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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Personal Switch Routers as an element in SOHO network design

Robert Hillery

December 9, 2000

This paper presents a model for small network design appropriate for use in a small office/home office (SOHO) environment. It presents the concepts of layered defense, combining hardware, software, and design elements to improve small network resistance against hacking or other intrusion attempts. While it presumes some knowledge - enough to have caused the reader to look at this paper in the first place - it will, I hope, be comprehensible to non-technical business people who are in truth the majority of professional computer users.

Introduction

Small companies with few employees have a hard time executing good network practices even when they know that they should. If a business can be considered as a collection of generalized functions, all businesses clearly need similar "functions" accomplished. Planning, budgeting, marketing, sales, operations, personnel, record keeping, and so on are examples of such functions. With the smaller numbers of people in small companies, everyone wears many hats. So, network or systems security is a de facto part-time job.

Security can no longer be relegated to as role of "add-on" function. Information and information security are clearly part of any enterprises "core business." The increase in online system use essential to business growth simultaneously increases the risks to information. The bad news is "security through obscurity" never really worked; the good news is that thoughtful design and clever systems setup can reduce the need for a staff of rocket scientists dedicated to protecting the net. However, this concept must be infused throughout the organization and not left to chance as an add-on duty.

Concept overview

One of the key challenges with computer networks designed to communicate is…that they communicate. Remember that when you simply "ping" another computer, it may create 6 messages: ARP (broadcast), DNS (unicast to DNS server), and (in Windows) 4 ICMP echo requests. While Solaris sends only 1 echo request, Linux echoes, and echoes, and echoes - the Energizer Bunny™ of ICMP. It is important to know what your network is normally sending and when. This is the only way to properly manage your systems traffic and to be able to detect abnormal traffic. (see: What am I seeing, Graham, http://www.robertgraham.com/pubs/firewall-seen.html)

A second fundamental group of ideas involves Threat, Vulnerability, and Countermeasure (Security in Computing, Pfleeger, PrenHall, 1999). The threat consists of all those nasties that can attack the net - they belong to the enemy (Spitzner, 1999, http://project.honeynet.org/papers/enemy/). You don't control the threats. You must know what they are, but you can't change them. Vulnerability is those conditions of your network and workstations that are susceptible to exploitation by the threats. You can manage vulnerabilities - eliminate by keeping software patches up-to-date, control both physical and network access to systems, train people to reduce "social engineering." Countermeasures are those systems - software, hardware, and policy - put in place to specifically address vulnerabilities to threats. This would include signed appropriate use statements and Intrusion Detection Systems.

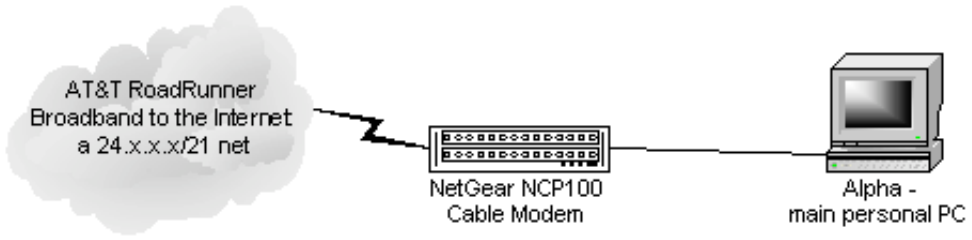
The dilemma of "persistence"

The rapidly increasing use of broadband and DSL promises to increase access to high-speed Internet capability. Unfortunately, it also means persistent connections that spend more time exposed and susceptible to discovery, mapping and intrusion. This begs for greater defense than normally considered on SOHO "on-demand" access connections that log on for email or relatively quick specific research questions and spend less time on the net.

The simplest connection of a single system to a broadband or DSL pipe has limited defense in depth. The primary user controlled options are entirely host based, and that host is in this case also the primary PC. The only "depth" is in the inherent network management of the connecting "bridge" or "bridge-router" that is incorrectly dubbed a "modem." Bridges relay all broadcast, multicast, and unicast (addressed to you) traffic. The ISP probably also filters some traffic, such as NetBIOS queries from out-of-the-box Windows 9x/NT installations. This would be at the ISP's routers to reduce some traffic throughout their network, but would not reduce this added "noise" on your segment or your part of the cable shared with some hundreds or thousands of other users before arriving at the first router on the net.
Since most ISPs dynamically assign client IPs (DHCP), you are generally limited to a single address. As long as your system is on, it is also "on" the network and responding to traffic. Your host based anti-virus, intrusion detection, and

© SANS Institute 2000 - 2005 Author retains full rights.

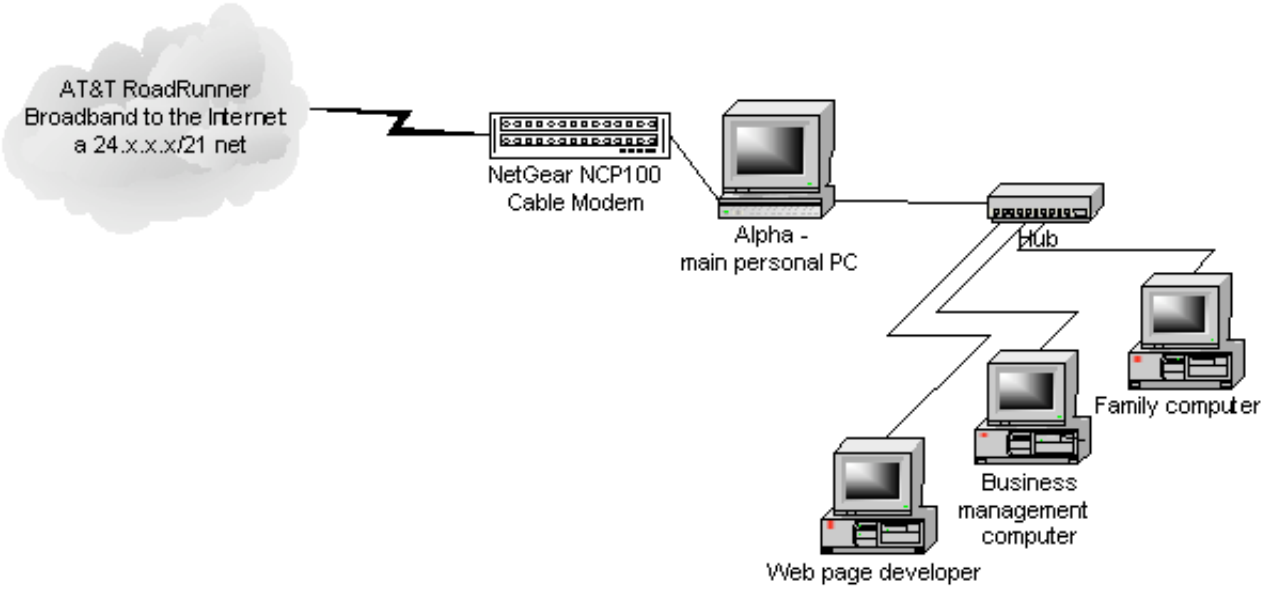
firewall (filtering) software is essential for defense. Unfortunately, it's a thin shell.



A second way to connect is with one system, two Network Interface Cards (NICs), and a hub for several machines. This dedicated machine connected to the Internet is specially configured in either POSIX (Unix/Linux) or Windows NT to act as a router in a setup called 'dual-homed". One NIC is registered in DHCP with the ISP, the other has a separate IP address and connects to one or more (through a hub) other systems that are the machines where work is actually done. This second IP is often an internal or "private" IP from one of the reserved ranges, such as 192.168.x.x in the Class C range.

This setup, with 2 different IPs or networks joined in one computer, normally something called Network Address Translation or NAT. This is a separate program or utility that translates your one or more internal numbers to the single external IP that connects to the Internet. Sygate, WinGate, and Windows 2000, among others, have this built in. A separate system is available for private use from www.gnatbox.com.

The dedicated box enables you to add filtering (firewall) and other systems defense software further away from the assets you are protecting. This is beginning to become a better defensive perimeter around your data. However, it is also more complex to setup and maintain than many small SOHO organizations will manage: perhaps the can, but because of competing demands on time they won't.



If they can't get to you…

One way to simplify this conceptual arrangement, adding depth to your defensive positions, is to add a router. Most default router IOS software does not forward broadcast traffic and only passes that traffic destined for you and your IP address.

Routers can be configured to drop all ICMP (ping, trace route) requests from outside and can have Access Control Lists (ACLs) set up to further filter out unwanted incoming traffic. When first designed, these features were intended

© SANS Institute 2000 - 2005 Author retains full rights.

primarily as traffic or bandwidth management features. They are also excellent methods to keep out many of the more basic network mapping efforts of most hackers and hacker "wanna bees."

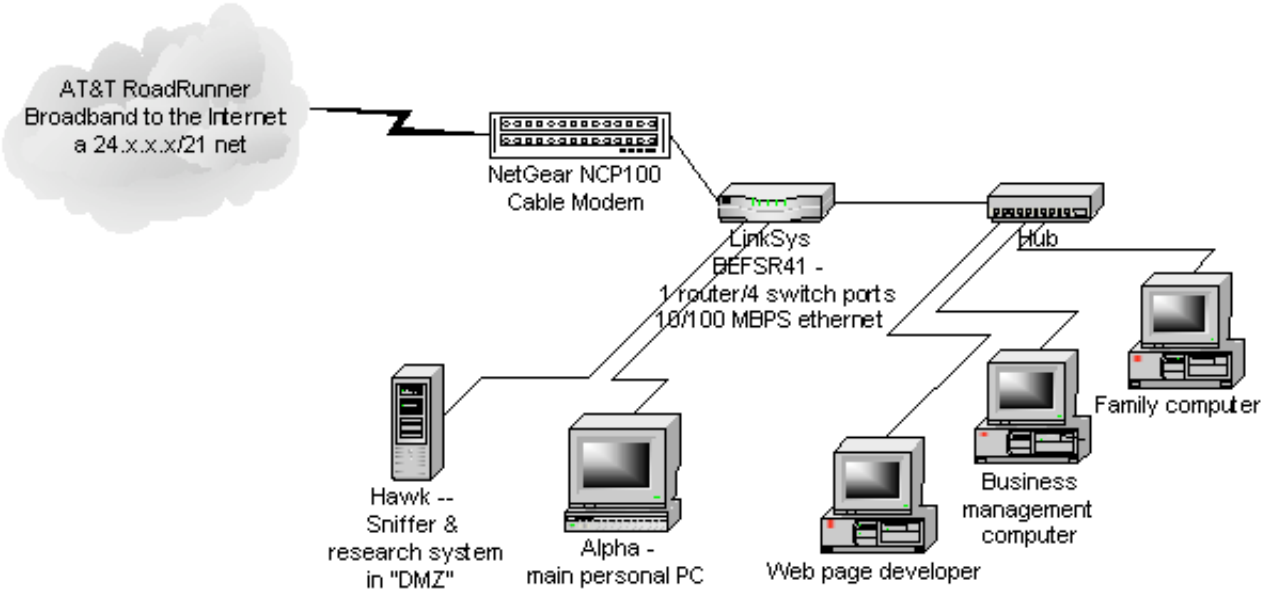
For something around $150, this one piece of equipment can add multiple paths for high-speed connectivity. It has built in NAT and will do its own DHCP for the internal addresses, simplifying the SOHO network administration. It restricts both IP and port access (inbound) by default. It can be configured to allow inbound traffic based on IP or by port. It can also establish a virtual "DMZ" by forwarding any inbound traffic to a specified internal IP.

The LinkSys BEFSR41 - EtherFast 4-Port Cable/DSL Router is an inexpensive switch-router that can improve small network security and management. From the LinkSys web site:

> "Built-In 10/100 4-Port Switch! Supports up to 253 users!
>
> The Linksys Instant Broadband EtherFast Cable/DSL Router is the perfect option to connect multiple PCs to a high-speed Broadband Internet connection or to an Ethernet backbone. Allowing up to 253 users, the built-in NAT technology acts as a firewall protecting your internal network.
>
> Configurable as a DHCP server, the EtherFast Cable/DSL Router acts as the only externally recognized Internet device on your local area network (LAN). The router can also be configured to block internal users' access to the Internet. A typical router relies on a hub or a switch to share its Internet connection, but the Linksys EtherFast Cable/DSL Router channels this connection through the blazing, full duplex speed of its built-in EtherFast 10/100 4-Port Switch."
> (http://www.linksys.com/products/product.asp?prid=20&grid=5)

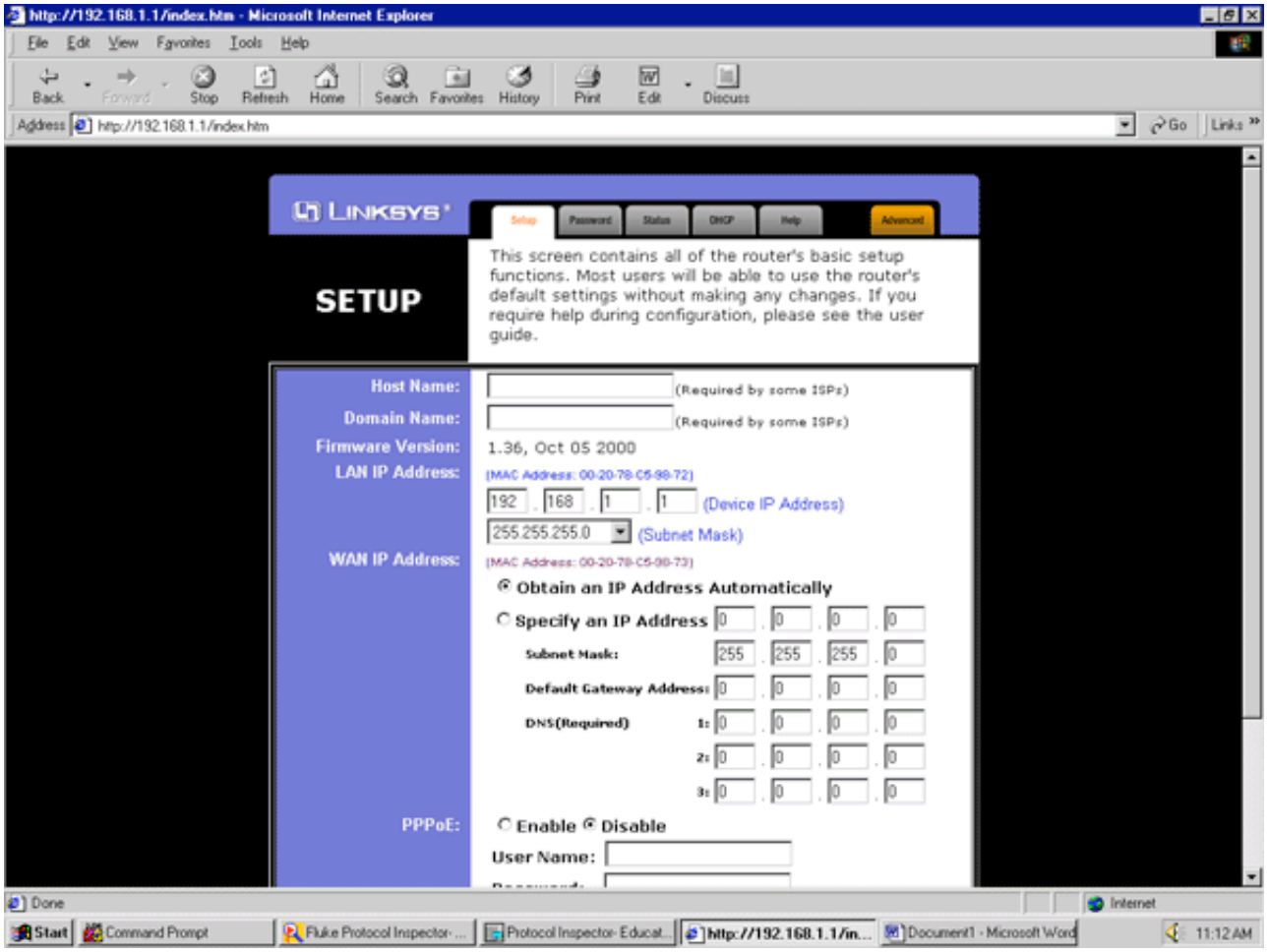
When combined with even lightweight host-based FW software, it becomes a rather effective network design. It is not a perfect device, but because it is easy to set up, is inexpensive, and is by design a NAT box with no default port openings it would certainly help reduce the likelihood of a few thousand home users becoming the launch points of the next major DDOS! (ftp://ftp.linksys.com/pdf/befsr41ug.pdf)

The design elements



This diagram shows one possible arrangement to take advantage of the segregation available with a router. With all defaults in place (including no DMZ), the "Sniffer" box has almost nothing to watch. The combination of switching and routing, with a browser-based configuration GUI to set port options, reduces the network to external traffic specifically addressed - and by default returning from established connections only.

© SANS Institute 2000 - 2005 Author retains full rights.

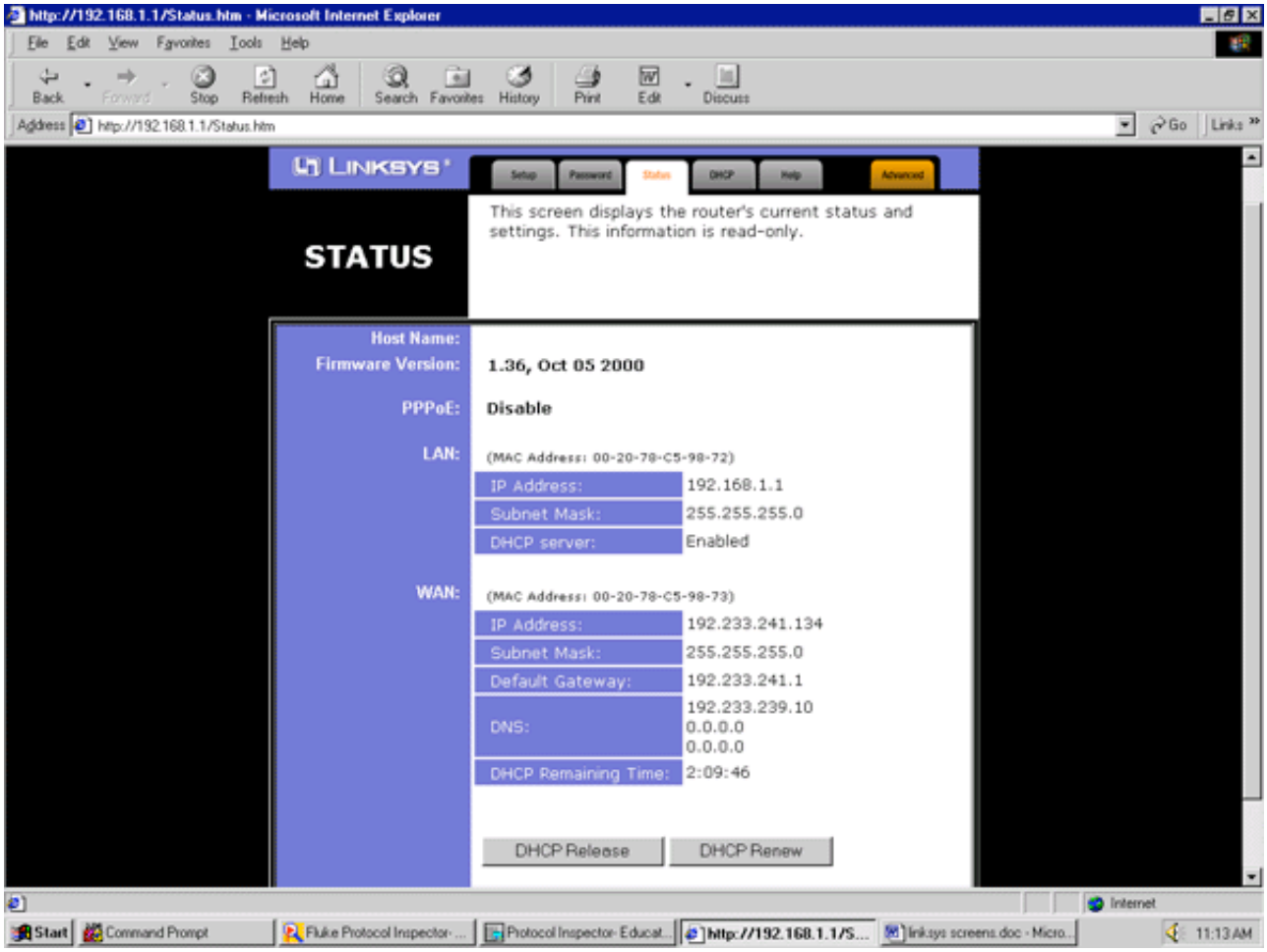


Opening setup screen. Note auto detect of MAC addresses and both DHCP & static IP options.

The above screen capture show the basic setup beginning. Just off frame are buttons for DHCP release & renew. It doesn't get much simpler, yet the defaults are biased in favor of internal systems security.
As seen in the next screen shot:

© SANS Institu

© SANS Institute 2000 - 2005 Author retains full rights.



This is the Status screen after DHCP. The built in NAT function translates any traffic from the internal net destined for the world from the 192.168.x.x "private" to the "legal" external address obtained by DHCP. Simply stated, the external traffic from your systems all appear to be coming from a single, legal IP. This significantly reduces the intelligence gathering opportunities (net mapping) of most "hackers."

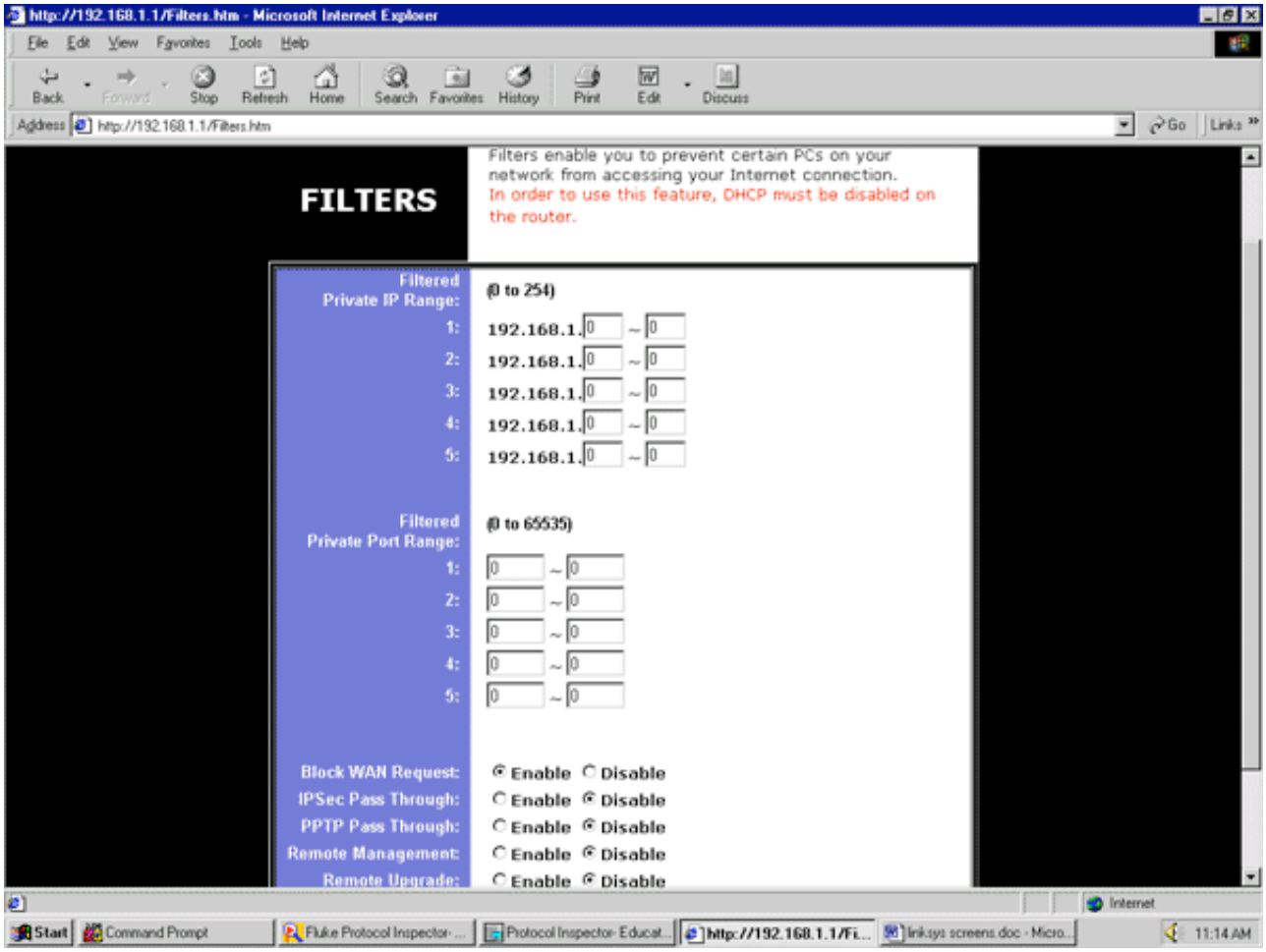
If they don't know you have a network behind here, it attracts much less attention. There are plenty of other targets that draw attention to hackers' interests, and your network simply will not appeal to most. For those who are seriously targeting systems like this, there are still very few ways to get beyond the NAT. The current IOS (1.36) includes a logging feature:

216.23.162.156	113
64.45.30.186	23
24.218.232.52	27374
207.96.122.252	1024
63.216.196.88	111
136.142.110.18	5232
24.128.1.34	68

This table shows several hostile attempts, to such tcp ports as 111 (portmap & SunRPC) and 27374 (Sub-seven Trojan Horse). This provides a simple check for inbound (and outbound) activity. I would recommend an additional box (perhaps an older legacy system) as a DMZ "listening" post with firewall or sniffer software. This is a low maintenance approach that still affords significant improvements for a small office and small business staff.

Furthermore, with filtering the LinkSys can prevent some of your internal systems from access external addresses or the Internet.

© SANS Institute 2000 - 2005 Author retains full rights.



All in all, this is a very capable system for the money and will significantly improve the defense in depth of a SOHO with minimal network administrative impact. It will actually improve bandwidth management with only a minimum of design effort.

With no DMZ enabled, no one will be initiating connections to an internal system. With a DMZ, or specific systems enable to respond to specific ports (forwarding), only those systems you have designated will respond to external traffic enquiries. It may not prevent you from being compromised by a remote access Trojan, but it will certainly reduce the odds.

Conclusion

No one gadget or software package can be "the solution" to the complex and dynamic challenges of controlling system access and connectivity. This is not a "firewall" - it filters packets by IP. However, that is sometimes the marginal definition used by software vendors to promote their "Security" software.
This system should be considered as one element in an overall system design providing network defense in depth. Only when a range of systems and techniques are combined can you really begin to approach system security.

References

GNAT Box, Inc. Web page. Gnat Box Light. URL: http://www.gnatbox.com/Pages/gblight.html (8 Dec 2000)

Graham, Robert. "FAQ: Firewall Forensics (What am I seeing?)" version 0.4.1, 20 June 2000. URL: http://www.robertgraham.com/pubs/firewall-seen.html (8 Dec 2000)

LinkSys, Inc. Web page. BEFSR41 - EtherFast 4-Port Cable/DSL Router. URL: http://www.linksys.com/products/product.asp?prid=20&grid=5 (8 Dec 2000)

© SANS Institute 2000 - 2005 Author retains full rights.

LinkSys, Inc. Web page. LinkSys EtherFast Cable/DSL Routers: User's Guide. © 2000. URL: ftp://ftp.linksys.com/pdf/befsr41ug.pdf

Pfleeger, Charles. "Security in Computing." Boston. Prentice Hall, 16 September 1996. Chapter 1.

Spitzner, Lance. "Know Your Enemy: The Tools and Methodologies of the Script Kiddie." 21 July 2000. URL: http://project.honeynet.org/papers/enemy (8 Dec 2000)

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