

Network Access Control

Opus One's **JOEL SNYDER** asks the questions as Symantec Network Access Control's **PATRICK WHEELER** discusses network access control



Windows XP Service Pack 3 (SP3) has just been released, completing the deployment of Microsoft's initial network access protection (NAP) architecture. How is Symantec Network Access Control going to fit into this Microsoft NAP world, and what does that mean for Symantec Network Access Control customers?

PW Microsoft NAP has been a great addition to the Network Access Control (NAC) space and offers a new option to customers who are looking to provide NAC in their environments. Symantec has had a solution in this space for some time, based on the original Sygate solution. Since the Sygate acquisition, we have been very active in moving it forward.

Symantec Network Access Control has three main components. The first is our policy manager, which is called Symantec Endpoint Protection Manager, the same policy manager used to manage Symantec Endpoint Protection 11.0. Endpoint personal firewall policies, antivirus policies, LiveUpdate policies, device control and NAC are all done in one place. This consolidated policy management is very important to our users. From the client perspective, we have a persistent client, as well as other assessment options for endpoints that do not have our agents on them. NAP fits into Symantec NAC around our Enforcers. Enforcers are devices that sit in the network and run as appliances or server-side plug-ins; for example, inline behind a virtual private network (VPN) gateway or wireless access point, or connected to an 802.1X enabled switch as a RADIUS proxy. These Enforcers are the devices that talk to the clients, challenge them for their compliance status and then make the enforcement decisions to allow or deny them on the network based on whether they are compliant. When we looked at Microsoft NAP, we saw the opportunity to allow the customer to leverage their Microsoft infrastructure. Instead of using a LAN enforcer appliance, for example, the customer can leverage their NPS server and do 802.1X-based enforcement using their NPS server. This also allows the customer to streamline their deployments. In that regard, NAP is another of several enforcement options in Symantec NAC 11.0. We have 802.1X-based LAN enforcement and DHCP-based enforcement for users on the LAN. Our Microsoft NAP enforcement option has a plug-in called the Integrated NAP Enforcer that runs directly on the Microsoft NPS, essentially as system health validator (SHV). In addition, we have inline Gateway Enforcement, and for the customer who wants the basics, we have the Self Enforcement option. This option uses the personal firewall of the client to provide host-based assessment and enforcement.

In the world of NAP, there is Symantec Endpoint Protection V11, which just came out. Can we do anything with Symantec Network Access Control Endpoint Protection and Microsoft NAP pre-Windows XP SP3?

PW Yes. Because Symantec NAC allows deployment and management in a single environment with multiple enforcement options, customers who are using Symantec Endpoint Protection, or even just the standalone Symantec NAC

client, can actually do NAC for clients back to XP SP2, Windows 2000 and for on-demand clients for Windows. Policies can all be managed together in the Symantec Endpoint Protection Manager. Hence, it is unnecessary to have two different management environments for your client NAC compliance policies.

The critical issue is going to be the debugging and reporting question. Where are the reports going to show up? Is there concern about network managers suddenly being on unfamiliar territory?

PW The technical answer is that within the Symantec Endpoint Protection Manager, we have logs and reporting from the client and the NAP Enforcer. You can create user roles and granular access for users based on groups or resources within the policy manager. This way, your network administrators can easily access the logs and the reporting needed for troubleshooting your NAP enforcement. At the same time, if they are familiar with the NPS interface, our Integrated NAP Enforcer also displays logs for the client and for the system logs for the Enforcer; the system logs for the Enforcer record actions such as "client detected" or "client blocked," so the NAC administrator or policy manager can get this information directly from the server. From a practical perspective, however, we are seeing that NAC administration is shifting from the network managers to the domain of the security and endpoint managers, for whom network access control is really an extension of their overall endpoint protection strategy. This is why having the ability to manage Symantec Endpoint Protection and Symantec NAC policies in the same policy manager console is so important.

What value does Symantec add to NAP?

PW There are a couple of areas in which Symantec can extend and augment the native capabilities of Microsoft NAP. The first is in the checking capabilities themselves. Within the Microsoft framework, the predefined checking capabilities are fairly coarse in that you do not have quite as many options for granular monitoring. We include a very robust, unique checking capability that allows users to create their own checks. Additionally, we configure policies and apply them to client groups in the policy manager. You can actually have clients with different policies all report their statuses to an NPS using the Symantec Integrated NAP Enforcer. This provides much more flexibility for end-users, especially from a policy perspective.

Do you do that by Active Directory (AD) groups or physical location?

PW Sure. User groups and client groups in the policy manager can be configured either based on location, other business criteria or be imported as OUs from AD, which gives you the ability to define your Symantec Endpoint Protection Manager



environment so that it mirrors your preexisting production environment. You can apply one policy to the top level group and have it propagate down to all groups below using automated inheritance. Alternatively, you can actually then break out the policies a bit more granularly and have, for example, a power users group, IT group or a marketing group that each has different policies. From an enforcement perspective, this provides the control and flexibility needed for a solution to be workable in an enterprise environment.

We've been talking about Microsoft NAP-based enforcement so far, but I know Symantec Network Access Control has other enforcement options. Can you describe them?

PW Certainly. Symantec Network Access Control covers the spectrum of enforcement options, from host-based to network-based. First, there is self-enforcement. This is where the Symantec Endpoint Protection client leverages the personal firewall on the client to essentially self-quarantine the client. When the client connects to the network, it can check itself for its host integrity compliance status. If it is compliant it continues on its way; if it is not, it can dynamically change to a quarantined personal firewall policy that can restrict its access to certain IP addresses, subnets, ports, protocols and services. All of the rule options that you can configure for your Symantec Endpoint Protection personal firewall are available in the quarantine firewall policy. Self-enforcement is often a very attractive option for the customer who is looking to get started with NAC; it allows the customer to deploy Symantec NAC on his Symantec Endpoint Protection 11.0 client without having to add another agent or deploy anything in the network. We have also recently added a Peer-to-peer Enforcement mode, in which clients communicate directly with each other and enforce compliance locally, rather than relying on a network-based Enforcer. In the Peer-to-peer Enforcement mode, there is a requestor and an authenticator: the authenticator challenges the client for its compliance status and its client ID to verify its status before allowing it to connect.

What about on the network level?

PW On the network level, we have a range of offerings. For remote clients, we have Gateway Enforcement, which is an appliance that is deployed inline behind a VPN or a WAN link. It can block a client based on its compliance status, and it is a transparent Ethernet bridge, so it is a very easily deployed solution. For the

endpoints on the LAN, Symantec Network Access Control offers two options. We have DHCP based enforcement, where we can use an Enforcer that resides directly on a Microsoft DHCP server, or an inline appliance that sits in front of any DHCP server. Essentially, we insert ourselves in the DHCP request process, challenge clients and then either quarantine clients or allow them on the network based on their compliance status. At the end of the enforcement spectrum is our LAN Enforcement mode, which is 802.1X-based enforcement. In this case, the LAN Enforcer interoperates with an 802.1X-enabled switch, essentially configured as a RADIUS proxy. It is vendor neutral; as long as the switch follows the 802.1X standards, our LAN Enforcer will work well with it.

Suppose someone wants to pursue a NAC based on Microsoft NAP. Let's assume they already have Symantec Network Access Control Endpoint Protection or an earlier version. What does the customer need to add in terms of licensing to use this with Microsoft NAP?

PW Symantec Network Access Control is available in two editions. There is a full edition that includes all of the enforcement options that I just described. Then, there is Symantec NAC 11.0 Starter Edition includes the ability to do Gateway Enforcement, Self-enforcement, which are the most commonly deployed NAC 'baby steps', and third party enforcement, which includes NAP integration. A customer who has, for example, Symantec Endpoint Protection 11.0 would be able to license Symantec NAC Starter Edition and use the Integrated NAP Enforcer to leverage their Microsoft infrastructure and get a NAC deployment up and running very quickly.

Great. Give me a summary of what someone is going to get when using Symantec Network Access Control Endpoint Protection as part of a large-scale NAC deployment.

PW One of the things we hear most often from customers is the concern about having to deploy an additional agent or client, whether to perform NAC or anything else. With the NAC-ready Symantec Endpoint Protection 11.0 client, you have an integrated protection client that can be the foundation for adding NAC to your environment without having to increase the number of agents that you have to manage. Symantec Endpoint Protection as part of a large scale deployment enables customers to take a "phased" approach to NAC implementation. Customers can embark on a NAC implementation focused on their managed endpoints immediately, become comfortable with this process, and then move on to their unmanaged endpoints next. **BTQ**



PATRICK WHEELER is Senior Manager for Endpoint Compliance solutions at Symantec, where he leverages more than eight years of product management and software development experience. In his current role, Wheeler drives the development and delivery of the company's market-leading Endpoint Security solutions. He also works closely with enterprise customers to understand and address their security challenges.



JOEL SNYDER is an internationally known expert in the area of telecommunications and networks, with an emphasis on security. He is currently a Senior Partner at Opus One, a consulting firm in Tucson, Arizona. As a consultant with over 25 years of experience, Dr. Snyder leads teams deploying enterprise-class messaging and security systems, designs and develops hardware and software products, and helps some of the world's largest companies and organizations with their messaging, networking, and security projects.