Trusted Network Connect Frequently Asked Questions
May 2007

Q. What is Trusted Network Connect?
A. 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.

TNC includes collecting endpoint configuration data; comparing this data against policies set by the network owner; and providing an appropriate level of network access based on the detected level of policy compliance (along with instructions on how to fix compliance failures).

Q. Why is Trusted Network Connect necessary?
A. 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.

Q. What are the TNC specifications?
A. TNC specifications include

- TNC architecture specification
- IF-IMC and IF-IMV, which provide standardized APIs for client plug-ins (IMCs) and server plug-ins (IMVs) to enable TNC functionality
- IF-TNCCS, which specifies interoperability between the TNC Client (TNCC) and the TNC Server (TNCS)
- IF-TNCCS-SOH, a special version of IF-TNCCS that enables interoperability among TNC products and Windows clients and servers (see below for more information)
- IF-T for Tunneled EAP Methods, which is the specification for support of various transports
- IF-PEP for RADIUS, specifying a standard integration with Policy Enforcement Points (PEP).

Q. What is the status of TNC?
A. TCG's TNC work group counts some 70 companies as members, with active participation from dedicated network hardware, software, and security companies, as well as security organizations and companies from various countries and backgrounds. Industry research has shown a high level of awareness of TNC and its benefits, and we are starting to see successful implementations of TNC in the enterprise.

Q. What are some attributes of TNC?
A. 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, interoperating seamlessly with products from a variety of vendors.

Another key attribute is that clients with a Trusted Platform Module (TPM) are offered additional security in that identity and integrity can be easily established through hardware. Optional for use with the TNC standards-based specifications, the TPM provides a trusted boot mechanism that uniquely helps thwart root kits, which are stealthy infections that are otherwise almost impossible to detect. When used in concert, the TNC standards and the TPM offer users and enterprises a complete, end-to-end root of trust, from the end device's edge to the network's core.

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.

Q. How does the TNC architecture work? What are some of its key elements?
A. The TNC architecture is constructed on top of traditional network access architecture; for instance, the switches in a wired LAN environment. 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 level of 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.

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

However, administrators do not have to have systems with TPMs to benefit from TNC. TNC solutions can be deployed with or without TPM clients.

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. The TNC standards and the TPM, when used together, offer users and enterprises trusted, integrity-driven network connected from the end device's edge to the network's core.

Incidentally, TPMs are shipped now in new enterprise notebook and desktop systems available from virtually all top 20 systems vendors, with tens of millions of TPM-based systems in deployment.

Q. Are clients with TPMs required to implement these new specs or any TNC specs?
A. Currently, TPMs are not required to implement these new specifications but TCG is providing a specification to enable the use of the TPM in TNC.

Q. Does the Trusted Network Connect architecture use any existing industry standards?
A. The TNC architecture uses existing industry standards, such as EAP, TLS, RADIUS, and others.

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

A. 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.

Q. When will we see TNC-based products?
A. Products implementing the TNC specifications have been shipping for several years. Companies currently providing compatible products include Extreme Networks, HP ProCurve, Juniper Networks, Meru Networks, OpSwat, Patchlink, Q1 Labs, StillSecure, Wave Systems, General Dynamics and others.

Q. How does TNC compare to Cisco Network Admission Control?
A. The TNC architecture is differentiated from Cisco Network Admission Control (C-NAC) by the following key attributes and benefits:

- Supports multi-vendor interoperability
- Leverages existing standards
- Empowers enterprises with choice

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.

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.

Q. What about the Microsoft Network Access Protection architecture?
A. In May 2007, TCG and Microsoft announced the interoperability of the TNC and NAP architectures. The initial interoperability is made possible by the new TNC IF-TNCCS-SOH (Statement of Health) specification contributed by Microsoft. This specification will enable products based on TNC to operate with Windows clients and servers and vice versa, thus creating a range of product choices and deployment options for customers.For more information on this, see the documents at www.trustedcomputinggroup.org

Q. How will users know that products built on various TNC standard specifications are interoperable? Is there any certification or compliance program planned?
A. A number of companies demonstrated interoperability of their TNC products at a second interoperability event, hosted by the University of New Hampshire-InterOperability Laboratory (UNH-IOL), in first quarter 2007. The event showed that products based on the various TNC standard specifications worked together successfully in a simulated enterprise environment. The organization is planning future compliance and certification programs.

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

Q. When will we see additional TNC specifications?
A. The specifications available today offer critical elements of network access control; developers can use these now to create products to protect the network. Additional functionality will be added to the TNC architecture as the group deems necessary.

Q. Are there any open source implementations of the TNC specifications?
A. Yes, several open source groups including libtnc and FHH have open-source support for TNC, and both have demonstrated at various events, including Interop.

-- 30 –

For more information, go to https://www.trustedcomputinggroup.org/groups/network/

Contact: Anne Price
1-602-840-6495
press@trustedcomputinggroup.org