



Trusted Network Connect and Microsoft Network Access Protection Interoperability May 2007

Q1. What do you mean by interoperability between Trusted Network Connect (TNC) and Microsoft Network Access Protection (NAP) network access control architectures?

A. TCG, with member company Microsoft, is announcing interoperability between two network access control architectures: Microsoft Network Access Protection (NAP) and Trusted Network Connect (TNC) from Trusted Computing Group (TCG). TCG is incorporating the Microsoft client-server protocol (statement of health, or SOH) that allows NAP clients to participate in a TNC-protected network and TNC clients to participate in a NAP-protected network. NAP clients and servers are now TNC clients and servers and are welcomed into the TNC architecture.

Q2. How will you make this new interoperability available?

A. TCG is publishing a new specification supporting the Statement of Health. This new specification, IF-TNCCS-SOH 1.0, is available beginning May 21, 2007 on the TCG website at <https://www.trustedcomputinggroup.org/groups/network>. Vendors can download this specification and begin development immediately.

Q3. What does this mean for customers?

A. The IF-TNCCS-SOH 1.0 protocol now is an open standard published by TCG (under the TCG royalty-free cross-licensing model) and available for anyone to implement for free. It is implemented in Windows Vista and to be implemented in Windows XP and Windows "Longhorn". We believe it will become the prevalent method for network access control client-server protocols. IF-TNCCS-SOH will enable any device to participate in a TNC or NAP network and have its health checked. As a result of making SOH part of TNC, customers benefit in several ways:

- **Interoperability:** Customers can now be assured of interoperability between Microsoft NAP and other TNC implementations.
- **Choice:** Customers can now choose from any of the wide array of products that support Microsoft NAP and TCG TNC based on customer needs.
- **Compatibility:** Network access control products will now be much more compatible, allowing customers to interconnect a wide range of network, client, and server components.
- **Clarification:** Customers who have been waiting for consolidation and clarification in the confusing maze of network access control architectures and standards can now proceed with deployments of NAP and TNC products, confident that they will interoperate.
- **Single Client Agent:** Computers running Windows Vista, Windows Server "Longhorn", and future versions of Windows XP include the NAP Agent component as part of the core operating system. The NAP Agent will be used for both NAP and TNC, greatly simplifying deployment of a network access control solution. To support client operating systems other than Windows, Microsoft will license elements of the NAP client technology that support both NAP and TCG TNC to third-party software developers.

Q4. Why did Microsoft and TCG do this?

A. Customers have made it clear they want Microsoft NAP and TNC systems to be able to interoperate with one another. This interoperability gives customers the flexibility to choose the security solution that best meets their needs, including interoperable components from a variety of vendors. This joint initiative strengthens Microsoft and TCG's commitment to helping customers address the increasing threats of malicious code, hackers and other attacks on our networks and IT environments.

Q5. Why are you announcing this now?

A. There are several reasons why the time is right. Many companies are working in earnest on their TCG TNC efforts and on migration to the next-generation Microsoft client and server platforms. Microsoft previously announced its commitment to the TNC architecture and its plans to align the NAP and TNC architectures, and Microsoft and TCG agreed that standardizing SOH was the best way to begin the process since it enables client-server interoperability

Q6. What is the status of Microsoft's involvement in TCG?

A. Microsoft was a founding member of TCG, holds a permanent position on the TCG Board of Directors and is an active participant in a number of TCG work groups. Microsoft Windows Vista includes a feature named BitLocker Drive Encryption that can be used to encrypt hard drive contents, protecting them against theft or unwanted disclosure. For maximum security, BitLocker can store the encryption key on a Trusted Platform Module (a hardware security module specified by the TCG and included on most business-class laptop and desktop computer systems).

Q7. What are the components of the NAP and TNC interoperability?

A. The NAP and TNC interoperability consists of the following components:

- Endpoint – The system that is requesting network access and being checked. This may be a NAP client such as a computer running Windows Vista or another kind of TNC client
- Policy Decision Point – The system that evaluates the endpoint and decides what access should be granted. This may be a NAP server such as a Microsoft Network Policy Server or another kind of TNC server.
- Policy Enforcement Point – A network element that denies or limits network access based on instructions from the Policy Decision Point. This may be a switch, router, VPN gateway, or other network element with enforcement capabilities.

Q8. How does the NAP-TNC interoperability work?

1. When an endpoint is connected to a network protected with NAP or TNC, its health is checked by the Policy Decision Point. The endpoint and Policy Decision Point communicate using the IF-TNCCS-SOH protocol.
2. Based on the endpoint's health (and generally also the user's identity and a set of policies configured by the administrator), the Policy Decision Point decides what access should be granted and what remediation (if any) is needed.
3. The Policy Decision Point sends remediation instructions to the endpoint via the IF-TNCCS-SOH protocol.
4. The Policy Decision Point instructs the Policy Enforcement Point about what network access (if any) should be granted.
5. The endpoint may follow the remediation instructions and then request another health check.

Q9. How is that different from having parallel but incompatible architectures?

A. The new shared standard client-server protocol IF-TNCCS-SOH allows TNC clients and servers to interoperate with NAP clients and servers. A NAP client can be used with a TNC server or a TNC client can be used with a NAP server, as long as they are all using the IF-TNCCS-SOH protocol. A mixed environment of NAP and TNC clients accessing a single server is also possible.

Q10. Are two servers (TCG and Microsoft) required for NAP-TNC interoperability?

A. No. Only one server is needed. However, there are several cases where two servers may be desired. For instance, one server (responsible for checking system compliance) may be managed by the PC system management team while the other server (responsible for network quarantine and enforcement) may be managed by the networking team

Q11. Do customers need to upgrade to take advantage of NAP-TNC interoperability?

Policy Enforcement Points (switches, routers, etc.) generally do not need upgrades since they don't need to implement IF-TNCCS-SOH. Endpoints and Policy Decision Points may need software upgrades to support IF-TNCCS-SOH. However, all Windows Vista systems include IF-TNCCS-SOH support out of the box and Windows XP will be enhanced to add IF-TNCCS-SOH support.

Q12. When will customers be able to take advantage of NAP-TNC interoperability in production deployments?

A. Endpoints that support NAP-TNC interoperability are shipping now (Windows Vista). Policy Decision Points that support NAP-TNC interoperability are expected to be available in the first half of 2008.

Q13. When can we see a demonstration of NAP-TNC interoperability?

A. Several vendors, including Microsoft, Juniper, Wave Systems and others, will be demonstrating NAP-TNC interoperability in the TCG booth and in their own booths at the Interop Las Vegas 2007 (see https://www.trustedcomputinggroup.org/news/events/interop_2007 for documents). There also will be a number of other multi-vendor TNC demonstrations at Interop in the TCG and members' booths as well as at the show's Interop Labs.

Q14. What's next for NAP-TNC interoperability?

A. The TNC work group is working to extend NAP-TNC interoperability. Areas under evaluation include adding features and improvements that might include enhancements to the IF-TNCCS-SOH protocol, further integrating support for the TPM, and assessing alignment on other TCG and NAP interfaces.

Q15. How does the integrated NAP-TNC solution relate to industry standards?

A. TNC is an open standards architecture created by an organization of some 170 members and available to non-members. The addition of the IF-TNCCS-SOH protocol as a TNC specification allows anyone to interoperate with TNC or NAP clients or servers. TCG also supports existing standards whenever possible, including RADIUS, EAP, 802.1X,X.509 and IPsec.

Q16. What about Cisco-Microsoft Interoperability?

A. TCG is announcing the IF-TNCCS-SOH specification and interoperability with NAP and its ecosystem of NAP partners and their products that support NAP. Cisco or Microsoft can comment on the issue of Cisco and NAP interoperability.

Q17. What is the role of the Trusted Platform Module in all of this?

A. NAP-TNC interoperability allows NAP clients and servers to make use of the Trusted Platform Module (TPM) in network access control scenarios, substantially increasing security. For example, the TPM can be used to provide strong user authentication (like a built-in smart card). In a network access control situation, the TPM can provide particular value by measuring and attesting to the software loaded on the system. Because the TPM comes early in the boot sequence, rootkits and other infections that might evade software detection are clearly evidenced in TPM-based detection. TPM integration will be demonstrated at Interop Las Vegas 2007.

Q18. What should customers do to get ready to deploy a network access control system?

A. Three steps are most important when preparing for a network access control system. First, identify the critical resources you want to protect. Second, inventory the endpoints connected to your network and (optionally) the authorized users. Third, decide on policies for what constitutes a healthy endpoint on your network and what network access you want to grant based on user identity and endpoint health. You may want to take an incremental approach to deployment, starting with certain especially risky or especially sensitive parts of your network.

Q19. What if customers are ready to deploy a network access control system now?

A. NAP-TNC interoperability allows customers to deploy NAP and TNC incrementally or concurrently. Therefore, customers who need a network access control system now can use this approach:

- **Deploy TNC now:** Customers can begin deploying TCG TNC today. This works with existing Windows and non-Windows systems. There are a number of products available.
- **Test NAP now:** Customers should take the opportunity to test Windows Vista and Beta 3 of Windows Server codenamed Longhorn. This will allow them to prepare their IT and security processes and infrastructure for broader deployment when NAP is broadly available.
- **Migrate to a NAP-TNC environment:** As customers deploy Windows Vista and the version of Windows Server codenamed Longhorn, these NAP components can be deployed into their existing TNC environment, preserving their TNC investment while taking advantage of the NAP Agent built into Windows Vista.

Q20. What infrastructure does a customer need to deploy the integrated solution?

A. At minimum, a Windows Vista or other NAP client, a Policy Decision Point that is either TCG or NAP, and compatible networking equipment. Installations vary depending on the type of NAP deployed.

Q21. How should NAP partners and TNC members view this interoperability?

A. NAP-TNC interoperability gives NAP and TNC technology partners access to new markets since those products will now work with either architecture. In addition, customers attracted by the considerable benefits provided by this announcement will flock to NAP and TNC products and platforms.

NAP-TNC interoperability also simplifies partners' choices and reduces development costs. Instead of wondering whether to integrate with NAP or TNC, partners can now integrate with one architecture and automatically gain access to the other.

Q22. How exactly does a NAP or TNC partner ensure their solutions support this interoperability?

A. NAP and TNC partners can implement to either the NAP or TNC interfaces. TNC will continue to host testing events for members at which implementations can be tested.

Q23. TNC previously released a TNC client-server protocol. Will products developed to support this be compatible with those using the IF-TNCCS-SOH specification?

A. The previously released IF-TNCCS protocol is not compatible with the new IF-TNCCS-SOH. Some TNC server vendors may support both versions of the protocol for maximum compatibility. Others may choose to focus on IF-TNCCS-SOH due to the large and growing installed base of Windows Vista clients.

Q24. I see that there is a new group, the OpenSEA Alliance, focused on an open source supplicant. What is TCG's position on this?

A. TCG is and has been a strong supporter of open source; there have been a number of implementations of TCG specifications from the open source community, including those in networking security. In fact, libTNC and FHH both are supporting TNC with open source implementations. As far as OpenSEA Alliance specifically, the group's FAQ notes that it will support TNC (see http://www.openseaalliance.org/index.php?option=com_easyfaq&task=cat&catid=15&Itemid=34), which we applaud.

More information on TCG and TNC can be found at <https://www.trustedcomputinggroup.org/groups/network/>.

Contact: Anne Price
602-840-6495
press@trustedcomputinggroup.org