

Microsoft, TCG, Juniper Tie the NAC Knot

A lot of vendors selling a lot of components that have to agree on how to measure a lot of things have to come together to make an effective Network Access Control system.

This involves vendors of hardware, security, network security, client security and operating systems deciding how to tell who's running a system trying to access the network, whether that system's healthy, whether it needs to be quarantined, how to give it the proper level of network access and how to fix it if it's not up to snuff.

Microsoft and the Trusted Computing Group on May 21 are making an announcement that will provide the fabric to mesh much of all that.

At Interop in Las Vegas, the two are letting it be known that the TCG's TNC (Trusted Network Connect) NAC architecture will adopt Microsoft's NAP (Network Access Protection) protocol, which is primarily a client/server NAC spec.

Juniper Networks at the same time is announcing that it's working with Microsoft on interoperability between Juniper's UAC (Unified Access Control) NAC standard and Microsoft's NAP.

The NAP-TNC move streamlines customer choices in this nascent security architecture. Up until May 21, interested organizations have been faced with three standards: NAP, TNC and Cisco's NAC (Network Admission Control). At this point, the only influential NAC player left out of the loop is Cisco, since it has eschewed joining the TCG. The TCG is an industry consortium—of which Microsoft is a member—that develops open standards for computing security.

Paul Mayfield, Group Program manager of Microsoft's Windows Enterprise Networking Group, said that together with industry partners, the company will be demonstrating products based on the new protocol at Interop. "You'll see things like the Vista operating system out of the box working against a Juniper server to control the access a client receives," he said in an interview with eWEEK.

Vista supports the standard now, and the next release of Windows XP will as well. Microsoft hasn't publicly committed to a ship date yet, but the XP release is targeted near the ship of Windows Server 2008—toward the end of the year, he said. Support for the standard is being built into Windows Server 2008 as well. Other TNC members—Juniper, for example—are targeting having commercial availability of products that support the standard in the first half of next year, he said.

Mayfield said that Microsoft has heard from a number of customers that in spite of the momentum they're seeing behind the NAC industry, there's been one solution from Microsoft and one from the TCG. "[They're asking,] 'Which one do I buy?' We've driven a lot of clarity into this announcement, regarding [the question of] 'Should I buy one or the other?' They can [now] buy one. ..."

"I think it simplifies things," said Lawrence Orans, an analyst with Gartner, in an interview with eWEEK. "It's good for the industry, for organizations looking to deploy generic access control. You no longer have to choose between NAP and the TNC framework. They'll be interoperable: Components that worked in the TCG's TNC framework should also work in a NAP framework."

Steve Hanna, co-chair of the TCG TNC work group and distinguished engineer at Juniper Networks, said that deciding which of the three architectures to go with has been one barrier as technology customers try to decide how to tackle NAC, which is a complex and costly proposal that few have even begun to deploy.

"By having two major players aligning with Microsoft NAP, that's a pretty big alignment and helps make

the decision a lot easier for customers. It's going to make deployment easier for customers, too. It means somebody can take a Vista machine, which supports the NAP architecture and standards, and have it work easily with a TCG TNC implementation like Juniper's. And the Juniper server would be able to check the health of a Vista laptop or client without having to load any extra software on there. ... As long as the server and the client support the same standards," a NAC installation should be plug and play, Hanna said during an interview with eWEEK.

"That's how people want their machines to work," he said. "You plug it in and start it up and it works. From a NAC perspective, it will just work."

The first step in the interoperability of NAP and TNC will be enabled by Microsoft's contribution of its SoH (Statement of Health) protocol to the TCG. The two organizations are releasing a new spec—the IF-TNCCSSOH—on May 21 as part of the TNC architecture. Vendors, which have lined up to cheer on the integration, can begin implementing the IFTNCCS-SOH spec immediately. Microsoft and the TCG will be demonstrating the new spec at work at their Interop booths (the TCG's in booth 211 and Microsoft's at #1548) during the week.

Besides interoperability and the freedom it brings to choose best-of-breed products, the NAP-TNC merge means that customers can now start deploying TNC-based products, such as Juniper's NAC technology, and be assured that their investments will hook up to Windows Vista—which already fits into the arrangement—and Windows Server 2008 when it ships, Hanna said. Upcoming versions of Windows XP will also include the NAP Agent component as part of the core operating system.

Many networking and security companies are cheering it all on. A release from TCG quotes Symantec, trusted endpoint vendor Wave Systems, Hewlett Packard, WiFi infrastructure vendor Colubris Networks, Nortel and more, all voicing support for the move.

"Customers have made it clear that interoperability amongst the major network access control architectures and solutions is critical to helping them reduce overall cost of ownership and time to value," Karthik Krishnan, senior product line manager at Juniper Networks, was quoted as saying in the release. "Today's announcement from Microsoft and the Trusted Computing Group is a watershed event for our industry. Interoperability between Juniper Networks [UAC] and Microsoft [NAP] leveraging this new TNC specification will provide customers with greater choice, flexibility and investment protection for their network access control deployments."

As much as vendors would like us to believe that interoperability has been keeping customers from deploying NAC—and it has, indeed, been one hampering factor—there are other issues keeping the platform from bursting onto the scene, even though enterprises are definitely interested.

"We're seeing a lot of interest in NAC from our clients," Gartner's Orans said. "A lot of large organizations are very interested in NAC. But there hasn't been many large implementations. Where we are now, people are looking at pilots and small projects ..."

"[But] I don't think they've been put off by the variety of standards. That hasn't been an overriding obstacle. Complexity is an obstacle, and price has been an obstacle. There are a few options: an infrastructure-based approach, which hasn't been ready for primetime yet. NAP isn't available because Longhorn [aka Windows Server 2008] is not available yet."

Specifically, Cisco switches, which provide enforcement, aren't ready yet. Instead, Cisco has been pushing its NAC appliance, but those too can be expensive. Another approach to NAC is to use endpoint agents. There, however, you have yet another agent syndrome, Orans said. "A lot [of enterprises] don't want

another agent out there on their PCs."

There are too many operational issues associated to NAC. Enterprises aren't necessarily enthusiastic about quarantining users and keeping them off the network. "That can be a political problem," Orans said. "Those are all reasons for the slowness in adoption of NAC."

As for Cisco's absence in the TCG, Orans pointed out that the company has submitted its NAC proposals through the IETF, so it is certainly not shying away from open standards. "You can make the argument that the IETF is a true standards body while the TCG is just this industry consortium," he said.

And, given Cisco's installed base and influence in the market, it doesn't have to participate in the TCG if it doesn't choose to, Orans pointed out. Besides, as it is, many of Cisco's NAC products are interoperable with Microsoft's, including its 802.1X switches and wireless access points.

"We can use any Cisco switch or wireless access point as enforcement points, because of the standards they already support," Mayfield said. "It would be nice to have other Cisco stuff there as well. [But] from an architecture standpoint, you could buy a Juniper or Microsoft server and a Vista laptop, because of [this] interoperability. We don't really need anything [from Cisco]. But you wouldn't get the ability to have a Cisco decision point and a Juniper client or something like that."

"We'd be glad to have them join [the TCG]," Hanna said. "But the fact that they're not a member doesn't mean their equipment can't participate in a TNC environment. Their stuff supports 802.1x, and Radius, so we can use [Cisco products] in some parts of the architecture."

Another aspect to the news is that stronger security is coming to the table with the TCG's TPM (Trusted Platform Module). The TPM is a hardware/software chip or function built into a laptop or desktop. All commercial-grade machines shipping now include this chip, often built into the chip set on the motherboard.

The TPM has manifold security functions. One is disk encryption, which ensures that a lost or stolen system won't give up its data. The TPM is also used for strong authentication, much like a smart card built into the motherboard.

Also, TPM enables a trusted boot. When a machine boots up, everything that loads onto the system machine gets checked. If any infection, such as a rootkit or virus, is lurking on the machine, the TPM picks up on it. When the system attempts to connect back up to the network, the server then discovers the infection and is ready to quarantine the system. That's much stronger security than NAC alone gives with its checking of up-to-date patches and anti-virus signatures, given that NAC can't get to the hardware level to see what's on a machine preboot, Hanna said.

Preboot security checks relate to hardware hacking that's recently been discovered by security researcher Joanna Rutkowska. Rutkowska has specifically focused on PCI cards, for example, and how they can be fooled by virtualization software.

"A rootkit is an example of virtualization being used for bad purposes," Hanna said. "[Rutkowska] says what if you have an evil rootkit on a machine, can a [PCI] card detect it? The answer is no, unfortunately. This TPM module, because it comes before software runs on a machine, it can detect rootkits."

Copyright 2007 by Ziff Davis Media, Distributed by United Press International

This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.