



CONTACT: Anne Price
1-602-840-6495
Mobile1- 602-330-6495
press@trustedcomputinggroup.org

TRUSTED NETWORK CONNECT (TNC) EXPANDS NAC ARCHITECTURE WITH EXTENSIONS INTO NETWORK SECURITY, MORE PRODUCTS AND PROVEN INTEROPERABILITY

New IF-MAP Protocol Lets Devices on the Network Share Data in Real Time, Improving Network Defense

LAS VEGAS, April 28, 2008 – The Trusted Network Connect ([TNC](#)) architecture, the open solution for network security, continues to expand both its industry support and capabilities. Here today at Interop, the networking industry's leading event, members of the [Trusted Computing Group](#) demonstrated a number of available products based on TNC, the only non-proprietary solution for network access control. Among the demonstrations is a new TNC protocol, IF-MAP (Interface for Metadata Access Point), which is available beginning today.

TNC Extends Capabilities Beyond Admission Control to Enable Real-Time Defense

Threats to networks have become more sophisticated, creating the need for integrated security beyond endpoint admission control. TCG is addressing this need for broader capabilities for network security. With input from many of its more than 140 member companies, TCG has created the [IF-MAP](#) (Interface for Metadata Access Point).

IF-MAP defines a powerful publish/subscribe/search protocol that enables a wide range of systems to share data in real time about network devices, policies, status and behavior. For example, an intrusion detection system with a built-in IF-MAP client can publish an alert to an IF-MAP server indicating that a particular endpoint is sending anomalous traffic, and a firewall that subscribes to information involving that endpoint will receive a real-time update from the IF-MAP server, triggering an automatic response. This powerful integration of network and security components can strengthen the network beyond just admission control and assurance of endpoint integrity to continuous post-admission assessment and control.

Implementation of the IF-MAP protocol also is anticipated to better protect the network by allowing access to be more finely tuned to individual users or groups of users based on the information shared among various devices. For example, an IF-MAP enabled network could recognize and allow peer-to-peer file sharing among one group while blocking it for other groups not authorized for that activity.

Noted David O'Berry, the director of Information Technology Systems and Services for the South Carolina Department of Probation, Parole, and Pardon Services, "From my perspective as a practitioner and customer of various companies, TCG's IF-MAP adds a very real workable path to a heterogeneous solution from what recently would have been considered only wishful thinking. With the addition of this standard, we can transcend individual products and realistically look to add valuable agility back into the network via an extensible standards-based security framework. This is revolution, not evolution."

-- more --

“While identifying and stopping unauthorized or infected users at admission is valuable and necessary, true network security involves continually monitoring the network with a variety of devices and components,” noted Stuart Bailey, TNC work group specification editor and CTO and founder, Infoblox. “By enabling real-time exchange of data among products from any vendor, TNC is pushing NAC standards to new levels, enabling systems that go beyond perimeter access and provide continual coordinated defensive-in-depth – at reasonable cost and with vendor choice.”

The complete IF-MAP specification, TNC architecture document and other materials to implement the specification are available at <https://www.trustedcomputinggroup.org/groups/network/>.

TNC Now Widely Implemented

The TNC architecture has been adopted by a number of companies that build equipment or software that is interoperable with others in the market. TNC enables the application and enforcement of security requirements for endpoints connecting to the corporate network.

Companies showing products implementing or supporting TNC in TCG's Interop Booth #421 and in the show's InteropLabs include ArcSight, Aruba Networks, Avenda Systems, Enterasys Secure Networks, Fujitsu Ltd., Identity Engines, Infoblox, Juniper Networks, Lumeta, MacAfee, Microsoft, nSolutions, ProCurve Networking by HP, Q1 Labs, Symantec, Trapeze Networks and Wave Systems. Demos include those for the new IF-MAP protocol.

Proven Interoperability

Many of these participants participated last month in TNC's third annual interoperability event, where members tested hardware and software supporting the TNC specifications in a simulated enterprise environment. Over two days, Enterasys, FreeRADIUS, Identity Engines, Infoblox, Juniper Networks, libTNC, OpenSEA, ProCurve Networking by HP, Symantec, TNC@FHH, and Trapeze Networks successfully demonstrated interoperability across six TNC interfaces: IF-IMC, IF-IMV, IF-MAP, IF-PEP, IF-T, and IF-TNCCS.

Products tested covered a wide variety of functions, including switches and access points, RADIUS servers, TNC integrity measurement collectors and verifiers, and TNC clients and servers. A highlight of the testing was the first known interoperability testing of leading open source TNC implementations, featuring a FreeRADIUS RADIUS server, TNC@FHH TNC server, OpenSEA 802.1X supplicant, and libTNC TNC client and integrity measurement collectors and verifiers.

About Trusted Computing Group

Trusted Computing Group, an industry organization that enables computing security, has created a portfolio of specifications to enable more secure computing across the enterprise. These specifications are implemented by manufacturers of PCs, servers, networking gear, applications and other software, hard drives and embedded devices.

More information and the organization's specifications and work groups are available at the Trusted Computing Group's website, www.trustedcomputinggroup.org. A new blog, www.trustedcomputinggroup.org/blog, offers commentary from work group chairs and experts in the fields of computing and security.