

What is Microsoft's Network Access Protection?

The most significant differences between Microsoft's Network Access Protection architecture and other NAC architectures you see in the iLabs come because Microsoft simply doesn't make switches or routers. Therefore, the path for handling enforcement was different, focusing on server enforcement rather than switch. MS-NAP is not designed as a security system, but for the purpose of finding, and quarantining, non-compliant clients in the enterprise LAN. As the interest in NAC has increased, Microsoft has adjusted their architecture to include many more enforcement components, and it's the 802.1X part of MS-NAP that we tested for interoperability in the iLabs.

It's important to realize that MS-NAP is part of Microsoft's Vista/ Longhorn product, which means that it is a minimum of 9 months away from full availability. This means that any testing you do of MS-NAP is complicated by the client and server platforms, neither of which have entered public beta testing. Microsoft has stated that it will back-port NAP to Windows XP as they have done with other security technologies bound to "new" versions of Windows. (The 802.1X supplicant and IPsec client are good examples of this). But if this happens, it likely won't be until after Vista (the Windows client platform) ships and probably around the Longhorn (the server platform) release.

When reading this white paper, you may find it helpful to have at hand our companion white paper, "Network Access Control Architecture Alphabet Soup," with the diagram showing the different parts of a NAC architecture.

Access Requestor in MS-NAP

Following the common NAC architecture, the Microsoft client side is broken into three parts. At the top are the System Health Agents, taking on the function of collecting end-point security information about the client, such as the state of the anti-virus software or whether the firewall has the right policy. Currently only Microsoft has provided a System Health Validator, but many 3rd parties have declared their intent to provide System Health Validators of their own. These agents are responsible for generating Statements of Health that can be used to assess end-point security. Tying the System Health Agents into the rest of the architecture is Microsoft's Network Access Protection Agent, analogous to the IETF's Client Broker component. Below the Network Access Protection Agent are Microsoft's Enforcement Clients, which match up to the Network Access Requestor. MS-NAP includes 802.1X supplicant and VPN enforcement clients as typically found in other architectures, but also includes DHCP clients as an enforcement option.

More importantly, though, is that Microsoft has defined the API connecting its three layers of Network Access Protection on the client. By creating an API that describes how the three pieces of the client will fit together, Microsoft eliminates an enormous amount of risk and variability in the entire Network Access Control space. The Microsoft API provides a defined method for third party vendors to integrate their products into the MS-NAP solution. Even if Microsoft's entire Network Access Protection product plans were jettisoned internally, the contribution of having these defined APIs shipping with Windows cannot be underestimated.

Of course, the trick will be convincing every other NAC architect in the industry that Microsoft's API is both necessary to a good NAC design and sufficient for the task. No vendor is proposing to make this middleware piece a moneymaking differentiator. It simply exists to let desktop security vendors have a way of communicating the status of their products back to the Policy Decision Points. By simply adopting Microsoft's model, which happens to mesh almost perfectly with the other important NAC models, IT managers won't have to worry about interoperability or vendor lock-in at that point in the scheme.

Policy Enforcement in MS-NAP

The role of Policy Enforcement Point in Microsoft's architecture is assumed by Enforcement Servers. Because Microsoft doesn't make switch or router hardware, its engineers originally envisioned access control enforcement as a service rather than a choke-point type control that a company like Cisco might consider as the more natural approach.

With Vista/Longhorn, Microsoft says it will release Enforcement Servers as part of its own Routing and Remote Access Service (RRAS) -based VPN servers, operating for both PPTP and L2TP as well as at the IPsec layer. It's very clear from the public documents Microsoft has released that it views Network Access Protection primarily as a tool for giving end users either no access, full access, or limited access to some sort of remediation and quarantine network. The lack of a firm place for authentication in Microsoft's architecture shows the heritage of this product family, primarily designed to help existing managed desktops and laptops in a Microsoft domain environment stay compliant with end point security policies, rather than as a generic network access control mechanism. However, because of the addition of 802.1X to the MS-NAP model, the access control limitations are more an issue of switch capability rather than MS-NAP capability.

At the back end Policy Decision Point, Microsoft offers up its new Network Policy Server (to ship with Longhorn server), a RADIUS-based server replacing Microsoft's older Internet Authentication Service. The Network Policy Server contains the functionality of the Network Access Authority, including authentication and policy management, with a separate Network Access Protection Administration Server which handles the same functions of the IETF's Server Broker component, gluing the authentication server to third-party health verifier plug-ins. On top of the Administration Server, using a Microsoft-defined API, are System Health Validators, the equivalent of IETF-defined Posture Verifiers, which receive Statements of Health from System Health Agents on the client and provide answers back to the Administration Server.

Like other new NAC architectures, MS-NAP is accompanied by a great deal of hand waving when it comes to the actual protocols and data streams involved in making the client, the Enforcement Server, and the Network Policy Server all talk to each other. In the case of Microsoft's original DHCP and Routing and Remote Access Service-based Enforcement Servers, it's all Microsoft software, so having an open protocol is not really critical. However, when it comes to the 802.1X Enforcement Servers, the MS-NAP that we tested has no special support access control beyond what a network manager might manually configure into 802.1X switches.

Microsoft's Big Picture

The diagram below, taken from one of the MS-NAP architecture white papers, summarizes the components and protocols that Microsoft sees as part of their NAC architecture. An interesting twist on other NAC architectures is the Health Certificate Server device marked "HCS". This is key to the concept of a "Health Certificate." Using a combination of existing products to create a Web-based PKI server (called the Health Certificate Server), MS-NAP supports the idea of creating a digital certificate that can be used in place of Statements of Health. Rather than try and send Statements of Health around at authentication time, a client proves its health to the Health Certificate Server using normal System Health Agents and Statements of Health over an HTTP/S connection. It then receives a digital certificate that it can use as a statement of health (instead of normal user credentials for authentication) when using VPN connections, thus providing a faster connection to the end user.

