Global Information Assurance Certification Paper

A Hardware Based Firewall Option for the SOHO (Small Office/Home Office) User.
A look into the LINKSYS Etherfast Cable/DSL Router.

Scott Kisser
December 4, 2000

SOHO (Small Office Home Office) Security of Cable/DSL (Broadband) Connection is becoming more critical for businesses that offer the option for employees to work from home. These SOHO users must take the responsibility to ensure a level of security to the business and the level of security must follow the companies specific Security Policy. Since we know a good security policy is rooted within the three principles of Prevention, Detection, and Response, this paper will focus on using the hardware firewall offered by LINKSYS as a solid foundation into the preventive measures.

Despite society's knowledge of security and the numerous security products on the market, the Internet is becoming an increasingly dangerous place of business. These days, almost everyone knows that when they choose the 'always on' Cable or DSL connectivity, they are opening their system (s) up to multiple vulnerabilities and risks. Hackers, Crackers and the proverbial 'Script Kiddies' are continually searching for other computers to break into. One of the many things they often do, is use these computers as a springboard or launching platform to release malicious scripts or even just as a challenge to crack into and snoop at some personal information. To attempt to defeat against these mischievous bands of denizens, SOHO users must first start with preventive measures that ensure a solid foundation for Security.

A short time ago I became a Cable user and was selected as a beta tester for the local Cable Company. Knowing the inherent risks with the 'always on' connection I figured it would be in my best interest to get a firewall. Essentially, a firewall is a port closer. With each IP address having potential 65,535 ports, these potential security holes need to be monitored or blocked. What firewalls provide to the user is the ability to form a defensive barrier against the threats they face. Firewalls that form these defensive barriers limit the threats to the system(s).

Establishing criteria was an important first step in my search for a firewall. When I started looking for a reasonable choice to secure my computer to the Internet, my plan was to keep my options as open as possible. I wanted to experiment with other Operating Systems so I knew that my firewall choice would have to be platform independent. I also wanted the ability to add other computers to my network in the future. Keeping in mind a simple principal I learned in flight school called K.I.S.S - Keep it Simple Stupid, I strove to find a solid all encompassing product that wouldn't require an extreme amount of time or trouble.

After searching around for an option that fit my needs, I soon found out that I might have to change my selection criteria. It appeared that a lot of software based Firewalls, such as NetworkICE's BLACKICE Defender or Symantec's Norton Personal Firewall, were platform specific. I figured that I was out of luck until a 'gadgeteer' friend at work suggested a few options that might meet my needs. I could both take an old 486 computer and convert it to an Unixed-based firewall/router, (adding many more levels of magnitude to my limited, but growing Unix experience). Or I could spend about one hundred and fifty dollars (possibly even less with coupons from http://www.techbargains.com) and purchase a newly released hardware based Router/Firewall from LINKSYS. The LINKSYS Cable/DSL Router Firewall allowed for my personal needs and also the ability to add multiple machines in the future without 'buying' another IP Address from my ISP.

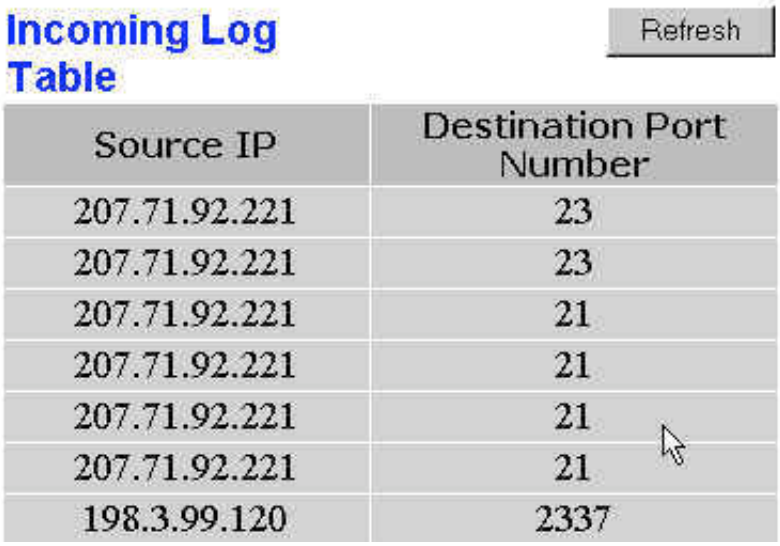
One of the advantages to thee LINKSYS Router is the Administration is based on an internal IP Address that allows users to change settings on the system. Users can configure the Router through any browser. Setup of the Router is very simple and easy to operate through the browser. Advanced settings that allow for Forwarding, Port Filtering, Blocking Internal IP Blocking, etc. can get a little bit confusing for someone with no Network experience but it is fairly strait forward and you always have to ability to reset the settings.

Another advantage of the LINKSYS Router is that it uses NAT (Network Address Translation). NAT Translates multiple IP addresses within the private LAN to one public IP address. This adds a cost savings feature to the router because many Internet Service Providers' are charging PER IP Address and since there is only one published IP Address; the LINKSYS user only pays for the one! This feature also adds a security measure to your network because you are publishing only one IP number when in fact you could have multiple machines behind the router.

The filtering feature of the LINKSYS Router enables the user to block specific INTERNAL IP addresses from accessing the Internet through an IP address or a network Port Number. The Port Forwarding feature that is also offered can allow the LINKSYS user to give permission to publish Public Services such as a Web Sever, FTP Server or EMAIL Server. Allowing this option on the Router will forward specific requests such as Port 80/Http to the

computer specified.

In the latest firmware version 1.36 (12 October 2000), LINKSYS supports IPSEC and PPTP, an advantage that allows for Virtual Private Networks to be able to use the Routers features. This firmware also provides logging incoming and outgoing requests.



Incoming Log Table

Refresh

Source IP	Destination Port Number
207.71.92.221	23
207.71.92.221	23
207.71.92.221	21
207.71.92.221	21
207.71.92.221	21
207.71.92.221	21
198.3.99.120	2337

Logging is somewhat limited. Below shows the ability from incoming data.

Despite the advantages of the LINKSYS Router there are several disadvantages. For instance, the Port Forwarding option is limited to only 10 Ports. Another disadvantage is that there is currently no ability to specify TCP or UDP connection on specific Ports like software firewalls can. Without this the user loses the ability to configure specific connections on the firewall. Lastly with the LINKSYS Router, only one computer has the ability to be set up on the DMZ (De-Militarized Zone). DMZ a setting that is normally used when applications need multiple TCP/IP Ports to be open. The user will then designate a DMZ computer on the Router and puts it outside the firewall. (However word from LINKSYS is that multiple DMZ support is coming).

In conclusion, I would like to stress that even though this paper focuses on one product, proper security of anything **DOES NOT** come in a box. Solid security is a process, not a product. For my situation the benefit of having a platform independent firewall combined with the ability to add multiple machines at a later date was the best option. Different users might need something else, they must be sure to properly weigh their needs and options accordingly when choosing a product.

Top Ten Ports Scanned – Distributed Intrusion Detection System from 03, December 2000. http://www.dshield.org/topports.php.

Top 10 Target Ports

This list shows the top 10 most probed ports.

Service Name	Port Number	Protocol	Explanation
netbios-ns	(137)	udp(17)	Windows File Sharing Probe
???	(0)	icmp(1)	Ping.
netbios-dgm	(138)	udp(17)	Windows File Sharing
???	()	ip()	
route	(520)	udp(17)	used for routing information
nntp	(119)	tcp(6)	News Server
asp	(27374)	tcp(6)	Scan for SubSeven Trojan
???	(2048)	tcp(6)	
domain	(53)	udp(17)	Domain name system. Attack agains old versions of BIND

Tech Specs for the LINKSYS Router:

Standards: IEEE 802.3, IEEE 802.3u
Certifications: FCC Class B #L2115639
Protocol: TCP/IP, RIP1, RIP2, PPTP(VPN)

Ports:
4 10BaseT/100BaseTX RJ-45 Ports
One 10BaseT Broadband WAN Port
One 10BaseT/100BaseTX RJ-45 Uplink Port

Cabling Type:
10BaseT: UTP/STP Category 3 or 5
100BaseTX: UTP/STP Category 5 or Better

Topology: Star

Speed:
WAN Router: 10Mbps (10BaseT Ethernet)
LAN: 10Mbps (10BaseT Ethernet) or 100Mbps (100BaseTX Fast Ethernet)
LEDs: Power, Ready/Test, Link and Activity for both WAN and LAN port(s), Partition and Collision for LAN ports

A probe of the Ports at Gibson Research, http://grc.com/ shows us:

21	FTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
23	Telnet	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
25	SMTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
79	Finger	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
80	HTTP	**OPEN!**	The web is so insecure these days that new security "exploits" are being discovered almost daily. There are many known problems with Microsoft's Personal Web Server (PWS) and its Frontpage Extensions that many people run on their personal machines. So having port 80 "open" as it is here causes intruders to wonder how much information you might be willing to give away.
110	POP3	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

References:

"Navas Cable Modem/DSL Sharing Guide". (20 November 2000) URL: http://cable-dsl.home.att.net/sharing.htm (03 December 2000).

"Navas Cable Modem/DSL Tuning Guide". (20 November 2000) URL: http://cable-dsl.home.att.net/index.htm (01 December 2000).

Gibson Research Corporation. "Internet Connection Security for Windows Users". (No Date Provided) URL: http://grc.com/su-firewalls.htm (28 November 2000). ALSO for Reference: http://www.hackerwhacker.com (01 December 2000).

"Support Page: Cable/DSL Router". (No Date Provided) URL: http://www.linksys.com/support/support.asp?spid=1 (27 November 2000).

"LINKSYS Etherfast Cable/DSL Router Product User Guide". (No Date Provided) URL: ftp://ftp.linksys.com/pdf/befsr41ug.pdf (25 November 2000).

"LINKSYS Etherfast Cable/DSL Router Data Sheet". (No Date Provided) URL: ftp://ftp.linksys.com/datasheet/befsr41ds.pdf (25 November 2000).

"Security of the Internet". (No Date Provided) URL: http://www.cert.org/encyc_article/tocencyc.html (01 December 2000).

Last Updated: May 23rd, 2017

Upcoming Training

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
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 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 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 Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
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
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
SANS Munich Summer 2017	Munich, Germany	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
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event