



**Networking Industry and IT Support for Trusted Network Connect and Its IF-MAP Specification
April 2008**

IT Community

"The world has changed and the stakes have been raised to the point that doing things in the old proprietary way simply will not suffice going forward. What we are consistently seeing now with the increasing speed of attack cycles coupled with the precision of the attack vectors is that open standards with frameworks that allow true pluggability are now the only valid way to implement real-world solutions," said **David O'Berry, the director of ITSS for the South Carolina Department of Probation, Parole, and Pardon Services.**

O'Berry continues, "Proprietary and closed solutions, as well as those that only pay lip-service to the standards simply do not give participants in the "digital ecosystem" the interoperability, scalability, and flexibility that we require. Open solutions like the TNC give us all of the above, which in turn contributes directly to the agility we require to bring secure solutions to our business thereby enhancing business operating efficiency on a number of levels. That agility is not a nice to have at this point, it is a must."

David O'Berry
803-261-3132
David.oberry@gmail.com

"General Dynamics C4 Systems is working with users across the government enterprise to deploy solutions utilizing the Trusted Network Connect (TNC) architecture for network security in cross-domain environments. The TNC based products and services are built with interoperability, openness and scalability in mind which afford users the greatest efficiencies available today for enterprise security," said Bill Ross, director of Information Assurance systems and programs for General Dynamics C4 Systems. "The advantages to our customers of TNC can be measured in reduced development time, reduction in operating cost and improved interoperability."

Fran Jaques
480-441-2885
480-586-1886
fran.jacques@gdc4s.com

Networking Industry

"Increased network security requires open standards in order to bring as many different product types together to provide end-to-end business and security solutions. This is why **ArcSight** supports TCG's standard for "Trusted Network Connect", says Rick Caccia, VP of Product Marketing at ArcSight. He continues, "ArcSight envisions a vital role for the ArcSight platform to collect, normalize, correlate and prioritize events from a variety of sources, including the new IF-MAP extension. The ArcSight platform can then act on the prioritized list of events through our integrated auto-response solution, by quarantining malicious endpoints and traffic on the network automatically. This provides for an end-to-end security solution including event collection, normalization and analysis, and automatic remediation."

Axel Tillmann
508-529-6100
Axel.tillmann@arcsight.com

"As a widely supported, open architecture, Trusted Network Connect enables us to further enhance our industry-leading identity-centric access control solutions by integrating end-point health assessment," noted Sean Convery, **Identity Engines'** CTO and representative to TCG. "By supporting the TNC's open-standards NAC framework, we give our customers both choice and control over the kinds of solutions they can implement, and we help them scale their deployments while keeping them interoperable with existing and future infrastructure."

Danielle Argenti
650-480-4013
Danielle@eastwick.com

According to Jiwei Wei, **Huawei Technologies Co., Ltd.**, "By utilizing IF-MAP, various security devices can be integrated into the network infrastructure, hence then the real-time monitoring on the security status of the endpoint can be implemented by the network operator. This protocol is capable of sharing/transferring the posture, especially the posture change of the endpoint, among different security devices. Then, the defending of security risk is changing from isolated security product to concentrated security management, and from passive protection to active protection. This reinforces the security of the whole network, when it is widely deployed."

Jiwei Wei,
86-10-59721861
jiwei.wei@huawei.com

“Trusted Network Connect has been dedicated to providing choices for enterprises seeking open, standards-based, best-of-breed network access control solutions,” noted Richard Kagan, vice president of marketing at **Infoblox**. “Now, with the new IF-MAP specification, the TNC architecture can be extended to enable coordinated network defense from a wider variety of products and services. The result will be networks that are more secure, easier to implement, and less costly to build and operate.”

Jennifer Jasper
408-625-4309
jjasper@infoblox.com

“**Juniper Networks** supports standards defined by TNC for network access control because we believe organizations are best served when they have the freedom to build or choose products and solutions that have the highest levels of openness and interoperability,” said Karthik Krishnan, director of product management at Juniper Networks. “It’s a compelling proposition for vendors to support open, interoperable standards because as customers seek to deploy integrated security systems with the best intrusion protection and prevention, they don’t want to be locked in to any single vendor.”

Cindy Ta
408-936-6131
510- 786-8476
cta@juniper.net

“**Lancope** advocates the development and adoption of network access control standards as defined by Trusted Network Connect,” said John Jerrim, chief research officer and founder of Lancope. “As a best-of-breed network and security monitoring solution provider, Lancope supports this effort to establish an industry-standard approach using IF-MAP to extend interoperability with other leading network infrastructure providers and gives enterprise customers the flexibility and choice they increasingly require.”

“The open standards being developed as part of the Trusted Network Connect (TNC) will allow for the fulfillment of the promises which we all hoped NAC would deliver. IF-MAP presents a breakthrough innovation which **Lumeta**’s customers have been asking for years – a standard way to leverage information, like that discovered by Lumeta IPsonar, across platforms and solutions for a more holistic and comprehensive security approach,” says Michael Markulec, COO, Lumeta Corporation. “Trusted Network Connect offers users the ability to leverage existing investments for better management and security of the network.”

“Lumeta’s Network Assurance solutions leverage the TNC architecture and the new IF-Map Protocol to enable enterprises to add a global network perspective to enterprise risk management programs. This allows for complete interoperability with existing network management, and system and data security measures.”

Rebecca Hagen
732-357-3525
rhagen@lumeta.com

“Trusted Network Connect’s philosophy of enabling more secure computing environments, without compromising functional integrity, is a mantra all IT providers should adhere to,” said Kamlesh Mehta, CTO and VP Engineering, **nSolutions**. “nSolutions subscribes to this open standard. Our NOVA change and configuration management product line hardens IT infrastructure resources — physical and logical devices as well as applications — against unauthorized access. Specifically, IF-MAP will allow nSolutions to seamlessly integrate configuration change management into multi-vendor deployments which address post-connect and clientless endpoint security.”

Michael Emerton
603-766-3688
mike@bridgeviewmarketing.com

“As the industry’s second largest enterprise networking vendor, ProCurve believes strongly in the benefits of Trusted Network Connect as an open framework to help protect our customers’ networks against threats,” noted Kevin Porter, Security Solutions Manager, **ProCurve Networking by HP**. “TNC support with ProCurve solutions enables our customers to select from a number of options for endpoint integrity, user authentication and other functions without compromising interoperability and scalability.”

Ben Stricker, Public Relations Manager
916-785-4599
ben.stricker@hp.com

"As the open standard for NAC and network security, TNC gives our customers and users everywhere a flexible architecture for implementing a number of endpoint integrity and other capabilities," noted Gary Ochs, **Q1 Labs**. "The addition of support for metadata in the TNC's new IF-MAP specification broadens the scope of TNC and enables additional features that will appeal to those concerned with network security."

"As a long-standing supporter of Trusted Network Connect and open standards, **Symantec** believes that the proactive endpoint compliance checking and automated remediation capabilities enabled by the TNC standards is an essential element to an enterprise's security practices." noted Paul Sangster, TNC Co-Chair and Distinguished Engineer at Symantec. "Our products can build on the open standards based architecture provided by TNC to give our customers effective solutions against the ever changing threat environment that networks face today."

"For enterprise customers concerned with the security of their networks, we at **Wave** have found that Trusted Network Connect is the choice for implementing NAC and other network security features," said Brian Berger, executive vice president, marketing and sales. "Wave's applications can leverage TNC's open architecture, interoperability with Microsoft's NAP architecture and capabilities to give customers convenient and cost-effective ways to determine who is on their network, control the introduction of malware and ensure security of corporate data and assets."

Michael Wheeler MARCOM
Wave Systems Corp.
413-243-7026
mwheeler@wavesys.com

Brian Berger, EVP Marketing & Sales
Wave Systems Corp.
949-716-3116
bberger@wavesys.com

TCG Contact: Anne Price
602-840-6495
anne@prworksonline.com