



Technology Update

The Top Five Challenges to Achieving Outstanding Enterprise Security

And How to Overcome Them

NORTEL
NETWORKS™

The greater the reach and availability of an organization's network, the greater that organization is vulnerable to threats. The openness of networked communication introduces new ethical, financial and regulatory pressures to protect networks and enterprises from internal and external threats and attacks. What exactly are the requirements and vulnerabilities? What technology options and implementation choices are available? And how do you protect the network at all levels?

Every IT executive and security professional should be up-to-date on the Top Five challenges in enterprise security – and the latest recommendations to address those challenges. By doing so, they can succeed in the implementation of a conceptual, physical and procedural framework for high-performance, multi-level, multi-faceted security that protects campus networks, data centers, branch networking, remote access, wireless LANs, and IP Telephony services.

The top five security challenges have been identified as:

Challenge #1: The Internet was designed to share, not to protect

Challenge #2: The bad guys have good guns

Challenge #3: It's not enough to guard the front gate

Challenge #4: There's no stock blueprint

Challenge #5: Frisking everybody and everything takes time

The challenges and recommendations summarized below will start you on the road to achieving greater enterprise security. For those interested in a more detailed approach to these issues, a white paper is available, entitled "Unified Security Architecture for Enterprise Network Security." To download this paper, [click here](#).

Challenge #1 The Internet was designed to share, not to protect

Enterprises are leveraging IP-based intranets and the worldwide Internet to bring remote offices, mobile workers and business partners into their trusted network environments. Many businesses are capitalizing on the growing reach and reliability of IP data networks to completely redefine the way they deliver and manage corporate applications.

While this enables broader interaction with customers, the streamlining of operations, reduced operating costs and increased revenues, it also comes at a price. The very openness and ubiquity that make the Internet such a powerful business tool also make it a tremendous liability.

Simply put, the Internet was designed to share, not to protect.

The ports and portals that welcome remote sites, mobile users, customers and business partners into the trusted internal network may also be welcoming cyber-thieves and hackers who would misappropriate network resources for personal gain.

This problem has been further compounded by the growth of wireless networks. The release of the 802.11a and 802.11b standards makes wireless an almost seamless extension of an Ethernet network. As a result, Gartner Group reports 5.3 million WLAN adaptor cards shipped and 1.8 million access points installed last year alone. So with major corporations installing WLANs for customer use, wireless technology now makes the network more vulnerable than ever.

So, how do you manage mission-critical communications on an inherently insecure medium? Managing that flow is somewhat like guarding a revolving door. You can't lock it unless you also close out the traffic your business depends upon.

Have you considered closed-loop policy management?

A properly designed and implemented security policy is an absolute requirement for all types of enterprises and has to be owned by one group. It should be a living document and process, which is enforced, implemented, and updated to reflect the latest changes in the enterprise infrastructure and service requirements.

The security policy must clearly identify the resources in the enterprise that are at risk and the resulting threat mitigation methodologies. It should define which users or classes of users have access to which resources. The policy must define the use of audit trails to help locate violations and the appropriate responses.

Users think of the network in terms of people, applications, locations, time of day, etc. – not in technical terms such as firewall stateful inspection or access lists. Security policies should use non-technical vocabulary to the extent possible for user-facing issues, automatically translated by the policy management system into technical security mechanisms for network implementation.

Policy management addresses the full realm of security components – firewalls, intrusion-detection systems, access lists and filters, authentication techniques and more – along with a system-wide view of network environments such as data center, remote office and campus networks.

Ultimately, policy operates at a granular level to address pieces of the solution while providing centralizing control and accountability.

Centralization ensures that security parameters are set consistently across multiple nodes, and that multiple policies for different domains all reflect enterprise-wide policy and inter-domain consistency.

Closed-loop policy management includes configuration management of network devices, enforcement of policies in the network, and verification of network functionality via audit trails. Verification and audit trails close the loop on policy management, and result in updates to the policy to reflect corrective actions.

Challenge #2 The bad guys have good guns

Attackers have a broad repertoire of tools and techniques they can use to compromise a network. With these tools of the trade, they can launch multi-level attacks to access the network – creating an access hold to intrude upon the network and then using secondary attacks to exploit other zones.

Attackers, for example, can and do take advantage of weak user authentication and authorization tools, improper allocations of hidden space, shared privileges among applications, or even sloppy employee habits to gain unauthorized access to network resources. Even the best security technologies and procedures can be rapidly nullified unless you know the precise methods and tools being employed against you.

It is crucial, therefore, to be able to identify the various tools of the hacker trade, how they operate and what kinds of protections thwart these attacks. This includes a thorough knowledge of the following tools and techniques:

A. IP spoofing or session hijacking

IP spoofing (also known as session hijacking) is defined as: "Inserting the IP address of an unauthorized user into the transmission of an authorized user in order to gain illegal entry to a computer system.

IP spoofing is a complex attack that exploits trusted relationships. The attacker assumes the identity of a

trusted host in order to sabotage the security of the target host. As far as the target host knows, it is carrying on a conversation with a trusted host.

In this assault, the attacker first identifies a trusted host whose identity will be assumed, perhaps by first determining the "patterns of trust" for the host – that is, the range of IP addresses that the host trusts. The next step involves the disabling of the host (such as by TCP SYN flooding attacks), since the attacker will assume its identity.

IP spoofing attacks succeed because it is easy to forge IP addresses, and network-based address authentication techniques are limited. The IP spoofing attack is blind, since the attacker may not have access to the responses from the target host. However, the attacker can obtain two-way communication if routing tables are manipulated to use the spoofed source IP address. IP spoofing attacks are often used as the first step for other assaults.

B. Network sniffers

Network sniffers are basically defined as software and/or hardware that analyze traffic and detect bottlenecks and problems in a network. Using sophisticated network sniffers that can decode data from packets across all layers of the OSI model, hackers can steal user names and passwords, and use that information to launch deeper attacks.

By using sniffers, attackers can obtain valuable information about user names and passwords across public or private networks, in particular from applications such as FTP, telnet and others that send passwords in the clear. Protocols for remote access to e-mail such as IMPA, POP3 and POP2 use simple user name and password authentication techniques and are especially

susceptible to sniffer attacks.

Since users tend to reuse passwords across multiple applications and platforms, attackers can use the acquired information to obtain access to various resources on the network, where their confidentiality could be compromised. Moreover, these resources could also be used as launch pads for other attacks.

In general, attackers can use sniffers by compromising the physical security of the corporation – say, walking into the office and plugging a laptop into the network. With the growing use of wireless networks, someone in the parking lot with a wireless device can access the enterprise's local network. Gaining access to the core packet network enables the attacker to determine configurations and modes of operation for further exploitation.

C. Denial of Service (DoS) attacks

A DoS attack is defined as an assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted. Unlike a virus or worm, which can cause severe damage to databases, a DoS attack interrupts network service for a period of time. A Distributed Denial of Service (DDoS) attack uses multiple computers throughout the network that it has previously infected. All of these zombie computers work together to send out bogus messages, thereby increasing the amount of phony traffic. This prevents legitimate users from accessing their service.

DoS attacks are easy to implement and can cause significant damage, disrupting the operation of the enterprise and effectively disconnecting it from the rest of the world. They can take various forms. For example, a SYN flooding attack uses bogus half-open TCP connection

requests that exhaust memory capacity of the targeted resource.

DoS attacks exploit weaknesses in the architecture of the system under attack. In some cases, it exploits the weakness of many common Internet protocols, such as the Internet Control Message Protocol (ICMP). For example, some DoS attacks send large number of ICMP echo (ping) packets into an IP broadcast address. The packets use a spoofed IP address of a potential target. The replies coming back to the target can cripple it. These types of attacks are called smurf attacks.

D. Bucket brigade attacks

Bucket brigade attacks are also known as "man-in-the-middle" assaults. In this form of assault, the attacker intercepts messages in a public key exchange between the server and the client.

The attacker retransmits the messages, substituting their public key for another one, and in the process tricks the original entities/users into thinking they are communicating with each other. The attacker may just have access to the messages or may modify them. Network sniffers can be used to launch such attacks.

E. Back door entries

A back door or trapdoor is a secret way of gaining access to a program or online service. Back door entries to access network resources can be accidentally or intentionally opened by users and procedural oversights such as:

- Deliberately placed by system developers to allow quick access during development and not turned off upon delivery
- Placed by employees to facilitate performance of their duties
- Part of standard operating system installs that have not

been eliminated by "OS hardening," such as retaining default user logon ID and password combinations

- Placed by disgruntled employees to allow access after termination
- Created by the execution of malicious code, such as viruses

F. Masquerading

Masquerading means to pose as something you are not. Also known as elevation of privilege, masquerading enables a hacker to pose as a valid administrator or engineer to access the network. By masquerading as a user with administrative privileges, the intruder can modify accounts, configuration data, network signaling, billing data and usage data.

G. Eavesdropping

Eavesdropping is an electronic way of "listening in" on online communications. Eavesdropping takes advantage of promiscuous mode of off-the-shelf Ethernet adapters that are sold on the market.

This mode of attack enables an attacker to capture every packet on the network to listen and record data communications on the enterprise LAN. There are plenty of free network sniffers on the Web today that an attacker can use for eavesdropping

By understanding the tools of the trade of potential attackers, knowing how they function and the type of threat potential posed by the various methods, it is possible to establish a secure perimeter around any enterprise.

Have you considered uniform access management?

Obviously, it takes the coordination of many security tools and procedures to prevent such a wide range of

potential assaults. One approach, however, that goes a long way toward safeguarding the enterprise from attack is uniform access management.

Access management refers to authentication and authorization services that control a user's access to resources. During authentication, users identify themselves to the network; during authorization, the network determines user's level of privileges based on their identity as defined in policy.

Access management is controlled by multiple methods such as IP source filtering, proxies, and credential-based methods – often used in combination and each with its advantages and limitations. For example, an enterprise may choose to manage access for workstations using IP source filtering, and may choose to use a credential-based scheme for other users. Since users could be employees, network technicians, supply chain partners, inter-organization team members, or even customers, it is important to have robust centralized access control enforced by the local or remote network device interfacing to the user.

Uniform access management includes stringent authentication and role-based authorization of access to all resources for all users, with granular access policies defined at the application level and managed enterprise wide. Several methods, for example, can be used to authenticate a user, such as: permanent or one-time passwords, biometric techniques, smart cards and certificates. Password-based authentication must use strong passwords that are at least eight characters in length with at least one alphabetic, one numeric and one special character.

Where stronger authentication is required, password authentication can be combined with another

authentication and authorization process based on protocols such as RADIUS and LDAP to provide authentication, authorization and accounting services. Additionally, key management can be based on Internet Key Exchange, certificate management on Public Key Infrastructure, Certificate Management Protocol, Online Certificate Status Protocol, and Simple Certificate Validation Protocol.

Challenge #3 It's not enough to guard the front gate

Every component of the IT infrastructure is susceptible to attacks, not just obvious gateways to the Internet. Hosts, applications such as IP telephony, routers, and switches can be attacked internally and externally. At the network level, the use of firewalls, proxy servers, and user-to-session filtering can add protection, but hackers seem to get smarter all the time. Using user access control at the network and application level with appropriate authentication and authorization can minimize the risks of unauthorized access.

But the sheer diversity of the types of attacks – and the multi-level nature of many attacks – requires that IT managers understand how security breaches are instigated and be able to assess and recover from any inflicted damage. That means the only effective network security strategy is one that permeates the end-to-end architecture and enforces corporate policies on multiple levels – user, application and network – and at multiple network points.

Have you considered multi-layer security across application and network levels?

The OSI, or Open System Interconnection, model defines a

networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

Recognizing the multi-layered, interdependent nature of networks – and the critical need for security at more than the application level – security must be organized into multiple levels.

A. The Network Security Layer provides security functions at OSI layers 1 to 3 (physical, link and data layers).

Let's take a brief look at Layer 3 switching and routing security, for example. Network address translation (NAT) enables an organization to present a public IP address to the world and hide internal addresses from public view. Processing NAT in hardware with a switch is an innovative strategy for converting internal addresses into public addresses (and vice versa), making routing and firewall solutions highly efficient.

B. The Network-Assisted Security Layer provides security functions at OSI layers 4 to 7 (network to application/presentation layers) on top of the network level for added security.

Layer 4 to 7 switches, for instance, provide control services to application, management and traffic to improve resource utilization and performance, provide network scalability and offer failsafe network assurance. They are typically deployed near security devices and in server farms. Integrated security filtering offloads firewall processing of NAT, monitors network activity, protects against denial of service attacks and some virus types such as Code Red/Blue, and protects data without compromising throughput.

C. The Application Security Layer provides security in layer 7 of the OSI model, the application layer, and includes all security built into the server.

Layer 7 Deny Filters, for example, allow network administrators to create filters and assign URLs to those filters to deny certain traffic. This is particularly useful for added anti-virus protection for preventing access to disallowed Web content.

Some functions, such as access lists and VLANs, operate purely at the Network Security level. Others, such as firewalls, operate at either the Network or Network-Assisted Security Levels. Others such as Secure Sockets Layer can be viewed as network-assisted or application security. By leveraging industry-defined security functions in a structured fashion, security is tightened overall.

Challenge #4 There's no stock blueprint

There is no one exact security blueprint that works for every enterprise. Each business evolves its own unique networking environment based on business needs. So, there is no one-size-fits-all security system. And as the network is evolving, security is not a static proposition.

The "right" security strategy, then, is more of a prescription of functionality and characteristics than a stock blueprint. So, what is the "right" strategy for your organization? Such a strategy must be able to function within the bounds of any enterprise design. This includes:

* Closed Enterprise

The closed enterprise uses logical (e.g., frame relay) or physical lines between sites with PC dial access provided selectively for employees needing access into the Internet.

Web presence is achieved through an Internet data center provided by a service provider (responsible for a secure environment). The organization also provides conventional dial access for remote employees. The company uses private e-mail among employees with no external access. Wireless LANs are also starting to be used.

Despite its closed nature, such an architecture has major security concerns – not just from disgruntled internal users but also because there are a number of ‘back door’ exposures. Users with dial access to the Internet from their desktop PCs, employees surfing the Net from laptops they use at home or on the road, and wireless LANs all introduce Internet-related threats. Perhaps the greatest risk, however, comes from the specious belief that the closed enterprise is immune to external risk.

* Extended Enterprise

An extended enterprise is an extension of a closed enterprise. Web presence is still achieved via a service provider. Support for remote employee and office access over IP VPNs over the Internet is provided, delivering higher-speed, lower-cost connectivity. The enterprise provides general purpose access for all employees into the Internet, allowing them to leverage the abundance of business-related information available on the Internet. Inter-working between the internal e-mail system and the rest of the world is provided.

For the extended enterprise, the diversity of supported services and access mechanisms translates into multiple paths into the enterprise network, and, in turn, increases risk.

* Open Enterprise

The open enterprise leverages the

Internet by allowing partners, suppliers, and customers to have access to an enterprise-managed Internet Data Center, even allowing selective access to internal databases and applications (e.g., as part of a supply chain management system.). Internal and external users access the enterprise network from home, remote offices, or other networks using wired or mobile devices.

Naturally, risk increases exponentially with the open enterprise. This architecture has the greatest susceptibility to application-layer and network-layer threats, unauthorized access, and eavesdropping. Infrastructure, applications and network management systems are equally vulnerable. The most immediate and pressing element to secure, however, is the network.

Have you considered secure network operations?

On the one hand, network management is like other data applications, running on servers and workstations, complemented by application-level security and taking advantage of network-level and network-assisted security. On the other hand, network operators are specialized users who should be subject to more stringent authentication and authorization procedures.

Because of the greater access authority and functional privilege granted to network management personnel, their access and activities must be carefully secured to protect network configuration, performance and survivability. The more open the enterprise and the more centralized the network management system, the greater the requirement for stringent security for network management processes.

Secure network management requires a holistic approach, rather than a specific security feature set on a net-

work element. This must address nine critical areas:

Secure activity logs provide a verifiable trail of user or administrator activities and events generated by network devices. Secure activity logs must contain sufficient information to establish individual accountability, reconstruct past events, detect intrusion attempts, and perform after-the-fact analysis of security incidents and long-term trend analysis. Activity log information helps identify the root cause of a security problem and prevent future incidents. For example, activity logs can be used to reconstruct the sequence of events that led up to a problem.

Network operator authentication, based on strong centralized administration and enforcement of passwords, ensures that only authenticated operators gain access to management systems. Centralized administration of passwords enables enforcement of password strength and removes the need for local storage of passwords on the network elements and EMS (Element Management Systems).

Authorization for network operators uses authenticated identity to determine the user's privileges. This helps determine what systems they can access, what functions they can perform and what areas, systems and functions they are NOT permitted to access.

Encryption of network management traffic protects the confidentiality and integrity of network management data traffic – especially important with the growing use of in-band network management. Encryption provides a high degree of protection from internal and external threats, with the exception of the small group of insiders that have legitimate access to encryption keys.

Secure remote access for operators:

Security must be provided for operators and administrators who manage the network from a remote location over a public network. Providing a secure virtual private network using IPsec is the mandatory solution, as this will provide strong encryption and authentication of all remote operators.

Firewalls and VLANs partition the network to segment management devices and traffic from other, less confidential systems such as public Web servers and WLANs. The firewall controls the type of traffic that can transit the boundary between security domains.

Intrusion detection systems incorporated into management servers defend against network intrusions by warning administrators of potential security incidents such as a server compromise or DoS attack.

Hardening operating systems, used for network management, close potential security gaps in general-purpose operating systems and embedded real-time operating systems. OS hardening should use the latest procedures and patches from the OS manufacturer.

Anti-virus protection involves scanning all in-house and third-party software packages with virus-detection tools before incorporating the software into a product or network. A rigorous established process ensures that network management software is virus free.

Challenge #5 Frisking everybody and everything takes time

Anybody who has traveled by airplane recently understands that the trade-off of enhanced security is delay. The more closely you inspect bags and travelers, the longer the lines at security and the slower the journey.

Similarly, with enterprise security, turning on all facets of security features can slow Web servers and network services to a crawl as they bog down with processing-intensive encryption, decryption, key management and more. Bolting IP-VPN capabilities onto legacy routers brings its own brand of performance penalty. Voice applications, such as Webcasts and IP Telephony are very sensitive to delay and jitter and are therefore affected by traditional security mechanisms.

Have you considered variable-depth security?

It is possible to improve security while minimizing delays by introducing variable-depth security. Defining security at multiple network levels produces a security strategy where each security level builds upon the capabilities of the layer below and provides finer grained security the closer you get to resources.

VLANs provide basic network compartmentalization and segmentation, enabling business functions to be segregated in their own private local area networks, with cross-traffic from other VLAN segments strictly controlled or prohibited. The use of VLAN tags enables the segregation of traffic into specific groups such as Finance, HR, and Engineering, separating their data without leakage between disparate functions.

Perimeter and distributed firewall-filtering capabilities provide another level of protections at strategic points within the network. Firewalls enable the network to be further segmented into smaller areas, and enable secure connections to the public network. Firewalls limit access to inbound and outbound traffic to the protocols and authentication methods that are explicitly configured in the firewall. Firewalls that support Network Address Translation (NAT) enable optimization of IP addressing within the network. Firewalls provide an extra layer of access control that can be customized based on business needs. Distributed firewalls add the benefits of scalability. Personal firewalls can be deployed on end-user systems to protect application integrity.

VPNs provide an even finer granularity of user access control and personalization – enabling secure access at the individual user level from remote sites and business partners without requiring dedicated pipes.

For more information, download the white paper "Unified Security Architecture for Enterprise Network Security."



26610 Agoura Road, Suite 210, Calabasas, CA 91302

<http://www.nortelnetworks.com>

Copyright © 2003 Nortel Networks. All Rights Reserved. Nortel Networks, the Nortel Networks logo and the Globemark are trademarks of Nortel Networks. Information subject to change without notice. Nortel Networks assumes no responsibility for any errors or omissions that may appear in this document. Printed in the USA.