GIAC
CERTIFICATIONS

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 Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Layers of Defense for the Small Office and Home Network

Derek Krein

July 24,2001

With the information age in full swing and the popularity of broadband technology increasing, home users as well as small offices are now connected to the Internet 24 hours a day via cable or DSL, and the need for securing your small office or home network is essential. Believe it or not the Internet is a battleground for information warfare and if not properly prepared you may be an unwilling participant and/or victim. Many Internet threats exist in the form of Attackers, Trojan horse programs, Viruses, Worms, and other malicious code.

This year malicious activity has increased significantly and as a result, so has the compromise of home computers. Intruders are targeting home users; especially those connected with cable/DSL connections available 24 hours a day, mainly for use in the attacks of other computers on the Internet. (1)

Covering all areas of malicious activity takes more than any one product can handle. Applying more than one layer of defense to your network is extremely important. A complete hardware/software package is a cost-effective comprehensive method of securing your network. The average home user or small office worker, for a relatively low cost and with minimal technical knowledge, can apply several methods of defense.

The first layer of protection should be a cable/DSL router with a built in switch as your network backbone. This hardware device will allow you to share your high-speed connection and provide security. A router is a device that connects different networks together and chooses different paths, usually the shortest, based on the IP address. Linksys and Netgear make a nice unit usually selling for around $99.00 to $349.00 depending on features. A switch is a device that establishes a direct line of communication from the port of origin to the destination port, and offers dedicated bandwidth to each port, vice sharing bandwidth like a hub. Bandwidth is like a pipe, if you have a 4-port 100 Meg hub, and all ports are used, each port only has 25 Megs of bandwidth. On the other hand a 4 port 100 Meg switch with all ports used, each port gets a full 100 Megs of bandwidth. A switch is preferred over a hub because it provides some separation to your network; if your network is compromised it'll be harder for the attacker to "sniff" the traffic on the other ports of the switch. A sniffer is a program that allows somebody to see the traffic on a network, switching makes this much more difficult. Another benefit of the switch is much more bandwidth is available to each computer increasing network speed significantly. These cable/DSL routers provide security through obscurity using network address translation (NAT). Network address translation allows the use of one IP address for multiple computers; the Internet only sees one IP address, hiding your internal network. The byproduct of this is you don't need to purchase additional IP addresses for additional computers, saving money. The internal network utilizes IP addresses reserved by the Internet Assigned Numbers Authority (IANA) for private networks and cannot be routed on the Internet. These addresses are:

Class	Address Range

© SANS Institute 2000 - 2005 Author retains full rights.

"A"	10.0.0.0 to 10.255.255.255
"B"	172.16.0.0 to 172.31.255.255
"C"	192.168.0.0 to 192.168.255.255

Refer to RFC 1918 for more information about recommendations for private addresses.

IP Addresses reserved for private use (2)

These routers are fairly easy to setup via your web browser and most include advanced features for filtering Internet access, logging inbound and outbound activity, some even offer content filtering, central administration, virus software, Dynamic DNS, and a print server built in. I'll discuss briefly some of the features of two very common products available at most CompUSA and Bestbuy stores.

1. Linksys Products (3)

Some of the features include:

- Support for up to 253 users
- Accepts PPPoE protocol
- Can act as either a DHCP server or client
- Accepts either static or dynamic IP addresses
- Compatibility with all standard Internet applications.

Some of the more advanced features of the Linksys products include:
Log viewer, allowing advanced access to your log files. Filtering, let's you block Internet access by either port number or IP address. Forwarding, the router will forward Internet requests for certain services to the appropriate computer. Dynamic Routing, the router will automatically adjust to changes in the network and determine the best route based on the least number of hops from source to destination. Static Routing, allows you to manually input routes. DMZ host, the DMZ (demilitarized zone) allows one computer to be exposed to the Internet, for special purposes such as game server, sniffer, or web server.

2. Netgear Products (4)

Features depending on the model include:
Stateful packet inspection + Denial of Service protection, allows administrators or parents to restrict access based on time of day, time of week, web address, or web address keyword. Receive regular e-mail reports and instant alerts on browsing activity and hacking attempts. Netgear also offers a router with an optional content filtering subscription to further restrict access. Content filtering prevents users or children from accessing pornographic or inappropriate sites.

Other Products

Here are some of the other products available and the websites for reviews and information on

© SANS Institute 2000 - 2005, Author retains full rights.

them; these are not listed in any particular order.

D-link: DI-704 (5)
Maxgate: u-gate 3100 (6)
Nexland: ISB SOHO (7)
SMC: Barricade (8)

For even more routers and reviews go to: http://www.firewallguide.com/hardware.htm and http://www.practicallynetworked.com/

I highly recommend going to the different manufactures websites and doing a little comparison-shopping, looking over their tech support, and customer testimonials. Getting the right product for your network the first time is just a matter of a little research.

The second layer of protection should be a host-based (personal) Firewall on each computer. Should an attacker get by your router, a host-based firewall is your next line of defense. A firewall shields your host from the Internet receiving each packet of inbound or outbound data and inspecting it. The firewall will pass data based on the rules you set. This gives you a great deal of security and can be tailored to fit your networks needs. Some of the methods used to control this data are packet filtering, stateful inspection, and proxy service. Packet filtering simply checks packets and passes or drops them based on filters you set. Stateful inspection is a little smarter; the firewall remembers the status of each connection and builds their context into memory, it then utilizes this information to make a better-informed decision. Proxy service: a proxy server is the go between from the inside network to the outside network and vise versa. A client will request information from the Internet, the proxy server intercepts that request from the client and it will make the request. When the server responds, the proxy will intercept that response, and send the response back to the client. To both the client and the server the only computer seen was the proxy server.

Most of the personal firewalls on the market have some sort of IDS (Intrusion Detection System), alert screens, or logging features to allow you to see whose knocking on your door, so to speak. This information is helpful in seeing who is probing or scanning your network, and if an attacker gets in, can help you discover when and how. The interfaces vary quite a bit and some are easier to use then others. A little research will be invaluable here, as all personal firewalls are not created equal. One of the features to consider is whether or not the firewall blocks application access to the web. Most firewalls block all ports from inbound Internet access, but not all will block outbound access to the Internet from Trojans or spyware.

Home users can benefit from many of the free firewall software readily available and downloadable from the Internet. (9)

Three very popular firewalls are:

- Zone Alarm from Zone Labs
- Tiny Personal Firewall

© SANS Institute 2000 - 2005 Author retains full rights.

- Sygate Personal Firewall

All these firewall's block outbound applications from reaching the Internet without your permission.

Zone Alarm is available free for personal use and $20 for business use. Zone Alarm PRO is available for only $39, and includes a host of features designed to keep your network secure and you in control. Zone Alarm offers immediate and complete port blocking, putting your computer in Stealth mode effectively hiding your computer from attackers, it is easy to use, no need to learn ports, protocols, or programming. It immediately alerts you of activity and gives you simple yes or no control over which applications have access to the Internet. Zone Alarm PRO includes Advanced Mail Safe-email attachment protection that recognizes and quarantines suspect attachments, and is customizable, also password protection, Advanced logging, and more. (10)

Tiny Personal firewall (TPF) is based on the Tiny Software's ICSA-certified WinRoute Pro technology. It is available free for personal use and $39 for business use. TPF uses a combination of IP filtering, Stateful packet inspection, and MD5 signature authentication to secure the system. TPF includes a wizard that detects unknown activity and prompts the user for action, making rule creation relatively easy for the novice. TPF can be monitored and admistered remotely allowing the administrator to configure remote client computers and a "view-only" access of remote logs. It offers advanced features that appeal to most administrators and considerable protection from attackers and malicious activity. (11)

Sygate Personal Firewall (SPF) is available free for personal use and $39.95 for business use. SPF is a host-based system that enforces rule based security policies based on any combination of Application, Trusted IP addresses, Ports, Protocols, and Schedule. SPF offers advanced logging features with four different logs and filtering capabilities for each. Installation is relatively easy and the configuration can be password protected. SPF offers advanced features for the enterprise with optional client/server software that enables a centrally managed security and policy enforcement solution for mobile, distributed, and stationary workers. (12)

There are many more firewalls available; most will offer considerable protection against attack. A good place to look is http://www.firewallguide.com/software.htm.

The third layer of protection should be Antiviral software. Malicious code is a serious threat to the Internet and your network hosts; it can be a virus, worm, or a Trojan horse. A major concern is that malicious code can easily bypass your perimeter defenses such as firewalls by masquerading as legitimate traffic. AntiVirus software is your host based perimeter defense against viruses and most common malicious code. Viruses are programs that are designed to self-replicate, be executed by the user without his or her knowledge, and can be very damaging. Trojans are malicious programs masquerading as useful software; they can capture information from your system or allow a malicious attacker to remotely control your system. Worms are programs that are designed to be spread across a network replicating themselves and infecting any machine on the network. The newest threat comes from java applets and active X controls. These are small programs designed to run within your web browser while accessing a web page

© SANS Institute 2000 - 2005 Author retains full rights.

that contains an applet. Applets tend to run within the web browser without the users knowledge. While these applets are supposed to be safe, a number of holes have been found. Just installing antiviral software is not enough; you must keep it updated at least weekly. Some antiviral software offer automatic updates, making this task much easier for the consumer. (13)

There are number of AntiVirus software tools available, prices range from free for personal use to around $100. The following software is free for personal or non-profit use: InoculateIT Personal Edition, and AVG Antivirus.

InoculateIT Personal Edition 5.x.x offers free download, free updates, and free support. While it lacks the speed, features, and the appealing interface of most paid-for scanners, it offers a low cost comprehensive virus protection solution. (14)

AVG anti-virus 6.0 offers free downloads and free updates as well as a new approach to anti-virus scanning with the AVG Active Modular Core. Unlike traditional scanners that utilize several completely separate programs bundled together, AVG uses a single Anti-Virus engine that every module shares. As a result the scanners cannot become unsynchronized with respect to finding viruses. (15)

Ranking among the best pay-ware are Norton AntiVirus 2001, McAfee VirusScan, and Trend Micro's PC-cillin 2000. Both Norton and PC-cillin offer a downloadable 30-Day free trial.

Antiviral software is abundant and there is no clear-cut winner in the race. Unfortunately in today's environment AntiVirus software is mandatory if you're connected to the Internet. Check the manufactures websites and some online reviews. (16)

With so many home users, small business, and big companies connecting to the Internet with 24-hour high-speed connections, the threats are increasing as well. The threat to the home user can be an attacker trying to steal your personal information such as bank accounts, brokerage accounts, or take control of your computer to attack other computers. Surely you don't want strangers sending thousands of junk e-mails from your computer, reading your e-mails, or personal information. The threat to businesses can be loss of service to their customers, financial information, or industrial espionage. What if you discover an intrusion to your system? Often times the only way to make sure you rid your system of the intruder, a back door, and/or Trojan software is to reload the system from the disk, apply all patches, and start fresh. Making regular backups of your system/s will help you retain important data should an attacker or malicious code wreak havoc on your network.

To help protect the online community from malicious activity, anyone connected to the Internet should do their best to secure their systems. The hardware, software, and information resources are abundant online. A little time, money, and effort will reap huge rewards for yourself, businesses, and the Internet as a whole.

In addition to putting together a hardware/software security solution for your network, it's important that you keep up with vulnerabilities, apply the latest patches to your operating system,

© SANS Institute 2000 - 2005 Author retains full rights.

open only trusted e-mail attachments, and only download software from trusted sites. The home user can have the ultimate in security through obscurity by turning off their computer/s while not in use. If your computer is not available, it's very hard to target. Subscribing to a security newsletters from http://www.incidents.org and http://www.cert.org to keep up with bulletins and vulnerabilities is extremely helpful and a time saver.

To fully secure your network takes a layered approach, no one product will do in today's rapidly changing technologically advanced society. The technology is changing and vulnerabilities are being discovered faster than the security professionals and manufactures can keep up with it. A layered approach while not full proof is the best means of protecting your home or small office network. A complete software/hardware solution to protect against attackers, spyware, and malicious code is as simple as a router/switch, host based firewall, and antiviral software on every computer. The industry, seeing the need for a layered security approach, has responded with a hardware/software package of its own.
Linksys, Trend Micro, and Zone Labs are putting together a complete Broadband Internet Security Solution for the small/medium business and the home network market, designed to provide an extensive, easy to use security solution. (17)

While this package may not fulfill the needs of your network, with a little research of the available products, you can put together a complete hardware/software security solution protecting your systems, and the Internet community as a whole from malicious activity.

References:

(1) http://www.cert.org/advisories/CA-2001-20.html
(2) http://www.faqs.org/rfcs/rfc1918.html
(3) http://www.linksys.com/products/product.asp?prid=20&grid=5
(4) http://www.netgear.com/categories.asp?xrp=4&yrp=12
(5) http://www.dlink.com/products/broadband/di704/
http://www.avault.com/hardware/getreview.asp?review=dlinkgate
(6) http://www.maxgate.net/products/ugate3100.html
http://www.speedguide.net/reviews/umax/index.shtml
(7) http://www.nexland.com/products.htm
http://www.speedguide.net/reviews/nexland/isb_soho/index.shtml
(8) http://www.smc.com/smc/common/prodPreview.cfm?prod_code=SMC7004ABR
http://www.hardwarezone.com/php/pcodes/reviews.php3?_di=2&_c=7&_aid=2001-01-18+14%3A44%3A49
(9) http://www.webattack.com/freeware/security/fwfirewall.shtml
(10) http://www.firewallguide.com/zap.htm
http://www.pcworld.com/reviews/article.asp?aid=18670
http://home.cnet.com/software/0-352108-8-6321078-2.html?tag=st.sw.352108-8-6321078-1.arrow.352108-8-6321078-2
(11) http://www.tinysoftware.com/tpf_datasheet.pdf
http://techweb.techreviews.com/sections/topReviews/article/TT20010122S0010

© SANS Institute 2000 - 2005 Author retains full rights.

(12)http://www.sygate.com/products/spf_ov2.htm
http://www.sygate.com/products/sen/enterprise_security_solutions.htm
http://securityportal.com/articles/pf_sygate20001112.html
(13)http://www.pcworld.com/resource/printable/article/0,aid,31002,00.asp
(14)http://cws.internet.com/reviews/virus-inoculate5.html
(15)http://www.grisoft.com/html/us_t_amc.cfm
(16)http://www.firewallguide.com/anti-virus.htm
http://content.techweb.com/winmag/reviews/software/2000/04/0425_a.htm
(17)http://www.zonelabs.com/pressroom/pressreleases/2001/linksys_tm_zl.html

More References:

http://dmoz.org/Computers/Security/Firewalls/Products/Personal_Firewalls/
http://www.internetnews.com/intra-news/article/0,,7_529661,00.html
http://grc.com/lt/scoreboard.htm
http://grc.com/su-firewalls.htm

© SANS Institute 2000 - 2005, Author retains full rights.

.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: April 27th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS