NORTEL

Position Paper

Mitigating security threats to your VoIP network

In January 2006, Nortel engaged EWA Global Sentry, an international leader in building secure information infrastructures, to conduct a vulnerability assessment on the Nortel Communication Server 1000 (CS 1000). Results were impressive, especially when the Nortel Secure Multimedia Controller (SMC) 2450 was added to the system mix.

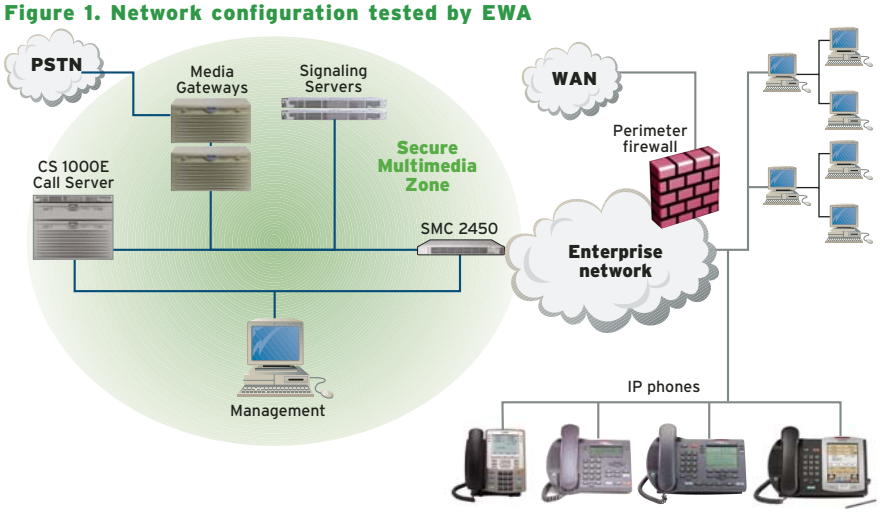
Nortel: Vigilant against security threats

Increasingly, enterprises are leveraging data networks such as the Internet to connect users. And while these converged networks offer enterprises attractive benefits such as cost savings, convenience and efficiency, they have also become attractive targets for network abuse, viruses, information theft and a host of other threats.

Converged networks can potentially expose IP PBXs and phones to a more hostile environment than their traditional counterparts. Voice over IP (VoIP) networks, for example, are far more vulnerable to hijacking, command injection and Denial of Service (DoS) than traditional networks.

"Nortel has taken the step of actively identifying security issues within its systems in order to correct them as quickly as possible, minimizing the exposure to their customers."[1]

Figure 1. Network configuration tested by EWA



Nortel and EWA Global Sentry

In 2006, Nortel hired EWA Global Sentry to perform a vulnerability assessment and penetration test (VA/PT) on the Nortel Communication Server 1000E (CS 1000E). The CS 1000 is a server-based, full-featured IP PBX that provides the benefits of advanced applications and offers more than 450 telephony features over a converged network.

The objective of the assessment and test was to identify potential threats to availability, integrity, reliability and confidentiality in a CS 1000 deployment that might subject CS 1000 users to threats such as hijacking, command injection and DoS attacks. Security assessment activities included port scanning, TCP fingerprinting, banner grabbing, Web server scanning, verification of vulnerabilities, DoS testing and protocol testing.

The results are in

Assessment results indicated that the CS 1000, when configured according to recommended security guidelines, presents a 'low level' of risk. The versions of the components tested, as deployed in the lab environment, presented no issues that were deemed high or medium risk.

[1] Nortel Enterprise Voice over IP Security Vulnerability Assessment, EWA Global Sentry, January 2006

According to EWA Global Sentry, any residual low-risk issues that did exist could be mitigated by using the SMC 2450.

A new type of firewall

The SMC 2450 is a purpose-built firewall that delivers an integrated inside threat security solution to protect Nortel's IP phones and multimedia communication servers.

Unlike other firewalls that offer only strict filtering and rate limiting between untrusted networks and the protected network, the SMC 2450 also provides the secure UNIStim protocol. This protocol implements public-key cryptography between the IP Phone and the Call Server to ensure that messages originate from the correct server and that commands cannot be replayed, thereby preventing the:

- Hijacking of ongoing sessions between the IP Phone and server
- Issuing of arbitrary commands to the IP Phone
- Disconnecting of the IP Phone from its server

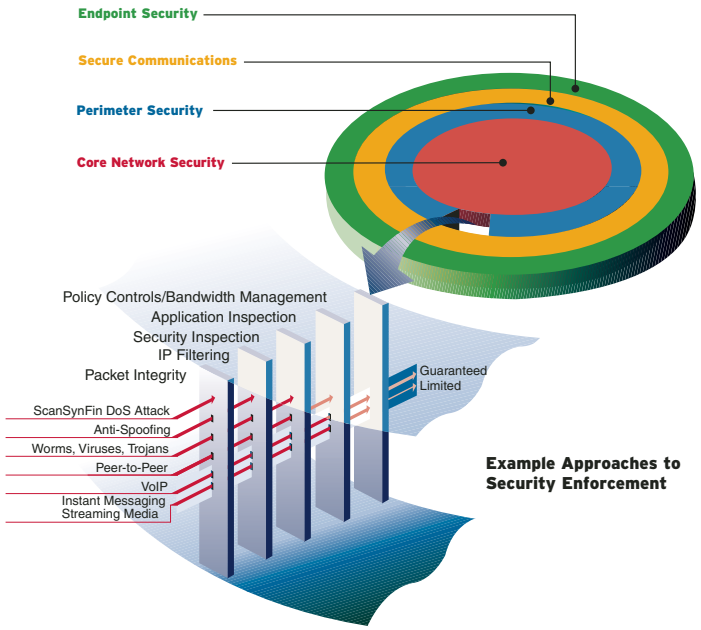
Why Nortel Secure Multimedia Solutions

Nortel is redefining the security environment for converged enterprise networks, building on our 100-year history of creating some of the world's most secure networks.

Nortel offers an array of security solutions for enterprises — from high-performance backbones to business LANs. Equipment design features enable components to protect themselves and report security aberrations to network management systems. In addition to security within network components, Nortel offers security products that protect multiple network elements and entire networks.

Nortel's Layered Defense approach to security ensures complete, end-to-end network protection for endpoints, perimeter, communications and the network core. This strategy is encompassed within a conceptual, physical and procedural framework for securing the entire IT infrastructure.

Figure 2. Nortel's Layered Defense approach



A key element of the Layered Defense strategy, Nortel's Secure Multimedia VoIP Solution enables enterprises to deploy VoIP and multimedia applications while meeting or exceeding their requirements to protect information, infrastructure and services. In particular, the Secure VoIP Multimedia Solution prevents theft of intellectual property, abuse of resources and disruption of services due to network attacks.

Conclusion

Nortel continues to build security into its portfolio of offerings, observing security best practices and validating results with third-party experts such as EWA Global Sentry — all with the objective of delivering the most advanced, secure and cost-effective solutions to enterprises.

"Assuming that Nortel continues to consider security and proactively identify and correct security issues, this low level of risk should be maintainable even with the product and threat environment evolving over time."[2]

[2] "Nortel Enterprise Voice over IP Security Vulnerability Assessment," EWA Global Sentry, January 2006.

A blueprint for securing IT infrastructures

The Nortel Unified Security Framework provides a blueprint for enterprise customers to secure their networks by considering all aspects of network security, including people, processes and technologies. One aspect of this framework is to use Nortel products to provide a layered approach to security that provides endpoint, perimeter, communications and core network security.

To access a copy of the EWA Global Sentry report, "Nortel Enterprise Voice over IP Security Vulnerability Assessment," please visit http://www.nortel.com/products/01/succession/es/collateral/cs1000_ewa_report_test.pdf.

NORTEL

NN115601-040506