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

USING THE D-LINK DI-604 TO SECURE YOUR NETWORK

Scott Walker
GSEC Practical Version 1.4b

ABSTRACT

The D-Link Express EtherNetwork DI-604 is an inexpensive 4-port ethernet broadband router, and has many security features found in higher-end routers. Some of the features include Stateful Packet Inspection (SPI) Firewall, Content Filtering, Demilitarized Zone (DMZ) support, Virtual Private Network (VPN) support, Network Address Translation (NAT), logging and web-based management. The DI-604 can improve security by making the setup and administering these features an easy endeavor. A PC Magazine review stated, "The easiest, most secure way to share a cable or DSL Internet connection is with a router. Two things recommend the new D-Link Express EtherNetwork DI-604 Cable/DSL router above all others for consumer use—price and features." -1 (Ellison). With the release of worms like Code Red, the recent Blaster worm, and the virus W32.Sobig.F earlier this summer, having an inexpensive router with the above features should be on the mind of anyone with an Internet connection. This paper will examine the DI-604 starting with an overview of features, initial setup configuration, and lastly discuss more advanced security functions as they relate to a network security policy.

OVERVIEW

A router is a device or software that forwards network data packets using Internet Protocol (IP) addresses from a source to a destination, directing the traffic according to programmed or learned routing tables. A router basically determines the next network point to which a packet should be forwarded toward its destination. They can also be used to inspect and filter packets using ACL rules, but a firewall setup will usually provide more robust rules.

A firewall is a device or software that is placed in front of your computer or network; it prevents unauthorized access to or from your network. A firewall like a router is used to inspect and filter unauthorized traffic from your network, but can include more advanced rules for allowing or preventing different types of traffic. For example, blocking telnet requests and allowing only secure shell (ssh) connections, blocking specific ports used by worms or virus payloads, and blocking or allowing only specific IP addresses to certain ports. By monitoring security alerts and being aware of any new security threats, you can help mitigate risks by keeping firewall rules up to date. An important rule to remember is Risk = Threat X Vulnerability. If you're vulnerable and threat is introduced, your risk goes up!

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The DI-604 provides many router and firewall options that a user would require to secure a small network against threats and vulnerabilities. The configurations are easy and done via a web-based interface. You will require a web browser; Netscape Communicator, Microsoft Internet Explorer and other java-enabled browsers work with the product. No command line interface (CLI) is available; hopefully most administrators will be comfortable with the web GUI interface. The DI-604 also includes NAT and Dynamic Host Configuration Protocol (DHCP). NAT helps to keep the internal computers hidden, by not using routable Internet IP addresses. NAT also reduces the need for a large amount of public IP addresses by creating a separation between publicly known and privately known IP addresses. DHCP allows for ease of adding new systems to the 4-port switch of the DI-604. DHCP can be used to automatically assign NAT IP addresses, and to deliver TCP/IP information such as the subnet mask and default router to computers on the network. Figure 1 shows the DI-604 setup in a simple network scenario.

Figure 1



Here is a look at some of the firewall and access control features offered by the DI-604. By utilizing these features, a network administrator can secure access to their network.

Firewall rules include allowing or denying traffic from passing through the DI-604. This is done by creating rules for a source and destination IP address range. You can select which interface (LAN, or WAN), TCP or UDP and a port range for a rule. Firewall rules can also be scheduled. For example, rules can be active on certain days for a specific amount of time (hours or minutes), or scheduled as always on.

Content filtering based on IP Address, MAC Address, URL or Domain Name can be turned on and allows or denies users from accessing the Internet via different types on content. Content filtering can be scheduled as well.

Virtual servers enable exposing services on your network, making them accessible to Internet users. Using an internal IP address with a private port and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

a public port mapping allows this feature. For example, you could provide only http access to a specific server on the DI-604.

DMZ support allows a computer connected to the DI-604 to be fully exposed to the Internet, while it and the remaining computers on the internal LAN are continually behind the firewall and access control features. This allows you to protect certain computers and still be able to leave a computer directly connected to the Internet.

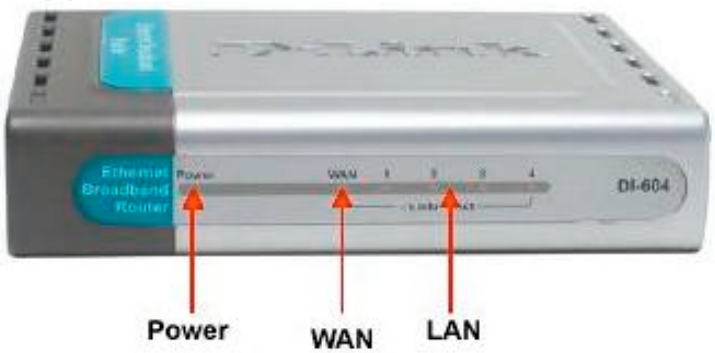
Applications requiring multiple connections can be sensed, and then a multi-port tunnel will be opened for it. Some examples of this are Internet gaming, video conferencing, and voice over IP. This is accomplished using an internal trigger port and external public port mapping.

VPN support includes up to fifty IP Security (IPSec) and twenty Point –to-Point Tunneling Protocol (PPTP) concurrent sessions. This provides secure access to networks through a variety of VPN clients, and can be very useful if you have many VPN clients on the network. VPN connections are most commonly used with connecting to a work/corporate environment. Most companies nowadays will only allow for employees to connect over a corporate VPN session, as it provides an additionally security layer. That additional security is that data is encrypted over the VPN session from source to destination.

INTIAL SETUP CONFIGURATION

The DI-604 includes the following on the front panel, Power indicator, Wide Area Network (WAN) status indicator, and four Local Area Network (LAN) indicators. The LAN link lights are green when a computer is connected and the ethernet connection is good. The lights blink fast when traffic is high, and slowly when traffic is minimal. Figure 2 shows the front panel display.

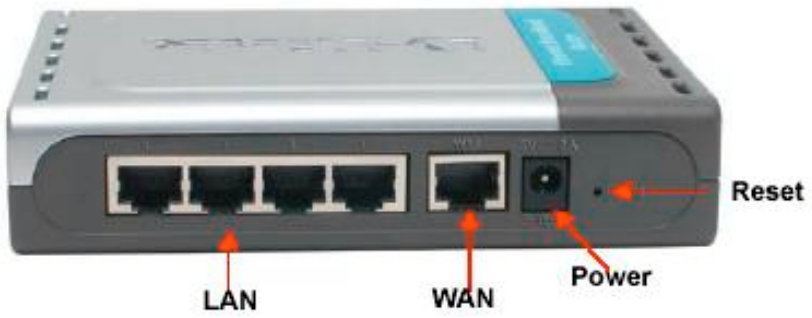
Figure 2



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

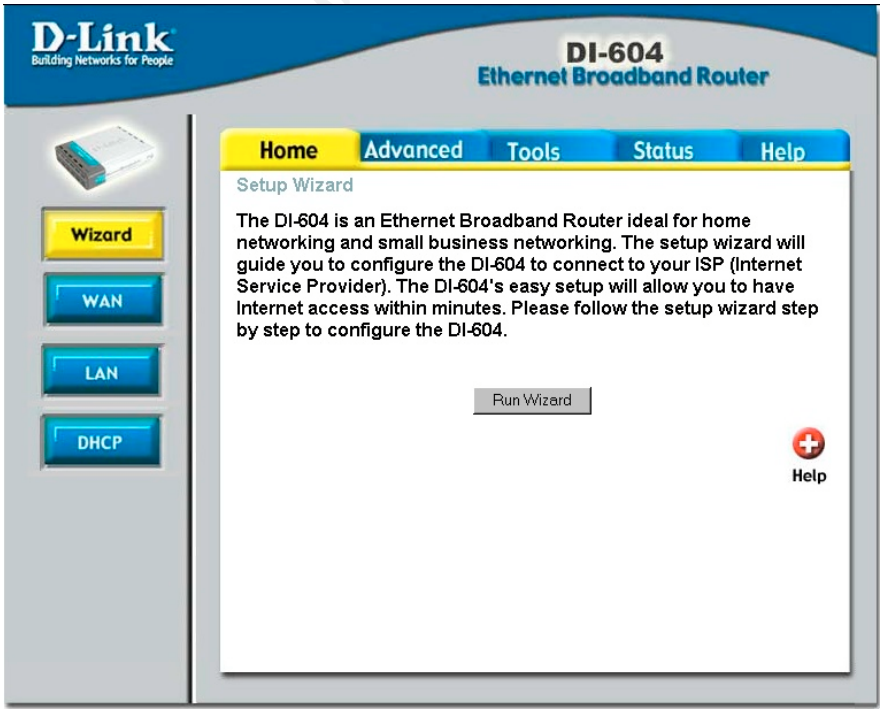
On the back panel the DI-604 includes a WAN ethernet port, four LAN ethernet ports, reset button and a power supply port. Figure 3 shows the back panel of the DI-604

Figure 3



To connect to the DI-604 plug an ethernet cable from your system to one of the available LAN ports. The default IP block used by the router is 192.168.0.0/24. Opening a web browser to http://192.168.0.1 you will be presented with a login and password screen. Default login is admin with no password. I would recommend as soon as you login to reset the admin password to something you will remember, but is rather cryptic. Having a strong password to break is a good security practice, and will help keep your router save from prying eyes. Once connected you will be presented with the main interface shown in Figure 4.

Figure 4



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

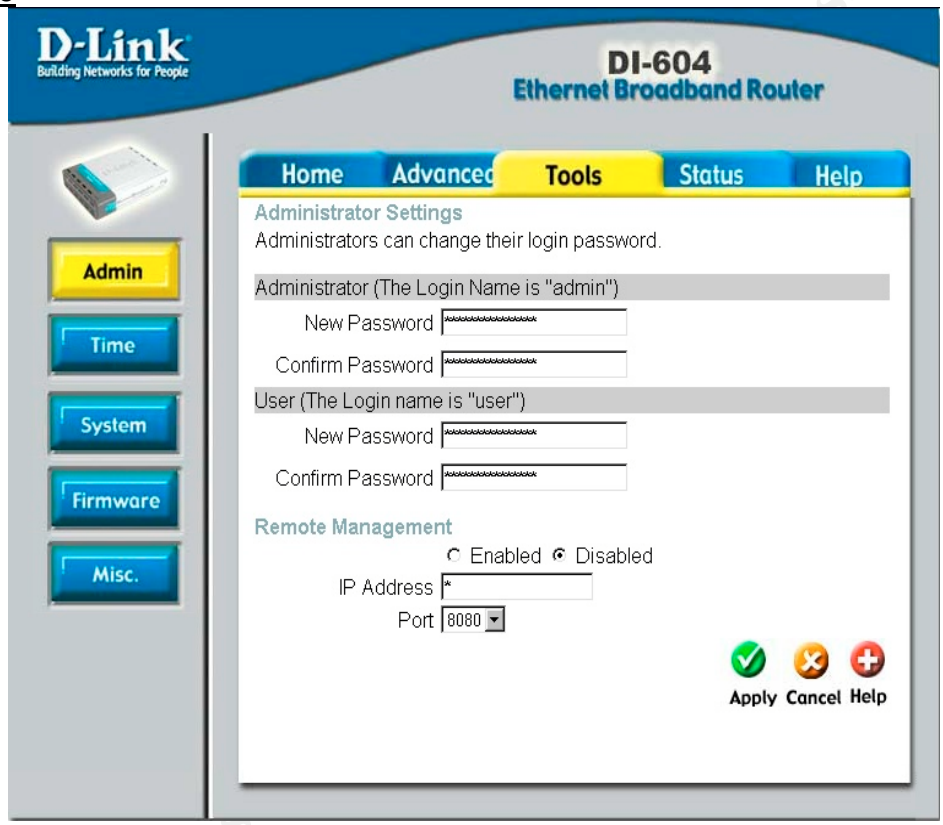
From here you can run the Wizard to help configure your WAN, LAN and DHCP settings. If you prefer you can configure the settings without the wizard. WAN settings include selecting dynamic IP address, static IP address or Point-to-Point Protocol Over Ethernet (PPPoE). Within the WAN tab you can also specify a MAC address, along with primary and secondary Domain Name Servers (DNS). DNS is used to resolve human readable website addresses to numbered IP addresses. Maximum Transmission Unit (MTU) is another setting available in the WAN tab. MTU is the size setting for the chunks of data you will send over the Internet. These network settings will depend on what your Service Provider has given you. In the LAN settings you can configure the routers IP address and subnet mask. The DHCP tab allows for the selection of a NAT IP address range (i.e. 10.10.10.X). Once these settings are configured properly you will be able to connect to the Internet with the DI-604 router default configuration. The default configuration does not have any firewall or access controls initialized.

The Tools tab shown is Figure 5 provides an Admin tab where the administrator can change the "admin" and "user" accounts passwords. The admin account has full read/write access and the user account has only read access to the router. I recommend that you keep the passwords for the admin account and the user account separate. This will give only the administrator the power to make changes on the router. I would also recommend a lengthy cryptic password (at least 8 characters) that includes numbers, letters and special characters; this will take a longer time to crack. You should change the password frequently or as your security policy dictates. The admin account cannot be renamed, so good passwords and timely changes are always good practice. The DI-604 also has an option here of allowing remote management via the Internet, which is disabled by default. I recommend keeping the remote control feature disabled. It only allows for access through http, which is not very secure (your password will be sent in plain text). No other secure protocols are available for the remote control (https, or ssh), so I would recommend maintaining the router from a system behind and protected by the DI-604. The Time tab allows for setting of the local time and daylight savings. Keeping correct time is important for any logs you will generate. You can also setup to use a Network Time Protocol (NTP) server, if one is available. This will keep the routers time in sync with any servers that use the same NTP master server. On the System tab you can save your router settings (firewall rules, NAT subnets used) to a local hard drive, or load settings from a file on a local drive. There is also a button to restore the DI-604 to factory default settings. The Firmware tab, which is next, allows the administrator to download firmware images from the Internet and load them on the DI-604. I recommend checking for new firmware from the vendor often, as it can help plug any new security holes that may be available on the router. Lastly the Misc tab has options for rebooting the device, doing ping tests, blocking external WAN pings. Blocking pings is a helpful security measure, as it is a common method used by hackers to test whether your WAN IP address is valid. Universal Plug and Play (UPnP) can also be enabled, UPnP is a networking architecture that provides compatibility among

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

networking equipment, and software. Gaming mode can be enabled to make gaming and voice application work smoother. VPN Pass-Through should be enabled to allow for VPN clients on the network to function properly. The last options of the Tools tab is Dynamic DNS, which is a method for keeping your hostname linked to your changing dynamic IP address. This would be used for most high-speed cable and DSL connections, where a dynamic IP address is usually assigned for a certain duration.

Figure 5



ADVANCED SECURITY

Security of a network can be a daunting task to cover, with all the different threats, exploits and attacks that are out there in the wild. When securing a network, a good place to start is auditing or questioning your environment to see what you have and would like to protect. According to Bill Hayes, "An information security audit is one of the best ways to determine the security of an organization's information without incurring the cost and other associated damages of a security incident." – 2 (Hayes). Some example security auditing questions to ask are; which applications and services do I want users to have access to, which ports should be available to internal and external users, are systems patched to latest stable level, what is the value of the resources I am going to protect, and what would be the impact on my business or personal life if threaten. By asking and answering some questions similar to these about your

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

network you can begin to define a security policy to protect your network. Then you will be able to relate a security policy to the DI-604's more advanced features.

A network security policy in practical terms means, a philosophy or strategy with regard to confidentiality, integrity and availability of information. Hayes also mentions, "as organizations evolve, their security structures will change as well. With this in mind, the computer security audit is not a one-time task, but a continual effort to improve data protection." – 3 (Hayes). Here is a brief summary of the three areas within a security policy that you should consider:

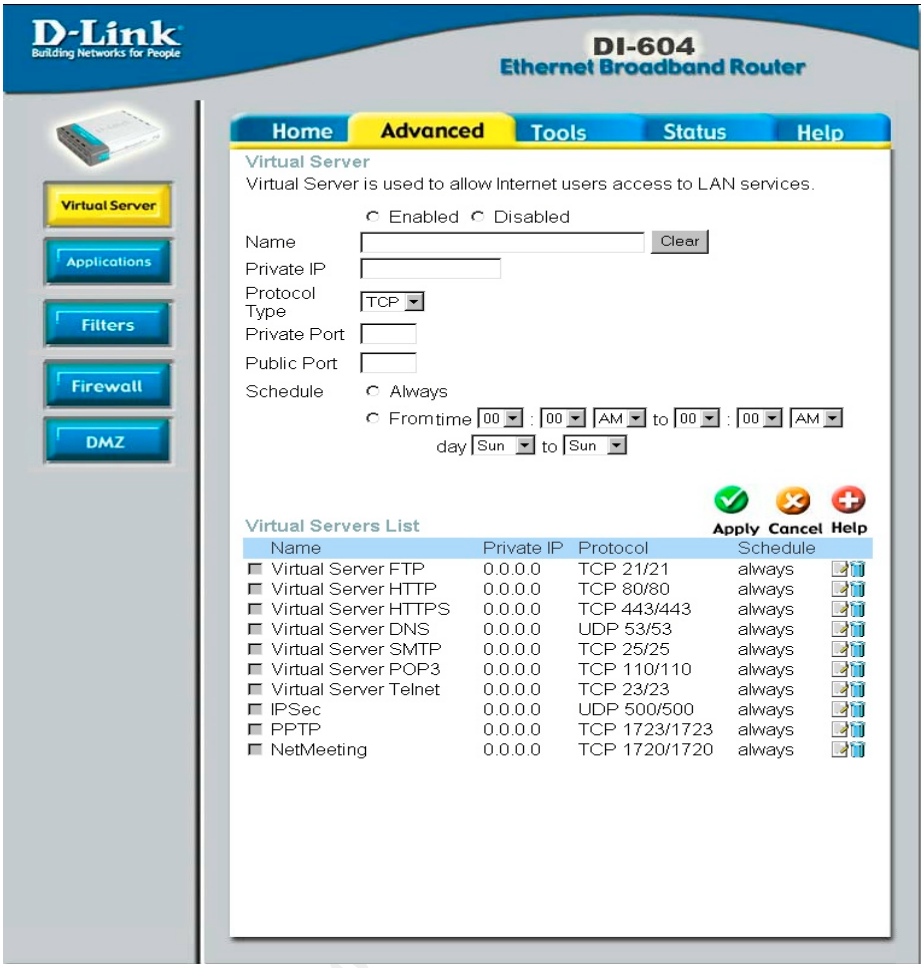
- Confidentiality is about keeping your valuable information private and in your hands only. Making sure only authorized persons have access to information and are able to do so.
- Integrity is about making sure information cannot by tainted, modified or destroyed in a malicious way. Incorrect information would be of no value; therefore protecting information from authorized access keeps integrity.
- Availability is about ensuring information is always available to you and your authorized users.

Once you have you have an idea of what you would like to protect you can begin to use the security features of the DI-604 to harden your network. Charl Van Der Walt mentions of a security policy, "Your IP network security policy will ensure that machines are always installed in a part of the network that offers a level of security appropriate to the role of the machine and the information it hosts." – 4 (Van Der Walt). Lets start by looking at some of the more advanced features that can be utilized within a security policy.

The DI-604 can configure up to ten virtual servers so that remote Internet users accessing services via WAN IP address can be redirected to local servers on LAN network. This is completed by mapping a private NAT IP address, port number and protocol type (UDP/TCP) to an external public port. You can also schedule when the virtual service will be available. Using the virtual server feature enables you to have your trusted services available from different hosts on your internal LAN network. You may have FTP open on computer1 and Simple Mail Transport Protocol (SMTP) open from computer2, while keeping other services on the computers hidden. This makes the services fully available and open to the Internet, but you should be aware of any vulnerabilities to the services you allow and keep them patched to the latest level from vendors. This would be accomplished by being vigilant of security alerts of patches/hotfixes available from your vendors. Figure 6 shows the Virtual Server tab and some default services to choose from.

Figure 6

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Some applications require multiple connections, such as gaming, video conferencing, and voice over IP. These applications can sometimes have trouble working with the internal LAN NAT IP addresses. If you need to run applications that require multiple connections, the DI-604 allows twenty special connections by using an internal trigger port and trigger protocol type (TCP/UDP). Allowing these special connections offer an availability feature rather than a security feature. A good security policy and firewall rules will allow for these services to be available to specific users that utilize them. Some well-known special applications are setup by default (shown in Figure 7), and simply need to be enabled.

Figure 7

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



The DI-604 router uses filters to deny or allow internal LAN computers from accessing the Internet. This is achieved by using rules containing IP addresses, MAC addresses or restricted websites URL's. The setup up of these rules is straight forward, as described below. These filters allow for availability of information, and can keep other information confidential by blocking access.

IP Filters deny particular LAN IP addresses from accessing the Internet. You can also block specific ports associated to the IP address. In order to setup the ruleset you must select an IP address range, port range, Protocol type, and schedule. Figure 8 shows the IP filters setup screen.

MAC Filters deny computers within the local area network from accessing the Internet via their MAC address. You can manually add MAC addresses or select MAC addresses from the list computers connected.

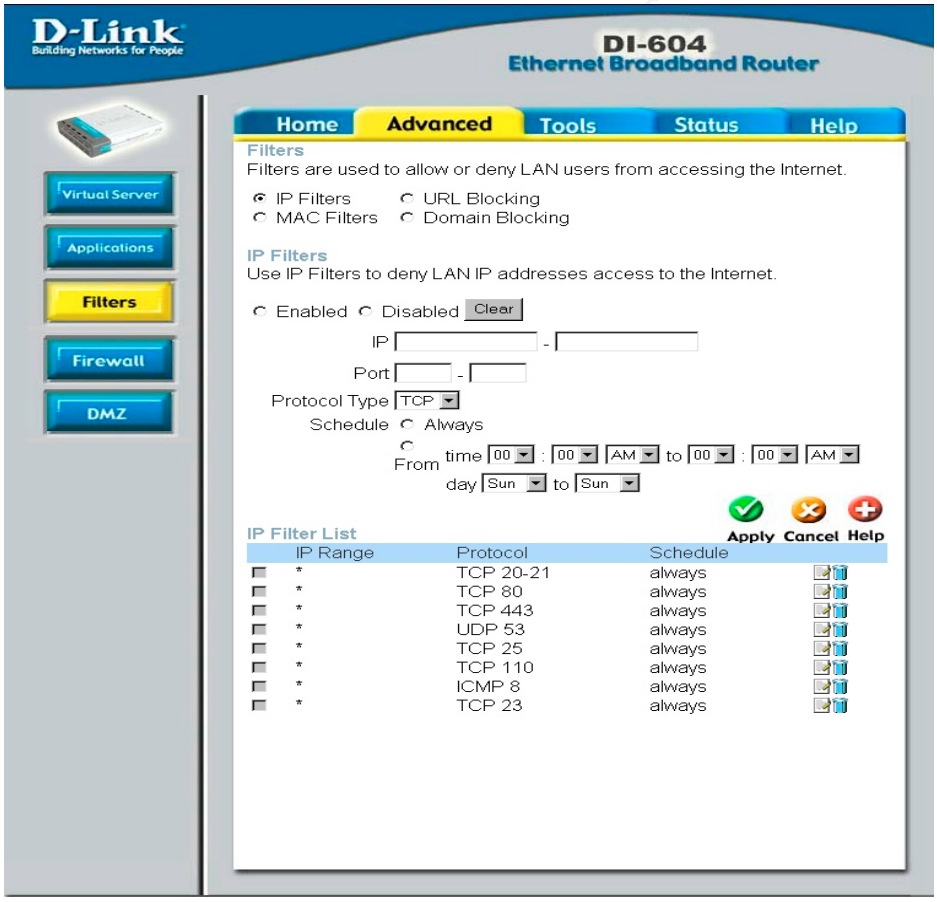
Uniform Resource Locator (URL) Blocking filter is used to deny LAN computers from accessing restricted web sites, via a keyword in the URL address. If any part of a websites URL contains the blocked word, the web page will not display. Blocking the word "sex", would not allow any sites with a URL containing the keyword sex to display.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Domain Blocking filters deny or allow computers on the internal LAN from accessing specific web sites by its URL. The URL can be either ftp or http based. Some examples would be to allow news sites (cnn.com) and deny sex sites (sex.com).

The IP, MAC, URL, and domain blocking features would be great for anyone with kids, where they would like to prohibit viewing of certain web addresses or keep entire systems off the Internet. It could also work well in a small office environment, blocking employees from being distracted from anything from online gaming sites to offsite email addresses such as hotmail or yahoo.

Figure 8

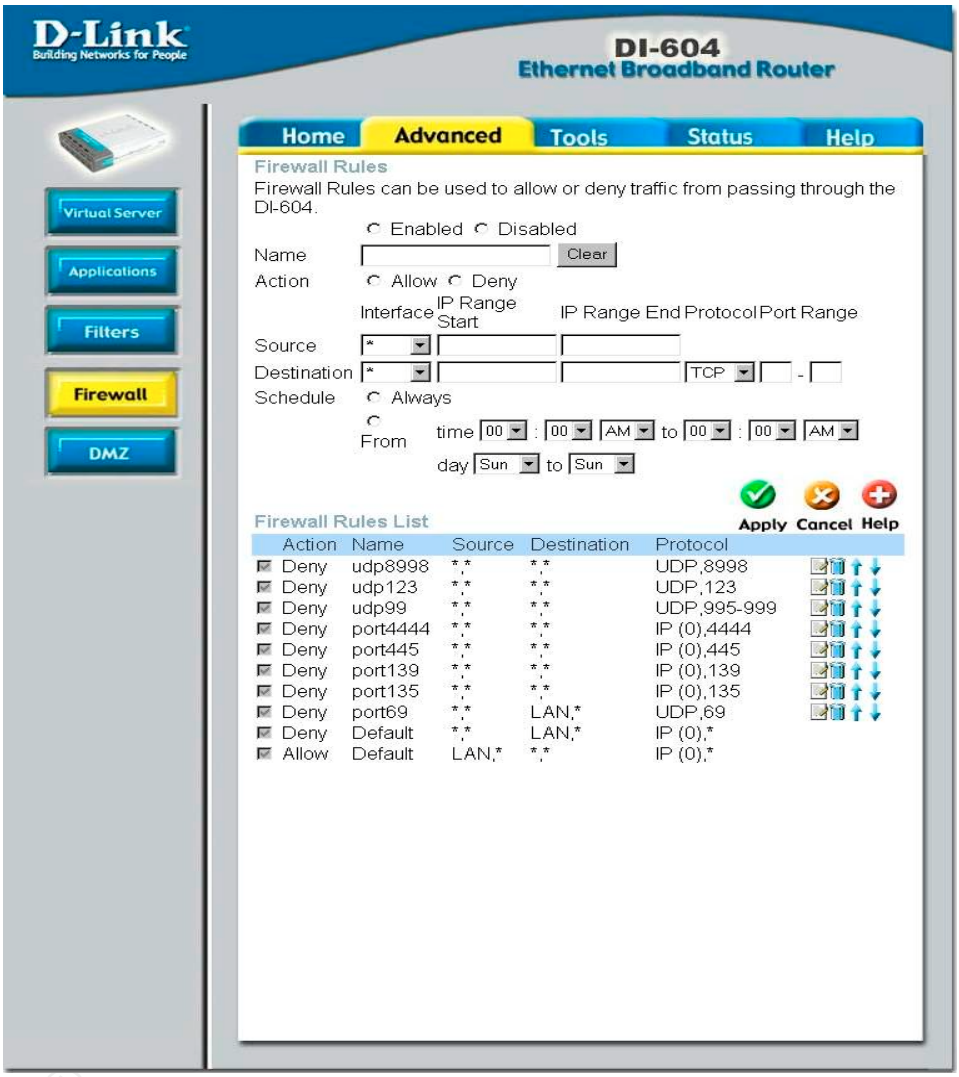


Setting up DI-604 firewall rules is the next available tab. Firewall rules deny or allow traffic from passing through the router, they act like filters but have more detailed rules. Firewall rules will contain all filter rules pertaining to IP addresses, and will also pick up any virtual services rules. Setup involves naming your ruleset, selecting allow or deny, selecting source interface

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

(WAN/LAN or * for both), IP address range, then destination interface, IP address range, protocol type, and finally port range. The firewall rules are used in priority from top to bottom, with top being the highest priority. In Figure 9 “Deny” would be the highest priority rule. A special note is that MAC address filtering has precedence over the firewall rules.

Figure 9



By setting up rules to block or allow specific ranges of IP addresses to specific ports, you can have a more granular approach to hardening your network. A finely tuned firewall can help keep your network available, by keeping unwanted intruders or malicious attacks at bay. It can maintain your computers and data integrity by keeping unauthorized persons from handling your information. Lastly by not allowing unauthorized access, your information can be kept safe and confidential. In August 2003 a new worm was released

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

onto the Internet, that affected Microsoft Windows based machines. It is describe in the following statement from CERT:

> The W32/Blaster worm exploits vulnerability in Microsoft's DCOM RPC interface as described in VU#658148 and CA-2003-16. Upon successful execution, the worm attempts to retrieve a copy of the file msblast.exe from the compromising host. Once this file is retrieved, the compromised system then runs it and begins scanning for other vulnerable systems to compromise in the same manner. In the course of propagation, a TCP session to port 135 is used to execute the attack. However, access to TCP ports 139 and 445 may also provide attack vectors and should be considered when applying mitigation strategies. Microsoft has published information about this vulnerability in Microsoft Security Bulletin MS03-026. – 5 (Dougherty…)

Systems that were not patched or protected by a firewall could easily be infected within minutes or even seconds. Within the alert issued by CERT there were specific ports that can be blocked to avoid being infected. The following ports were announced to be involved:

> Sites are encouraged to block network access to the following relevant ports at network borders. This can minimize the potential of denial-of-service attacks originating from outside the perimeter. The specific services that should be blocked include
>
> - 69/UDP
> - 135/TCP
> - 135/UDP
> - 139/TCP
> - 139/UDP
> - 445/TCP
> - 445/UDP
> - 593/TCP
> - 4444/TCP - 6 (Dougherty…)

By keeping up to date with security alerts, you would be able to block the worm from infecting your systems using the DI-604's firewall features. You could setup firewall rules to block the above ports, while you apply or wait for patches to be released by the vendor. For security alerts I would recommend getting on security bulletin mailing lists (cert.org for example).

Firewalls are not generally used to prevent viruses from spreading. But in the case of the W32.Sobig.F virus recently released onto the Internet, a firewall

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

can definitely help mitigate some of the damage of the virus. W32.Sobig.F tries to contact the list of 20 IP addresses contained in its malicious code in order to download a backdoor Trojan and Wingate proxy server. By blocking the ports involved, which were UDP port 8998, UDP 123 and UDP ports 995, 996, 997, 998 and 999, the DI-604's firewall can help decrease the damage caused by this type virus. Network administrators had a busy summer keeping up with the virus and worm writers out there!

With the DI-604 you can also place a computer in a DMZ; which will be behind the firewall but exposed to full Internet access. This is excellent for a system that cannot run services/applications properly from behind the DI-604 or a honeypot setup. A honeypot is a computer with vulnerabilities that acts as a decoy, luring in hackers to watch their activities and monitor how they break into the computer. By studying the break-in an administrator can start to design more secure systems. The DMZ allows for unrestricted Internet access on that system, and may expose that host to a variety of security risks. Setup is simple, you just need to enter the IP address of the computer on the DMZ tab and enable. The DMZ tab is shown in Figure 10.

Figure 10



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Lastly the DI-604 has system logging capabilities. The router doesn't include logging of network traffic (http, ftp, etc), but does log system activity; debug info, attacks, dropped packets and notice alerts. You can analyze network traffic with sniffer software on one of your internal computers. Network traffic can generally produce vast amounts of data, so the DI-604 being a small inexpensive router without hard disk space can only capture so much. You can email logs off the DI-604 by providing a SMTP server and email address. The router will also email logs when full, which is two hundred lines. Keeping track of your logs is an important security task; it can help you see what is happening on the network and might help catch a new threat or vulnerability in case you missed a ruleset in the setup!

Joseph Moran gave the following summary of the DI-604 router:

> If this were a review, solely ignoring the price issue, the Dlink would come out of my testing with flying colors. The management interface is easy to navigate; basically as easy to use as any other router I've come across, and is arranged in a logical manner. The online help system is yet another bonus. It's been an issue free device, which is as it should be.
>
> The clincher here is the price. Dlink's raised the bar (or lowered it, depending on how you look at it) of expectations, and come out with a great Home/SOHO class product at an unheard of price level. With an MSRP of $49US, it's already a great bargain, but on the street, it's already selling for $39US. In that light, honestly, there's no need for ANYONE to consider going the software NAT/ICS/Wingate route to save a few bucks. Go get one of these great D-link DI604 Residential Gateways. For the price it's really only a few dollars more than the software approach, and is vastly more convenient. HIGHLY RECOMMENDED!! – 7 (Moran)

If your network is small, the D-Link DI-604 is a robust and inexpensive router, containing full firewall, filter and VPN features. The features allow an administrator to fully harden a small home or office network, reduce risks via keeping threats and vulnerabilities under control and by doing so maintain availability, confidentiality, and integrity of information.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

RESOURCES

"dslreports.com - glossary definition router." 1999-2003.
URL: http://www.dslreports.com/information/kb/router (15 July 2003).

"D-Link DI-604 4-Port Broadband Router." 2 July 2003.
URL: http://www.dlink.com/products/?pid=62 (15 July 2003).

Higgins, Tim. "Small Net Builder Product Review." D-Link Express EtherNetwork 4 Port Broadband Router (DI-604). 2001–2003.
URL: http://www.smallnetbuilder.com/Reviews-10-ProdID-DI604.php (4 July 2003).

Ellison, Craig. "Express EtherNetwork DI-604 reviewed by PC Magazine." D-Link Introduces a $49 Router. 1996-2003.
URL: http://www.pcmag.com/article2/0,4149,332154,00.asp (26 June 2003).

Moran, Joseph. "D-Link Express EtherNetwork 4-port Ethernet Broadband Router - PracticallyNetworked.com." 17 July 2002.
URL: http://www.practicallynetworked.com/review.asp?pid=470 (26 June 2003).

Hayes, Bill. "SecurityFocus BASICS Infocus: Conducting a Security Audit: An Introductory Over." 26 May 2003.
URL: http://www.securityfocus.com/infocus/1697 (17 June 2003).

Van Der Walt, Charl. "Introduction to Security Policies, Part One: An Overview of Policies." 27 Aug 2001.
URL: http://www.securityfocus.com/infocus/1193 (17 June 2003).

Van Der Walt, Charl. "Assessing Internet Security Risk, Part One: What is Risk Assessment?." 11 June 2001.
URL: http://www.securityfocus.com/infocus/1591 (18 June 2003).

Dougherty, Chad Havrilla, Jeffery Hernan, Shawn Lindner, Marty. "CERT® Advisory CA-2003-20 W32/Blaster worm." 11 August 2003.
URL: http://www.cert.org/advisories/CA-2003-20.html (14 August 2003).

D-Link DI-604 – Manual. Taiwan: D-Link Corporation, 2002.
Figure 1, Figure 2, Figure 3, 1 - 73.

D-Link DI-604 - Quick Installation Guide. Taiwan: D-Link Systems, 2002. 1 – 12.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.