Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

B. Marcus Badley

GSEC Version 1.3

Broadband Routers: Security Features and Comparison

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Abstract

The Internet has driven a huge rise in the residential broadband industry the past few years. These connections are usually either DSL or Cable Modem based. This new technology has increased the number of home based networks. This new type of connection has it fair share of network security issues. The implementation of broadband routers can increase the functionality of the home network as well as help ease some of the security issues.

These features allow for DMZ creation for game servers and public access, VPN support for access to corporate networks and wireless technology to solve the extra cabling requirements of most networks. All of these uses have their own security issues; there are routers that can help with the problems in theses areas. Some even have personal firewall software rule sets built into their products. I review a few of these routers and briefly discuss some pros and cons, as well as offer up my own preference.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Introduction

There has been a big increase in the number of homes and small businesses using high speed Internet access. Cable Datacom News publisher Kinetic Strategies Inc. estimates the number of North American residential broadband Internet subscribers more than doubled in 2001. Cable modem, DSL, Satellite and fixed wireless subscribers rose to 6.4 million in 2001, making that market total 13.3 million homes. At the end of 2001 U.S. broadband penetration reached 10 percent, compared to over 22 percent in Canada bringing the total penetration rate of North America to 11.5 percent. The increase of cable modems from the year 2000 was 3.3 percent (Cable Datacom News).

	Res DSL	**Cable**	**Other**	**Total**
Total U.S. Subscribers	3,487,870	7,170,617	180,000	10,838,487
Total Canada Subscribers	845,268	1,596,800	20,000	2,462,068
Total N. American Subscribers	4,333,138	8,767,417	200,000	13,300,555
Total N. American Additions	2,380,838	3,933,203	110,000	6,414,041

Cable Datacom News, March 2002

Many of these users now want to share their Internet connection among two or more computers. To do this, these users need an easy way to properly secure this connection. For users maintaining open connections over high speed cable and digital subscriber lines, security is a must, especially when home systems become gateways to corporate networks through dial up or VPN connections.

The only way to make your computer hacker proof is to turn it off or disconnect it from the Internet. This is not a very good option, so people need to find ways to make their computers 99 percent hacker proof. An unprotected computer connected to the Internet via a cable modem or DSL is an open invitation for hackers. A broadband connection is easier to hack because these connections often use a static IP address, or one that doesn't change. This means that is easy for hackers to find it on the network. Most dial up services use a new IP address each time a user log in, which make sit much harder to find, unless a Trojan horse has infected the computer. Also, many dial up services have an idle disconnect time that will logoff a computer with no activity for a specific time period.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Broadband Routers

A broadband or barrier router makes it easy to securely share this high speed connection among multiple users, and is quickly becoming an essential piece of equipment for securing home networks as well as small businesses. These devices offer a wide range of protection for home and small business networks, while still enabling file sharing and other functionalities of the small network (Janowski).

Almost all broadband routers include a multi-port 10/100 Ethernet switch along with basic firewall protection with Network Address Translation (NAT), which hides internal systems from outside view behind a single IP address. Along with this, is a Dynamic Host Control Protocol (DHCP) feature that uses private IP address space. This is an added security feature as these addresses are not routable and make it harder for hackers to use an unsuspecting computer (Taschek).

Most also offer basic VPN support, typically through PPTP or point to point tunneling protocol, which is becoming increasingly popular for users to remotely connect to their corporate networks. VPN technology makes it possible for users on an untrusted network to connect to a private network in an easy and secure fashion (Lear).

A few also include stateful packet inspection (SPI), which prevents unauthorized access and DoS attacks and denies intrusions by identifying hacking attempts and blocking data movement (Lear).

Another important feature are the DMZ capabilities, which allow any outside computer full access to your system. These uses include multiplayer games or videoconferencing. It is also a must if you want to run email, Web or an FTP server. Of course operating a computer in the DMZ does place the computer outside the private network and make it visible to the Internet, so additional security such as a software firewall would significantly lower the risk (Lear).

Port forwarding is another way to support internal Web, FTP or email servers. This feature is usually on the more advanced broadband routers. This lets you forward traffic on certain ports to specific computers on your network. This is similar to a DMZ host except it just opens up a specific port or ports and doesn't expose an entire computer to the outside world. In addition to the security benefits, port forwarding is also useful because many broadband routers only permit a single DMZ host, limiting the Internet server options (Lear).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Redundancy is an important feature often forgotten about when dealing with security. This is one of the newer features on some of the broadband routers available. An asynchronous port lets users use a backup Internet connection in case the primary cable/DSL connection fails. This is more important for small or home businesses that depend heavily on the Internet connections and might be an important consideration where a connections reliability is at stake.

Many routers also offer a wireless access point that will allow a connection from anywhere within range of the antennae. Wireless connections have many security issues inherent to the product. As wireless devices become more widespread for both home and business use, the need for a more robust security policy increases as well. Vulnerabilities of Wired Equivalent Privacy (WEP) encryption show that this alone is not adequate security (Morris & Taylor).

To protect data on wireless networks, the 802.11 standard specifies three basic methods of securing access to wireless access points.

The Service Set Identifier (SSID) allows a wireless LAN to be segmented into multiple networks, each with a different identifier. Each of these networks is assigned a unique identifier, which is programmed into one or more access points. To access any of the networks, a client computer must be configured with corresponding SSID for that network. The SSID acts as a simple password, providing one level of security. The problem with this is that the SSID is widely known and shared (Linksys).

Another way to increase security is to configure each access point with a list of MAC addresses associated with the client computers that are allowed access to the access point. If a clients MAC address is not on the list, the access point will deny access. This method provides good security but is only suited to smaller networks. The labor intensive work of entering MAC addresses and maintaining the database of lists on all of the access point limits the scalability of this option (Linksys).

To minimize the risk of radio frequency interception by somebody nearby, WEP is specified for encryption and authentication between clients and access points according to the 802.11 standard. WEP security is based on an encryption algorithm called RC4. It is generated based on a key entered and controlled by the user. All clients and access points are configured with the same key to encrypt

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

and decrypt transmissions of data. WEP keys are 40 or 128 bits in length (Linksys).

An access point can be set up to provide encryption only protection in open system mode or to add authentication in shared key mode. MAC address filtering is often used together with this encryption. WEP security is best suited for small networks, because there isn't a key management protocol. Keys must be manually entered into every client. This can be a huge management task, especially as keys need to be changed regularly to provide a higher level of security (Linksys).

For business networks, a VPN solution for wireless access is currently the most suitable alternative to WEP and MAC address filtering. The Internet Protocol Security (IPSec) is the most widely used way for securing VPN traffic. IPSec can use multiple algorithms for encrypting data, keyed hash algorithms for authenticating packets and digital certificates for validating public keys. VPNs will support a variety of user authentication methods. IPSec includes three security elements (Linksys).

The Authentication Header provides authentication and integrity by adding authentication information to the IP data. This ensures that the data will not be available to an unauthorized client and will not be altered en route. Authentication techniques used are MD5 (message Digest Algorithm 5) and SHA (Secure Hashing Algorithm)(Linksys).

The Encapsulation Security Payload (ESP) provides confidentiality and can also provide integrity and authentication. This is dependent on which algorithm is used. With ESP, part of the ESP header itself and all data is encrypted. Tunnel or transport modes are available, with tunnel mode being the choice for remote access. Encryption techniques are DES (Data Encryption Standard) which uses a 56 bit key and Triple DES which uses 168 bit keys (Linksys).

Internet Key Exchanges are management protocols that are used to negotiate the cryptographic algorithm choices to be used by the Authentication Header and ESP. The mechanisms employed provide to a scalable solution. Keys are maintained, exchanged and verified using these protocols (Linksys).

Wireless Solution

For home and small businesses using a Wireless Access Point, the combination of SSID + MAC + WEP is the most common type of security. This provides the best combination of security in this situation because you have

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

to make the attempt to access the network as opposed to a constant polling of the access point (Linksys).

For medium to large networks, VPN is probably the best choice for wireless security. Stronger methods are used to ensure that network access is strictly limited to users who can be authenticated and that privacy of message traffic is ensured.

Product Reviews

Linksys EtherFast Cable/DSL Router (model BEFSR41)

This router contains a hardware based DHCO server that will allow for up to 253 clients. It also has built is firewall features that provide security for the home or small business network. There is also a 10/100 switch, rather than a non switching hub. This allows for expansion beyond the 4 port limit and has an uplink port to connect other types of switches (Johnson).

The user interface for the Linksys comes in a web based form. The setup menu is a GUI based program that can be accessed by any web based browser. The internal IP address is 192.168.1.1 (Johnson). The default user name is blank and the default password is "ADMIN", this of course should be changed immediately. When the router is first turned on, the HTTP setup interface is accessible via the WAN by default. Again, this should be turned off immediately and a strong password used for the router administrator.

There is a feature that can filter out 5 LAN IP addresses from accessing the DHCP server, which will block internet access for these particular client machines. There is also a feature that can forward any service to any IP address on the LAN. One example would be an FTP server on the LAN; you can forward the port 21 to the IP address of the FTP server so that all FTP requests get sent directly to that machine. However, you cannot specify UDP or TDP and there are only 10 fields allowed (Johnson).

This model also allows for a DMZ host. Which means you can have a computer on the network in a DMZ mode. This removes the PC from the firewall protection of the router. This will leave that particular machine unprotected but all ports are still able to send and receive data from the Internet. This, however, allows for only one computer in the DMZ (Johnson).

Linksys has also built into their router, a feature that uses ZoneAlarm Pro and PC-cillin both sold separately. ZoneAlarm features provide additional protection from the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Internet's hackers, while the PC-cillin works on viruses. These products provide rule enforcement at the router based on these products specifications (Freed).

D-Link DI-701 DSL/Cable Residential Gateway Router

This router does not have a built in switch or hub, so one will have to be provided if there is a LAN that needs connectivity. It does have DHCP capabilities and can handle 253 clients. Accessing the setup is done through a web browser at the 192.168.0.1. There is a default password and login to the router that should be changed immediately.

Many of these devices have problems with various IRC or FTP services, this one did not have any problems in this area. It does not have a DMZ function. It does have firewall features that allow you to control inbound and outbound traffic by IP addresses or port number (Freed).

One issue was the process of upgrading the firmware on the router. Most routers will allow an upgrade to come from any client connected to the router or switch to which it is connected. D-Link thought this might be a security risk by allowing anyone access to sensitive features on the router, that they put a serial port on the router to perform this upgrade. Being designed for home use, this is kind of an odd feature and can be difficult for the average user to comprehend (Filipov).

Netgear FR314 Cable/DSL

This router provides a high level of security includes a hardware based firewall. This incorporates Stateful Packet Inspection technology to prevent DoS attacks and malicious packets. It also has an Internet Access filtering capability, high speed internet sharing, VPN pass-through and logging and reporting capabilities (Freed).

This model includes parental controls with a content filtering capability that keeps children away from certain sites. It uses a program by SurfControl called CyberNOT which is a website blocking program. These sites are broken down by categories such as pornography, hate sites and adult sites. A 30 day trial is included, but to keep this feature a purchase is a must. It includes a 4 port switch, but it is designed for 8 users but is only expandable to 45 users. However, this is an extra cost. 20 users will cost $109 and 45 users is $248. The setup is web based and is accessible by any web browser (Freed).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Netgear makes an 8 port version but is includes an option to upgrade to a VPN endpoint, which lets the unit act as a single user VPN server. Using this, a user or another VPN router can create a secure, encrypted connection over the Internet. The protocol used is point-to-point tunneling protocol (PPTP) as well as port forwarding (Netgear).

SMC Barricade Router SMC7004ABR

The features the traditional hardware based DHCP server using NAT services. It also has additional firewall features to block common hacker attacks such as IP spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, user datagram protocol port loopback, Snork Attack, TCP null scan and TCP SYN flooding (Ferrill).

This model allows for filtering of Internet access for local clients based on IP address, application type or time of day. For example, FTP traffic can be blocked for certain hours of the day. You can also specify the IP address of a remote administrator host to enable access to the Web configuration interface remotely. This router also offers a backup connectivity option using a COM port and an external modem to connect to the Internet. It also has a printer port to act as a print server. SMC also offers VPN support using PPTP, layer 2 tunneling protocol or IPSEC pass through (Ferrill).

ZyXEL Prestige 310 Router

This product has a built in hardware firewall and DHCP services. It supports IP routing, NAT/SUA, PPTP. Most cable modem authenticate by a couple different methods. Probably the most popular is to use the hardware address of a network card in your computer to identify the user to the network. This way, passwords don't have to be sent and the login process appears to be transparent to the user. The ZyXEL can get the address from a computer, and then pass this ID to the network authenticator. This model supports hardware authentication, Toshiba authentication, RR login, PPPoE and PPTP for VPNs (Blakely).

This router lets you assign up to 12 rules per filter and up to 6 filters for a total of 72 rules. You can apply as many as 24 rules to a single port. This also lets you open up ports individually to run a specific service. This also can be used to stop various types of traffic by port. This also allows for multiple public servers in a DMZ to run FTP, email or game server (Blakely).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

This router uses NAT, but ZyXEL also adds something they call Single User Account of SUA. This allows multiple inside addresses to be mapped to one public address. This router also can handle subnetting. Out of the box it allows for 253 usable IP addresses, but it can handle a total of 759 with subnetting. This model also supports Dynamic DNS, which associates a domain name with a dynamically addressed system. A DDNS server will hold an IP address for a domain, and then authenticate you when you log on, then reroute all requests for that domain to the new dynamic address (Blakely).

One down side to this router is the configuration. The default configuration has just a few basic filters set up in the firewall. This can be difficult to setup for a novice or if you don't understand the rules you are implementing. These features tend to be for the more advanced users (Blakely).

UMAX UGate-3000

This model supports the standard 253 DHCP clients. You can also group clients into groups and then build limits to each of the groups. You can limit groups to email only for example. There is a special application service, you type in the name of the application and the port range it needs for up and downstream communications. It is a simper way of port forwarding or removing a computer from the firewall protection (Stoltenborg).

This model also has a specific menu for Road Runner users. It also supports Dynamic DNS. This is a paid service, but you get a year of it for free for purchasing the router. It comes with a 4 port 10/100 Fast Ethernet Hub. This model's firewall product is based on packet monitoring and port closing. Setup is done through a web browser (Stoltenborg).

Conclusion

As the Internet makes sharing access and peripherals more prevalent, the security demands on protecting these networks will rise. Ethernet based and wireless home networking solutions show tremendous benefits to home users as well as home and small businesses. The issues of scalability, cost of maintenance and performance will all weigh against the security issues. The rise of wireless networking will continue to be a major player in this area; however the security problems will always affect the type of purchase.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The choice of which router to buy is based on the type of applications you are doing. You need to examine all the security features of the router and make sure they will support your needs. If you plan on running a game server in a DMZ, this will play into your decision. The security features are important, but if you don't know how to use them it wouldn't be worth the investment. Do you want expansion capabilities? How many computers are you going to need? Most home networks don't go anywhere near the 253 IP addresses supported by most brands. Are features such as parental control important?

Built in personal firewall features such as ZoneAlarm are very good. Purchasing just the router itself is not enough. Having a software firewall or other means of security in addition to the hardware is always a better choice. More is better in this case. Software such as Norton Internet Security or Tiny personal firewall are very good choices in addition to the hardware of the routers. Whatever works for you is fine here.

We took a brief look at the wireless technology, it is imperative to use as many of the features as possible to ensure security with this inherently insecure technology. Use the SSID, lock in the MAC address and use the highest WEP capable. When choosing a wireless adapter the security features are very important. You need to make sure all these features are available on the product.

I didn't mention price for these devices, mainly because the prices have fluctuated so much. But on average, these devices range from about $80.00 to as much as $400.00, depending on the features installed and capabilities of each router. I consider security of my network to be an investment. I purchased a model from Linksys a single port model; however I have my own switch in place. I like the ability to shut off all WAN requests. I have tested my router through www.grc.com and have passed all their tests. I also have installed Norton Internet Security as well. I liked the way it updates, support the virus software and has a parental control feature that can protect my children. What meets your needs is what determines what to purchase in this area. This model was inexpensive, around $100.00 and fit into exactly what I want to do.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Works Cited

Blakely, Tom. "The ZyXEL Prestige 310 Router: Cool, Custom and Complex." SpeedGuide.net 15 April 2000. 27 March 2002 <http://www.speedguide.net/reviews/zyxel/index.shtml>

Cable Datacom News. "Broadband Subscriber Base Doubles in 2001" Cable Datacom News 1 March 2002. 27 March 2002 <http://www.cabledatacomnews.com/cgi-bin/printer.cgi>

Ferrill, Paul. "Residential Gateways" Net.Worker News 22 October 2001. 27 March 2002 <http://www.nwfusion.com/techinsider/1022broadband/rev.html>

Filipov, Philip. "D-Link DI 701 DSL/Cable Residential Gateway Router" SpeedGuide.net 26 July 2000. 27 March 2002 <http://www.speedguide.net/reviews/dlink/index.shtml>

Freed, Les. "Share the Wealth: Broadband Routers" PCMagazine 12 February 2002. 27 March 2002 <http://www.pcmag.com/article/0,2997,s=1474&a=21248,00.asp>

Gill, Kamal. "NetGear RT 314 Cable/DSL router and four-port switch." CNet.com 19 June 2001. 27 March 2002 <http://computers.cnet.com/hardware/0-7052-405-2319553.hteml?tag=rev-rev>

Janowski, Davis D. "Share the Wealth: Broadband Routers" PC Magazine 12 February 2002. 27 March 2002 <http://www.pcmag.com/printarticle/0,3048,a=21238,00.asp>

Johnson, Brent. "Linksys EtherFast Cable/DSL Router Review" Speedguide.net March 2000. 27 March 2002 <http://www.speedguide.net/reviews/linksys/index.shtml>

Lear, Anne. "*Wire Labs Roundup: Broadband Routers" 8Wire.com 8 January 2002. 27 March 2002 <http://8wire.com/articles/?aid=2286>

LinkSys Corporation. "How to Network: VPN and Wireless Security" ND. 27 March 2002 <http://www.linksys.com/edu/vpnwireless.asp>

Morris, John & Taylor, Josh. "Wireless networking: It's so easy! And so insecure!" ZDNet.com 5 March 2002. 27 March 2002 <http://www.zdnet.com/anchordesk/stories/story/0,10738,2852419,00.html>

NetGear Inc. "NetGear Product Features." Netgear.com ND. 27 March 2002. <http://www.netgear.com/product_view.asp?xrp=4&yrp=12&zrp=55>

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Stoltenborg, John. "UMAS UGate-3000 Review" Speedguite.net 26 April 2000. 27 March 2002 <http://www.speedguide.net/reviews/umax/index.shtml>
Taschek, James. "SOHO Sentinels" ZDNet.com 29 June 2001. 27 March 2002 <http://www.zdnet.com/products/stories/reviews/0,4161, 2772193,00.html>

© SANS Institute 2000 - 2002, Author retains full rights.