Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing the Broadband Network

This paper addresses combining broadband access technologies with integrated security solutions, so enterprises and service providers can safely and securely capitalize on all of the benefits of the broadband Internet.

Copyright SANS Institute
Author Retains Full Rights

AD

SECURING THE BROADBAND NETWORK

Submitted by: Sushilkumar Nahar
Submitted on: August 9, 2001
Version 1.2e

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Securing the Broadband Network

Introduction

"**Broadband**" describes a medium that can carry signals from multiple independent network carriers on a single coaxial or fiber optic cable by establishing different bandwidth channel. Broadband in the general term also referred to high-speed network connections. In this context, Internet connections via cable modem and Digital Subscriber Line (DSL) are frequently referred to as broadband Internet connections. Most current dial-up modems can support a bandwidth of 56 kbps (thousand bits per second). There is no set bandwidth threshold required for a connection to be referred to as "broadband", but it is typical for connections in excess of 1 Megabit-per-second (Mbps) to be so named.

Cable modem - allows a single computer (or network of computers) to connect to the Internet via the cable TV network. The cable modem usually has an Ethernet LAN (Local Area Network) connection to the computer, and is capable of speeds in excess of 5 Mbps.

DSL- is based on the phone systems regular copper wires. Digital Subscriber Line (DSL) Internet connectivity, unlike cable modem-based service, provides the user with dedicated bandwidth. However, the maximum bandwidth available to DSL users is usually lower than the maximum cable modem rate because of differences in their respective network technologies. The DSL providers offer little or no guarantee of bandwidth all the way across the Internet. Following are the variants of DSL.

ADSL or Asymmetric Digital Subscriber Line is a new form of technology, which allows very high bandwidth over standard copper telephone wires. When you have DSL installed, the local phone company provisions your line by adding a single twisted pair of network cables to your line at your local office. DSL lines can carry voice and data to allow simultaneous transfers. ADSL provides speeds up to 8 Mbps downstream (to the user) and up to 1 Mbps upstream, depending upon line length and loop and line conditions.

SDSL is Symmetric Digital Subscriber Line, which can carry same amount of data in both directions i.e. upstream & downstream.

VDSL is DSL delivered over fiber.

RADSL is *rate adaptive* DSL, this means speed dynamically varies according to line conditions.

IDSL is based on ISDN technology.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The Dark Side of an 'Always-On' Connection

While the benefits are compelling, there are still a number of challenges with moving to the broadband Internet. Spotty geographic coverage and installation challenges are a significant impediment. As cable and DSL providers accelerate their deployment plans, this situation is improving, but there are still significant challenges. Network security is another very significant issue, and one that is becoming increasingly visible as hacker attacks on home PCs and major web sites escalate.

Broadband introduces two new security challenges:

a. Increased vulnerability to hacker attacks, and
b. Establishing secure connections to other networks across a public IP network (see Figure 1).

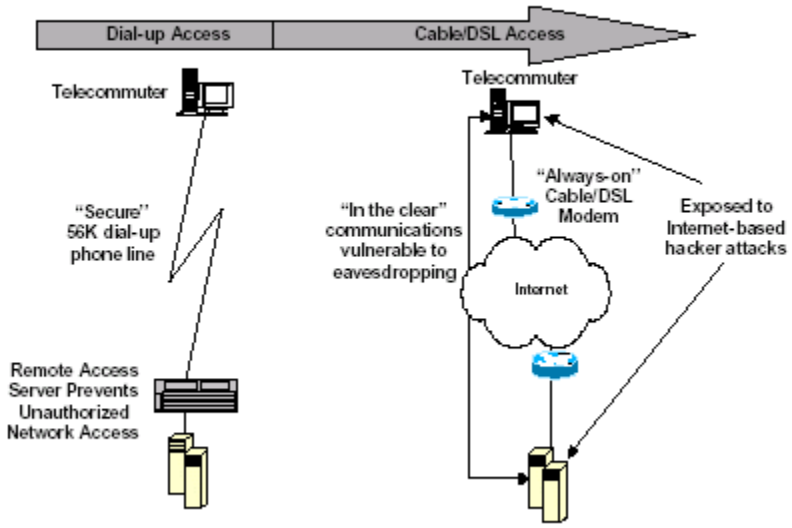

Figure 1: Broadband Access Security Challenges

Hacker attacks are a more significant issue on broadband attached networks for two major reasons.

1. These are "**always-on**" connections meaning that a hacker can attempt to breach security at odd hours when no one is likely to notice.

2. Further, these connections often use static IP addresses so a hacker can consistently come back to the site to work on their attacks.

Hackers have easy-to-use tools that can scan the Internet looking for insecure computers. Many broadband users report that their computers are scanned 2 or 3 times every day by hackers looking for vulnerabilities. DSLReports.com recently reported that 97% of the broadband attached PCs they tested had some security issues.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

A most common mistake is to turn on Windows file and printer sharing, which then makes the computer visible and accessible to the outside world. Once a hacker has compromised a system they can steal sensitive information, maliciously damage files or uses the computer to launch attacks on other sites including some recent high profile denial of service attacks. Following the recent high profile attacks on Yahoo, eBay, and other sites, an unsuspecting broadband users PC was seized by authorities in Oregon after it was determined that his PC had been one of the “Zombies” used to launch the attacks. Fortunately, easy-to-use, high-performance broadband security appliances are now available that can eliminate these security holes.

SOHO Security Issues

SOHO attached to the broadband Internet need to make sure they have a firewall security solution in place that can allow employees to access the Internet, while preventing unauthorized access to the internal network (see Figure 2). If they want to run a web server on their premises it will require that they add more sophisticated security policies to allow outsiders web access to just that server and not the rest of the network. Other security functions they may want include: deterring denial of service attacks launched against their network, preventing the launch of a DoS attack from within their network (e.g., prevent IP spoofing), and implementing URL filtering to prevent employees from surfing to inappropriate web sites.

Figure 2: Secure Small Business with a Locally Run Web Server

Until recently, most small businesses were blissfully unaware of the security issues associated with attaching their company to the Internet. However, recent publicity about hacker attacks launched on companies, or launched from a company’s PCs that have been taken over by hackers has significantly increased awareness of security issues. These small businesses may want to buy and manage their own security product, but in most cases they will be unsophisticated users who would prefer to have their service provider or a VAR install and manage their security solution.
In many cases, it is becoming a requirement for service providers to deliver an effective security solution. In other cases, an incremental revenue opportunity can be capitalized

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

on by offering a managed security service. An affordable, easy-to-deploy appliance, combined with centralized management and service provider class features are required for a service provider to cost effectively deliver a managed security service.

Extending the Enterprise Security Perimeter to Branch Offices and Telecommuters

One of the most compelling uses of broadband connections is to allow enterprises to connect branch offices and telecommuters into the corporate network with high-speed remote access. Broadband connections can significantly reduce access charges compared to slow dial-up lines, which will often require a long distance call be made to connect to the central site.

Virtual Private Network (VPN) technology using IPSec encryption is the key enabler that allows the enterprise to extend their network out to these branch offices and telecommuters. VPNs use public IP infrastructures, such as the Internet, as the network backbone to securely interconnect company sites, mobile workers and telecommuters--substantially reducing the costs associated with previously available solutions. According to industry analysts, VPNs are nearly half as expensive as dedicated networks and about a quarter cheaper than frame relay networks. Utilizing a VPN for remote access connections can save enterprises anywhere from 30 percent to 70 percent, analysts' report.
Telecommuters can connect back to the corporate network by installing VPN client software on their PC, which creates an encrypted tunnel from the PC to a VPN gateway at the central site. However, many enterprises run into issues with using just VPN client software for these telecommuters. These issues include:

- Challenge of installing and updating networking software on a large number of remote PCs

- Lack of client availability for many operating systems other than Windows – Linux, Mac, Solaris, BSDI clients are hard to find and if IS can find them they need to deal with installation issues, compatibility issues and support issues across a large number of platforms

- Lack of security on the remote PC which is being used for confidential corporate work

- Creating new security holes, which allow hackers to breach the corporate network security through a U-turn attack on the remote PC (see Figure 3). In a U-turn attack the hacker gains access to the insecure telecommuter PC and then uses that PC to connect into the corporate network via the VPN tunnel which gives them full access to the corporate network and compromises the enterprise security infrastructure.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

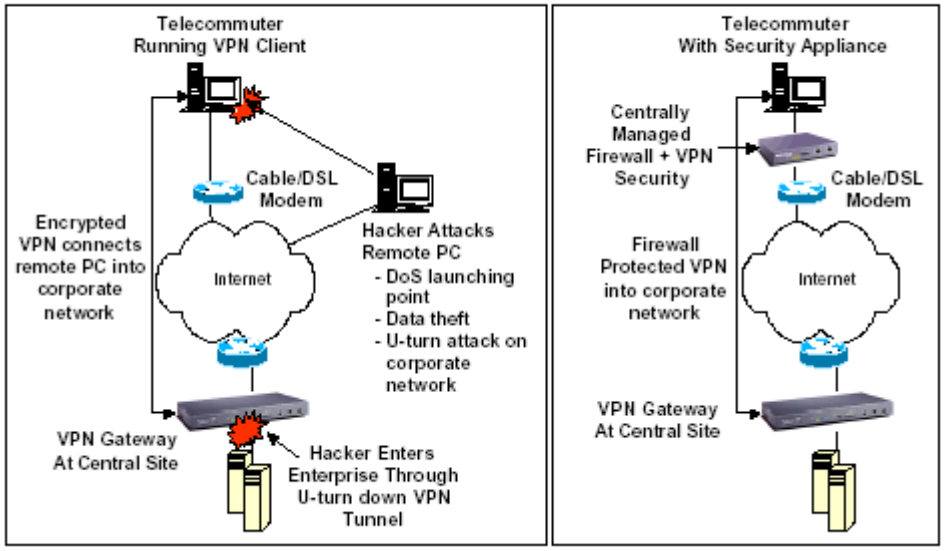

Figure 3: Secure VPN Access to Corporate Network via Security Appliance

Another security issues associated with extending the enterprise network to branch offices and telecommuters is the fact that these corporate computers could be compromised and used as launching points for other attacks, which creates a potential liability for the enterprise.

Broadband Network Security Solution Tips

It is recommended to look at following security solutions:

1. Firewall: The Firewall enforces an access control policy between two networks. Firewalls could be Software like Checkpoint, Symantec, CA or Hardware appliance based like NetScreen, Watchguard, Sonicwall, Nokia etc. Home users can even look for personal firewall solutions like Network ICE, Symantec etc.

2. Anti-Virus: Anti-Virus look for patterns in the files or memory of your computer that indicate possible presence of a known virus. Anti-virus software like Norton, McAfee, TrendMicro, CA etc. is highly recommended for use with any broadband connection.

3. Encryption: For communications, which are particularly sensitive then, you should consider encrypting traffic at your PC. The Firewall with VPN protection secures sensitive data at the remote site and prevents both U-turn attacks and the launching of denial of service attacks from these computers VPN, SSL provide secure means of e-commerce transactions. Products like NetScreen PGP, PKI solutions, Cisco etc. can be looked into as per the business needs.

4. Modem Security: In some cases modem configuration & authentication information would be stored on modem, in others, stored on your computer. Safeguard this information by consulting your vendor.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

5. Shared Cable Modem Connection: Cable networks are shared among numerous subscribers in a given neighborhood. As a result, neighbors could monitor your transmission by using sniffer. Please ensure service provider upgraded networks and equipments to DOCSIS (Data over Cable Service Interface Specification).

6. Content Inspection: Since interactive technologies like Java, JavaScript, ActiveX are a big part of broadband content sites & emails, as well as potentially an emerging vehicle for hack attacks. It is recommended that disable mobile codes such as Java, JavaScript & ActiveX. Disable scripting features in e-mail programs. You may want to explore active content security products such as TrendMicro, CA, Finjan etc.

7. System Security:
    a. It is recommended that you log off & power down your PC when you are not using your connection.
    b. Many Chat clients allow exchange of executable codes, they present risk similar to e-mail clients. Avoid chat room, if at all possible.
    c. Regular system backups are only effective remedy for disk failure. Also keep a boot disk to help to recover from hacking or disk failure incidence.
    d. Keep all applications, including OS, patched
    e. Don't run programs of unknown origin. Don't open unknown email attachments.
    f. Turn off file and print sharing unless they are absolutely necessary.
    g. Use login id and password with minimum of 8 alphanumeric characters

Conclusion

All in all, once you get broadband connection, you must realize that you are now connected to the net 24/7 ("always-on"). And personal safety should now be turned into a consideration more so than before. Many crackers/hackers have become wise to the holes/bugs in many of today's firewalls. This being a result of rushed delivery, and quantity not quality! If you value your privacy, and if you have important documents / data, then it would be wise of you to back up every so often. Also an integrated broadband security appliance eliminates these security concerns. By combining broadband access technologies with integrated security solutions, enterprises and service providers can safely and securely capitalize on all of the benefits of the broadband Internet. Last word, consult your IT security personnel to frame policies & procedures relating to the security of your network.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References

BROADBAND SECURITY. An investigation into **Broadband** technology in relation to **security** issues. By- Bhopinder Thiara. (1 August, 01)
http://www.scit.wlv.ac.uk/~c9705859/home.htm

Article1: **Broadband security** recognized (1 August, 01)
http://hardware.earthweb.com/hsnet/hsbroad/article/0,,12431_619611_3,00.html

DSL/Cable security guide
By Joe Paone January 19,2000 (1 August, 01)
http://desciple5.netfirms.com/BroadBand.html

Home Network Security 22 June, 2001 (1 August, 01)
http://www.cert.org/tech_tips/home_networks.html#introduction

Next Generation Security Solutions for Broadband Internet (1 August, 01)
White Paper by NetScreen February 2001
http://www.netscreen.com/solutions/

Broadband Internet Security Basics (1 August, 01)
The ABCs ... and XYZs of protecting your always-on, high-speed connection
http://www.cable-modem.net/features/mar00/story1.html

DSL FAQ May 00 (8 August, 01)
http://www.dslreports.com/faq

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**