The Disappearance of the Trusted Network

Network Security of Varied Degrees of Untrust

January 2002

A White Paper By
NetScreen Technologies Inc.
http://www.netscreen.com

Table of Contents

Introduction

Basic network security issues have changed very little over the past decade. Protecting the confidentiality of corporate information, preventing unauthorized access, and defending against external attacks: these remain as primary concerns of IT professionals today. To defend against these threats, IT managers have historically deployed legacy security solutions whose performance was matched to the speed of the WAN. Many of today's security threats, though, are appearing inside the enterprise, forcing a new security paradigm that is WAN –and LAN– focused.

Deployment of extranets and wireless local area networks (WLANs) are turning networks inside out from a security perspective. Smarter, deadlier web-enabled worms and viruses are launching attacks from within networks. Disgruntled and dishonest employees are becoming more computer-savvy and capable of perpetrating mischievous and illegal acts.

To combat these escalated threats, enterprises must find better ways to resolve these vulnerability issues. New internal threats, together with higher-performance infrastructures, now require security solutions that match the LAN rather than the WAN. In other words, the security solution must match the infrastructure. The capabilities built into NetScreen's existing and new products provide the flexibility and performance needed to defend against attacks from all these sources and can easily adapt to the security requirements of emerging technologies.

Enterprise Network Vulnerabilities

Network vulnerabilities created by the Internet, unauthorized personnel, and telecommuter environments have been, and will continue to be, an ongoing challenge for network security professionals. The Internet exposes corporations to security risks such as denial-of-service attacks that can cripple mission-critical e-business applications, and intrusions from hackers that can sabotage or gain control of servers and other network resources. Smaller, remote office environments with corporate network access may not apply the same rigor to who accesses what desktop, opening a window for unauthorized personnel to access corporate resources.

Telecommuter and branch sites with both local Internet access and corporate VPN access can expose companies to U-turn attacks in which intruders gain access to the network behind the remote-site VPN and then use the VPN tunnel as the conduit into the trusted corporate intranet. Forcing Internet-bound traffic through the corporate VPN network, however, creates propagation delays and possible network congestion. This could impact not only the telecommuter, but mission-critical applications such as e-commerce that utilize the same central site links, resulting in potential negative economic consequences.

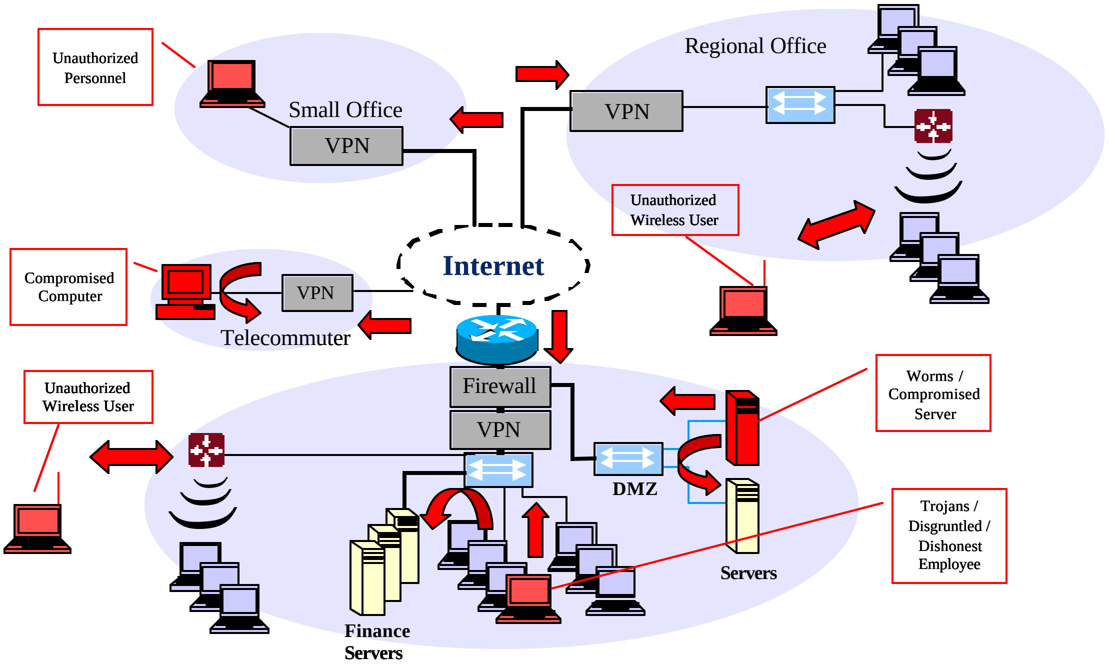

Figure 1: Common Enterprise Vulnerabilities

Historically, these threats have been addressed through existing NetScreen security solutions. However, new technologies and business models are elevating the impact of old network vulnerabilities. Changing levels of trust, Trojan Horse attacks, compromised servers, and disgruntled or dishonest employees have taken center stage in the effort to secure the network.

Changing levels of trust

With their adoption having become commonplace, extranets and partner network access no longer represent a radically new business model for enterprises. Nonetheless, IT departments responsible for security continue to struggle with their proper implementation. Today, these networks extend around the world, serving not only employees, but partners, customers, suppliers, and consultants. This business model and the technology to implement it are changing the definition of who is trusted and to what level within the organization. While the enterprise may be secure, just how secure is the partner, customer, supplier, or consultant end of the extranet connection?

Another business/technology model that has many of the same issues of trust as extranets, plus some additional technical ones, is the deployment of wireless LANs, often called WLANs. WLANs employ a broadcast medium unlike today's switched, hard-wired circuits, raising well-placed concerns about confidentiality, authentication, and trust. Security inadequacies of the current IEEE 802.11b Wireless Equivalency Protocol (WEP) have been well documented. Unlike wired networks, where an attacker must be physically connected to a network, a wireless hacker could be in a car or walking around a building in which a WLAN is installed. Inadequate encryption allows unauthorized users to either eavesdrop or use a wireless gateway to access other resources and/or potentially compromise servers. Once connected to the WLAN, intruders most likely have access to nearly all the network without further authentication.

Enterprises may choose to circumvent these security issues by banning WLAN devices in the network. The minimal cost of such devices, however, enables departments and even individuals to purchase their own WLAN equipment and connect it to the corporate network without authorization. Such bootleg devices pose a blind risk to network managers who may be better equipped to deal with WLANs by embracing them and establishing policies under which they can be controlled.

Viruses, worms, and compromised servers

Servers are prime targets for hackers and the viruses and worms they create. While a recognized problem for years, computer viruses and worms are becoming more sophisticated with the potential for greater damage. Recent examples include the Code Red and Code Blue worms that can spawn denial-of-service attacks against other networks from within compromised servers, and the Code Red II worm that additionally installs a Trojan Horse backdoor, allowing an attacker remote access to the system.

Malicious employees and Trojan Horse attacks

As enterprises struggle with levels-of-trust issues for partners, customers, suppliers, and consultants connected to the corporate network, these businesses cannot overlook their own employees, who can knowingly—and even unknowingly—initiate a security attack

As computer expertise grows among employees, the potential threat from disgruntled and dishonest staff grows as well. Unlike external threats that can be fended off with rigid firewalls, these internal attacks are carried out by individuals who are “trusted parties” at the time they commit these acts.

Disgruntled employees often launch attacks just as they are voluntarily leaving or being terminated. A disgruntled programmer at Omega Engineering, a defense contractor, for example, caused over $10 million in damages when he set off a digital bomb. Dishonest employees can cause similar losses, such as a brokerage firm clerk who altered computer records, changing the ownership and price of 1,700 shares of Logan Industries stock.

Trojan Horse attacks, on the other hand, are often launched unknowingly by employees who download attachments without proper security screening in place. Potentially destructive programs, Trojan horses can often masquerade as benign applications. These programs infect an internal workstation and then can launch attacks on the internal network. Some can even initiate external contact with a hacker, allowing the hacker to direct internal attacks by tunneling or embedding control commands inside legitimate HTTP traffic, which generally pass through traditional Internet gateway firewalls undetected.

NetScreen Solution

A properly deployed security device is the keystone for enterprise network security. NetScreen devices combine integrated firewall, network address translation (NAT), policy management, and VPN services within a single platform, simplifying network design. NetScreen devices integrate seamlessly with third-party security products like Public Key Infrastructure (PKI), RADIUS, and LDAP user authentication servers. NetScreen devices also can be deployed in redundant pairs for High Availability.

The foundation of every NetScreen device is a custom ASIC. NetScreen's GigaScreen ASIC is the first to combine encryption, authentication, PKI, and firewall acceleration in a single chip, and the first silicon-based stateful packet inspection firewall.

RISC processors used in NetScreen devices run NetScreen ScreenOS, a security-hardened, low maintenance, real-time operating system designed specifically for security enforcement in tandem with NetScreen ASICs. NetScreen ASICs and NetScreen ScreenOS cooperate to accelerate security processing. By scanning for attack signatures and selectively applying proxy technology, NetScreen ScreenOS offers exceptional defense against common denial-of-service attacks. By offering fast, robust packet inspection in a seamless fashion, NetScreen devices can form an integral part of nearly any secure network.

While traditional vulnerabilities have been largely resolved by existing NetScreen solutions, new technologies, new business models, and the ever-increasing sophistication of network attacks have lead to the need for more granular levels of permission to network resources and for encryption and attack protection measures to be available anywhere inside or outside the network. At the same time, these new security measures must substantially limit the overall performance of the network. To meet these new challenges, NetScreen has introduced new products and new capabilities.

Universal features on all interfaces

In the past, functionality was bound to specific interfaces such as the Untrust, Trust, and DMZ. Today, existing NetScreen devices, like the NetScreen-500 upgraded to the latest version of NetScreen ScreenOS, and new devices such as the NetScreen-208, have the ability to support multiple security zones, in conjunction with multiple physical interfaces (and virtual interfaces for the NetScreen-500) to provide the required additional control and segmentation. All traffic interfaces (except dedicated management or High Availability interfaces) can be activated and used for any purpose.

To provide a greater level of security, these devices now enable up to 28 firewall attack preventions that can be independently configured on all physical and virtual interfaces, not just the Untrust interface. This provides a very granular control to prevent internal and external attacks from impacting the entire network.

In addition, VPN tunnels can be terminated to any interface, not just the Untrust, and can be bound to any security zone. As a result, new network topologies, such as partner extranets and WLANs, can be more easily supported with VPN tunnels terminated to an interface in the internal security zones.

Flexible architecture that addresses individual requirements

Security zones have historically been implicit to the physical interface in products such as the NetScreen-500. For example, the DMZ interface was in the DMZ security zone. Today, the role of the interface and security are separated, each with definable and customizable parameters and characteristics, enabling extremely granular control of levels of trust and encryption. Policies are defined between security zones, and traffic management is a function of the security zone, not the interface. In addition, security zones can have multiple interfaces and sub-interfaces within them. Untrust, Trust, and DMZ will continue to exist as default security zones for ease of initial configuration and backward compatibility.

Resolving Network Vulnerabilities

Traditional enterprise vulnerabilities associated with the Internet, unauthorized personnel, and telecommuter environments have been addressed through NetScreen's integrated stateful packet inspection firewall, VPN, and traffic management solution. Robust attack prevention, encryption, authentication, and DMZs reduce the ability for unauthorized personnel to gain access to corporate resources from remote, telecommuter sites, while NetScreen's high-performance solutions are able to keep up with DoS and distributed denial of service (DDoS) attacks.

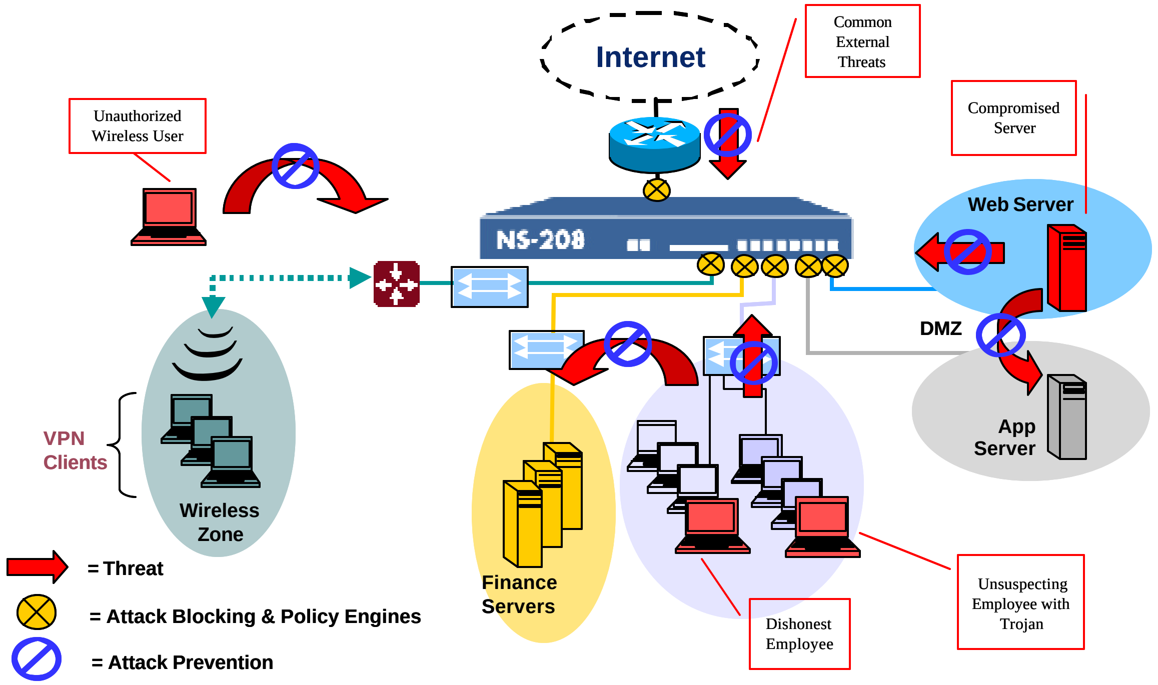

Figure 2: Resolving Emerging Vulnerabilities

Vulnerability issues involved with changing levels of trust, compromised servers, and disgruntled or dishonest employees are being dealt with more effectively through new and enhanced NetScreen systems and appliances.

NetScreen mitigates internal attacks with attack prevention on every interface and multiple interfaces on every device such as the NetScreen-208. This feature limits the impact of denial-of-service attacks from internal Trojan Horses and disgruntled employees and prevents URL attacks from being launched from compromised servers.

NetScreen also maximizes internal security with policy enforcement between every security zone. Increased network segmentation through increased interface density, and the ability to apply unique policies to every security zone, allows NetScreen devices to prevent or limit a security breach in a particular segment of the network. This additionally prevents exposure to the rest of the network from that same breach. Dishonest employees, for example, are denied access to the finance server, and a compromised server or computer can't traverse the network freely because they don't have network access, as opposed to server access control by passwords alone. Policy is applied to incoming and outgoing traffic for every security zone and user authentication can be applied for access to secured areas. For large sites where greater segmentation is required, enterprises can deploy the NetScreen-208 and the NetScreen-500, which provide up to eight physical interfaces and, in the case of the NetScreen-500, many virtual interfaces through the implementation of VLAN tagging.

With the growing popularity of extranets and WLANs, IT professionals struggle with whom or what is trusted or untrusted and what traffic must be encrypted. NetScreen solutions address these issues by allowing separate and unique security zones that can be deployed specifically for those applications. WLANs, for example, pose one of the greatest potential threats to enterprises. NetScreen's ScreenOS 3.1 and subsequent releases help protect against wireless attacks by connecting wireless LANs through separate interfaces and using a custom security zone for WLAN entry to the network. Segmenting wireless access points compartmentalizes the security and mitigates the effects of a security breach. In this way, NetScreen reduces the vulnerability where multiple points of untrust or limited trust and the need for encryption in multiple parts of the network exist.

To increase internal security, NetScreen enables a VPN termination point to be associated with the same interface. VPN clients are used to prevent eavesdropping on wireless connections. Corporate wireless traffic is decrypted and policies are applied to permit, deny, or encrypt to another destination or security zone. This is a very powerful capability. Traffic can be encrypted and authenticated. Based on that authentication, the system recognizes the source (person) and can determine to which segments on the network access can be granted.

NetScreen's platforms are designed to cope with the potential stress placed upon a network security device by an enterprise or a carrier. Beginning with its first products, and continuing with existing and new platforms, NetScreen's unique hardware design ensures that providing greater levels of security and encryption to compartmentalize or departmentalize an enterprise's security posture does not adversely impact network capacity and throughput.

Conclusion

While basic network security issues have remained largely the same, new business practices and new technologies are making these old concerns more challenging. Changing levels of trust, compromised servers, malicious employees, and the constant threat of viruses and worms are putting enterprises on the defensive. Businesses must find new ways to address these escalating vulnerabilities.

NetScreen has created a solution that is sufficiently flexible and scalable to protect against attacks from all sources, whether internal or external, and can easily adapt to the security requirements of emerging technologies. Traditional enterprise vulnerabilities have been addressed through NetScreen's integrated firewall, VPN, and traffic management solution. A high-performance solution, NetScreen appliances and systems match the performance levels of the LAN as well as the WAN, eliminating security as the chokepoint in enterprise environments.

To address evolving business models and technologies, NetScreen has introduced new products and new capabilities that provide more granular levels of permission to network resources and allow attack protection to be available anywhere inside or outside the network. New support for multiple security zones and multiple physical interfaces deliver added control and segmentation. All physical interfaces can independently have firewall and denial-of-service protections activated. VPN tunnels can now be terminated to any device, enabling extranets and WLANs to be supported more easily. In addition, the role of the interface and security has now been separated. Each interface (physical and virtual) can be assigned to separate security zones, allowing far more granular control of trust and encryption.

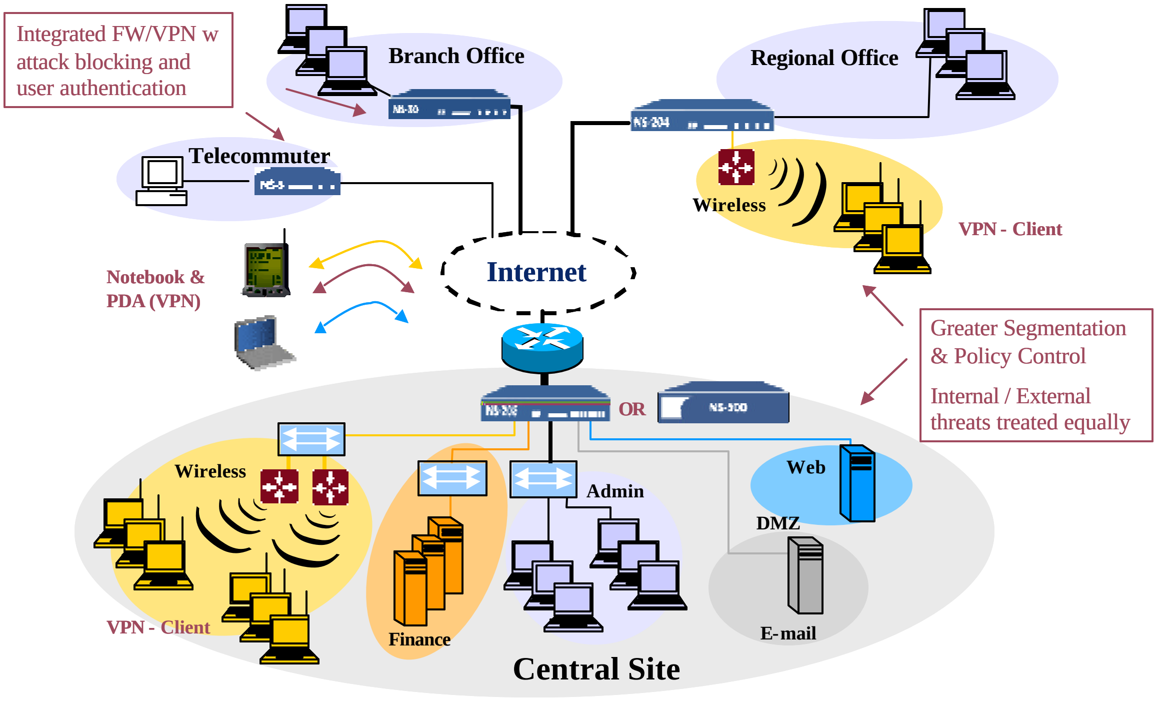

Figure 3: Addressing Existing and Emerging Vulnerabilities