



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 permitted 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>

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 Unix-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 the 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>.

© SANS

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
???	0	ip0	
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:

© SA

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	<u>POP3</u>	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).

Upcoming Training

Click Here to
{Get CERTIFIED!}



Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event