THE TOLLY GROUP

No. 208302 SEPTEMBER 2008

TOLLY Up to Spec CERTIFIED

Test Summary

Nortel

Secure Network Access Solution

Validation of Open and Flexible Network Access Control Features, Enterprise Performance, Scalability and Redundancy

Premise: Nortel's Secure Network Access (SNA) solution provides a rich set of features and functionality that delivers enterprise-class, solutions-oriented network access control for Nortel and third-party Ethernet switching environments. Nortel's NAC offering not only supports Windows, Linux, and Mac operating systems but also integrates into IP Telephony environments while supporting industry standards like 802.1X and Microsoft NAP. Nortel's solution scales to more than 23,000 concurrently connected devices and also supports enterprises' green initiatives by demonstrating efficient energy consumption.

Nortel commissioned The Tolly Group to evaluate its Secure Network Access (SNA) Solution, which controls and automates network access for both managed and unmanaged users and devices.

Tolly Group engineers examined two models: the Nortel Secure Network Access Switch (SNAS) 4050 and 4070. Engineers validated an assortment of key network access control features and functions, as well as verified scalability capabilities of the device and energy consumption.

Tests were conducted in August 2008.

Test Highlights

- Delivers deployment flexibility by supporting multiple NAC enforcement protocols including 802.1X, DHCP, Nortel SSCP, and SSCP-Lite (SNMP)
- Provides investment protection by supporting a broad range of Ethernet switches including Nortel, Cisco, and HP
- Allows users to benefit from joint Nortel SNA/Microsoft NAP integration before upgrading to Windows Server 2008
- Scales to more than 23,000 concurrently connected simulated devices and more than 2,000 simulated enforcement points
- Supports a broad range of devices including Windows, Linux, Mac PCs, IP phones, and printers

Nortel Secure Network Access Control Verified Features/Functions

Characteristics	Audited
Microsoft Network Access Protection (NAP) integration on both client and server levels	✓
Authentication support for all user types including guests, contractors and employees via Captive Portal and Installed Agent	✓
Support for devices throughout the enterprise including Windows, Linux, Mac, IP phones and printers	✓
Rich health assessment (Verifies that devices conform to security policies)	✓
Post admission control (Network behavior anomaly detection) via integration with IDS/IPS	✓
Resiliency (User sessions are maintained even during an outage of the primary SNAS appliance)	✓

Source: The Tolly Group, August 2008

Figure 1

Executive Summary

Nortel's Secure Network Access Solution delivers a rich set of features to provide network access to Windows, Linux, Mac PCs and other devices, and supports major standards, such as Microsoft NAP, Trusted Computing Group and 802.1X, while also providing a solution that scales to more than 23,000 devices, and demonstrates efficient energy usage.

Tests show that Nortel's Secure Network Access Solution delivers enormous flexibility — in terms of its support for clients, access methods, enforcement modes, and devices.

Nortel's SNA platform combines a degree of flexibility, along with robustness of features and functions, that is unique among NAC offerings tested by The Tolly Group. SNAS appliances can scale from 3,000 users supported by a single device, to almost 8X that number with multiple appliances clustered.

Compared to a Cisco NAC solution, the SNAS used 63% less energy during hands-on tests.

Nortel has integrated support for Microsoft's Network Access Protection (NAP) creating a unified network access control solution supporting Windows NAP endpoints and non-NAP endpoints including: Macintosh, Linux, IP phones and other non-interactive devices like printers.

In effect, Nortel blends a compelling mix of robust features, flexible policy enforcement options, broad scalability, efficient power consumption and standards support to deliver high-end network access.

Results

Enforcement Modes

Tolly Group engineers verified that Nortel's SNAS enforces security policies through 802.1X, SSCP, SSCP-Lite (SNMP) and DHCP.

SNAS Enforcement Mode Definitions

Enforcement protocol	Description	Method of enforcement
802.1X	IEEE NAC standard that provides authentication for devices trying to gain network access. 802.1X is based on the EAP protocol and provides port-based authentication access to a LAN. Supports 802.1X-enabled Ethernet switches from any vendor.	VLAN, ACL
SSCP	Nortel's SNAS-Switch Communication protocol (SSCP) is a purpose-built, TCP-based command/notification protocol that uses SSH encryption for bidirectional communication between the SNAS and Nortel policy enforcement points. SSCP provides full network access controls without requiring any 802.1X components in order to enforce policy. Supports Nortel Ethernet Routing Switches.	VLAN, ACL
SSCP-Lite (SNMP)	Nortel's enforcement and notification method for controlling third-party policy enforcement points. SSCP-Lite uses standards-based communications methods such as SNMP (v1/2c/3) and direct CLI interaction (telnet/SSH) in concert to mimic the policy enforcement capabilities of SSCP. Supports Nortel and third-party switches including Cisco and HP.	VLAN
DHCP	A DHCP server onboard the SNAS enforces policy on a host by directly controlling the host's IP configuration. These DHCP enforcement techniques require no interaction between the SNAS and network devices, allowing it to work with all switches/hubs	IP, ACL

Source: The Tolly Group, August 2008

Figure 2

(For a more detailed understanding of the Nortel SNA enforcement modes, see Figure 2.)

Support for the four enforcement modes means that SNAS can support all Nortel and third-party network infrastructures including Cisco and HP, providing enterprises with the flexibility they need to integrate existing switches with SNAS appliances.

Additionally, the flexibility delivered by the SNAS provides Nortel with an advantage over NAC competitors such as Juniper Networks. In its administration guide for the company's Unified Access Control Release 2.1 NAC offering, Juniper discusses switch communication support for only 802.1X enforcement.

Nortel's support for four different enforcement modes gives users the choice, flexibility and investment protection needed for full-scale NAC deployments.

Scalability

This test focused on benchmarking the ability of the SNAS appliance to be clustered into groups of four, and the resulting increase in the number of devices concurrently supported via continuous health-check monitoring.

Tests show that a single Nortel Secure Network Access Switch 4050 can support 3,000 users for network access. When that same device is clustered into a group of four, the number of users supported surges to 10,920 — an increase of 3.6X. (See Figure 3.)

Engineers also tested a SNAS 4070 and found it supports 6,000 users. Further, when clustered in a group of four units, it supports 23,932 an increase of nearly 4X.

Microsoft NAP Integration

Tolly Group engineers verified that Nortel's SNAS supports integration with Microsoft's NAP framework.

Microsoft's NAP provides a framework of client and server technologies, including APIs, that Nortel has integrated into its Secure Network Access solution. The NAP framework includes three main integration points: System Health Agents (NAP SHA), Quarantine Enforcement Clients (NAP EC), and System Health Validators (NAP SHV). Microsoft's built in NAP SHA includes support for Windows Defender, Windows Update, and Windows Firewall.

The Tolly Group's hands-on examination of Nortel's SNA solution shows that Nortel has taken advantage of and integrated at all three levels:

- the Nortel Health Agent is integrated as a Universal System Health Agent (Nortel SHA) extending NAP to support hundreds of security applications. (Tests validated two applications — one from Symantec Corp and another from Microsoft Corp.)
- the Nortel Health Agent has been integrated as a Quarantine Enforcement Client (Nortel EC) supporting both 802.1X and HTTPS
- the Nortel SNAS includes a System Health Validator (SHV) that verifies the status of NAP health components either locally (on the SNAS) or remotely (by communicating with Windows Server 2008).

Tolly Group engineers attempted logins with different user credentials and health states and demonstrated that Nortel SNAS and Microsoft NAP work together to grant access to authenticated users and compliant devices, while noncompliant devices are sent to a network quarantine area. Network quarantine is enforced through

Nortel

Secure Network Access Solution

Validation of Network Access Features, Scalability and Power Consumption

TOLLY Up to Spec CERTIFIED

Product Specifications

Vendor-supplied information not necessarily verified by The Tolly Group

Secure Network Access Solution

Benefits:

- Deployment flexibility, integration and investment protection
- Automated network access security and availability resulting in improved productivity, business continuity and regulatory compliance
- Reduced costs through a decrease in the number and impact of potential security breaches

Features:

- Unified Access Policy
- Authentication & Device Health Assessment
- Authorization enabling role-based access
- Ongoing Threat Analysis
- Quarantine & Remediation

Nortel Security Portfolio:

Nortel uses a Layered Defense approach to network security, designed to ensure there are no single points of security failure in a network. This is accomplished by using multiple approaches to security enforcement at multiple areas within a network. Nortel's Security Portfolio includes NAC, firewall, VPN and IDS/IPS products to address security needs at the following layers:

- Endpoint security
- Perimeter security
- Secure communications
- Core network security

For more information, contact:

Nortel
URL: www.nortel.com

Scalability of Concurrently Connected Devices for SNAS 4050/4070

SNAS model (# units)	Number of simulated users supported
SNAS 4050 (1)	3,000
SNAS 4050 (4 - Cluster)	10,920
SNAS 4070 (1)	6,000
SNAS 4070 (4 - Cluster)	23,932

Source: The Tolly Group, August 2008

Figure 3

customizable VLANs and/or Access Control Lists (ACLs).

Client integration allows the joint solution to be deployed not only using industry-standard 802.1X, but also with other enforcement protocols including Nortel SSCP and SSCP-Lite (SNMP) enforcement mechanisms. These options provide users with a wider choice and enhanced NAP deployment flexibility.

Tests show that server integration allows NAP to be deployed using the SNAS to validate NAP health information in place of Windows Server 2008. SNAS can also communicate with a remote Windows Server 2008 allowing it to validate the Windows information.

This server integration allows customers to deploy NAP before upgrading their servers to Windows Server 2008 (not an option with NAP alone as Windows Server 2008 is a requirement). Even without Windows Server 2008, the SNAS can support auto remediation for the Windows NAP components including: Windows Firewall, Windows Defender, and Windows Update.

EndPoint Support

Tolly Group engineers verified that SNAS supports Microsoft Windows XP, Windows Vista, Windows 2000, Linux and Apple Macintosh operating systems. In addition, Nortel SNAS supports IP phones (Nortel and third party), and other non-interactive devices such as printers.

Access Methods Supported

In this test, engineers verified that the SNAS appliances offer support for multiple access methods.

First, engineers opened a Web browser and were redirected to a captive portal for clientless operation. Upon first login, the user and device were placed in a “quarantined” VLAN because the device was not compliant with the configured security policies; Engineers enabled required security applications, such as a firewall, and re-authenticated and were subsequently granted network access.

Engineers also tested the Nortel Health Agent desktop version which is a Java Web Start agent used to authenticate the user and perform device health assessments. Tolly Group engineers verified the same tests as performed with the captive portal operation and witnessed successful login without a dependency on a Web browser.

The third option consists of an installed Nortel Health Agent version. Tolly Group engineers verified that this single sign-on option integrated with Windows login provides the same level of security as the other two versions while granting seamless access to the corporate network.

Nortel’s clientless captive portal operation is suited for customers who need to support guests, contractors and consultants without having to install or configure the Nortel Health Agent or an 802.1X supplicant. The installed Nortel Health Agent (or the 802.1X supplicant) on the other hand is suited for customers requiring single sign-on and transparent operation for corporate employees utilizing managed assets.

The Tolly Group also validated Nortel Health Agent operation in 802.1X mode and verified that users who login via the integrated 802.1X supplicant are redirected to a captive Web portal login in the event that the 802.1X authentication fails.

Additionally, engineers validated that in situations where a PC is plugged into a phone in order to access the network, the PC is still required to authenticate via the various login options.

Health Assessment Support

Engineers verified the ability of the Nortel Health Agent to check anti-virus, anti-spam, and firewall applications on devices to ensure they are in compliance with the corporate security policy. *(Note: Nortel claims that its Nortel Health Agent supports hundreds of security applications from over 70 leading vendors including Symantec, McAfee, Sophos, Trend Micro and more. The Tolly Group validated an anti-virus product from Symantec and a software firewall from Microsoft.)*

Tolly Group engineers also validated additional granular security features provided by the Nortel Health Agent including checking for specific files, registry entries and the ability to prevent access if applications considered to be a threat to the organization (such as instant messaging and P2P) are running.

Devices that do not meet the security policy are moved to a quarantined area, while devices that meet policy requirements are granted a specific level access based on the user's role.

Network Behavior Anomaly Detection Integration

Tolly Group engineers verified that the Nortel SNAS has the ability to cooperate with network-based intrusion detection and prevention systems (IDS/IPS) such as Nortel's Threat Protection System and the Sourcefire 3D System, to detect compliant users who attempt to engage in malicious activity. Through this integration, the SNAS can either disconnect these users and devices from the network or restrict network access through network quarantine.

Resiliency

Engineers verified that when a SNAS appliance fails within a cluster, the users and devices do not lose network connectivity as the sessions automatically are migrated to available units in the cluster.

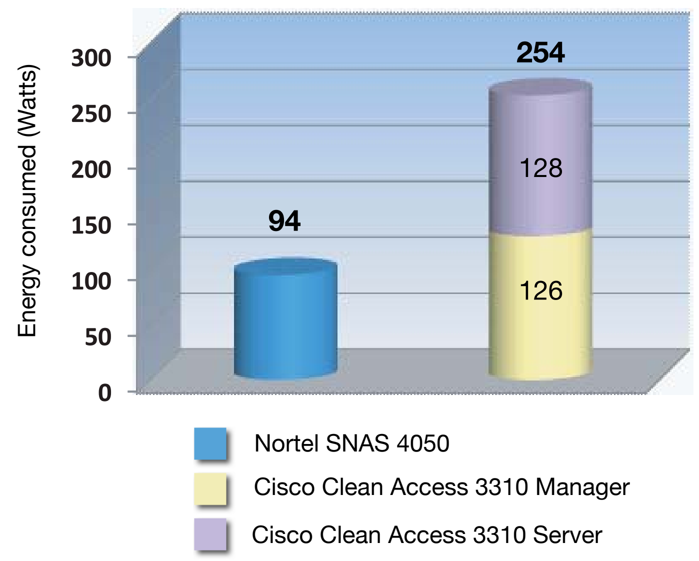
Tests also show that when a remote site loses connectivity to the SNAS controller, with Nortel Ethernet Routing switches, the "fail open" feature provides the option for users to gain a specified level of network access.

Power Consumption

Engineers examined the energy consumed (Watts), between the SNAS 4050 appliance and a Cisco Clean Access (CCA) 3310 Manager and Cisco Clean Access 3310 Server. *(Note: The Cisco solution requires the use of at least one CCA Manager and one CCA Server while the Nortel solution requires one SNAS.)*

The Nortel device used 26% less energy than either of the Cisco 3310 devices tested individually and 63% for the Cisco devices combined — 94 watts versus 254 watts for the Cisco solution.

Nortel SNAS Appliance versus Cisco Clean Access 3310 Power Consumption Analysis



Note: Cisco devices reside on separate hardware devices; measured watts are strictly for appliance, not other ancillary devices required.

Source: The Tolly Group, August 2008

Figure 4

Test Setup & Methodology

Tolly Group engineers verified features on and measured the power consumption of the Nortel Secure Network Access Switch (SNAS) running software 2.0.1. *(For more info on SNAS, visit:* www.nortel.com/nac*)*

For the power consumption tests, engineers measured the energy used by a CCA 3310 Server and CCA 3310 Manager. The tests measured the power consumption of the three appliances at idle mode without any Category 5 cables plugged in. The test was run three times and the results were averaged.

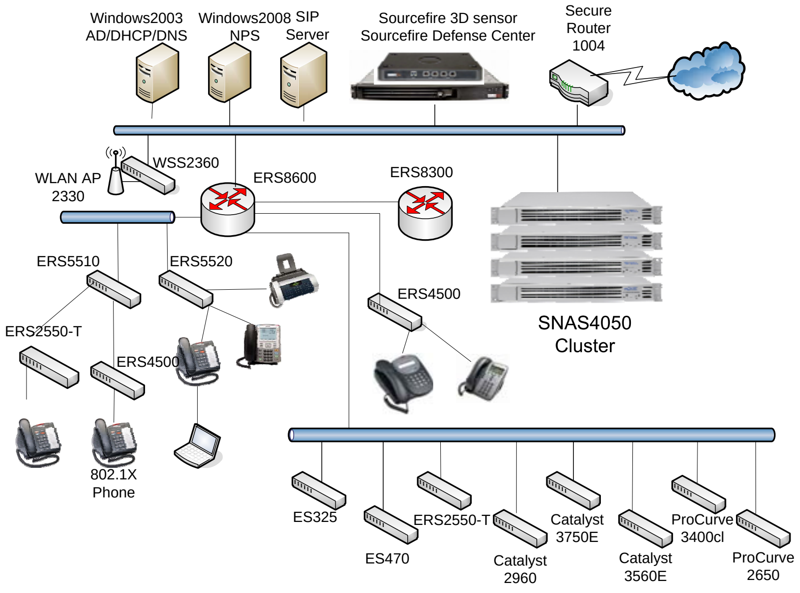
The test bed network was divided into three areas. The first area contained a Secure Network Access Switch, as well as a Network Policy Server on a Windows 2008 server with an Intel Core2 Duo 2.4-GHz processor and 2GB of RAM. The Nortel Threat Protection System Defense Center and Intrusion Sensor with software version 4.6 and the Sourcefire 3D System Defense Center 1000 and 3D2000 with software version 4.7.0.5 were used to test post admission assessment. The Nortel Secure Router 1004 was used to provide Internet access via NAT.

The network Active Directory, DNS and DHCP servers were installed in a Windows 2003 Server environment. This server was configured with an Intel P4 2.8-GHz processor and 512MB of RAM. A Nortel Ethernet Routing Switch 8600 routed traffic to the two other areas.

The second area included three switches: a Nortel Ethernet Routing Switch (ERS) 4500, running software version 5.1.0., an ERS 5520 running software version 5.1.0 and an ERS 5510 running software version 5.0.8. In addition to an HP LaserJet 4050 printer, six IP phones also were deployed: a Cisco IP Phone 7912, Avaya 4602SW, Nortel i1120, i1110, i2002 and i2004.

Engineers configured a series of switches in the third area. The

Test Bed Diagram



Source: The Tolly Group, August 2008

Figure 5

connected third-party switches included an HP2650 running software M.10.50, HP3400cl H.10.41, Catalyst 3560 IOS: 12.2(44) SE2, Catalyst 2960 IOS: 12.2(44) SE2. Nortel switches included the ERS 8300 running software 4.1.0, ERS 2500 running software version 4.2.0, ES470 software version 3.7.2 and the ES325 software version 3.6.2.

Clients were connected to the switches to verify interoperability.

The client configuration consisted of: Windows Vista, running on an Intel Core2 Duo 2.0-GHz CPU with 2GB of RAM; Windows XP SP2 running on an Intel Pentium M 1.6-GHz processor with 512MB of RAM; Windows XP SP3 Intel Pentium III 1.0-GHz CPU with 512MB of RAM and Windows 2000 SP4 Pentium III 1.0-GHz CPU with 1GB of RAM.

The Tolly Group is a leading global provider of third-party validation services for vendors of IT products, components and services.

The company is based in Boca Raton, FL and can be reached by phone at (561) 391-5610, or via the Internet at:

Web: http://www.tolly.com,
E-mail: sales@tolly.com

Terms of Usage

USE THIS DOCUMENT ONLY IF YOU AGREE TO THE TERMS LISTED HEREIN.

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability.

This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental and consequential damages which may result from the use of information contained in this document.

The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers.

When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site.

All trademarks are the property of their respective owners.