



Trusted Network Connect (TNC)

**Open Standards for Integrity-based Network Access Control
and Coordinated Network Security**

April 2011

Trusted Computing Group
3855 SW 153rd Drive, Beaverton, OR 97006
Tel (503) 619-0562 | Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

Trusted Network Connect (TNC) - Open Standards for Integrity-based Network Access Control and Coordinated Network Security

Evolving Cyber Threats Pose Growing Problems

Recently we have seen cyberthreats evolving from being passive requiring users' actions for transmission, to stealthier tactics that would infect entire network without any user involvement. Threats are now taking on a new dimension as they become more targeted, distributed and sophisticated causing maximum damage to the sphere where it matters most. The IT landscape is also changing as networks converge, services move to cloud, and endpoints become more mobile. Thinning network boundaries, vulnerabilities in unpatched software running in corporate computers, jail broken cell phones and tablets with malicious unverified apps allow code altering root kits and worm infections to infiltrate devices and gain access to confidential data. The resulting theft or modification of proprietary data by professional attackers—cracker hobbyists, organized criminals or corporate spies—costs billions, ruins businesses and wreaks havoc on identity theft victims.

Fortunately, Trusted Network Connect (TNC) technology offers a range of network security and coordinated security solutions today that can protect networks from these threats and attacks proactively and on the fly.

Six reasons why TNC makes sense for today's enterprise network:

- 1) Open, interoperable, standards-based network security solution.
- 2) Visibility of all users and devices on network, their behavior and security state, for coordinated security.
- 3) Count on the added security of trusted hardware.
- 4) Choose which hardware or software vendor works best for your situation.
- 5) Save money as you gain control of decisions on security design components.
- 6) Wide industry support (100+ TCG member companies).

TNC Proactively Secures Systems and Keeps Information Safe

The Trusted Network Connect (TNC) working group of the Trusted Computing Group (TCG) has created an open, standards-based architecture for endpoint authentication, platform integrity measurement and integrating security systems. The TNC architecture inspects endpoints (network clients and servers) for compliance with security policies before allowing them on the protected network. This ensures that all endpoints are equipped to defend against attacks from rogue systems or compromised devices. Information sharing between network security systems is standardized for better decision making so your business and data are constantly well protected.

TNC Offers Open Architecture and Standards for All Platforms

By defining an open architecture with standard interfaces, TNC ensures that components from different vendors work together smoothly and securely. An artist with a Macintosh, an accountant with Windows, a UNIX server, an executive with a tablet, and a salesman with a smartphone are all properly checked and verified before gaining network access. Major vendors have announced their support for TNC and more are coming. Strong interoperability and platform support allow customers to maintain vendor choice, leverage installed equipment, and ensure security across their installed base.

TNC Simplifies and Strengthens Network Security

TNC Builds on Established Standards

TNC builds on established standards such as EAP, TLS and SOAP. This allows it to support a variety of networking technologies: 802.1X (wired or wireless), IPsec or SSL VPNs, conventional LANs, and even dialup. Adoption costs are minimal. Customers can often reuse existing equipment, avoiding the need to sacrifice interoperability or freedom of choice, and still improve their security.

TPMs Make Endpoint Software Spoof-proof

TNC includes optional support for trusted hardware: the Trusted Platform Module (TPM). This hardware, a single computer chip embedded at the PC board level, serves as the “root-of-trust” for subsequent machine activities. For instance, the TPM can be used to verify exactly what software is running on an endpoint during a TNC handshake. The TPM or other trusted hardware simplifies the detection of kernel rootkits, which modify the operating system to hide themselves from security software. TPM and TNC work hand-in-hand to form the industry’s strongest available endpoint integrity solution.

Future-proof Your Network

Pervasive computing is driving the need for smart devices that securely interconnect without users needing to do anything. But adding security to devices can be a daunting job for developers, especially if they lack expertise in cryptography, key management and secure coding practices. TNC’s open standard helps vendors more easily establish a common interoperable endpoint integrity model for all nodes on the network.

Today nearly 100 vendors are preparing and offering TCG-compliant products. Starting now, networks of the future will build in security benefits and administrative efficiencies to servers, routers, switches, devices, applications, and Web services.

Who Benefits by Using Trusted Network Connect Products?

- Enterprises reduce system compromises, downtime and data loss by ensuring all endpoints on the network comply with security policies
- IT departments benefit because network devices, endpoint hosts and corporate applications can interact smoothly, allowing efficient and effective security management.
- Users and customers can still use their favorite devices and platforms, virus scanning software, or security appliance.
- Vendors reduce cost and complexity by supporting one set of standards instead of many proprietary interfaces.

TNC Checks Security Policy Compliance During Network Access Control

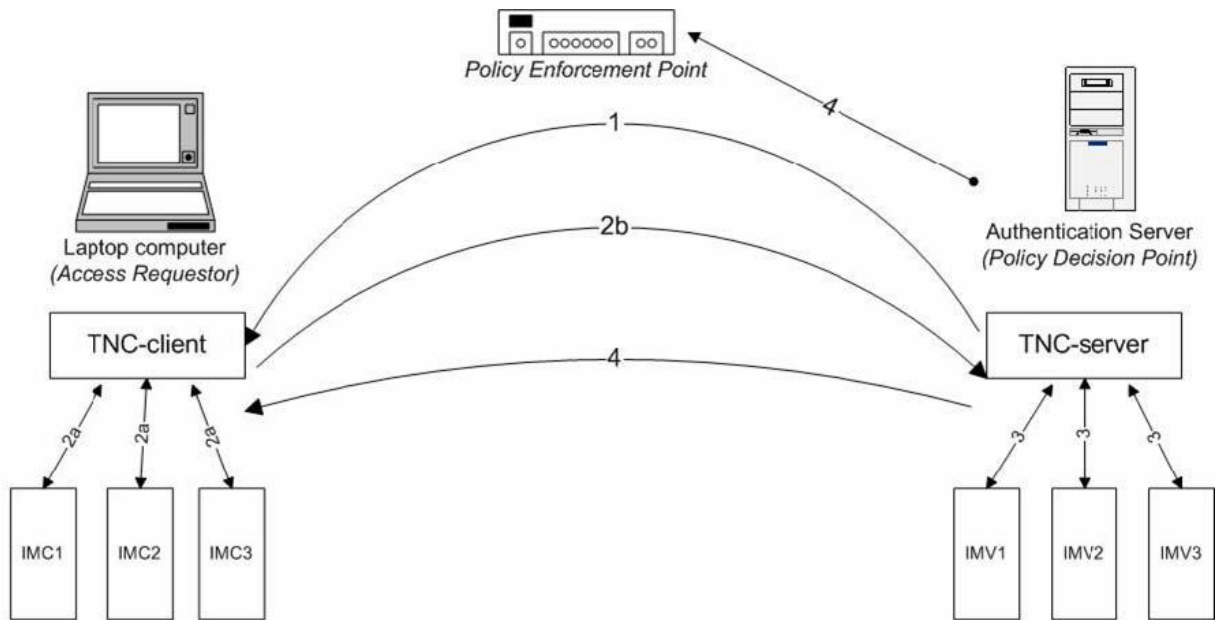


Figure1. Network Connection with Integrity Protection

Figure 1 illustrates how TNC extends a traditional network access control check, adding a verification of endpoint security policy compliance. In this example, a user with a laptop computer (the Access Requestor) is trying to connect to a protected network. The network is guarded by a Policy Enforcement Point (PEP), which consults a Policy Decision Point (PDP) to determine whether or not the endpoint meets the criteria for full connectivity. This is typical of today's networks, but here the Access Requestor and PDP both contain additional software components which are shown above. The Access Requestor contains a TNC client and plug-in components (Integrity Measurement Collectors, IMCs) that collect integrity measurements from anti-virus and other security packages. The PDP contains a TNC server and plug-in components (Integrity Measurement Verifiers, IMVs) that verify these integrity measurements against security policies.

During authentication and authorization stage of network access, the following steps are performed:

1. TNC-server on PDP initiates integrity check
2. a. TNC-client collects integrity measurements from IMCs
b. TNC-client passes integrity measurements to TNC-Server through PEP
3. TNC-server passes integrity measurements to IMVs, which compare them against security policies and provide access recommendations to TNC-server.
4. TNC-server makes final access decision, sends access decision to PEP and Access Requestor

If the integrity check succeeds, the PEP places the Access Requestor on the protected network. If the integrity check fails, the PEP places the Access Requestor in a quarantine environment for remediation.

TNC Integrate multiple security devices for coordinated network security

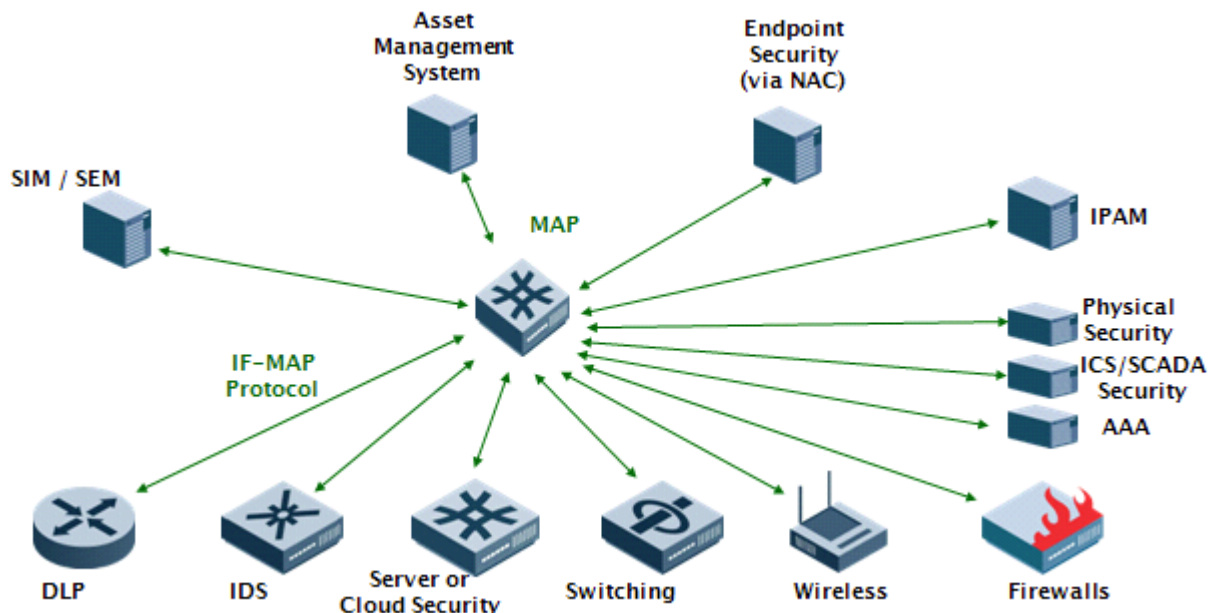


Figure2. Coordinated Network Security

Figure 2 illustrates how TNC allows sharing of information among devices to take coordinated and intelligent decisions. The TNC architecture lets you integrate Sensors and Flow Controllers like Intrusion Detection Systems, Leakage Detection Systems, switches and so on with each other and with your NAC system using Metadata Access Point (MAP). MAP is a database that stores information about who's on your network, what device they're using, what their behavior is, and all sorts of other information. It's a central database for sharing information between different security systems. TNC uses a single standard SOAP based protocol called IF-MAP for publishing data to the MAP and querying or subscribing to get data from it. So all the security systems can share information with each other using the standard IF-MAP protocol and take intelligent decisions providing unprecedented security.

For instance post admission following steps are possible

1. IDS detect attack from IP x.x.x.x
2. IDS publishes the IP x.x.x.x to MAP server with appropriate information to raise security event
3. MAP server notifies the PDP that earlier authenticated and authorized user from IP x.x.x.x
4. PDP instructs switch (PEP) to block access from IP x.x.x.x immediately

The TNC Architecture with the Trusted Platform Module (TPM)

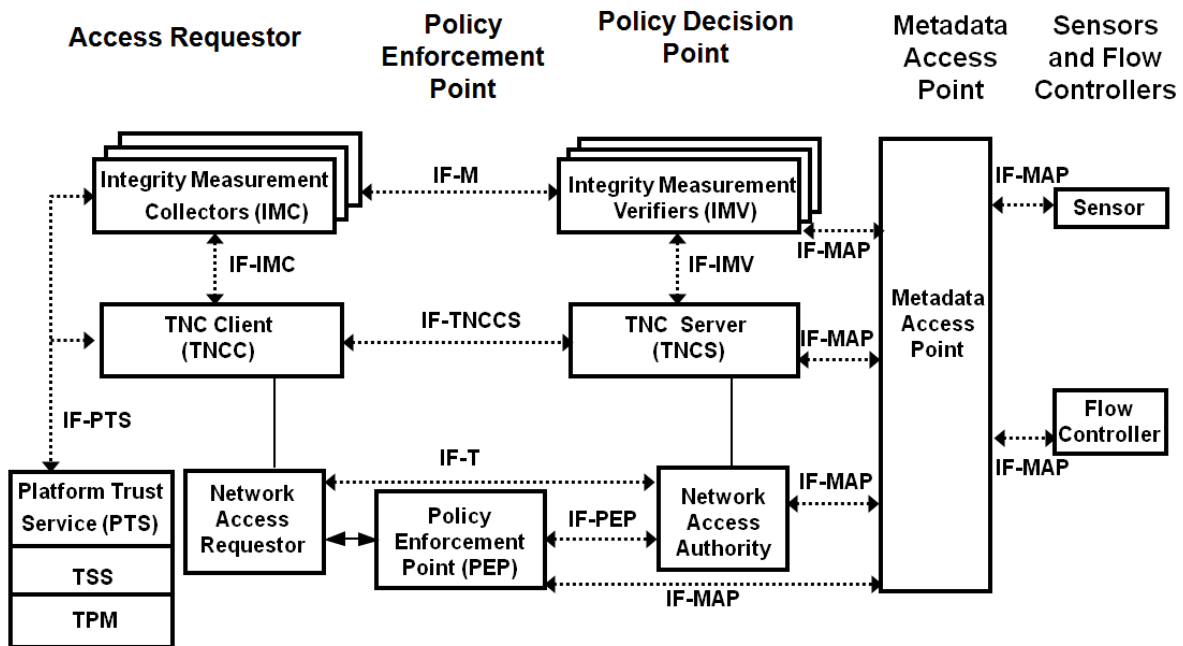


Figure3. The TNC Architecture

Figure 3 illustrates the components of the TNC architecture, including the optional Trusted Platform Module (TPM) and Metadata Access Point (MAP). The dotted lines are standard interfaces (protocols and APIs).

A quick description of this architecture will show the flexibility of the architecture.

The components on the left comprise the Endpoint or Access Requester (AR). IF-PTS is a standard interface for the TPM-related components. IF-IMC allows security software vendors to develop plug-ins to support their endpoint software (anti-virus, personal firewall, etc.).

The Policy Enforcement Point (PEP) guards access to the Protected Network. It passes messages (IF-M and IF-TNCCS) over a transport protocol like EAP-FAST (IF-T). The Policy Decision Point (PDP) makes network access decisions (such as allow, deny, quarantine) based on integrity of the endpoints. It uses IF-IMV to communicate with plug-in policy evaluators and IF-PEP to instruct the PEP when to grant network access.

The Metadata Access Point (MAP) has a complete view of the network with PDP, sensors and flow controllers publishing information to it. The same devices can take intelligent decisions by subscribing or querying interesting information from MAP. This is achieved through the IF-MAP protocol.

The TCG has published specifications for the above mentioned interfaces. Products implementing the TNC interfaces have been available for more than five years.

TNC Architecture Provides Conclusive Advantages

By integrating the trusted hardware of the TPM into a network access control framework and sharing information across security systems using MAP, the TNC architecture provides unprecedented security. The TPM enables detection of any unauthorized software including kernel rootkits, platform authentication, protected storage, and other substantial benefits. In addition to this strong security, the TNC's open interfaces allow components such as flow controllers and sensors from different vendors to be integrated into a single whole. These advantages are driving rapid adoption of the TNC architecture and standards among vendors and customers.

Learn More about TCG and TNC

More information on the Trusted Computing Group and the TNC, including membership details and the organization's specifications, is available at <http://www.trustedcomputinggroup.org>