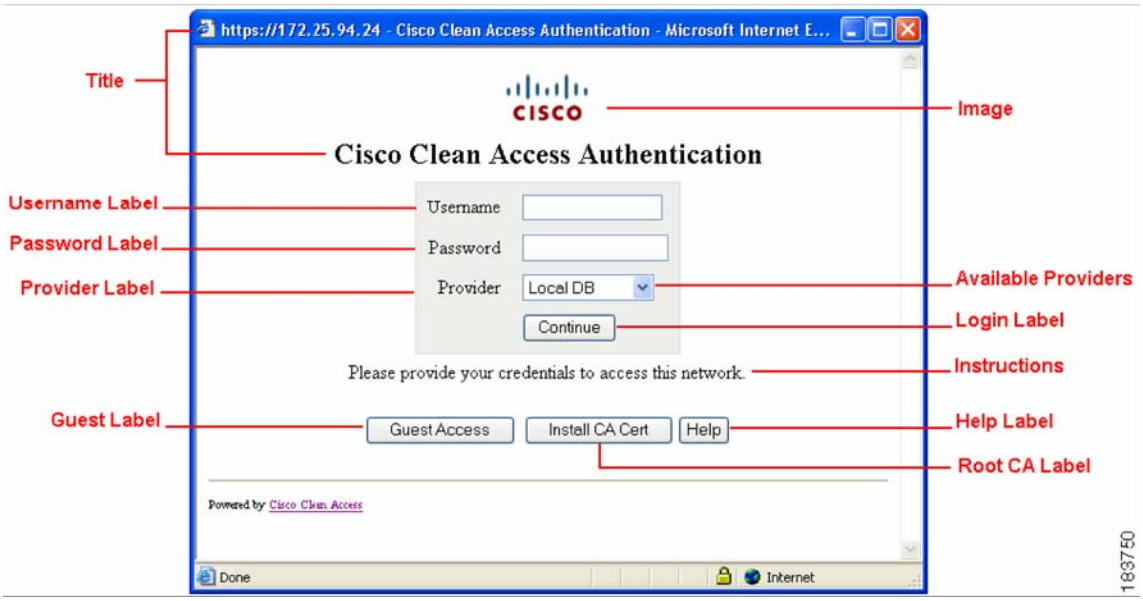
The NAC decisions made by the NAC Manager, Profiler, and Server constitutes the IDS Analyzer functionality of this TOE, and the data gathered and stored by these components in order to make the NAC decisions constitutes the Analyzer data.

As part of the NAC process in central deployments, SNMP communications must be sent to the access switch to which devices are connected. In order to do this the NAC Manager maintains SNMP credentials (user name, user authentication, and user privileges) for that switch and authenticates to begin the SNMPv3 session.

Device and User Authentication

Device and user authentication is the first phase of NAC decisions for devices that are not covered by the NAC Profiler. The device's MAC address is first compared to the certified devices list on the NAC Manager. Second the user authentication is done to the local database on the NAC Manager or the Cisco Secure ACS TOE component. Below is a sample of the challenge screen that is displayed to hosts to complete the authentication phase once they have requested access to the network. This page is controlled by the administrator on the NAC Manager.

Figure 5 Authentication Challenge Screen



If a user completes an administrator defined number of consecutive unsuccessful attempts, the user in not permitted access until an administrator unlocks the user's access. At that time, authentication may again be attempted. Definition of roles on the NAC Manager is also necessary for proper user authentication. Roles are integral to the functioning of Cisco NAC Appliance and determine traffic policies, session duration, Clean Access vulnerability assessment, and other policies within Cisco NAC Appliance for a particular group of users. The system puts a user and its associated device in a role when the user attempts to log in. There are four default user role types in the system: Unauthenticated Role, Normal Login Role, Clean Access Agent Temporary Role, and Clean Access Quarantine Role. The Unauthenticated role is the holding role for all users on the untrusted side of the NAC prior to authentication. The Normal Login role is where a user is put after a successful login. The Clean Access Agent Temporary Role is where users with the NAC Agent are placed post-authentication to allow the user limited network access to download and install required packages that will prevent the user's system from becoming vulnerable. The user is prevented from normal login role access to the network until the Clean Access Agent requirements are met. The Clean Access Quarantine role is where users are placed to allow the user limited network access to resources needed to fix vulnerabilities that already exist on the user system. The user is prevented from normal login role access to the network until the vulnerabilities are fixed. Additional roles can be defined by the NAC Manager under the Normal Login role.

Posture Assessment

Posture Assessment is the second phase of NAC decisions for devices that are not covered by the NAC Profiler. Posture assessment involves agent checks and vulnerability scanning. In order to do this the agent gathers registry settings. The agent contains:

- Built-in antivirus (AV)/ antispyware (AS) checking support for major AV and AS vendors.[5] AV/AS Rule and Requirement configuration facilitates checking that allows the Agent to automatically detect and update AV and AS definition files on the client machine. AV/AS product support is kept up-to-date on the CAM through the use of Clean Access Updates,
- Custom rule and check configuration. Administrators can configure requirements to check clients for specific applications, services, or registry keys using pre-configured Cisco checks and rules or by creating their own custom checks and rules.

The vulnerability scanning, which involves signature checking based on patterns of system settings for open vulnerabilities on the host, results in a set of potential vulnerabilities that is gathered by the agent and sent back to the NAC Server and Manager.

Remediation

Remediation is the third phase of NAC decisions for devices that are not covered by the NAC Profiler. If any items are found to be open based on the information collected in the posture assessment checks (note that this is referred to as an “intrusion” in the SFRs), those results are given to the user and must be addressed in order to pass the NAC decisions checks. Until the device is updated it’s traffic will be either blocked or quarantined by the NAC Server.

Profiling

The TOE is capable of addressing issues presented by devices such as printers, FAX machines, IP telephones and Uninterruptible Power Supplies, that are attempting access to the network but are not capable of running a NAC client. For Out-of-Band deployments, to accommodate these hosts Endpoint Profiling and Behavior Monitoring features are invoked and devices meeting a defined profile are allowed admission to the network. In-Band deployments rely on manual exclusion of these devices IP or MAC addresses in an exclusion table on the NAC Manager.

Endpoint Profiling records a network endpoint’s behaviors and analyzes the hardware and software characteristics of the device based on the recorded behavior in order to classify it to a particular group (Profile), and assesses its ability to participate in the standard NAC authentication, posture assessment, and remediation steps. The TOE classifies or profiles each endpoint it discovers and locates on the network into exactly one Profile according to the passive and active profiling mechanisms of the endpoint profiling engine.

Behavior Monitoring continuously collects and analyzes behavior information for all endpoints utilizing the network. When the behavioral attributes of an endpoint change, the NAC Profiler engine uses both statistical and signature analysis to identify deviations from normal behavior for that Profile and evaluates whether or not the behavioral changes warrant a change in the Profile of the endpoint. If a change in Profile is warranted, NAC Profiler transitions the endpoint Profile and provides alerts to network and security management. If the endpoint is found to be the problem the TOE changes the network access provided by the authentication or NAC system to deny access to the suspect device.

5 See Annex B: Supported AV and AS Vendors, page 77 for the list of support AV and AS vendors.

Audit Security Function

The TOE's Audit Security Functionality provides event auditing (based on the events listed in Table 14) and audit viewing for system functions and management functions. The following TOE components each have their own auditing facilities: NAC Manager, NAC Server, NAC Profiler Server, the host NME router, and the Access Switch. The events from Table 12 are met in the following manner:

Table 19 NAC Events

Component	Event	Applicable TOE Component	Details	NAC Event Type
FAU_GEN.1	Startup and shutdown of audit functions	All components	All audit function is automatically started during system initialization	NAC Manager, Server, and Profiler Server: All audit startup logs are stored in the audit log located in /var/log/audit and /var/log/messages Cisco Secure ACS: All audit startup logs are located in Logs\ServiceMonitoring Router or Access Switch: All audit startup logs are stored in the local logging buffer.
FAU_GEN.1	Access to Analyzer	NAC Manager	Both successful and failed attempts to access the Analyzer are recorded.	• Any Type • Failure • Success and /perfigo/logsperfigolog0.log
FAU_GEN.1	Access to TOE Analyzer Data	NAC Manager	Object ID, requested Access	• Any Type • Failure • Success
FAU_SAR.1	Reading information from the audit records	All components	This is not applicable. All Authenticated users are allowed at min read-only to the data	NAC Manager, Server, and Profiler Server. Audit information is presented to all authenticated users. Attempts to read the logs therefore are not logged. Router and Access Switch: All privileged and semi-privileged users are granted access to the logs, and there is no way for unauthenticated users to view the logs.

Table 19 NAC Events (continued)

Component	Event	Applicable TOE Component	Details	NAC Event Type
FAU_SAR.2	Unsuccess-ful attempts to read information from the audit records	All components	This is not applicable. All Authenticated users are allowed to read the data.	NAC Manager, Server, and Profiler Server: Audit information is presented to all authenticated users. Attempts to read the logs therefore are not logged. Router and Access Switch: All privileged and semi-privileged users are granted access to the logs, and there is no way for unauthenticated users to view the logs.
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	All components.	All components: Modifications to the audit configuration are recorded.	NAC Manager, NAC Server, and NAC Profiler Server: • Any Type • Failure • Success /perfigo/logs/perfigo-log0.log ACS Server: Logs\AdminAudit Router and Access Switch:All logs are stored in the local logging buffer.
FAU_UAU.1	All use of the authentication mechanism	NAC Manager or Cisco Secure ACS	User identity, location	• Any Type • Failure • Success
FAU_UAU.2	All use of the authentication mechanism	All components	User identity	• Any Type • Failure • Success
FAU_UID.1	All use of the user identification mechanism	NAC Manager or Cisco Secure ACS	User identity, location	• Any Type • Failure • Success

Table 19 NAC Events (continued)

Component	Event	Applicable TOE Component	Details	NAC Event Type
FAU_UID.2	All use of the user identification mechanism	All components	User identity	• Any Type • Failure • Information • Success
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	All components	Modifications to the behavior/functions are recorded	• Any Type • Failure • Information • Success
FMT_MDT.1	All modifications to the values of TSF data	All components		• Any Type • Failure • Success
FMT_SMR.1	Modifications to the group of users that are part of a role	All components	User Identity	• Any Type • Failure • Success
FCS_CKM.1	Success and failure of creation of cryptographic keys for remote administration.	All components	NAC Manager, NAC Server, and NAC Profiler Server: Keys are created during the initial configuration for both SSH and SSL. Success and Failure logs are created. Router and Access Switch: Keys are created during the initial configuration for SSH. Successes and Failures are logged, except when the failure involve incorrect command entry (i.e. the command is not accepted).	NAC Manager, NAC Server, and NAC Profiler Server: Certificate-related CAM/CAS connection errors. /perfigo/logs/perfigo-redirect-log0.log.0 SSL (certificates), Apache error logs /perfigo/control/apache/logs/* Router and Access Switch:All logs are stored in the local logging buffer.
FIA_UAU.5 (1)	Device and User Authentication	NAC Manager	All device and user authentication logs are available on the Manager	• Any Type • Failure • Success

Table 19 NAC Events (continued)

Component	Event	Applicable TOE Component	Details	NAC Event Type
IDS_RCT.1, FDP_IFF.1(1) FDP_IFC.1(1)	Posture Assessment, Reaction	NAC Manager	All posture logs are available on the Manager	• Any Type • Failure • Success
FDP_IFF.1(1) FDP_IFC.1(1)	Profiling on NAC Manager	NAC Manager	All devices added to the Manager by the profiler are tracked on the device filter list. An event is also created when the authenticated device is added to the device filter list.	• Any Type • Failure • Success
FDP_IFF.1(1) FDP_IFC.1(1)	Profiling on NAC Manager	NAC Manager	All devices authorized and unauthorized by the Profiler are logged on the NAC Profiler Endpoint Console	Endpoint Console

System statistics are generated for each CAS managed by the Clean Access Manager every hour by default.

Logs on the NAC Manager are presented in the Log Viewer. Through this viewer events are displayed and can be filtered and sorted by Type (Failure, Information, or Success), Category (Authentication, Administration, Client, Clean Access Server, Clean Access, Sw_Management (switch management – if out-of-band configuration), and Miscellaneous), Time, and Events. The user id that generated the event is included in the Event field. The following log files exist on the NAC appliances and include the log types displayed under “description”:

Table 20 NAC Audit Files

File	Description
/var/log/messages	Startup
/var/log/dhcplog	DHCP relay, DHCP logs (on CAS)
/perfigo/logs/perfigo-log0.log.*	Perfigo[6] service logs
/perfigo/logs/perfigo-redirect-log0.log.0	Certificate-related CAM/CAS connection errors.
/var/nessus/logs/nessusd.messages	Nessus plugin test logs
/perfigo/control/apache/logs/*	SSL (certificates), Apache error logs
/perfigo/control/tomcat/logs/localhost*.	Tomcat, redirect, JSP logs
/var/log/ha-log	High availability logs (for CAM and CAS)

6 Perfigo is the name of the company from which NAC was acquired by Cisco.

These log files on the NAC Manager include the decisions made based on analyzer data that is collected. The oldest events in these logs are overwritten if space becomes an issue on the Manager. Per Table 15 on page 33 under FAU_SAR.1, these logs are only accessible to the NAC Manager administrators (the Authorized Analyzer Administrator role). They are protected from modification and deletion by unauthorized users by the platform operating system and software.

Auditing can be turned on and off for the TOE, and logging levels are used to restrict which events are logged.

As the NAC components restrict access to audit records to authorized users there can be no unauthorized modifications to the stored audit records. Audit storage issues on the NAC components result in overwriting of the oldest audit records. To ensure that the administrator does not miss viewing records before they are deleted, SNMP traps are configured to be sent to the administrator once the free space on the device falls below a certain percentage (50% is the default). Also administrators are required to regularly review the audit trail.

On the router and Access Switch, the ability to empty the audit trail is only accessible by privileged administrators. There can be no unauthorized attempts to delete audit records, as users without privilege to the “clear logging” command on the CLI will not be able to execute it as the command will not be recognized. Audit storage exhaustion on the routers and Access Switch result in overwriting of the oldest audit records. To ensure that the administrator does not miss viewing records before they are deleted, they are required to regularly review the audit trail.

Timestamps are maintained locally on the router, Access Switch, and all NAC components. This timestamp is maintained by a hardware clock and is used for time-stamping audit events that are generated.

Administrator Identification and Authentication Security Function

All administrator interfaces to the TOE require identification and authentication. Identification and authentication is carried out by entering a user identifier and a password. The identification and authentication of users establishes the authorizations and the role (authorized NAC Server administrator, authorized Analyzer administrators, Profiler Administrator, Router Administrator, ACS Administrator, and Switch Administrator) an administrator has on the TOE. Note that SNMP users and users are not covered by this security function but by the Device and User Authentication portion of the NAC Decisions security function (See Device and User Authentication, page 18).

The administrator interfaces to the TOE are web based interfaces and command line interfaces (CLI). The web based interfaces require the user to enter identification and authentication credentials. Only after an administrator has successfully identified and authenticated themselves through the web interface will the TOE present the features and capabilities that may be used through these interfaces. The TOE stores administrator identification and authentication credentials (username, password, and authorizations) locally on each component to which authentication occurs. They are stored in an encrypted format.

The CLIs are accessible through a serial console interface, and the NAC Manager, NAC Server, router, Cisco Secure ACS, and access switch’s CLIs can also be reached through SSH. The CLI is used for initial configuration and setup of the TOE. The CLI requires a user to supply a user identifier and a password before they are allowed to carry out any other actions with the TOE.

Management Security Function

Administration functions for the TOE are accomplished through the use of web interface management GUIs on the NAC Manager, Cisco Secure ACS, and Profiler and management CLIs on the NAC Server, Manager, host router to the NME, Cisco Secure ACS, and access switch (for out-of-band deployments).

Communications through these mechanisms use established communication protocols for request transfer to command the TOE for configuration and maintenance. Administrative requests generated via the web interface management GUIs are transmitted via HTTPS as a secure communication channel that protects the confidentiality and integrity (detection of modification) of the administrative commands. If the integrity of any of the HTTPS communications is compromised the TOE will drop the networking packets that are corrupt based on the fact that the MAC is incorrect and request a resend of the dropped packet. The TOE will not accept any packet were the MAC is incorrect. The CLIs are used to carry out initial administrative configuration of the TOE. The web interface management GUIs are used for operational administration of the TOE once in the evaluated configuration.

Data from the TOE is made available to those connecting to the TOE through the web interface as long as the user is using Internet Explorer and that the workstation that the user is using to connect to the TOE from has a routable connection to the TOE.

Administrative access permissions are defined by the role associated with the user accessing the system. The non-user roles defined for the TOE are authorized NAC Server administrator, authorized Analyzer administrator, Profiler Administrator, Router Administrator, ACS Administrator, and Switch Administrator. These roles determine the level at which administration may be carried out.

- **Authorized NAC Server administrator** role: administrators operating in the authorized NAC Server administrator role may carry out all administrative operations on the NAC Server, configure set network settings on the device, generate SSL certificates, update their own password, and local audit log review. Authorized NAC Server administrators are composed of the administrators for the NAC Server Direct Access Web Console and NAC Server command line.
- **Authorized Analyzer administrator**: administrators operating in the authorized Analyzer administrator role have the ability to carry out all the administrative operations on the NAC Manager, including defining NAC policies, creating users of the TOE, view audit events, and viewing analyzer events. Authorized Analyzer administrators are composed of the administrator for the NAC Manager GUI and command line.
- **Profiler Administrator** role: administrators operating in the Profiler Administrator may carry out all administrative operations on the NAC profiler. Note that this is only relevant when the Profiler is included (i.e. Out-of-Band deployments). Profiler administrators are composed of the administrator for the GUI (admin), and the two administrative accounts at the Linux command line (root and beacon). There are also less-privileged roles maintained on the Profiler GUI: the operator and the analyst. The operator has full access to Cisco NAC Profiler with the exception of adding, deleting, and enabling/disabling users. The analyst has read-only access to Cisco NAC Profiler. The operator and analyst are not needed for TOE functionality and are not included in the TOE.
- **ACS Administrator** role: administrators operating as the ACS Administrator may carry out all administrative operations on the Cisco Secure ACS. ACS administrators are composed of the administrator for the command line, and other administrator defined administrative accounts for the GUI. The privileges of the other administrator defined administrative accounts are assigned at time of creation by the administrator for the command line.
- **Router Administrator** role: administrators operating in the router administrator role have access to all functionality on the host router for the NME. Note that this is only relevant when the NME is included (i.e. In-Band deployments). With regard to the TSF, this includes local identification and authentication, local audit review, and power control to the router (and embedded NME). This functionality is available to both the semi-privileged (after authentication but prior to entering the enable password) and privileged (after entering the enable password) users on the router.
- **Switch Administrator** role: administrators operating in the switch administrator role have access to all functionality on the access switch. Note that this is only relevant when the access switch is included (i.e. Out-of-Band deployments). With regard to the TSF, this includes local identification and authentication, local audit review, and SNMP communications with the NAC Server to configure which VLAN a device's connecting port is part of. The local identification and

authentication and local audit review functionality is available to both the semi-privileged (after authentication but prior to entering the enable password) and privileged (after entering the enable password) users on the router. All other functionality is available only to the privileged users.

Self Protection Security Function

The protection mechanisms employed by the TOE ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. More specifically, once a user has been authenticated (whether via the various Web interfaces, various CLIs, or as a host entering the network) the Identification and Authentication is used to query and return the user's role. The role is used to determine what functionality is presented to the user. No other means, other than described above, are provided for the user to interact with the TOE.

The Self-protection function is responsible for providing an execution domain that is protected from interference and tampering by unauthorized users. The NAC Appliance is a dedicated piece of hardware, with no general purpose operating system or programming interface. No untrusted processes are permitted on the NAC Appliance. Because the whole NAC Appliance is a separate physical domain and a dedicated platform solely supporting its own processes and the fact that it controls and mediates access to its interfaces, it provides a security domain for the TSF that is protected from interference and tampering. At all physical interfaces, the TOE intercedes to ensure domain separation. The collected data and/or unauthorized users cannot bypass the identification and authentication mechanisms, preventing interference and tampering by untrusted subjects and thereby maintaining a domain for its own execution.

The TOE provides cryptographic operations to protect communications between its components. The communication paths between components are protected by the following cryptographic methods, SSH, SSL, SNMPv3, cryptographic methods specified in RADIUS, and inter-TOE communication using a shared secret. The key generation, encryption/decryption operations, and key destruction are provided by the TOE.

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

Assurance Measures

The TOE satisfies CC EAL2 assurance requirements augmented with ALC_FLR.2. This section identifies the Configuration Management, Delivery and Operation, Development, Flaw Remediation, Guidance Documents, Testing, and Vulnerability Assessment Assurance Measures applied by CISCO to satisfy the CC EAL2+ assurance requirements. Table 21 lists the details.

Table 21 Assurance Measures

Assurance Component	How Requirement will be Met
ADV_ARC.1 Security architecture description	The architecture of the TOE that is used to protect the TSF documented by Cisco in their development evidence.
ADV_FSP.2 Security-enforcing functional specification	The externally visible interfaces of the TOE used by the users of the TOE along with the description of the security functions and a correspondence between the interfaces and the security functions from the ST are documented by Cisco in their development evidence. The development evidence also contains a tracing to the SFRs described in this ST.

Table 21 Assurance Measures (continued)

Assurance Component	How Requirement will be Met
ADV_TDS.1 Basic design	The design of the TOE will be described in the development evidence. This evidence will also contain a tracing to the TSFI defined in the FSP.
AGD_OPE.1 Operational user guidance	The administrative guidance is detailed to provide descriptions of how administrative users of the TOE can securely administer the TOE using those functions and interfaces detailed in the guidance.
AGD_PRE.1 Preparative procedures	Cisco documents the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.2 Use of a CM system	Cisco performs configuration management on configuration items of the TOE. Configuration management is performed on the TOE and the implementation representation of the TOE.
ALC_CMS.2 Parts of the TOE CM coverage	Cisco uniquely identifies configuration items and each release of the TOE has a unique reference. The Configuration Management documentation contains a configuration item list.
ALC_DEL.1 Delivery procedures	Cisco documents the delivery procedure for the TOE to include the procedure on how to download certain components of the TOE from the Cisco website and how certain components of the TOE are physically delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained. Further, the delivery documentation describes how to acquire the proper license keys to use the TOE components.
ALC_FLR.2 Flaw reporting procedures	Cisco documents the flaw remediation and reporting procedures so that security flaw reports from TOE users can be appropriately acted upon, and TOE users can understand how to submit security flaw reports to the developer.
ATE_COV.1 Evidence of coverage	Cisco demonstrates the interfaces tested during functional testing using a coverage analysis.
ATE_FUN.1 Functional testing	Cisco functional testing documentation contains a test plan, a description of the tests, along with the expected and actual results of the test conducted against the functions specified in the ST.
ATE_IND.2 Independent testing - sample	Cisco will help meet the independent testing by providing the TOE to the evaluation facility.
AVA_VAN.2 Vulnerability analysis	Cisco will provide the TOE for testing.

Rationale

Security Objectives Rationale

This section demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective. Table 22 and Table 23 provide the mapping and rationale for the security objectives identified in Security Objectives, page 28 and the assumptions, threats and policies identified in Security Problem Definition, page 26.

Table 22 Threats, Assumptions, and Policies to Security Objectives Mapping

	O. PROTCT	O.IDACTS	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O. EXPORT	O.COLLECT	OE.INSTAL	OE. PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.PROTCT	OE.VLAN
A.ACCESS																X					
A.PROTCT													X								
A.LOCATE													X								
A.MANAGE															X						
A.NOEVIL												X	X	X							
A.NOTRST													X	X							
A.HOST																				X	
T.COMINT	X				X	X			X											X	
T.COMDIS	X				X	X				X											
T.LOSSOF	X				X	X			X												
T.NOHALT		X			X	X															
T.PRIVIL	X				X	X															
T.IMPCON				X	X	X						X									
T.INFLUX							X														
T.FALACT			X																		
T.FALREC		X									X										
T.FALASC		X									X										
T.BYPASS												X									X
P.ANALYZ		X																			
P.DETECT		X						X									X				
P.MANAGE	X			X	X	X						X		X	X						
P.ACCESS	X				X	X												X			

Table 22 Threats, Assumptions, and Policies to Security Objectives Mapping (continued)

	O. PROTCT	O.IDACTS	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O. EXPORT	O.COLLECT	OE.INSTAL	OE. PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.PROTCT	OE.VLAN
P.ACCACT						X		X									X		X		
P.INTGTY									X												
P.PROTCT				X									X								

Table 23 Threats, Assumptions, and Policies to Security Objectives Rationale

Threat/ Assumption/Policy	Security Objectives Rationale
A.ACCESS	The OE.INTROP objective ensures the TOE has the needed access.
A.PROTCT	The OE.PHYCAL provides for the physical protection of the TOE hardware and software.
A.LOCATE	The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL	The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRST	The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.HOST	The objective OE.PROTCT upholds the assumption as: The agents will be installed on a physically secure, properly configured and maintained IT platform.
T.COMINT	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection. Similarly, The OE.PROTCT objective addresses this threat by providing self-protection of the host operating systems in the environment.

Table 23 Threats, Assumptions, and Policies to Security Objectives Rationale (continued)

Threat/ Assumption/Policy	Security Objectives Rationale
T.COMDIS	The O.IDAUTH (FAU_SAR.2, FAU_STG.2(1), FIA_AFL.1, FIA_UAU.1, FIA_ATD.1, FIA_UAU.5(1), FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, ADV_ARC.1, IDS_RDR.1, IDS_STG.1) objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.LOSSOF	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.NOHALT	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDACTS objective addresses this threat by requiring the TOE to collect all events, including those attempts to halt the TOE.
T.PRIVIL	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.IMPCON	The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.INFLUX	The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.
T.FALACT	The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

Table 23 Threats, Assumptions, and Policies to Security Objectives Rationale (continued)

Threat/ Assumption/Policy	Security Objectives Rationale
T.FALREC	The O.COLLECT and O.IDACTS objectives provide the function that the TOE will collect information and recognize vulnerabilities or inappropriate activity from a data source.
T.FALASC	The O.COLLECT and O.IDACTS objectives provide the function that the TOE will collect information and recognize vulnerabilities or inappropriate activity from multiple data sources.
T.BYPASS	The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The OE.VLAN objective states that VLANs must be used to properly route information through the TOE.
P.ANALYZ	The O.IDACTS objective requires analytical processes be applied to data collected from Sensors and Scanners.
P.DETECT	The O.IDACTS objective requires analytical processes be applied to data collected from Sensors and Scanners. The O.AUDITS objective addresses this policy by requiring collection of audit, Sensor, and Scanner data. The OE.TIME objective will provide a time stamp for each audit.
P.MANAGE	The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The O.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O. PROTCT objective provides for TOE self-protection.
P.ACCESS	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective provides for TOE self-protection. The OE.AUDIT_PROTECTION objective provides protection for audit events in the environment.

Table 23 Threats, Assumptions, and Policies to Security Objectives Rationale (continued)

Threat/ Assumption/Policy	Security Objectives Rationale
P.ACCACT	The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The OE.TIME objective will provide a time stamp for each audit. The OE.AUDIT_SORT objective provides the ability to sort audit events in the environment.
P.INTGTY	The O.INTEGR objective ensures the protection of data from modification.
P.PROTCT	The O.OFLOWS objective requires the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

Rationale for Security Functional Requirements

Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the Security Functional Requirements are suitable to address the security objectives. It identifies each Security Functional Requirement identified in section TOE Security Functional Requirements, page 31, and the TOE security objective(s) identified in section Security Objectives for the TOE, page 28, that addresses it. Table 26 “Environmental Security Functional Requirement to Environmental Security Objectives Mapping” and Table 27 “Environmental Security Functional Requirement to Environmental Security Objectives Rationale” provide the mapping and rationale for inclusion of each SFR in this ST.

Table 24 TOE Security Functional Requirement to TOE Security Objectives Mapping

	O. PROTCT	O.IDACTS	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O. EXPORT	O.COLLECT
FAU_GEN.1								X			
FAU SAR.1				X							
FAU_SAR.2					X	X					
FAU_SAR.3(1)				X							
FAU_SEL.1				X				X			
FAU_STG.2(1)	X				X	X	X		X		
FAU_STG.4							X	X			
FCS_COP.1(1) through (8)	X									X	
FCS_CKM.1(1) through (3)	X									X	

Table 24 TOE Security Functional Requirement to TOE Security Objectives Mapping

	O. PROTCT	O.IDACTS	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O. EXPORT	O.COLLECT
FCS_CKM.4	X									X	
FDP_IFC.1(1)			X		X						
FDP_IFF.1(1)			X		X						
FIA_AFL.1						X					
FIA_ATD.1						X					
FIA_UAU.1					X	X					
FIA_UAU.2						X					
FIA_UAU.5(1)					X	X					
FIA_UID.1					X	X					
FIA_UID.2						X					
FMT_MOF.1	X				X	X					
FMT_MSA.1				X							
FMT_MSA.2				X							
FMT_MSA.3				X							
FMT_MTD.1	X				X	X			X		
FMT_SMF.1	X	X	X	X		X	X				
FMT_SMR.1						X					
FPT_ITA.1										X	
FPT_ITC.1									X	X	
FPT_ITI.1									X	X	
FPT_ITT.1	X										
ADV_ARC.1	X			X		X		X	X		
FPT_STM.1(1)								X			
IDS_ANL.1		X									
IDS_RCT.1			X								
IDS_RDR.1				X	X	X					
IDS_STG.1	X				X	X	X		X		
IDS_STG.2							X				
IDS_COL.1		X									X

Table 25 TOE Security Functional Requirement to TOE Security Objectives Rationale

Security Objective (TOE)	Security Functional Requirement Rationale
O. PROTCT	The TOE is required to protect the audit data from deletion as well as guarantees the availability of the audit data in the event of storage exhaustion or attack [FAU_STG.2]. The Analyzer is required to protect the Analyzer data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure, or attack [IDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer may query the Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE provides the management security functions to manage the security attributes for users [FMT_SMF.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1]. The TSF protects data to and from its components with encryption [FCS_COP.1(1) through (8), FCS_CKM.1(1) through (3), FCS_CKM.4]. The TOE protects data between TOE components [FPT_ITT.1].
O.IDACTS	The TOE collects data [IDS_COL.1], performs intrusion analysis, and generates conclusions [IDS_ANL.1]. The TOE provides the management security functions to manage the rules and the sources for data to be analyzed that it applies its analytic processes that are used to derive its analysis conclusions [FMT_SMF.1].
O.RESPON	The TOE is required to respond accordingly in the event of a detected intrusion based on how it has been configured [IDS_RCT.1]. The TOE provides the management security functions that allows for the management of the TOE's response to intrusions [FMT_SMF.1]. The TOE requires successfully passing of the NAC SFP checks to gain admission to the network [FDP_IFC.1(1), FDP_IFF.1(1)].
O.EADMIN	The TOE must provide the ability to review and manage the audit trail of an Analyzer [FAU_SAR.1, FAU_SEL.1, FAU_SAR.3(1)]. The Analyzer must provide the ability for authorized administrators to view the Analyzer data [IDS_RDR.1]. The TOE provides the management security functions for the security functions of the TOE [FMT_SMF.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1]. The TOE provides the ability for authorized administrators to control cryptographic functions and edit the NAC SFP [FMT_MSA.1, FMT_MSA.2, FMT_MSA.3].

Table 25 TOE Security Functional Requirement to TOE Security Objectives Rationale

Security Objective (TOE)	Security Functional Requirement Rationale
O.ACCESS	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The Analyzer is required to restrict the review of TOE data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the audit data from deletion as well as guarantees the availability of the audit data in the event of storage exhaustion, failure, or attack [FAU_STG.2(1)]. The Analyzer is required to protect the Analyzer data from any modification and unauthorized deletion [IDS_STG.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1, FIA_UAU.5(1)]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer may query and add Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE requires successfully passing of the NAC SFP checks to gain admission to the network [FDP_IFC.1(1), FDP_IFF.1(1)].
O.IDAUTH	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The Analyzer is required to restrict the review of collected Analyzer data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2(1)]. The Analyzer is required to protect the Analyzer data from unauthorized deletion as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. Security attributes of subjects used to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UID.2, FIA_UAU.1, FIA_UAU.2, and FIA_UAU.5(1)]. The TOE is required to restrict the number of incorrect authentication attempts to the TOE data [FIA_AFL.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer may query and add Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE provides the security management functions for the security attributes for defining an authorized user of the TOE [FMT_SMF.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1].
O.OFLOWS	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2(1)]. The TOE must prevent the loss of audit data in the event its audit trail is full [FAU_STG.4]. The TOE provides the security management functions that manage the use of storing of data on the TOE [FMT_SMF.1]. The Analyzer is required to protect the Analyzer data from any modification and unauthorized deletion, as well as guarantees the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The Analyzer must prevent the loss of audit data in the event the its audit trail is full [IDS_STG.2].

Table 25 TOE Security Functional Requirement to TOE Security Objectives Rationale

Security Objective (TOE)	Security Functional Requirement Rationale
O.AUDITS	Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE prevents the loss of collected data in the event its audit trail is full [FAU_STG.4]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1]. Time stamps associated with an audit record must be reliable [FPT_STM.1(1)].
O.INTEGR	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The Analyzer is required to protect the Analyzer data from any modification and unauthorized deletion [IDS_STG.1]. Only authorized administrators of the Analyzer may query or add audit and Analyzer data [FMT_MTD.1]. The Analyzer must protect the collected data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1]. The TOE must ensure that all functions to protect the data are not bypassed [ADV_ARC.1]. The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1].
O. EXPORT	The TOE must make the Analyzer data available to other IT products [FPT_ITA.1]. The TOE must protect the Analyzer data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1]. The TSF protects the confidentiality of Analyzer data that is made available to other components with encryption [FCS_COP.1(1) through (8), FCS_CKM.1(1) through (3), FCS_CKM.4]. The TOE protects data between TOE components [FPT_ITT.1].
O.COLLECT	The TOE collects data that might indicate an intrusion so that decisions can be made for NAC access [IDS_COL.1].

Rationale for Security Functional Requirements of the IT Environmental Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the Security Functional Requirements are suitable to address the security objectives. It identifies each IT Environment Security Functional Requirement identified in TOE Security Functional Requirements, page 31, and the IT Environmental security objective(s) identified in Security Objectives for the Environment, page 29 that addresses it. Table 26 “Environmental Security Functional Requirement to Environmental Security Objectives Mapping” and Table 27 “Environmental Security Functional Requirement to Environmental Security Objectives Rationale” provide the mapping and rationale for inclusion of each IT environment SFR in this ST. The environmental security objectives that were not

mapped relate to physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. The purpose for these environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures.

Table 26 Environmental Security Functional Requirement to Environmental Security Objectives Mapping

	OE.TIME	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.PROTCT	OE.VLAN
FAU_SAR.3(2)			X		
FAU_STG.2(2)		X			
FCS_COP.1(9)				X	
FDP_IFC.1(2)					X
FDP_IFF.1(2)					X
FPT_STM.1(2)	X				

Table 27 Environmental Security Functional Requirement to Environmental Security Objectives Rationale

Security Objective (TOE)	Security Functional Requirement Rationale
OE.TIME	The IT Environment will provide reliable time stamp to the TOE. Time stamps associated with an audit record must be reliable [FPT_STM.1(2)].
OE.AUDIT_PROTECTION	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2].
OE.AUDIT_SORT	The IT environment must provide the ability to review and manage the audit trail of the System to include sorting the audit data [FAU_SAR.3,].
OE. PROTCT	The host Windows or Mac operating system provides the crypto libraries for use during SSL encryption between the agent and the NAC Server [FCS_COP.1(9)].
OE.VLAN	The Central Switch utilize VLANs to route traffic to the TOE.

TOE Security Functions

This section demonstrates the suitability of the security functions defined in TOE Security Functions, page 45 of meeting the TOE's Security Functional Requirements identified in Conventions, page 30and that the security functional requirements are completely and accurately met by the TOE's Security Functions identified in TOE Security Functions, page 45.

Table 28 demonstrates the correspondence between the Security Functions and the TOE Security Functional Requirements. With the demonstration of correspondence given in Table 29 and the descriptions of the security functions given in TOE Security Functions, page 45 on how the security functions are providing the functionality to meet the security functional requirements this provides the evidence of suitability of the security functions in meeting the security functional requirements stated in Conventions, page 30.

Table 28 TOE Security Functional Requirement to TOE Security Functions Mapping

TOE Security Functional Requirement	NAC Decisions Security Function	Audit Security Function	Administrator Identification and Authentication Security Function	Management Security Function	Self Protection Security Function
FAU_GEN.1		X			
FAU_SAR.1		X			
FAU_SAR.2		X			
FAU_SAR.3(1)		X			
FAU_SEL.1		X			
FAU_STG.2(1)		X			
FAU_STG.4		X			
FCS_COP.1(1) through (8)					X
FCS_CKM.1(1) through (3)					X
FCS_CKM.4					X
FDP_IFC.1(1)	X				
FDP_IFF.1(1)	X				
FIA_AFL.1	X				
FIA_ATD.1	X		X		
FIA_UAU.1	X				
FIA_UAU.2			X		
FIA_UAU.5	X		X		
FIA_UID.1	X				
FIA_UID.2			X		
FMT_MOF.1				X	
FMT_MSA.1				X	
FMT_MSA.2				X	

Table 28 TOE Security Functional Requirement to TOE Security Functions Mapping (continued)

TOE Security Functional Requirement	NAC Decisions Security Function	Audit Security Function	Administrator Identification and Authentication Security Function	Management Security Function	Self Protection Security Function
FMT_MSA.3				X	
FMT_MTD.1				X	
FMT_SMF.1				X	
FMT_SMR.1	X			X	
FPT_ITA.1				X	
FPT_ITC.1					X
FPT_ITI.1					X
FPT_ITT.1					X
FPT_STM.1		X			
IDS_ANL.1	X				
IDS_RCT.1	X				
IDS_RDR.1		X			
IDS_STG.1		X			
IDS_STG.2		X			
IDS_COL.1	X				

Table 29 Rationale of How the SF(s) Meet the SFR(s)

SFR	SF and Rationale
FAU_GEN.1	Is implemented by the Audit Security Function. The Audit security function generates audit records for access to the TOE which shows access to the TOE and analysis data stored and processed by the TOE. All users that operate in the Admin, Security Analyst, and Operator role are allowed to access and review all audit records and the audit trail. The TOE generates audit records when roles are changed; rules are created, modified, or deleted; when reporting devices, sensors, are added or deleted; and when alerts are created or modified.
FAU_SAR.1	Is implemented by the Audit Security Function. The TOE provides a web interface to users operating in the Admin, Security Analyst, and Operator roles to review the audit records of the TOE. The web interface provides the audit records in HTML format that is suitable for human users to review.

Table 29 Rationale of How the SF(s) Meet the SFR(s) (continued)

SFR	SF and Rationale
FAU_SAR.2	Is implemented by the Audit Security Function. The TOE only allows users operating in the Admin, Security Analyst, and Operator roles to review the audit records. The users operating in any one of these three roles must successfully identify and authenticate themselves to the TOE before they are allowed to access the TOE and therefore be able to review the audit records. Identification and authentication to the TOE is the explicit request of a user in one of the roles that must be successfully made to be able to review the audit records and the user must be granted the explicit read access by having a user account setup for the user with one of these roles and their identification and authentication information.
FAU_SAR.3(1)	Is implemented by the Audit Security Function. The TOE allows sorting of audit data by Type (Failure, Information, or Success), Category (Authentication, Administration, Client, Clean Access Server, Clean Access, Sw_Management (switch management – if out-of-band configuration), Miscellaneous, and DHCP), Time, and Events.
FAU_SEL.1	Is implemented by the Audit Security Function. The TOE allows events to be selected based on audit levels.
FAU_STG.2(1)	Is implemented by the Audit Security Function. The TOE requires users to successfully identify and authenticate themselves to the TOE before they are allowed to carry out any other actions with the TOE. All users that have permission to log into the TOE (those users operating in the Admin, Security Analyst and Operator roles) are allowed to view the audit records only the Admin role users are allowed to purge (back up) the audit records from the TOE. The purge event is audited when a user operating in the Admin role carries this activity out. The generation of the audit record is a detection capability that can be used to determine if an unauthorized modification to the stored audit records have occurred with the audit trail.
FAU_STG.4	Is implemented by the Audit Security Function. The TOE will send an SNMP trap to an administrator of the TOE indicating that the disk space has reached a certain capacity (default is 50%) and then overwrite the oldest stored audit records when the audit trail becomes full. For switches and routers no alarm is sent and the oldest events are overwritten.
FCS_COP.1(1) through (8)	Is implemented by the Self Protection Security Function. The TOE provides cryptographic operations to protect communications to and from its components.
FCS_CKM.1(1) through (3)	Is implemented by the Self Protection Security Function. The TOE provides cryptographic operations to protect communications to and from its components.
FCS_CKM.4	Is implemented by the Self Protection Security Function. The TOE provides cryptographic operations to protect communications between its components.
FDP_IFC.1(1)	Is implemented by the NAC Decisions Security Function. The TOE, as a result of the host authentication, posture assessment, remediation, and profiling functions results in the user/ host either being granted admission to the network or not.

Table 29 Rationale of How the SF(s) Meet the SFR(s) (continued)

SFR	SF and Rationale
FDP_IFF.1(1)	Is implemented by the NAC Decisions Security Function. The TOE, as a result of the host authentication, posture assessment, remediation, and profiling functions results in the user/ host either being granted admission to the network or not.
FIA_AFL.1	Is implemented by the NAC Decisions Security Function. The NAC Manager allows you to set a number of consecutive failed login attempts that triggers an account to be locked, and then must it be unlocked by the administrator.
FIA_ATD.1	Is implemented by the NAC Decisions and Administrator Identification and Authentication Security Functions. The NAC Decisions and Identification and Authentication security functions maintain the user security attributes of identifier, password information (authentication data), the user authorizations (the users role), and the group the user belongs for both administrative and non-administrative users.
FIA_UAU.1	Is implemented by the NAC Decision Security Function. The TSF only allows access configured for the unauthenticated user as defined by TOE Traffic policies prior to authentication.
FIA_UAU.2	Is implemented by the Administrator Identification and Authentication Security Function. The TSF does not allow any administrative actions prior to the user being authenticated.
FIA_UAU.5	Is implemented by the Administrator Identification and Authentication Security Function. The Administrative users of the TOE are required to successfully authenticate prior to accessing the TOE. Is implemented by the NAC Decisions Security Function. The users of the TOE must pass host authentication checks as part of the NAC SFP.
FIA_UID.1	Is implemented by the NAC Decision Security Function. The TSF only allows access configured for the unauthenticated user as defined by TOE Traffic policies prior to identification.
FIA_UID.2	Is implemented by the Administrator Identification and Authentication Security Function. The TSF does not allow any administrative actions prior to the user being identified.
FMT_MOF.1	Is implemented by the Management Security Function. The TSF restricts the ability to modify the behavior of the analysis and reaction capabilities of the TOE to the authorized Analyzer administrators, those users that operate at the Admin role level of privilege. The TSF restricts the ability to modify the behavior of the analysis and reactions capabilities of the TOE by requiring all users to successfully identify and authenticate themselves to the TOE before being allowed to carry out any types of administrative functions and by maintaining a user profile that contain a role security attribute. The role security attribute defines the types of actions that the user can carry out on the TOE and the TOE requires users to have the Admin role to modify the analysis and reaction capabilities of the TOE.
FMT_MSA.1	Is implemented by the Management Security Function. The TOE allows the administrator to control the cryptographic functions and NAC SFP settings.
FMT_MSA.2	Is implemented by the Management Security Function. The TOE establishes default secure values for cryptographic keys.

Table 29 Rationale of How the SF(s) Meet the SFR(s) (continued)

SFR	SF and Rationale
FMT_MSA.3	Is implemented by the Management Security Function. The TOE allows the administrator to control NAC SFP settings.
FMT_MTD.1	Is implemented by the Management Security Function. The TSF restricts the ability to query and add analyzed data and audit data and to query and modify all other TOE data to those users that have defined user profiles on the TOE and further restricts the ability carry out these types of actions based on the role the user is operating at. The user has to be operating and the Admin or Security Analyst role to carry out the combination of these actions. The TSF restricts these capabilities of the TOE by requiring all users to successfully identify and authenticate themselves to the TOE before being allowed to carry out any types of querying and modification of analysis data and audit data and by maintain a user profile that contains a role security attribute. The role security attribute defines the types of actions that the user can carry out on the TOE and the TOE requires users to have the Admin or Security Analyst role to carry out the capabilities defined in the FMT_MTD.1 security functional requirement.
FMT_SMF.1	Is implemented by the Management Security Function. The TOE provides a capability to allow for users to communicate with the TSF through a web interface. The web interface provides access to those authorized to those management functions that are necessary to management the security attributes and security functions defined in the security functional requirement defined in section 5 of this ST.
FMT_SMR.1	Is implemented by the Management and the NAC Decision Security Functions. The Management Security Function implements the roles of authorized NAC Server administrator, authorized Analyzer administrator, Profiler Administrator, Router Administrator, ACS Administrator, and Switch Administrator. Each role has specific capabilities that it can or can not use. The NAC Decision Security Function implements the roles of SNMP User and User. Each role has specific capabilities that it can or can not use.
FPT_ITA.1	Is implemented by the Management Security Function. The TOE uses SSL as the security capability to protect the confidentiality of communications that happen between it and the web browser interface that the TOE provides to authorized administrators of the TOE. The TOE supports the use of the Internet Explorer web browser for viewing audit records. The TOE is able to process requests received from the browser and return the results in less then 60 seconds.
FPT_ITC.1	Is implemented by the Self Protection Security Function. The TOE protects communications between its components.
FPT_ITI.1	Is implemented by the Self Protection Security Function. The TOE uses the features of SSL and SSH to detect modification of TSF data when the TSF data is being transmitted between the TOE and a web browser and between the TOE and an SSH client. Specifically the message authentication code (MAC) is used of SSL and SSH to detect modification of TSF data. If any of the transmissions are modified in transit the MAC will indicate this with an error and the packet(s) will be dropped. The TOE will request a resend of dropped packets and will only accept those packets that have the proper MAC.

Table 29 Rationale of How the SF(s) Meet the SFR(s) (continued)

SFR	SF and Rationale
FPT_ITT.1	Is implemented by the Self Protection Security Function. The TOE provides protected communications between its components.
FPT_STM.1	Is implemented by the Audit Security Function. The TOE components have internal system clocks which are used to generate timestamps for audit records.
IDS_ANL.1	Is implemented by the NAC Decisions Security Function. The TOE performs signature and statistical, analysis on the data that it collects from devices attempting admission to the network. This analysis is performed based on policies that are configured in the TOE by an authorized administrator with the proper privileges.
IDS_RCT.1	Is implemented by the NAC Decisions Security Function. Upon detection of open items from the posture assessment the TOE will log the event, display for the user what needs to be updated and block or quarantine the device's traffic.
IDS_RDR.1	Is implemented by the Audit Security Function. The Audit security function only allows those explicitly authorized and authenticated users operating in the authorized Analyzer administrator role to review the incidents, auditing data, and reports generated by the TOE. The TOE presents this data to users through the web interface to the TOE which allows human users to understand the data the TOE is presenting them.
IDS_STG.1	Is implemented by the Audit Security Function. The TOE requires users to successfully identify and authenticate themselves to the TOE before they are allowed to carry out any other actions with the TOE. All users that have permission to log into the NAC Manager (those users operating in the authorized Analyzer administrator role) are allowed to view the audit records only the Admin role users are allowed to purge (back up) the analysis data from the TOE. The purge event is audited when a user operating in the Admin role carries this activity out. The generation of the audit record is a detection capability that can be used to determine if an unauthorized modification to the stored analyzer data have occurred with the stored analysis data. The TOE will ensure that all analyzer data stored on the hard drives of the TOE are maintained when the physical hard drive resources are exhausted or attacked.
IDS_STG.2	Is implemented by the Audit Security Function. The NAC Manager stores logs within its Linux operating system, and when they reach capacity the oldest analyzer events are overwritten.
IDS_COL.1	Is implemented by the NAC Decisions Security Function. The TOE requires that the agent collect data on the device to be used in the NAC decisions process, including registry settings and information on known vulnerabilities.

TOE Security Functional Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified TOE and IT Security Functional Requirements include the appropriate hierarchical SFRs and dependent SFRs. Table 30 lists the TOE Security Functional Components and the Security Functional Components each are hierarchical to and dependent upon and any necessary rationale.

N/A in the Rationale column means the Security Functional Requirement has no dependencies and therefore, no dependency rationale is required. Satisfied in the Rationale column means the Security Functional Requirements dependency was included in the ST.

Table 30 TOE Security Functional Requirements Dependency Rationale

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components	FPT_STM.1	Satisfied
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components	FAU_SAR.1	Satisfied
FAU_SAR.3	No other components	FAU_SAR.1	Satisfied
FAU_SEL.1	No other components	FAU_GEN.1 FMT_MTD.1	Satisfied
FAU_STG.2	FAU_STG.1	FAU_GEN.1	Satisfied
FAU_STG.4	FAU_STG.3	FAU_STG.1	Satisfied by FAU_STG.2 because of hierarchy
FCS_COP.1	No other components	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	Satisfied
FCS_CKM.1	No other components	FCS_COP.1 FCS_CKM.4 FMT_MSA.2	Satisfied
FCS_CKM.4	No other components	FCS_CKM.1 FMT_MSA.2	Satisfied
FDP_IFC.1	No other components	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components	FDP_IFC.1 FMT_MSA.3	Satisfied
FIA_UAU.1	No other components	FIA_UID.1	Satisfied
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA UID.2
FIA_AFL.1	No other components	FIA_UAU.1	Satisfied
FIA_ATD.1	No other components	No dependencies	N/A
FIA_UAU.5	No other components	No dependencies	N/A

Table 30 TOE Security Functional Requirements Dependency Rationale (continued)

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FIA_UID.1	No other components	No dependencies	N/A
FIA_UID.2	FIA_UID.1	No dependencies	N/A
FMT_MOF.1	No other components	FMT_SMR.1 FMT_SMF.1	Satisfied
FMT_MSA.1	No other components	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Satisfied
FMT_MSA.2	No other components	FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	Satisfied
FMT_MSA.3	No other components	FMT_MSA.1 FMT_SMR.1	Satisfied
FMT_MTD.1	No other components	FMT_SMR.1 FMT_SMF.1	Satisfied
FMT_SMF.1	No other components	No dependencies	N/A
FMT_SMR.1	No other components	FIA_UID.1	Satisfied
FPT_ITA.1	No other components	No dependencies	N/A
FPT_ITC.1	No other components	No dependencies	N/A
FPT_ITI.1	No other components	No dependencies	N/A
FPT_ITT.1	No other components	No dependencies	N/A
FPT_STM.1	No other components	No dependencies	N/A
IDS_ANL.1	No other components	No dependencies	N/A
IDS_RCT.1	No other components	No dependencies	N/A
IDS_RDR.1	No other components	No dependencies	N/A
IDS_STG.1	No other components	No dependencies	N/A

Table 30 TOE Security Functional Requirements Dependency Rationale (continued)

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
IDS_STG.2	No other components	No dependencies	N/A
IDS_COL.1	No other components	No dependencies	N/A

Assurance Measures Rationale for TOE Assurance Requirements

EAL2 augmented with ALC_FLR.2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2 augmented with ALC_FLR.2, the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment. The assurance claim is consistent to meet the requirements of a Basic Robustness TOE environment.

Table 31 provides an EAL2 dependency analysis.

Table 31 EAL2 SAR Dependencies

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
ADV_ARC.1	Security architecture description	ADV_FSP.1 ADV_TDS.1	Yes
ADV_FSP.2	Security-enforcing functional specification	None	N/A
ADV_TDS.1	Basic design	ADV_FSP.2	Yes
AGD_OPE.1	Operational user guidance	ADV_FSP.1	Yes
AGD_PRE.1	Preparative procedures	None	N/A
ALC_CMC.2	Use of a CM system	ALC_CMS.1	Yes
ALC_CMS.2	Parts of the TOE CM coverage	None	N/A
ALC_DEL.1	Delivery procedures	None	N/A
ALC_FLR.2	Flaw reporting procedures	None	N/A
ATE_COV.1	Evidence of coverage	ADV_FSP.2, ATE_FUN.1	Yes
ATE_FUN.1	Functional testing	ATE_COV.1	Yes

Table 31 EAL2 SAR Dependencies (continued)

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
ATE_IND.2	Independent testing-sample	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	Yes
AVA_VAN.2	Vulnerability analysis	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1	Yes

Annex A: Cisco NAC Agent System Requirements

Table 32 lists the minimum agent and NAC Manager (aka CAM) and Server (aka CAS) versions recommended to install and authenticate with the Clean Access Agent on client systems.

Table 32 Clean Access Agent System Requirements

Supported OS	Windows XP Professional, Windows XP Home, Windows 2000, Windows 98, Windows SE, Windows ME
	Windows XP Media Center Edition, Windows XP Tablet PC
	Windows Vista Home, Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise[7]
	Japanese Windows XP Professional SP2, Japanese Windows 2000 Professional SP4 [8, 9]
	Japanese Windows Vista Home, Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise [8, 9]
	Windows XP SP2 with Simplified Chinese
	Mac OS X (10.2, 10.3, 10.4)
	64-bit Windows OS (Authentication-only)[10] Windows XP Professional x64, Windows Vista Home Basic x64, Windows Vista Home Premium x64, Windows Vista Business x64, Windows Vista Ultimate x64, Windows Vista Enterprise x64
Supported Language Templates [11]	German, Italian, Finnish, Czech, Norwegian, Spanish, Danish, French, Russian, Swedish, Turkish, Serbian, and Catalan
Supported OS Locales	English, International English, French, Italian, German, Spanish, Norwegian, Swedish
Supported Browsers	Internet Explorer 6.0 Internet Explorer 7.0
Required Hard Drive Space	Minimum of 10 MB of free hard drive space
Required Hardware	No minimum hardware requirements (works on various client machines)

7 For checks/rules/requirements, the Agent can detect "N" (European) versions of the Windows Vista operating system, but the CAM/CAS treat "N" versions of Vista as their US counterpart.

8 For Japanese Windows OS, Windows user names must be ASCII.

9 For Japanese Windows OS, only ASCII characters are supported for rules/checks.

10 The Clean Access Agent only supports authentication/posture assessment/remediation on 32-bit operating systems. Any client operating system that is not listed is not supported, even if the Agent can be installed on the client (e.g. Embedded XP is not supported).

11 The Agent picks the correct language template based on the local computer Locale (under Control Panel > Regional and Language Options). Cisco recommends using the localized Agent in the localized version of Windows (e.g. Russian Agent in Russian Windows). Agent language template support only controls what the viewer sees after the Agent is installed; it does not include support for different client operating systems for the Agent Installer or for AV/AS products.

Annex B: Supported AV and AS Vendors

Clean Access AV Support Chart (Windows Vista/XP/2000)

Table 33 lists Windows Vista/XP/2000 Supported AV Products as of the latest release of the Cisco NAC Appliance software. (See Table 34 for Windows ME/98).

Table 33 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)

Product Name	Product Version	Live Update[12]
AEC, spol. s r.o.		
TrustPort Antivirus	2.x	yes
AhnLab, Inc.		
AhnLab Security Pack	2.x	yes
AhnLab V3 Internet Security 2007 Platinum	7.x	yes
AhnLab V3 Internet Security 7.0 Platinum Enterprise	7.x	yes
V3Pro 2004	6.x	yes
V3 VirusBlock 2005	6.x	-
ALWIL Software		
avast! Antivirus	4.x	yes
avast! Antivirus (managed)	4.x	yes
avast! Antivirus Professional	4.x	yes
America Online, Inc.		
Active Virus Shield	6.x	yes
AOL Safety and Security Center Virus Protection	102.x	-
AOL Safety and Security Center Virus Protection	1.x	-
AOL Safety and Security Center Virus Protection	210.x	-
AOL Safety and Security Center Virus Protection	2.x	-
Authentium, Inc.		
Command Anti-Virus Enterprise	4.x	yes
Command AntiVirus for Windows	4.x	yes
Command AntiVirus for Windows Enterprise	4.x	yes
Cox High Speed Internet Security Suite	3.x	yes
Avira GmbH		
Avira AntiVir Windows Workstation	7.x	yes
Avira Premium Security Suite	7.x	yes
Beijing Rising Technology Corp. Ltd.		
Rising Antivirus Software AV	17.x	yes
Rising Antivirus Software AV	18.x	yes
Rising Antivirus Software AV	19.x	yes
BellSouth		
BellSouth Internet Security Anti-Virus	5.x	-
BullGuard Ltd.		
BullGuard 7.0	7.x	-
Check Point, Inc		
ZoneAlarm Anti-virus	7.x	yes
ZoneAlarm (AntiVirus)	7.x	yes
ZoneAlarm Security Suite Antivirus	7.x	yes
ClamAV		
ClamAV	devel-x	yes
ClamWin		
ClamWin Antivirus	0.x	yes
ClamWin Free Antivirus	0.x	yes
Computer Associates International, Inc.		

Table 33 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) (continued)

Product Name	Product Version	Live Update[12]
CA Anti-Virus	8.x	yes
CA eTrust Antivirus	7.x	yes
CA eTrust Internet Security Suite AntiVirus	7.x	yes
CA eTrustITM Agent	8.x	yes
eTrust EZ Antivirus	6.1.x	yes
eTrust EZ Antivirus	6.2.x	yes
eTrust EZ Antivirus	6.4.x	yes
eTrust EZ Antivirus	7.x	yes
eTrust EZ Armor	6.1.x	yes
eTrust EZ Armor	6.2.x	yes
eTrust EZ Armor	7.x	yes
Defender Pro LLC		
Defender Pro Anti-Virus	5.x	yes
EarthLink, Inc.		
Aluria Security Center AntiVirus	1.x	-
EarthLink Protection Control Center AntiVirus	1.x	-
EarthLink Protection Control Center AntiVirus	2.x	-
eEye Digital Security		
eEye Digital Security Blink Personal	3.x	yes
eEye Digital Security Blink Professional	3.x	-
Eset Software		
NOD32 antivirus system	2.x	yes
Fortinet Inc.		
FortiClient Consumer Edition	3.x	yes
Frisk Software International		
F-PROT Antivirus for Windows	6.0.x	-
F-Prot for Windows	3.14e	yes
F-Prot for Windows	3.15	yes
F-Prot for Windows	3.16c	yes
F-Prot for Windows	3.16d	yes
F-Prot for Windows	3.16x	yes
F-Secure Corp.		
F-Secure Anti-Virus	5.x	yes
F-Secure Anti-Virus	6.x	yes
F-Secure Anti-Virus	7.x	-
F-Secure Anti-Virus 2005	5.x	yes
F-Secure Anti-Virus Client Security	6.x	yes
F-Secure Internet Security	6.x	yes
F-Secure Internet Security	7.x	-
F-Secure Internet Security 2006 Beta	6.x	yes
GData Software AG		
AntiVirusKit 2006	2006.x	-
Grisoft, Inc.		
Antivirussystem AVG 6.0	6.x	-
AVG 6.0 Anti-Virus - FREE Edition	6.x	-
AVG 6.0 Anti-Virus System	6.x	-
AVG 7.5	7.x	yes
AVG Antivirensystem 7.0	7.x	yes
AVG Anti-Virus 7.0	7.x	yes
AVG Anti-Virus 7.1	7.1.x	yes
AVG Free Edition	7.x	yes
HAURI, Inc.		
ViRobot Desktop	5.0.x	-
H+BEDV Datentechnik GmbH		
AntiVir PersonalEdition Classic Windows	7.x	yes

Table 33 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) (continued)

Product Name	Product Version	Live Update[12]
AntiVir/XP	6.x	yes
Avira AntiVir PersonalEdition Premium	7.x	yes
IKARUS Software GmbH		
IKARUS Guard NT	2.x	-
IKARUS virus utilities	5.x	-
Internet Security Systems, Inc.		
Proventia Desktop	8.x	-
Proventia Desktop	9.x	-
Kaspersky Labs		
Kaspersky Anti-Virus 2006 Beta	6.0.x	-
Kaspersky Anti-Virus 6.0	6.x	yes
Kaspersky Anti-Virus 6.0 Beta	6.x	yes
Kaspersky Anti-Virus for Windows File Servers	5.x	yes
Kaspersky Anti-Virus for Windows Workstations	5.0.x	yes
Kaspersky Anti-Virus for Windows Workstations	6.x	yes
Kaspersky Anti-Virus for Workstation	5.0.x	yes
Kaspersky Anti-Virus Personal	4.5.x	yes
Kaspersky Anti-Virus Personal	5.0.x	yes
Kaspersky Anti-Virus Personal Pro	5.0.x	yes
Kaspersky Internet Security	6.x	yes
Kaspersky(TM) Anti-Virus Personal 4.5	4.5.x	yes
Kaspersky(TM) Anti-Virus Personal Pro 4.5	4.5.x	yes
Kingsoft Corp.		
Kingsoft AntiVirus 2004	2004.x	yes
Kingsoft Internet Security	7.x	yes
Kingsoft Internet Security 2006 +	2006.x	yes
McAfee, Inc.		
McAfee Internet Security 6.0	8.x	yes
McAfee Managed VirusScan	3.x	yes
McAfee Managed VirusScan	4.x	yes
McAfee VirusScan	10.x	yes
McAfee VirusScan	11.x	yes
McAfee VirusScan	4.5.x	yes
McAfee VirusScan	8.x	yes
McAfee VirusScan	8xxx	yes
McAfee VirusScan	9.x	yes
McAfee VirusScan	9xxx	yes
McAfee VirusScan Enterprise	7.0.x	yes
McAfee VirusScan Enterprise	7.1.x	yes
McAfee VirusScan Enterprise	7.5.x	yes
McAfee VirusScan Enterprise	8.0.x	yes
McAfee VirusScan Enterprise	8.x	yes
McAfee VirusScan Home Edition	7.x	yes
McAfee VirusScan Professional	8.x	yes
McAfee VirusScan Professional	8xxx	yes
McAfee VirusScan Professional	9.x	yes
McAfee VirusScan Professional Edition	7.x	yes
Total Protection for Small Business	4.x	yes
Microsoft Corp.		
Microsoft Forefront Client Security	1.5.x	-
Windows Live OneCare	1.x	-
Windows OneCare Live	0.8.x	-
MicroWorld		
eScan Anti-Virus (AV) for Windows	8.x	yes
eScan Corporate for Windows	8.x	yes

Table 33 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) (continued)

Product Name	Product Version	Live Update[12]
eScan Internet Security for Windows	8.x	yes
eScan Professional for Windows	8.x	yes
eScan Virus Control (VC) for Windows	8.x	yes
Norman ASA		
Norman Virus Control	5.x	yes
Panda Software		
Panda Antivirus 2007	2.x	-
Panda Antivirus 2008	3.x	-
Panda Antivirus 6.0 Platinum	6	yes
Panda Antivirus + Firewall 2007	6.x	yes
Panda Antivirus Lite	1.x	-
Panda Antivirus Lite	3.x	-
Panda Antivirus Platinum	7.04.x	yes
Panda Antivirus Platinum	7.05.x	yes
Panda Antivirus Platinum	7.06.x	yes
Panda Client Shield	4.x	-
Panda Internet Security 2007	11.x	yes
Panda Internet Security 2008	12.x	yes
Panda Platinum 2005 Internet Security	9.x	yes
Panda Platinum 2006 Internet Security	10.x	yes
Panda Platinum Internet Security	8.03.x	yes
Panda Titanium 2006 Antivirus + Antispyware	5.x	yes
Panda Titanium Antivirus 2004	3.00.00	yes
Panda Titanium Antivirus 2004	3.01.x	yes
Panda Titanium Antivirus 2004	3.02.x	yes
Panda Titanium Antivirus 2005	4.x	yes
Panda TruPrevent Personal 2005	2.x	yes
Panda TruPrevent Personal 2006	3.x	yes
WebAdmin Client Antivirus	3.x	-
Radialpoint Inc.		
Radialpoint Virus Protection	5.x	-
Zero-Knowledge Systems Radialpoint Security Services Virus Protection	6.x	yes
SalD Ltd.		
Dr.Web	4.32.x	yes
Dr.Web	4.33.x	yes
Sereniti, Inc.		
Sereniti Antivirus	1.x	yes
The River Home Network Security Suite	1.x	yes
SOFTWIN		
BitDefender 8 Free Edition	8.x	-
BitDefender 8 Professional Plus	8.x	-
BitDefender 8 Standard	8.x	-
BitDefender 9 Internet Security AntiVirus	9.x	-
BitDefender 9 Professional Plus	9.x	yes
BitDefender 9 Standard	9.x	yes
BitDefender Antivirus Plus v10	10.x	yes
BitDefender Antivirus v10	10.x	yes
BitDefender Free Edition	7.x	-
BitDefender Internet Security v10	10.x	yes
BitDefender Professional Edition	7.x	-
BitDefender Standard Edition	7.x	-
Sophos Plc.		
Sophos Anti-Virus	3.x	-
Sophos Anti-Virus	4.x	-
Sophos Anti-Virus	5.x	yes

Table 33 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) (continued)

Product Name	Product Version	Live Update[12]
Sophos Anti-Virus	6.x	yes
Sophos Anti-Virus	7.x	yes
Sophos Anti-Virus version 3.80	3.8	-
Symantec Corp.		
Norton 360 (Symantec Corporation)	1.x	yes
Norton AntiVirus	10.x	yes
Norton AntiVirus	14.x	yes
Norton AntiVirus	15.x	yes
Norton AntiVirus 2002	8.00.x	yes
Norton AntiVirus 2002	8.x	yes
Norton AntiVirus 2002 Professional	8.x	yes
Norton AntiVirus 2002 Professional Edition	8.x	yes
Norton AntiVirus 2003	9.x	yes
Norton AntiVirus 2003 Professional	9.x	yes
Norton AntiVirus 2003 Professional Edition	9.x	yes
Norton AntiVirus 2004	10.x	yes
Norton AntiVirus 2004 Professional	10.x	yes
Norton AntiVirus 2004 Professional Edition	10.x	yes
Norton AntiVirus 2004 (Symantec Corporation)	10.x	yes
Norton AntiVirus 2005	11.0.x	yes
Norton AntiVirus 2006	12.0.x	yes
Norton AntiVirus 2006	12.x	yes
Norton AntiVirus Corporate Edition	7.x	yes
Norton Internet Security	7.x	yes
Norton Internet Security	8.0.x	yes
Norton Internet Security	8.2.x	yes
Norton Internet Security	8.x	yes
Norton Internet Security	9.x	yes
Norton Internet Security (Symantec Corporation)	10.x	yes
Norton SystemWorks 2003	6.x	yes
Norton SystemWorks 2004 Professional	7.x	yes
Norton SystemWorks 2005	8.x	yes
Norton SystemWorks 2005 Premier	8.x	yes
Norton SystemWorks 2006 Premier	12.0.x	yes
Symantec AntiVirus	10.x	yes
Symantec AntiVirus	9.x	yes
Symantec AntiVirus Client	8.x	yes
Symantec AntiVirus Server	8.x	yes
Symantec AntiVirus Win64	10.x	yes
Symantec Client Security	10.x	yes
Symantec Client Security	9.x	yes
Symantec Endpoint Protection	11.x	yes
Symantec Scan Engine	5.x	-
Trend Micro, Inc.		
PC-cillin 2002	9.x	-
PC-cillin 2003	10.x	-
ServerProtect	5.x	-
Trend Micro Antivirus	11.x	yes
Trend Micro AntiVirus	15.x	-
Trend Micro Client/Server Security	6.x	yes
Trend Micro Client/Server Security Agent	7.x	yes
Trend Micro HouseCall	1.x	-
Trend Micro Internet Security	11.x	yes
Trend Micro Internet Security	12.x	-
Trend Micro OfficeScan Client	5.x	yes

Table 33 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) (continued)

Product Name	Product Version	Live Update[12]
Trend Micro OfficeScan Client	6.x	yes
Trend Micro OfficeScan Client	7.x	yes
Trend Micro OfficeScan Client	8.x	yes
Trend Micro PC-cillin 2004	11.x	yes
Trend Micro PC-cillin Internet Security 12	12.x	-
Trend Micro PC-cillin Internet Security 14	14.x	yes
Trend Micro PC-cillin Internet Security 2005	12.x	yes
Trend Micro PC-cillin Internet Security 2006	14.x	yes
Trend Micro PC-cillin Internet Security 2007	15.x	yes
VCOM		
Fix-It Utilities 7 Professional [AntiVirus]	7.x	yes
SystemSuite 7 Professional [AntiVirus]	7.x	yes
VCOM Fix-It Utilities Professional 6 [AntiVirus]	6.x	yes
Verizon		
Verizon Internet Security Suite Anti-Virus	5.x	-
Yahoo!, Inc.		
AT&T Yahoo! Online Protection [AntiVirus]	7.x	yes
SBC Yahoo! Anti-Virus	7.x	yes
Verizon Yahoo! Online Protection [AntiVirus]	7.x	yes
Zone Labs LLC		
ZoneAlarm Anti-virus	6.x	-
ZoneAlarm Security Suite	5.x	-
ZoneAlarm Security Suite	6.x	-
ZoneAlarm with Antivirus	5.x	-

12 The Live Update column indicates whether the Agent supports live update for the product via the Agent Update button (configured by AV Definition Update requirement type). For products that support "Live Update," the Agent launches the update mechanism of the AV product when the Update button is clicked. For products that do not support this feature, the Agent displays a message popup. In this case, administrators can configure a different requirement type (such as "Local Check") to present alternate update instructions to the user.

For Symantec Enterprise products, the Clean Access Agent can initiate AV Update when Symantec Antivirus is in unmanaged mode. If using Symantec AV in managed mode, the administrator must allow/deny managed clients to run LiveUpdate via the Symantec management console (right-click the primary server, go to All Tasks -> Symantec Antivirus, select Definition Manager, and configure the policy to allow clients to launch LiveUpdate for agents managed by that management server.) If managed clients are not allowed to run LiveUpdate, the update button will be disabled on the Symantec GUI on the client, and updates can only be pushed from the server.

Clean Access AV Support Chart (Windows ME/98)

Table 34 lists Windows ME/98 Supported AV Products as of the latest release of the Cisco NAC Appliance software. (SeeTable 33 for Windows Vista/XP/2000.)

Table 34 Clean Access Antivirus Product Support Chart (Windows ME/98)

Product Name	Product Version	Live Update[13]
Beijing Rising Technology Corp. Ltd.		
Rising Antivirus Software AV	18.x	yes
Computer Associates International, Inc.		
CA eTrust Antivirus	7.x	yes

Table 34 Clean Access Antivirus Product Support Chart (Windows ME/98) (continued)

Product Name	Product Version	Live Update[13]
eTrust EZ Antivirus	6.1.x	yes
eTrust EZ Antivirus	6.2.x	yes
eTrust EZ Antivirus	6.4.x	yes
eTrust EZ Antivirus	7.x	yes
eTrust EZ Armor	6.1.x	yes
McAfee, Inc.		
McAfee Managed VirusScan	3.x	yes
McAfee VirusScan	10.x	yes
McAfee VirusScan	4.5.x	yes
McAfee VirusScan	8.x	yes
McAfee VirusScan	9.x	yes
McAfee VirusScan Professional	8.x	yes
McAfee VirusScan Professional	8xxx	yes
McAfee VirusScan Professional	9.x	yes
McAfee VirusScan Professional Edition	7.x	yes
SOFTWIN		
BitDefender 8 Free Edition	8.x	-
BitDefender 8 Professional Plus	8.x	-
BitDefender 8 Standard	8.x	-
BitDefender 9 Professional Plus	9.x	-
BitDefender 9 Standard	9.x	-
BitDefender Free Edition	7.x	-
BitDefender Professional Edition	7.x	-
BitDefender Standard Edition	7.x	-
Symantec Corp.		
Norton AntiVirus	10.x	yes
Norton AntiVirus 2002	8.00.x	yes
Norton AntiVirus 2002	8.x	yes
Norton AntiVirus 2003	9.x	yes
Norton AntiVirus 2003 Professional Edition	9.x	yes
Norton AntiVirus 2004	10.x	yes
Norton AntiVirus 2004 (Symantec Corporation)	10.x	yes
Norton AntiVirus 2005	11.0.x	yes
Norton Internet Security	8.0.x	yes
Norton Internet Security	8.x	yes
Symantec AntiVirus	10.x	yes
Symantec AntiVirus	9.x	yes
Symantec AntiVirus Client	8.x	yes
Trend Micro, Inc.		
PC-cillin 2003	10.x	-
Trend Micro Internet Security	11.x	-
Trend Micro Internet Security	12.x	-
Trend Micro OfficeScan Client	7.x	-
Trend Micro PC-cillin 2004	11.x	-
Trend Micro PC-cillin Internet Security 2005	12.x	-

13 The Live Update column indicates whether the Agent supports live update for the product via the Agent Update button (configured by AV Definition Update requirement type). For products that support "Live Update," the Agent launches the update mechanism of the AV product when the Update button is clicked. For products that do not support this feature, the Agent displays a message popup. In this case, administrators can configure a different requirement type (such as "Local Check") to present alternate update instructions to the user.

For Symantec Enterprise products, the Clean Access Agent can initiate AV Update when Symantec Antivirus is in unmanaged mode. If using Symantec AV in managed mode, the administrator must allow/deny managed clients to run LiveUpdate via the Symantec management console (right-click the primary server, go to All Tasks -> Symantec

Antivirus, select Definition Manager, and configure the policy to allow clients to launch LiveUpdate for agents managed by that management server.) If managed clients are not allowed to run LiveUpdate, the update button will be disabled on the Symantec GUI on the client, and updates can only be pushed from the server.

Clean Access AS Support Chart Clean Access AS Support Chart (Windows Vista/XP/2000)

Table 35 lists Windows Vista/XP/2000 Supported Antispyware Products as of the latest release of the Cisco Clean Access software.

Table 35 Clean Access Antispyware Product Support Chart (Windows Vista//2000)

Product Name	Product Version	Live Update[14]
AhnLab, Inc.		
AhnLab SpyZero 2.0	2.x	yes
AhnLab SpyZero 2007	3.x	yes
AhnLab V3 Internet Security 2007 Platinum AntiSpyware	7.x	yes
AhnLab V3 Internet Security 7.0 Platinum Enterprise AntiSpyware	7.x	yes
America Online, Inc.		
AOL Safety and Security Center Spyware Protection	2.0.x	-
AOL Safety and Security Center Spyware Protection	2.1.x	-
AOL Safety and Security Center Spyware Protection	2.2.x	-
AOL Safety and Security Center Spyware Protection	2.3.x	-
AOL Safety and Security Center Spyware Protection	2.x	-
AOL Spyware Protection	1.x	-
AOL Spyware Protection	2.x	-
Anonymizer, Inc.		
Anonymizer Anti-Spyware	1.x	-
Anonymizer Anti-Spyware	3.x	-
Authentium, Inc.		
Cox High Speed Internet Security Suite	3.x	yes
BellSouth		
BellSouth Internet Security Anti-Spyware	5.x	-
Bullet Proof Soft		
BPS Spyware & Adware Remover	9.x	yes
BPS Spyware-Adware Remover	8.x	yes
BPS Spyware Remover	9.x	yes
Check Point, Inc.		
ZoneAlarm (AntiSpyware)	7.x	yes
ZoneAlarm Anti-Spyware	7.x	yes
ZoneAlarm Pro Antispyware	7.x	yes
ZoneAlarm Security Suite Antispyware	7.x	yes
Computer Associates International, Inc.		
CA eTrust Internet Security Suite AntiSpyware	5.x	yes
CA eTrust Internet Security Suite AntiSpyware	8.x	yes
CA eTrust Internet Security Suite AntiSpyware	9.x	yes
CA eTrust PestPatrol	5.x	yes
CA eTrust PestPatrol Anti-Spyware	8.x	yes
CA eTrust PestPatrol Anti-Spyware Corporate Edition	5.x	yes
PestPatrol Corporate Edition	4.x	yes
PestPatrol Standard Edition (Evaluation)	4.x	yes
EarthLink, Inc.		
Aluria Security Center AntiSpyware	1.x	-
EarthLink Protection Control Center AntiSpyware	1.x	-
EarthLink Protection Control Center AntiSpyware	2.x	-
Primary Response SafeConnect	2.x	-
FaceTime Communications, Inc.		
X-Cleaner Deluxe	4.x	yes

Table 35 Clean Access Antispyware Product Support Chart (Windows Vista//2000) (continued)

Product Name	Product Version	Live Update[14]
Grisoft, Inc.		
AVG Anti-Malware [AntiSpyware]	7.x	-
AVG Anti-Spyware 7.5	7.x	-
Javacool Software LLC		
SpywareBlaster v3.1	3.1.x	yes
SpywareBlaster v3.2	3.2.x	yes
SpywareBlaster v3.3	3.3.x	yes
SpywareBlaster v3.4	3.4.x	yes
SpywareBlaster v3.5.1	3.5.x	yes
Kingsoft Corp.		
Kingsoft Internet Security [AntiSpyware]	7.x	yes
Lavasoft, Inc.		
Ad-Aware 2007 Professional	7.x	yes
Ad-aware 6 Professional	6.x	-
Ad-Aware SE Personal	1.x	-
Ad-Aware SE Professional	1.x	yes
McAfee, Inc.		
McAfee AntiSpyware	1.5.x	yes
McAfee AntiSpyware	1.x	yes
McAfee AntiSpyware	2.x	yes
McAfee AntiSpyware Enterprise	8.x	yes
McAfee Anti-Spyware Enterprise Module	8.0.x	yes
McAfee VirusScan AS	11.x	yes
MicroSmarts LLC		
Spyware Begone	4.x	-
Spyware Begone	6.x	-
Spyware Begone	8.x	-
Spyware Begone Free Scan	7.x	-
Spyware Begone V7.30	7.30.x	-
Spyware Begone V7.40	7.40.x	-
Spyware Begone V7.95	7.95.x	-
Spyware Begone V8.20	8.20.x	-
Spyware Begone V8.25	8.25.x	-
Microsoft Corp.		
Microsoft AntiSpyware	1.x	yes
Windows Defender	1.x	yes
Windows Defender Vista	1.x	yes
PC Tools Software		
Spyware Doctor	4.x	yes
Spyware Doctor	5.x	yes
Spyware Doctor 3.0	3.x	yes
Spyware Doctor 3.1	3.x	yes
Spyware Doctor 3.2	3.x	yes
Spyware Doctor 3.5	3.x	yes
Spyware Doctor 3.8	3.x	yes
Prevx Ltd.		
Prevx1	1.x	yes
Prevx1	2.x	yes
Prevx Home	2.x	-
Radialpoint Inc.		
Radialpoint Spyware Protection	5.x	-
Zero-Knowledge Systems Radialpoint Security Services Spyware Protection	6.x	yes
Safer Networking Ltd.		
Spybot - Search & Destroy 1.3	1.3	yes
Spybot - Search & Destroy 1.4	1.4	yes

Table 35 Clean Access Antispyware Product Support Chart (Windows Vista//2000) (continued)

Product Name	Product Version	Live Update[14]
Spybot - Search & Destroy 1.5	1.x	-
Sereniti, Inc.		
Sereniti Antispyware	1.x	yes
The River Home Network Security Suite Antispyware	1.x	yes
SOFTWIN		
BitDefender 9 Antispyware	9.x	-
Sunbelt Software		
CounterSpy Enterprise Agent	1.8.x	-
Sunbelt CounterSpy	1.x	yes
Sunbelt CounterSpy	2.x	yes
Symantec Corp.		
Norton Spyware Scan	2.x	-
Trend Micro, Inc.		
Trend Micro Anti-Spyware	3.5.x	-
Trend Micro Anti-Spyware	3.x	-
Trend Micro PC-cillin Internet Security 2007 AntiSpyware	15.x	yes
VCOM		
Fix-It Utilities 7 Professional [AntiSpyware]	7.x	yes
SystemSuite 7 Professional [AntiSpyware]	7.x	yes
VCOM Fix-It Utilities Professional 6 [AntiSpyware]	6.x	yes
Verizon		
Verizon Internet Security Suite Anti-Spyware	5.x	-
Webroot Software, Inc.		
Spy Sweeper	3.x	-
Spy Sweeper	4.x	-
Spy Sweeper	5.x	-
Webroot Spy Sweeper Enterprise Client	1.x	-
Webroot Spy Sweeper Enterprise Client	2.x	-
Webroot Spy Sweeper Enterprise Client	3.x	-
Yahoo!, Inc.		
AT&T Yahoo! Online Protection	2006.x	yes
SBC Yahoo! Applications	2005.x	yes
Verizon Yahoo! Online Protection	2005.x	yes
Yahoo! Anti-Spy	1.x	-
Zone Labs LLC		
Integrity Agent	6.x	-

14 The Live Update column indicates whether the Agent supports live update for the product via the Agent Update button (configured by AV Definition Update requirement type). For products that support "Live Update," the Agent launches the update mechanism of the AV product when the Update button is clicked. For products that do not support this feature, the Agent displays a message popup. In this case, administrators can configure a different requirement type (such as "Local Check") to present alternate update instructions to the user.

For Symantec Enterprise products, the Clean Access Agent can initiate AV Update when Symantec Antivirus is in unmanaged mode. If using Symantec AV in managed mode, the administrator must allow/deny managed clients to run LiveUpdate via the Symantec management console (right-click the primary server, go to All Tasks -> Symantec Antivirus, select Definition Manager, and configure the policy to allow clients to launch LiveUpdate for agents managed by that management server.) If managed clients are not allowed to run LiveUpdate, the update button will be disabled on the Symantec GUI on the client, and updates can only be pushed from the server.

Annex C: References and Acronyms

References

The following documentation was used to prepare this ST:

Table 36 References

[CC_PART1]	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
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2007, version 3.1, Revision 2, CCMB--2007-09-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2007, version 3.1, Revision 2, CCMB-2007-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2007, version 3.1, Revision 2, CCMB-2007-09-004
[AIDSPP]	U.S. Government Protection Profile Intrusion Detection System Analyzer for Basic Robustness Environments, Version 1.3, dated July 25, 2007
Cisco NAC Appliance text	*Cisco NAC Appliance: Enforcing Host Security with Clean Access*, by James Heary. Cisco Press, 2008.

Acronyms and Abbreviations

The following acronyms and abbreviations are used in this Security Target:

Table 37 Acronyms and Abbreviations

Acronyms/ Abbreviations	Definition
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
EAL	Evaluation Assurance Level
HLD	High Level Design
HTTPS	Hyper-Text Transport Protocol Secure
IT	Information Technology
NAC	Network Admission Control
OS	Operating System
PP	Protection Profile
SNMP	Simple Network Management Protocol
SSH	Secure Shell

Table 37 Acronyms and Abbreviations (continued)

Acronyms/ Abbreviations	Definition
SSL	Secure Socket Layer
ST	Security Target
TCP	Transport Control Protocol
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html