Trusted Network Communications – FAQs

Contents

What is Trusted Network Communications?

In response to the global need for a more secure computing environment, TCG has developed and published Trusted Network Communications (TNC) standards since 2005, as an open architecture originally intended as a network access control standard with a goal of multi-vendor endpoint policy enforcement. In 2009, TCG announced expanded specifications which extended the scope of TNC to include security automation. Additional real-world applications of TNC include Industrial Control System (ICS) & SCADA security, as well as endpoint compliance and continuous monitoring. The TNC Architecture continues to evolve, expanding the existing end-to-end trust fabric from traditional use cases to emerging areas such as network infrastructure, Internet of Things (IoT), mobility, and cloud applications. TNC standards integrate security components across the endpoint, network, and servers into an intelligent, responsive, coordinated defense.

TNC specifications enable:

- ***Network visibility***— who is on the network, and what they are trying to access?
- ***Endpoint compliance***—are devices on the network secure, and is user/device behavior appropriate?
- ***Network enforcement***— the ability to block unauthorized users, devices, and/or behaviors, and to grant appropriate levels of access to authorized devices.
- ***Security automation***—sharing real time information about the environment without exposing sensitive, private, or protected data.

What problems does TNC solve?

The TNC Architecture is designed to enable posture checking, behavior monitoring, and remediation not only of user endpoints, such as PCs, laptops, phone, and other mobile devices, but also of infrastructure devices that are continually connected to the network and that are highly valuable targets of attack. The TNC architecture allows administrators to answer the questions

- "Is it vulnerable?"
- "Is it compromised?"
- "What actions should be permitted?"

for all the endpoints on their network and, more broadly, for the network itself.

Why is TNC necessary?

TNC standards integrate security components across the endpoint, network, and servers into an intelligent, responsive, coordinated defense.

The use of standardized protocols and schema offer benefits to both users and implementers of technology solutions. For users, the use of publicly-vetted protocols helps secure data in transit, reduces dependency on single-vendor solutions, and allows for architectural flexibility that meets the needs of myriad use cases. For implementers, standards can help meet the demands of international and national regulatory bodies, simplify interoperability with other vendor products, and provide more value to customers.

TNC standards deliver a wide range of benefits:

- TNC standards have a proven track record of delivering interoperable solutions to address endpoint, network, and server security. Products based on TNC standards have been shipping since 2005. There are many open-source implementations as well.
- TNC standards are widely deployed in real production scenarios. A broad range of customers across many sectors (Government, Healthcare, Finance, Retail and Education, among others) are benefitting from interoperable security solutions based on TNC standards.
- TNC standards are completely vendor-neutral. TNC based solutions leverage existing network infrastructure in a production environment, adding value to the existing investment.
- TNC standards are flexible. They support a broad range of assessment options (identity, health, behavior, and location; hardware-based & software-based security; and pre-admission & post-admission evaluation and monitoring). TNC standards also accommodate rapid change and can adapt to the evolving security landscape.
- TNC standards can and do easily integrate with other standards both existing and emerging, e.g. SWID Tags (ISO 19770-2) [9].

What is the scope of TNC solutions?

TCG's Trusted Network Communications (TNC) network security architecture and open standards enable intelligent policy decisions, dynamic security enforcement, and communication between security systems. TNC standards provide network and endpoint visibility, helping network managers know who and what is on their network, and whether devices are compliant and secure. TNC standards also enable context-based access control enforcement - granting or blocking access based on authentication, device compliance, and user behavior - and security automation, for orchestration of network and security systems.

What TNC specifications are available?

- TNC Architecture for Interoperability
- IF-IMC - Integrity Measurement Collector Interface
- IF-IMV - Integrity Measurement Verifier Interface
- IF-TNCCS - Trusted Network Connect Client-Server Interface
  - IF-TNCCS: TLV Binding
  - IF-TNCCS: Protocol Bindings for SoH
- IF-M - Vendor-Specific IMC/IMV Messages Interface
  - IF-M: TLV Binding
  - SWID Message and Attributes for IF-M
  - Attestation PTS Protocol: Binding to IF-M
  - IF-M Segmentation
- IF-T - Network Authorization Transport Interface
  - IF-T: Protocol Bindings for Tunneled EAP Methods
  - IF-T: Binding to TLS
- IF-PEP - Policy Enforcement Point Interface
  - IF-PEP: Protocol Bindings for RADIUS
- IF-MAP - Metadata Access Point Interface
  - IF-MAP Binding for SOAP
  - IF-MAP Metadata for Network Security
  - IF-MAP Metadata for ICS Security
  - MAP Content Authorization
- ECP - Endpoint Compliance Profile
- CESP - Clientless Endpoint Support Profile
- Server Discovery and Validation
- Federated TNC
- IF-PTS - Platform Trust Services Interface
  - Simple Object Schema
  - Core Integrity Schema
  - Integrity Report Schema
  - Reference Manifest (RM) Schema
  - Security Qualities Schema
  - Verification Result Schema

These are the current specifications as of the publication of this document; for the most up-to-date set of specifications, consult the TNC standards page.

What capabilities do TNC specifications provide?

The TNC architecture offers three primary capabilities:

- a ***Compliance*** capability, which evaluates an endpoint's adherence to network policy both at the point of connection and while it is connected to the network;
- an ***Orchestration*** capability, which provides a dynamic repository and notification service for real-time state and events; and

- an ***Access Control*** capability, which controls access to protected resources and networks based on endpoint posture and many other factors.

These cross-domain capabilities can be used for many purposes, including - but not limited to - security automation, continuous monitoring, asset management, endpoint compliance assessment and enforcement, protection of critical resources, leveraging of shared information, event correlation and assessment, and a variety of other key buzzword-compliant[1] functions. Application of these capabilities enables trusted network communications - the ability to understand the trustworthiness of an endpoint before, and while, it's allowed to communicate on the network.

Are TNC products compatible with today's infrastructure?

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

How does the TNC architecture work? What are some key elements?

TNC facilitates collection of information about an endpoint and secure delivery of that information to other components in the environment. The TNC Architecture recognizes the following high-level roles for entities involved in trusted network communication:

- ***Endpoints***, which are any entity - physical or virtual - that can be connected to a network
- ***Enforcement points***, which consume access control decisions from a policy server and apply them to endpoint requests
- ***Policy servers***, which collect and evaluate endpoint posture information and/or make access control decisions based on endpoint context (including role, state, location, behavior, and other factors) and communicate those decisions to enforcement points
- ***Configuration Management Databases (CMDBs)***, which store collected endpoint measurements
- ***CMDB clients***, which communicate endpoint information to and consume it from CMDBs
- ***Metadata Access Points (MAPs)***, which provide centralized coordination for producers and consumers of network and security information
- ***MAP clients***, which publish, search for, and subscribe to updates on endpoint and environment information via a MAP

A single entity may take on multiple roles; for example, a policy server may also be a MAP client as well as a CMDB client. Figure 1 illustrates the relationships between TNC roles:

[1] In all seriousness, these concepts are buzzwords for a reason; they represent critical functions that span operational use cases and disparate environments.

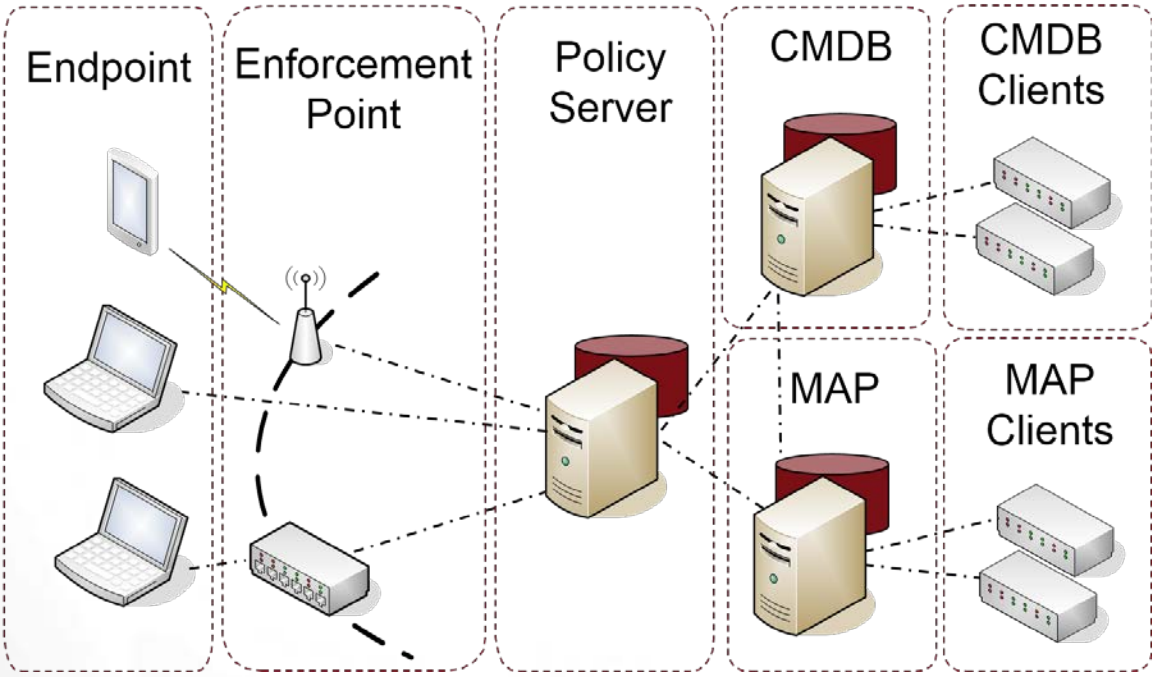

Figure 1: TNC Architecture Overview

What relationship does TNC have to the Trusted Platform Module (TPM) and other TCG efforts?

TNC enhances the value of the TPM by helping 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 compliance evaluations and 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; TNC enables that reporting. Products based on TNC architecture can operate in today's environments with and without TPMs, but if present, there is greater assurance that TNC integrity reports originated from the expected platform.

Is use of TNC dependent upon the presence of a TPM?

No - the TNC Architecture accommodates both platforms that have a TPM and those that do not. If no TPM is present, all TNC capabilities are available. For platforms with a TPM, TNC provides a connection between measurements stored in the TPM and policy servers seeking to make decisions based on endpoint trustworthiness. Adding a TPM to the TNC architecture enhances trust in the identity and measurements that TNC collects from an Endpoint, but is not required.

Where are TNC-enabled solutions available?

Companies currently providing TNC-enabled products include DECOIT, Extreme Networks, General Dynamics, HP ProCurve, Juniper Networks, macmon secure, Q1 Labs, Wave Systems, and others. In addition, several open-source implementations of TNC exist, including strongSwan VPN, TNC@FHH, omapd, and others.

What is TNC's relationship to other industry standards?

TNC is complementary with existing standards from TCG and other industry standards bodies. For example, the TCG's Trusted Platform Module (TPM) supports hardware-based "roots of trust", which help establish platform integrity, user security, and privacy. The TPM enables a “chain of trust” for a device’s core components responsible for its boot process

and ultimately the execution of the OS and applications. In the context of TNC architecture and solutions, TNC can leverage a TPM to increase trust in endpoint measurements, which improves detection of compromised devices so that appropriate controls can be applied. TNC mechanisms enable expression of that trust to a third party or back-end verifier, increasing confidence both in endpoint evaluation and in resulting actions such as access control decisions. The TNC Architecture provides more information on use of TNC with TPM.

Outside of TCG, several TNC specifications related to endpoint posture were contributed to the IETF, forming the basis for the IETF Network Endpoint Assessment standards. The IETF NEA Posture Assessment, Posture Broker, and Posture Transport protocols are all based on TNC interfaces. See the TNC Architecture for a more detailed mapping between TNC and NEA terms and concepts.

Where can I get more information on TNC?

The TNC home page provides links to TNC standards and other resources. Implementers are encouraged to start with the TNC Architecture; solution architects and other end users will find specific use cases addressed in the TNC Architects' Guides.