



Trusted Network Connect Frequently Asked Questions

Rev. May 2006

1. What is Trusted Network Connect?

Trusted Network Connect (TNC), an initiative of the Trusted Computing Group (TCG), is an open, non-proprietary standard that enables the application and enforcement of security requirements for endpoints connecting to the corporate network. The TNC architecture helps IT organizations enforce corporate configuration requirements and to prevent and detect malware outbreaks, as well as the resulting security breaches and downtime in multi-vendor networks. This effort spans:

The collection of endpoint configuration data in conjunction with user authentication information, for comparison with a pre-defined set of organization criteria for access to the protected network, thereby creating a "security" or "safe computing" profile for a system; and providing an appropriate level of network access based on the detected level of policy compliance, including full access, partial access or directed access, or no access.

2. Why is Trusted Network Connect necessary?

Networks, systems, software applications and data form the critical foundation and essential structure for the day-to-day operations of most organizations. Inappropriate and unauthorized access takes many forms and has many consequences. Viruses and email worms, Trojan horses, denial of service attacks, and other malicious activities frequently utilize end-user machines to penetrate enterprise environments, even when perimeter security mechanisms like firewalls are in place.

The TNC architecture has been designed to assist network administrators in protecting networks by allowing them to audit endpoint configurations and impose enterprise security policies before network connectivity is established. The TNC architecture builds on existing industry standards and defines new standards as necessary, with the objective of enabling non-proprietary and interoperable solutions within multi-vendor environments.

3. What is the Trusted Network Connect announcing today?

The TNC is announcing the availability of three new specifications. These specifications are:

- IF-TNCCS, which specifies interoperability between the TNC Client (TNCC) and the TNC Server (TNCS);
- IF-T for Tunneled EAP Methods, which is the specification for support of various transports; and,
- IF-PEP for RADIUS, specifying a standard integration with Policy Enforcement Points (PEP).

These specifications are in addition to the existing TNC specifications – IF-IMC and IF-IMV, which provide standardized APIs for client plug-ins (IMCs) and server plug-ins (IMVs) to enable TNC functionality; and the TNC architecture specification – which were all published in May 2005. The May 2005 specifications are receiving minor updates today to reflect implementation experience. All TNC specifications are available free to anyone who wishes to download them from the TCG website, www.trustedcomputinggroup.org.

4. How are these new specifications intended to be used?

These specifications are intended to be used in the following manner:

- IF-TNCCS describes a standard way for the TNC Client (TNCC) and the TNC Server (TNCS) to exchange messages. Since the TNC architecture is layered, IF-TNCCS carries messages from IMCs to IMVs and vice versa. It also carries control messages between the TNCC and TNCS. IF-TNCCS is transport-independent so it can be carried over a variety of transports.
- IF-T for Tunneled EAP Methods specifies how IF-TNCCS should be carried over Extensible Authentication Protocol (EAP) tunneled methods such as EAP-TTLS, EAP-FAST, and EAP-PEAP. Supporting these EAP methods allows the TNC architecture to work with a variety of network technologies that support EAP

authentication: 802.1x, IKEv2, etc.

- IF-PEP for RADIUS specifies how to use the RADIUS protocol for communications between a Network Access Authority (NAA) – typically an AAA/RADIUS server – and a Policy Enforcement Point (PEP). IF-PEP is used to send network access decisions from the NAA to the PEP, enabling the PEP to enforce the access decisions on an endpoint's network traffic. The network access decision will trigger enforcement action by the PEP, such as allowing access, denying access, or granting limited access.

Additional standardized interfaces, such as IF-PTS, are in the process of being specified and reviewed and will be provided soon.

5. How do the newly released TNC specifications fit into the architecture announced last May (2005)?

The new TNC specifications – IF-TNCCS, IF-T, and IF-PEP – fit seamlessly with the existing TNC specifications and architecture specification. These new specifications facilitate the development and implementation of richer, standards-based communication between the key layers of the TNC architecture, specifically the Access Requestor (AR), Policy Enforcement Point (PEP), and Policy Decision Point (PDP).

6. Will products based on these new specifications be compatible with products already on the market?

As is the case with all TNC and, for that matter, TCG specifications, these new specifications from the TNC use as a foundation existing standards and protocols. This enables seamless interoperability and compatibility with existing products. The open, standards-based approach taken by the TNC to address endpoint integrity and network access enables organizations to best leverage their existing infrastructure investments. The open, non-proprietary nature of the specifications also allows organizations the ability to select and deploy best-of-breed offerings throughout their network infrastructure without fear of compatibility or interoperability issues.

7. What is the status of TNC?

The TCG's TNC subgroup is strong and growing organization, with active participation from dedicated network hardware, software, and security companies, as well as security organizations and companies from various countries and backgrounds. We have come together to define and propagate an open, standards-based approach to endpoint integrity and network access. The subgroup is adding new participants at an average rate of several new members per month. The TNC's reputation is also quickly growing, as evidenced by a plethora of new articles and analyst reports espousing the advantages of TNC's open architecture and standards focus. We anticipate that the TCG and the TNC subgroup will continue to be an industry leader and trendsetter in secure networking for years to come.

8. What are some attributes of TNC?

TNC is based on the twin concepts of integrity and identity. *Integrity* is used in this case to describe the desired state of an endpoint's "health" or configuration, as defined by IT policies. Examples might be to check if the system adheres to pre-determined policies and determine the system is not engaged in unusual or malicious behavior. *Identity* ensures that systems are authenticated for authorized users only.

One key attribute of TNC is its focus on heterogeneous networking environments, with products from a variety of vendors.

Another key attribute is that clients with a TPM offer additional security in that identity and integrity can be established through hardware. The TPM also provides a trusted boot mechanism that uniquely helps thwart root kits, stealthy infections that are otherwise almost impossible to detect.

TNC support will enhance many existing products. Users can benefit quickly because they can implement TNC within the infrastructure products and vendors already deployed on their networks. The architecture is based on existing, widely used standards such as EAP and TLS, and integrates with mature technologies such as IPsec and 802.1x.

9. How does the TNC architecture work? What are some of its key elements?

The TNC architecture is constructed on top of a traditional network access architecture, for instance, the switches in a wired LAN. A *Network Access Requester* (NAR) is client software on the endpoint that begins the network access attempt. 802.1x supplicants, VPN clients or Web browsers initiating SSL connections could all be NARs in a TNC environment.

The *Policy Enforcement Point* (PEP) – usually a network infrastructure device like a switch, wireless access point, or a VPN concentrator – restricts network access. It is controlled by a *Policy Decision Point* (PDP), which determines whether the endpoint should be admitted to the network and what access should be granted.

The TNC extends this standard identity-based access control architecture to include integrity checking by adding two layers on the endpoint and two layers on the PDP. On the endpoint, a TNC Client gathers reports from Integrity Measurement Collectors (IMCs, plug-in modules that report on the endpoint's health). The TNC client delivers these reports ("integrity measurements") to a TNC Server on the PDP. The TNC Server delivers the integrity measurements to Integrity Measurement Verifiers (IMVs) on the PDP, which check the client state against integrity policies. The TNC Server manages an integrity check handshake, delivering messages to and from the IMVs and combining the IMV's recommendations into a TNCS action recommendation which is used in the PDP's final decision.

10. What relationship does Trusted Network Connect have to the Trusted Platform Module (TPM) and other TCG efforts?

TNC is an excellent application for the TPM in that it helps establish a link to a decision point where integrity reports may be evaluated. Use of the TPM by TNC is optional, but for platforms with a TPM, the convenient reporting infrastructure enables the TPM reports to be factored into network access control decisions.

A system with the TPM can protect sensitive data such as encryption keys and collected measurements. The TPM safely stores those measurements in a protected location until ready for reporting. It can protect the measurements from man-in-the-middle attacks that might occur anytime thereafter. Products based on TNC architecture can operate in today's environments with and without TPMs. But if a TPM is present, there is a greater assurance in the TNC integrity reports originating from the expected platform.

11 Which companies are working on Trusted Network Connect?

More than 60 of the TCG's 135 or so members are involved in the TNC architecture development. The participating companies include those with expertise in firewalls and anti-virus products; switches, routers and hubs; network security; systems management; and operating systems. More information on TCG membership and a complete list of members is available at www.trustedcomputinggroup.org.

12. Does the Trusted Network Connect architecture use any existing industry standards?

Trusted Network Connect architecture uses existing industry standards, such as EAP, TLS, RADIUS, and others.

13. What access methods are supported by the TNC architecture?

The architecture supports all commonly used enterprise access methods such as VPN-based or dial-up remote access; wireless networks (WLAN); 802.1x infrastructures; and traditional LAN technologies.

14. When will we see TNC products? What about products using the newly announced TNC specifications?

There are currently several products that are shipping that have implemented TNC compatibility, with more products to be announced at Interop 2006. It is expected that several of these products being announced will include support for the just-released TNC specifications.

15. How does TNC compare to Cisco NAC and Microsoft NAP?

While the TNC does not openly compare itself to the other common standards for network access – Cisco Network Admission Control and Microsoft Network Access Protection standards – the TNC does offer the following key attributes and benefits:

- Supports multi-vendor interoperability
- Enables choice
- Leverages existing standards

Also, the TNC architecture provides organizations with a clear future path. Future integration with the TPM – the IF-PTS specification – enables a complete trusted network trail from the client straight through to the network. This level of future roadmap and integration with standards-based hardware security is not available with any other endpoint integrity/network access architecture. Microsoft is a TCG member and has announced the alignment of the NAP architecture with TNC and planned interoperability.

There are also additional solutions available from other vendors which attempt to address endpoint integrity and access control in different, various ways. TCG welcomes participation and membership by any companies in the

TNC effort and believes that interoperable approaches to network access control are in the best interests of customers and users.

16. What products supporting TNC will be announced or shown during Interop 2006?

Our member companies will be announcing and demonstrating many new products based on the TNC specifications in their booths during Interop 2006. More information on these products will be coming soon. There is a complete list of products available on the TCG website.

17. Are clients with TPMs required to implement these new specs or any TNC specs?

Currently, TPMs are not required to implement these new specifications. However, a future TNC specification, whose development is already underway – IF-PTS – will define the integration of the TNC architecture with the TPM.

18. How will users know that products are interoperable? Is there any certification or compliance program planned?

TNC members HP ProCurve, IBM, Juniper Networks, Meetinghouse, Nortel, Symantec and Wave Systems participated last month in the group's first interoperability event, hosted by the University of New Hampshire-InterOperability Laboratory. The event showed that products based on the various specifications worked together successfully in a simulated enterprise environment. The organization intends to have similar events in the future and is considering future compliance programs.

19. What TNC components were tested at this interoperability event?

Products representing all the components in the TNC architecture, including IMCs, IMVs, TNC clients and servers and Platform Trust Services, were tested.

20. Does TCG intend to take the TNC specification to any formal standards bodies, such as IETF?

TCG has an informal liaison relationship with IETF; many companies participate actively in both organizations to ensure there is a good flow of communications between the organizations.

21. When will we see additional TNC specifications?

The specifications available today offer critical elements of network access control and developers can use these now to create products to protect the network. Additional functionality will be added to the TNC architecture via the IF-PTS specification and other specifications that will be released in coming months.

-- 30 --