

Case Study: Nortel Networks

Securing the perimeter of one of the largest corporate networks in the world

Situation:

Canadian telecom equipment giant Nortel Networks faced an immense security challenge. With one of the largest remote access user bases in the world, Nortel needed a robust, strategic security solution that would give easy but secure access to its global user community, dispersed throughout North America, Asia/Australia and Europe.

Nortel's biggest task was how to continuously maintain and upgrade current security policies for this large user base, and preserve network integrity – without involving end-users in any capacity. According to Bernard Murphy, Nortel's chief security specialist, "The greatest administrative challenge or social challenge is really not to have the security 'in the face' of the user. I guess the other thing there is that the threat model is really the fact that we want to protect the computer at the source versus at the firewall. We want to defend on the perimeter, as well as directly on the machine. That's the threat model. We want to protect the data on the machine. Whether it's on the corporate network, or whether it's on the Internet."

Solution:

The clear solution to managing this vast and dispersed user base was to implement centralized control over security, since deploying solutions to thousands of PCs in a distributed environment – where each required its own policy setting – would have been unfeasible as well as insecure. According to Murphy, "The driving requirement was scalability, and the ability to centrally collect and analyze the firewall logs. Essentially what this gives you is listening posts all over the corporation. So the central management was an absolute requirement for our business needs."

Centralization of control had to be accomplished through a software platform that allowed customizable policy management, and which was flexible enough to determine how a remote user was accessing the network, and allow each different class of user to have its own security policy operative. Murphy explained, "One of the reasons we chose the software was the fact that you could customize the policy, and the policy is totally flexible in the sense that you can have a different policy whether you're on a corporate network, whether you're on the Internet, or whether you're on a VPN service. So that was one of the required features that we wanted to have, and essentially InfoExpress built that for us."

At the time of Nortel's quest for strategic security solutions, the only software that could meet these requirements – as well as interoperate with Nortel's own Contivity VPN client – was InfoExpress' CyberArmor Enterprise Personal Firewall Suite.

CyberArmor was designed to run seamlessly, without the user being aware it is in operation. In the case of the Nortel deployment, a remote user launches the Contivity client and the user logs in, the CyberArmor client detects the PC in a different state, and dynamically changes its security rules. This also comes into effect if the user is on the Internet, where dynamic implementation of security policies is even stricter.

Murphy said, "The user of the PC has no idea and personally doesn't care what policy is running so long as he's able to do his job, right? So that's the strategy, you don't want to have the security in the face of the customer."

Results:

Since fully deploying CyberArmor in January 2001, every new machine issued to Nortel remote users has had CyberArmor issued as part of the standard software load, as well as made available through SMS. According to Nortel, Cyber Armor's interoperability performed as advertised, with only perhaps 100 "trouble tickets" by users requesting admin support out of the first 15,000 deployments – a less than 0.01 percent rate of software issues.

With regard to return on investment, Murphy noted, "We've worked with InfoExpress for several years and found them very responsive to our needs. What is the return on our investment? The ROI is you don't have thousands of computers compromised. What's that worth? Well, it could be the life of your company. It's kind of hard to put an ROI on that. I guess the answer would be to turn that around – what would happen if you didn't have that? And all your computers were compromised? This is why we've invested in the personal firewall. We felt that just the antivirus software was not adequate to protect your computer. You still have to protect the machine itself, and protect the data physically on the machine."

Future:

As emerging threats begin to materialize, one issue that Nortel is concentrating on is the problem posed by "network viruses", taking advantage of network architecture and file shares, to replicate widely and attack a network from within, where antivirus software alone will not be sufficient to deal with the problem.

According to Murphy, "This is where we find that CyberArmor has really picked up, because now CyberArmor will detect that kind of activity, and report it to the IS staff, so we sort of see the industry moving from what we call a 'total moat model', to protecting the data at the PC, and we see that as an evolution. We'll see what the rate of [adopting] that will be. We expect to see some very nasty viruses that will probably destroy

thousands of computers within a corporation even though they have antivirus software on them.”

Murphy added, “CyberArmor is certainly one of the products in this space that addresses this issue – correctly. And because it’s custom-tailorable, you can even detect the fact that a virus has planted itself in the computer. It’s hard to detect, but once you detect this kind of activity, you can put a rule in the CyberArmor software to detect that kind of activity, even though you wouldn’t have a signature, if you knew the module name you could block that activity. So we see that as an evolution.”