AUGUST 2004

Technology Backgrounder on Network Security Basics

By Larry Hettick and Steven Taylor

Company information is as valuable a company asset as money in the bank. In fact, some information can be even more valuable than cash. So protecting the company's information with appropriate security is critical to business success. This backgrounder will provide a basic introduction to data and network security; however, it is only intended as an introductory primer so business owners and managers can begin to understand the complexity of managing security.

Security exists on many layers. Network security considerations begin with (but are not limited to) a range of considerations including:

- *how company office facilities are selected and maintained,*
- *how potential employees are screened,*
- *the remote access policy to the company's systems and information, and*
- *what kind of encryption and firewalls are provided in the corporate network.*

Best-practice security isn't just good business - in some cases, it's also the law. And the legal requirements are different for specific industries and between different jurisdictions. For example, the Health Insurance Portability and Accountability Act (HIPAA) sets requirements for patient privacy in the United States. In California, privacy laws prohibit financial institutions from sharing personal financial information with unaffiliated third party partners without the consumer's consent. And in Europe, privacy laws protect certain employee information-even to the point where inappropriately sharing an employee's name and location in a company directory can be considered a violation.

So when considering security, it is important to consider business policy and practices, legal requirements, and technology. This technology backgrounder will introduce some of the technical aspects to consider in network security, with a particular focus on network security for small and medium-sized business.

Produced By: Webtorials

Sponsored By: NORTEL NETWORKS™

The network security problem

The first building block of any network that is connected to the outside world is the virtual private network, or VPN. Virtual private networks (VPNs) permit users to share the public network infrastructure, using a variety of devices and protocols both inside and outside the network to protect users against outside intrusion for voice and data sessions.

This broad definition of a VPN may seem a bit strange to people who tend to think of a VPN in the rather narrow context of using the Internet for connectivity. In reality, essentially all networks are shared and the concept of a "private network" is a myth.

Even a "private line" service is actually part of a "Layer 1 VPN." While the private line local loop may be dedicated to a particular site, eventually the local loops are bundled into larger cables, and the lines share time division multiplexed (TDM) public facilities in the service provider's core network.

Frame relay and ATM services can be considered a "Layer 2 VPN" since they statistically multiplex users' data on packet switches at the customer location or in the carrier's core network. IP-VPNs are a Layer 3 VPN service; they can be provided on a "private" IP connection, or they can use the very public Internet for wide area connections.

Each VPN should address layer-specific security precautions. Layer 1, the private line, relies principally on physical security, since the copper loops are separated by physical barriers, and the core TDM network doesn't allow "sharing" of unreserved time slots between users. Layer 2 VPNs, like those based on Frame Relay and Asynchronous Transfer Mode (ATM) services enjoy certain built-in protection. Even though layer 2 VPNs use statistical multiplexing, their connection-oriented switching protocols don't permit easy diversion of user data to the wrong recipient.

As a connectionless protocol, IP is the least secure protocol compared to TDM, Frame Relay, or ATM; therefore, IP-VPNs can be more susceptible to security breaches than a layer 1 or layer 2 VPN. The most susceptible VPN can be an IP-VPN that uses the Internet as a wide area network, since there's nothing inherently private about the Internet or its core infrastructure.

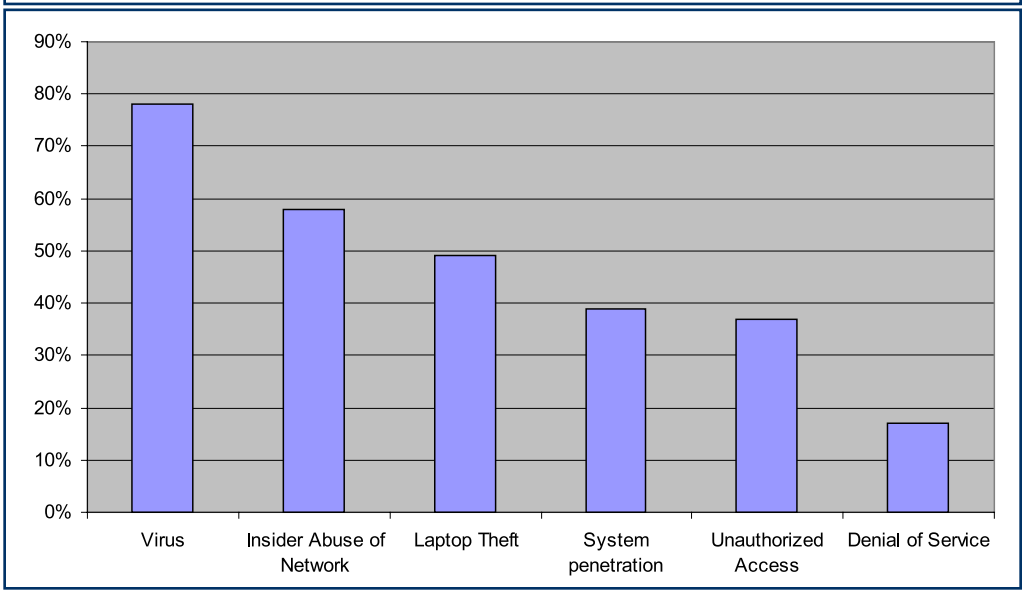
Remote access to any VPN, including dial access or remote connectivity using the Internet, also adds security holes to the network.

Protecting your network

For this discussion, computing devices like personal computers and servers are defined as part of the network. A shown in **Figure 1**, according to a 2004 survey of U. S. businesses and organizations by the Computer Security Institute (CSI) and the US Federal Bureau of Investigation (FBI), the biggest experienced threat to information security is the computer virus.

Another noteworthy finding of the survey: while denial of service attacks accounted for only 17% of attacks or misuse by category, they cost the survey's respondents over $50,000 in losses per incident. The most common way for viruses to enter the network is through email attachments

Figure 1: CSI/FBI 2004 Computer Crime and Security Survey Results. Source: http://www.gocsi.com



or files sent to employee. However, more sophisticated viruses can also be "caught" by browsing the Internet and looking at a web page.

Anti-virus software

To protect against a computer virus, every computer in the company's network must have anti-virus software, and the software must be kept current. Company IT managers should, as a minimum, configure computers for auto scan and auto update for their anti-virus protection software. Some companies have also installed software in their network that disallows a computer from gaining network access unless the network first verifies that the anti-virus software is installed and current.

Firewalls

Network firewalls are commonly used to protect against unauthorized access, system penetration, and denial of service attacks. A firewall provides "stateful inspection" of packets as they enter the network, allowing or preventing access to and from the network. Firewalls can also track and report on intrusion detection and denial of service attacks; reporting thresholds can be customized based on business requirements.

Firewalls can either be a separate hardware device or special software within a server or computer. Firewalls can be located on the business premise, they can be included as part of a service provider's network, or they can be used as a system of hybrid public and private firewalls.

Firewalls are especially important when the company's network is connected to the Internet, and when remote access is allowed by either dial access or by an Internet-based VPN. Firewalls should also be supplemented with additional measures to secure remote access. **Figure 2** shows a firewall's placement in the network.

Secure VPN: VPN Tunnels, IPSec, SSL, and Encryption

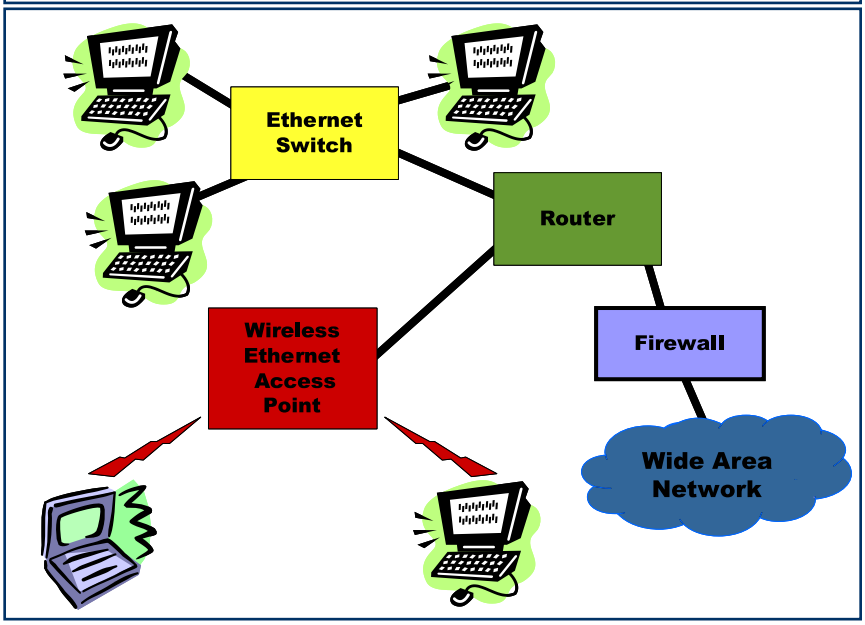
The first added measure is to include "secure tunnels" when using the Internet for wide area connections or for remote access. These "VPN tunnels" establish a secure session between the user's computer and the company's network router.

A secure VPN connection across the Internet is provided by using either Internet Protocol- (IPSec) or Secure Socket Layer (SSL) protocols. IPSec and SSL both encrypt session data to "scramble" information on one end of the session and "unscramble" it on the other end. By adding encryption, any intercepted data will be meaningless to unauthorized recipients.

IPSec runs in two modes. The first mode, called the transport mode, encrypts only the user's payload. The second mode also encrypts the routing information, and then it adds new routing information; therefore it provides additional routing functions by encapsulating the entire IP frame. In doing so, it hides original addresses from detection but adds more overhead and processing. IPSec can be created and maintained within software (for example, between a user's PC and the application's server); however; for heavy VPN users, a hardware-based VPN appliance can be deployed.

SSL was designed to offer application-level encryption specifically for web browsers. In addition to offering

Figure 2: Firewalls usually are placed between the wide area network and the router. While often deployed as a stand-alone appliance, firewalls also are integrated into both network services and other devices.



encryption, SSL can allow a server to authenticate itself to a client, and it allows a client to authenticate itself to a server. Similar to VPN appliances, an SSL accelerator is hardware-based and provides the intensive processing required to maintain SSL sessions.

Network Boundary Security

Some company networks are entirely self-contained; others don't even offer Internet access. However, most companies do allow remote access to employees; other companies even give "outsiders" like suppliers and customers access to some parts of the company network. Intra-company access offered to the LAN or by remote access is called an intranet. Multi-party access is called an extranet. While intranets are probably more secure than extranets, both intranets and extranets should include boundaries within and between the network types.

Network Address Translation and IP Address Schemes

Network address translation or NAT usually occurs between the local area networks (LAN) and the wide area Internet connection. When NAT is deployed, the LAN uses a local-only address. The LAN address is translated into the public address supplied by the Internet service provider. This approach is used because without it, the world would not have enough IP addresses for everyone.

Using NAT, local IP addresses can be duplicated on different sites without disrupting the site-specific routing. NAT provides a type of firewall by hiding internal IP addresses, and it lets a company select and use more internal IP addresses. Note that public IP addresses can be used, but buying a public IP address can be expensive since the pool of available public addresses is limited.

Added Precautions

Employee Involvement

Common sense and employee involvement are integral to preventing attack and misuse. For example, all employees should be required to use a personal network identifier (like their name) and a password to gain authorized access to the company's network, whether they are on the local area network or are using remote access. Passwords should be required to access data and applications on employee computers. Screen-savers should lock keyboards after a period of computer inactivity, requiring a password for the computer to restart. And companies should train employees to know how viruses are propagated and how to avoid them when processing email or using the World Wide Web.

Physical Security

Not to ignore the obvious, physical security is also important. Locking the doors to data centers is as important to network security as a firewall. Both limiting access to areas where employee computers and network appliances are stored and increasing mobile-warrior awareness about laptop theft are also important.

And remember, security is only as strong as the weakest link on the security chain. For example, a well-known credit card company stored their unassigned (yet active) credit card numbers on a server, providing information for "instant credit" assignments to the next new customer. Protected by IPSec, firewalls, and data-center card-keys, the bank felt their data was secure. Too bad they didn't anticipate a theft-prone employee carrying out the entire computer at the end of the workday!

Security Audits, Assessments and Policies

Professional security assessments are recommended. Systems integrators, value added resellers, equipment suppliers, service providers, and professional services firms with security practices are all available to help businesses understand their company's vulnerabilities and alternative solutions. As with all business practices, proper assessment and recommendations should include comprehensive business policies - policies that must be enforced.

Conclusions

Controlling the company's network security is all about trade-offs and making sound business decisions because no network can be completely secure. For example, military-level security techniques can be deployed by a business but such extensive techniques can discourage employees and be so costly as to turn the business into an unprofitable venture. So, every decision should be made weighing the costs of the security practice against the risk of attack or misuse.

Take, for example, using the Internet to send and receive voice calls. While the Internet is more susceptible to eavesdropping than a private line connection, in this situation businesses should consider:

- What would happen if competitors, customers, suppliers, or the general public overheard the information discussed on the call?
- What's the likelihood someone would want to listen in and misuse the information being discussed? How difficult would it be for them to do so?
- What's the relative cost versus the risk to provide secure VPN encryption for both the conversation and the signaling?
- How much more or how much less secure is the conversation when using the Internet than the same conversation using the PSTN or a private line?
- Does the cost of adding security to Internet-based calls exceed the cost savings achieved by using the Internet for a wide area connection?

In reality, every business phone call or data session that is connected to the outside world presents some security risks and uses shared public network facilities. But by taking prudent business measures and by making intelligent decisions about the risk versus the reward of security, business owners and managers should sleep a little easier at night.

Steven Taylor

Steven Taylor, consultant and broadband packet evangelist, is President of Distributed Networking Associates and Publisher of Webtorials. An independent consultant, planner, author, and teacher since 1984, Mr. Taylor is frequently quoted in the trade press and is one of the industry's most published authors and lecturers on high bandwidth networking techniques. He has served as a Contributing Editor for Data Communications magazine, publishes articles in both Business Communications Review and Network World, and co-authors two newsletters - Convergence and Wide Area Networking - distributed by Network World Fusion.

Larry Hettick

Larry Hettick has nearly 20 years of combined data communications and telecommunications experience. A capable and experienced speaker and writer, Larry possesses proven global expertise in product management and product marketing. Larry also writes for industry press, most notably as a co-author of Network World's bi-weekly Convergence Newsletter and as a periodic contributor to Business Communications Review. He is currently working as an independent consultant, specializing in the convergence market.

WEBTORIALS TECHNOLOGY BACKGROUNDER

Produced By
Webtorials, a venture of Distributed Networking Associates, Inc.
Greensboro, N.C.
www.webtorials.com

Design/Layout Artist
Debi Vozikis
dvozikis@rcn.com

For Editorial and Sponsorship Information
Contact Steven Taylor,
taylor@webtorials.com

A word from the sponsor Nortel Networks

By Anu Bandopadhay
Product Marketing Manager for Enterprise Data Networks, Security and Routing

Nortel Network has a broad range of products that provide business network security. They include:

Alteon SSL VPN – Remote access security solution that extends the reach of enterprise applications to mobile workers, telecommuters, partners and customers.

Alteon SSL Accelerator – Industry-leading platform for securing online transactions with high performance Secure Socket Layers (SSL) technology.

Alteon Switched Firewall System – Firewall System that maximizes capital investment by providing High Performance Security at a significantly lower cost than traditional solutions requiring multiple firewalls.

BayStack 325-24T Switch – Standalone Ethernet switch that provides 24 10/100BASE-TX auto-sensing ports

BayStack 325-24G Switch – Standalone Ethernet switch that provides 24 10/100BASE-TX auto-sensing ports plus 2 10/100/1000BASE-T ports for uplink connectivity to servers or core switches.

BayStack 425-24T Switch – Stackable Ethernet switch that provides 24 10/100BASE-TX auto-sensing ports, 2 flexible combo uplink ports, and built-in stacking ports.

BayStack 425-48T Switch – Stackable Ethernet switch that provides 48 10/100BASE-TX auto-sensing ports, 2 flexible combo uplink ports, and built-in stacking ports.

Contivity 1000 Secure IP Services Gateway Series – A VPN suite of products designed to serve the needs of Nortel Networks customers, the Contivity family features encrypted end-to-end connectivity with best-in-class IP Security, and bulletproof end-to-end security for branch-to-branch and remote access applications with comprehensive support of PKI for trusted extranets.

Contivity 200 VPN Switch Series – All-in-one SOHO solution that provides low cost secure connectivity across the Internet or managed IP networks to connect small offices and teleworkers into a secure corporate network.

VPN Gateway 3050 – A remote access security solution that extends the reach of enterprise applications and resources to remote users.

WLAN Security Switch 2250 – A security switch to protect and manage mobile communications transmitted over the wireless LAN.

For more information on Nortel Networks, SMB-related news, events, and additional information, visit our website at: http://www.nortelnetworks.com/solutions/smb/