Standardizing Network Access Control: TNC and Microsoft NAP to Interoperate

May 2007

Trusted Computing Group 3855 SW 153rd Dr. Beaverton, OR 97006
TEL: (503) 619-0563 FAX: (503) 664-6708
admin@trustedcomputinggroup.org www.trustedcomputinggroup.org

Microsoft Corporation One Microsoft Way Redmond, WA 98072
asknap@microsoft.com www.microsoft.com

Standardizing Network Access Control: TNC and Microsoft NAP to Interoperate

Table of Contents:

Standardizing Network Access Control:
TNC and Microsoft NAP to Interoperate

Two leading network access control standards — TCG's Trusted Network Connect (TNC) and Microsoft's Network Access Protection (NAP) — will now interoperate, providing enterprises with simpler, more cost-effective, scalable, and interoperable endpoint integrity and network access control.

To improve endpoint and network security, enterprises have been quick to embrace the notion of network access control. The concept is simple: when a device — also known as an endpoint — connects to a network, the user's identity and the health of the endpoint are checked. If they comply with the network's policies, access to the network is granted. If not, the endpoint may be remediated by applying the latest patches or scanning for viruses.

By improving endpoint security, companies can better defend against a number of increasingly complex Internet-borne attacks. Attackers — including organized criminal rings — now often utilize advanced malware which combines rootkits, Trojan applications, and operating system backdoors to exploit endpoints and steal sensitive data. Attackers' goals include extortion, identity theft, fraud, and even corporate espionage. Organizations must respond with more advanced endpoint security to effectively safeguard valuable information, comply with regulations, and avoid costly data breach notifications.

Yet since network access control products came to market, implementers have faced an uphill battle. First, they had to navigate a wide variety of often incompatible appliance, software, and infrastructure-based options. Then they had to select a proprietary approach, attempt to cobble multiple products together into a workable solution, or opt for one of several incompatible network access control frameworks.

As a result, even though network access control is a top enterprise spending priority — Forrester Research reports at least 40 percent of organizations will invest in such technology this year — many organizations have delayed their investments until discussions of network access controls evolve from point technologies to broad frameworks comprising interoperable products that deliver network access control in a cost-effective and scalable manner.

Now, however, network access control frameworks are reaching maturity. In particular, the Trusted Computing Group (TCG), an industry standards body focused on open security technologies, and Microsoft Corporation, a TCG member and active participant in TCG standards development, have announced that their respective network access control frameworks — Trusted Network Connect (TNC) and Network Access Protection (NAP) — will interoperate through the statement of health (IF-TNCCS-SOH) protocol, a new and open standard.

In short, beginning in 2008 with the release of products supporting the standard, products compatible with either of these two dominant network access control architectures will be able to interoperate in 1H 2008 when products supporting the standard are made commercially available. As a result, network access control implementers benefit from more product choices, enhanced interoperability, future-proof network access control investments, lower cost of implementation,

Benefits from TNC & NAP Interoperability

1. Increased interoperability and customer choice

2. Simplified network access control frameworks and protocols

3. Investment protection

4. Single network access control client

and — with Windows Vista and soon Windows XP — the potential for a single and consistent network access control agent.

Sharing a Statement of Health

Exactly how will TNC/NAP interoperability work? Microsoft has contributed its SOH protocol to TCG, which has published it as a new TNC specification, IF-TNCCS-SOH (available at https://www.trustedcomputinggroup.org/groups/network), and it is now an open standard available for anyone to freely download or implement. Briefly, IF-TNCCS-SOH is a client/server protocol for reporting on the health — that is, security state — of a client before providing a network connection. In particular, the IF-TNCCS-SOH protocol complements IF-TNCCS, which is the existing TNC protocol for such checks.

Some examples of health checks might include:

“Good” health:

- Security agent present
- Firewall running
- BIOS intact
- Latest OS patches
- Up-to-date antivirus
- No malware detected
- Only approved applications installed

On the other hand, the health check can detect problems, including:

- Disabled security agent
- No firewall running
- BIOS irregularities
- Missing patches
- Outdated antivirus signatures
- Scans detect malware

This integration now enables multiple network access control permutations:

- Use NAP products in TNC-protected networks and TNC products in NAP-protected networks
- Combine TNC and NAP servers
- NAP partners can support TNC clients and servers
- TNC implementers can support NAP clients, servers and protocols

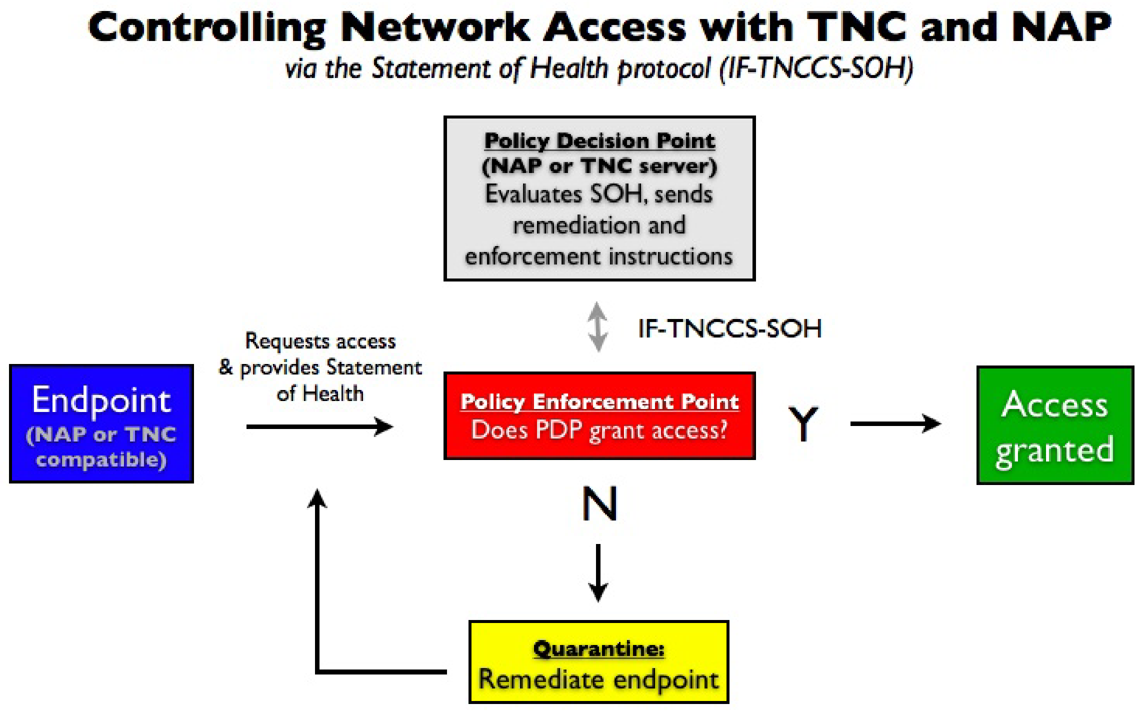
How TNC & NAP Interoperate

Microsoft NAP and the TCG TNC architecture interoperate at three points in either a TNC-compliant or NAP-protected network:

- **Endpoint:** When requesting access, an endpoint (a PC or other network-connected device) sends information about its security state (such as antivirus signature version, patches present, or BIOS integrity) to a Policy Decision Point, along with the user’s identity credentials, via the IF-TNCCS-SOH protocol. Because of this standard protocol, the endpoint can be a NAP client or a TNC client.
- **Policy Decision Point (PDP):** The PDP evaluates the user identity credentials and endpoint security state against policy and decides what access, if any, to grant the endpoint. The PDP then provides remediation instructions to endpoints via the IF-

TNCCS-SOH protocol and access instructions to the Policy Enforcement Point, typically via the RADIUS protocol. Again, the PDP can be either a NAP server or a TNC server.

- **Policy Enforcement Point (PEP):** Based on the PDP's instructions, the PEP (which may be a switch, router, gateway, or firewall) denies or grants network access to the endpoint. If remediation is required, the endpoint may be placed into a network quarantine — receiving access only to needed updates — until the endpoint remediates and resubmits its security state.


Controlling Network Access with TNC and NAP
via the Statement of Health protocol (IF-TNCCS-SOH)
Policy Decision Point
(NAP or TNC server)
Evaluates SOH, sends remediation and enforcement instructions
IF-TNCCS-SOH
Endpoint
(NAP or TNC compatible)
Requests access & provides Statement of Health
Policy Enforcement Point
Does PDP grant access?
Y
Access granted
N
Quarantine:
Remediate endpoint

In either a TNC- or NAP-protected network, endpoints must share their state of health (SOH) information. Endpoints which comply with health policies (specified by the PDP) receive relevant access (via the PEP). Endpoints which fail are shunted into a network quarantine with limited access, until remediated and reassessed.

Minimum Technology Requirements

To create either a NAP- or TNC-protected network, organizations must implement each of the above three elements. Thanks to TNC and NAP interoperability, organizations will only need a single PDP server, regardless of whether they choose a NAP server (such as Microsoft Network Policy Server) that is TNC-compatible; or a TNC server (such as a Juniper Infranet Controller appliance or similar products) that is NAP-compatible.

Some organizations, however, may opt to use multiple PDP servers, perhaps to leverage existing infrastructure (and especially after mergers and acquisitions introduce parallel, non-unified infrastructures), or simply to mirror organizational structure. For example, a company's desktop management team might prefer to manage a PDP which evaluates endpoint security policy compliance, while the networking team might manage a PDP devoted to network quarantine, user identification, and policy enforcement.

Utilize Existing Infrastructure

In spite of the TNC and NAP framework revisions, enterprises will not need to burn their current IT infrastructure — switches, routers, and so on — to take advantage of the improvements. Rather, existing network access control technology will become compatible with a much wider array of products, thus providing organizations with increased flexibility for implementing cost-effective network access control solutions. Likewise, product developers can reach a much wider audience.

What will TNC or NAP users need to upgrade? In general, Policy Enforcement Points including switches, routers, and gateways) will not need to be upgraded, as they do not need to support IF-TNCCS-SOH. Network access control clients and Policy Decision Point servers, however, may require software upgrades.

Expect widespread IF-TNCCS-SOH adoption by the 75 TNC member companies and 115 NAP partners. Already, Microsoft has announced that all Microsoft Windows Vista and Microsoft Windows Server Code Name “Longhorn” products include out-of-the-box IF-TNCCS-SOH support and that support in Microsoft Windows XP systems is forthcoming. Furthermore, Juniper Networks has announced that support for the protocol will be added to its Unified Access Control solution in the first half of 2008.

Roadmap to Increased TNC/NAP Interoperability

Products compatible with both the TNC and NAP frameworks will arrive in the first half of 2008. In the meantime, how should organizations interested in pursuing network access controls and taking advantage of TNC and NAP interoperability prepare?

1) Study the network. Which resources does the organization need to protect?
2) Catalog endpoints. Assess whether currently deployed security clients will work with desired network access control products — and tell vendors that TNC and NAP are important to the future of enterprise network security.
3) Define “healthy.” Network access controls will not be effective or enforceable unless organizations create written policies to specify access levels granted, based on user identity and endpoint health. Begin by identifying which endpoints most urgently need protection, and crafting related policies.
4) Begin NAP and/or TNC deployment. NAP and TNC-based products provide the best foundation for implementing network access controls today, because they are all based on the strong, secure TNC architecture, and the growing body of related standards. Organizations that deploy such products now will immediately enhance enterprise security while also positioning themselves to benefit from increasing NAP/TNC interoperability and product compatibility.

Interoperability Payoffs

Network access control practitioners will realize four immediate business and security benefits from TNC and NAP interoperability:

- **Improved interoperability and choice:** Users have an even greater choice of architecture and product options. They can select the best, most cost-effective components, infrastructure, and technology from any of the 75 TNC member companies or 115 NAP partners. Furthermore, because of the open IF-TNCCS-SOH client/server protocol for network access control, whatever they select will remain compatible with a wide range of other technology.

- **Simplified approach:** The days of confusing and competing network access control architectures and products are over. Two of the most important network access control industry participants — Microsoft and TCG — have agreed on common network access standards: the TNC specifications, including the IF-TNCCS-SOH protocol.

- **Single network access control client:** Windows Vista, as noted, includes a built-in NAP client, thus allowing all Vista PCs to interoperate with TNC-compliant technology. In other words, organizations running Windows Vista — and soon, Windows XP — will not need to install a new, standalone network access control client; it comes preinstalled.

- **Investment protection:** Thanks to TNC and NAP interoperability, companies can pursue network access control investments today and know this technology will continue to meet their needs and remain compatible with network access control frameworks as standards evolve.

Ongoing Benefits

The SOH interoperability between TNC and NAP is just the first step in an ongoing process of further integration and interoperability between the two frameworks. Expect future announcements, including details of enhanced protocols and improved integration with the tens of millions of Trusted Platform Modules (TPM) already installed in endpoints, helping to better identify individual users, thwart rootkits, and enhance overall network security. More information on rootkit prevention is available at https://www.trustedcomputinggroup.org/news/Industry_Data/Whitepaper_Rootkit_Strom_v3.pdf.

Learn More about TNC and NAP

For more information about the Trusted Computing Group and the TNC, including membership details and the organization's specifications, see: https://www.trustedcomputinggroup.org/groups/network/

For more information on Microsoft NAP, including details of the policy enforcement capabilities built into Microsoft Windows Vista and Windows Server Code Name "Longhorn," see: http://www.microsoft.com/technet/network/nap/default.mspx

The information contained in this document represents the current view of Microsoft Corporation and the Trusted Computing Group on the issues discussed as of the date of publication. Because Microsoft and the Trusted Computing Group must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft or the Trusted Computing Group, and neither Microsoft nor the Trusted Computing Group can guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT AND THE TRUSTED COMPUTING GROUP MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Microsoft and Trusted Computing Group members may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from the patent holder, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.