7 in a Series

Industry Options for Network Access

by Steve Hultquist

The challenge of protecting the network core from unauthorized, unauthenticated, or otherwise undesirable systems is a growing concern across the industry. Historically, enterprise systems were connected to the enterprise network 24 hours a day, so IT administrators and applications could access them, keep them updated, and manage them as needed. However, mobility has changed all that.

Today, most systems do not stay connected to any one network for more than a few hours. They also tend to enter and leave multiple networks during the course of daily activities, visiting home, office, coffee shop, hotel, and other networks as the user requires. As a result, there are multiple opportunities for infection, modification, and the creation of issues on the client systems. The networking and systems industry is responding to the need to limit and control network access and three initiatives have emerged: Cisco Systems Network Admission Control (NAC), Microsoft's Network Access Protection (NAP), and the Trusted Computing Group's (TCG) Trusted Network Connect (TNC).

As you might expect, Cisco has focused on network-centric actions to enforce network policies, Microsoft has focused on the systems elements necessary, and the TCG has focused on the standards necessary for creating interoperable environments for network access. Microsoft and Cisco are in a partnership to have NAC and NAP be compatible. However, TCG’s focus is on interoperability and driving industry standards in network admissions and access control. Furthermore, Microsoft and TCG have recently announced that Microsoft would have their NAP architectures compatible with the TNC definitions and be designed to be interoperable with the TNC.

NAC

Cisco's NAC uses the network infrastructure and related systems (such as AAA and 802.1x) to ensure that the network can only be accessed by trusted devices that comply with defined network policies, including anti-virus, operation system version, patches, and the like. As a result of this examination, devices may be allowed access to the network, denied, or given access only to a quarantine network from which they can remediate any issues.
Cisco’s initial version of NAC is a layer 3 solution, but they have plans for a future version that acts on layer 2.

NAP

Microsoft's NAP is a Windows policy enforcement platform that allows the setting of policies to restrict clients from accessing a network until the clients can prove compliance. Again, the focus is on client compliance in areas such as anti-virus, operating system, and related vulnerabilities. According to Microsoft, NAP is scheduled for delivery with Microsoft's next version of Windows (code-named "Longhorn").

NAP and NAC

According to Microsoft, their partnership with Cisco to provide compatibility between NAP and NAC "...will allow customers to integrate the embedded security capabilities of Cisco's network infrastructure with those of Microsoft Windows, enabling customers to choose components and implement a single, coordinated solution."

TNC

Trusted Computing Group's TNC is an effort to "develop specifications for interoperable security solutions that will assist network administrators in protecting networks from viruses, worms, and denial of service attacks by allowing them to enforce security policies to prevent untrusted systems or devices from connecting to their networks." (https://www.trustedcomputinggroup.org/downloads/TNC_NI_collateral_10_may_(2).pdf) As an organization focused on standards, the TNC will use existing standards when possible, and develop new standards as necessary to enable interoperable solutions across multi-vendor environments. The standards are likely to comprise both software interfaces and protocols as necessary. The focus of the TNC is very similar to that of NAC and NAP: setting of policies by administrators; measuring devices against the policies prior to network connection; and identifying, quarantining, and remediating non-compliant devices. The TNC furthermore will make use of 802.1x, EAP, and related standards.

TCG’s initial version of TNC is a layer 2 solution, but they have plans for a future version that acts on layer 3.