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

Filtering Routers a Small Office/Home Office with a Mixed OS Environment

Ricky D. Smith,

Introduction

In this area of networking, the Small Office or Home Office (SOHO) user usually does not have the resources to invest in a network security group or in the hardware and software necessary for a secure network. In most cases the security is either non-existent or left to the resident computer "expert." Either situation leaves much to be desired since the computer "expert" is usually does network administration, server/workstation administration, and help desk support in addition to computer security. This situation is acerbated in a mixed operating system (OS) environment when the "expert" is usually only knowledgeable in one of the OSs.

In this paper I will explore one layer of a multi-layered defense of the internal network of a SOHO user, how to configure the packet filtering capability of a cable or digital subscriber line (DSL) router for a mixed OS network. With the filter set limitations of most cable/DSL routers, a normal network security filter set must be reevaluated to determine the most important services that must be blocked. A reevaluation must also be done in a mixed OS environment since a normal network security filter set for a homogeneous network will generally not be sufficiently for a different OS. This paper is an extension of the work of Rick Thompson [1] and Patrick Harris [2]

The Example Network

The example network, Figure 1, that will be used is a mixed Windows and Macintosh network. The Windows environment is a Windows 2000 domain with various client OSs including Windows 2000 Professional, Windows NT 4.0, and Windows 9x. Print and File Services for Macintosh are running on the Windows 2000 server. In the Windows 2000 domain, DNS is running exclusively for the internal network. Web services are not published to the external network.

In the Macintosh environment, the machines are running Mac OS 9.1 with Apple File Protocol (AFP) running over TCP/IP and with web sharing disabled. In addition to the computers, a hardware print server is on the network supporting both PC and Macintosh printing needs.

For Internet access, a DSL line is being used via a DSL modem and a DSL router. The DSL modem connects to the ISP through Point-to-Point Protocol over Ethernet (PPPoE). Inside the DSL modem, a small DSL router is used to route traffic to the internal machines.

The generic DSL router that I will use for this paper is a combination router and 10/100

© SANS Institute 2000 - 2005 Author retains full rights.

4-port switch that also provides PPPoE logon capability, packet filtering, internal server publishing, and network address translation (NAT). The DSL router can also act as a DHCP client on the external port and also act as a DHCP server on the internal ports. The packet filter has a capability to log the actions taken on each packet. For this paper I will set the DSL router to log all dropped packets. This does require the SOHO user to review and manage the logs on a frequent basis.

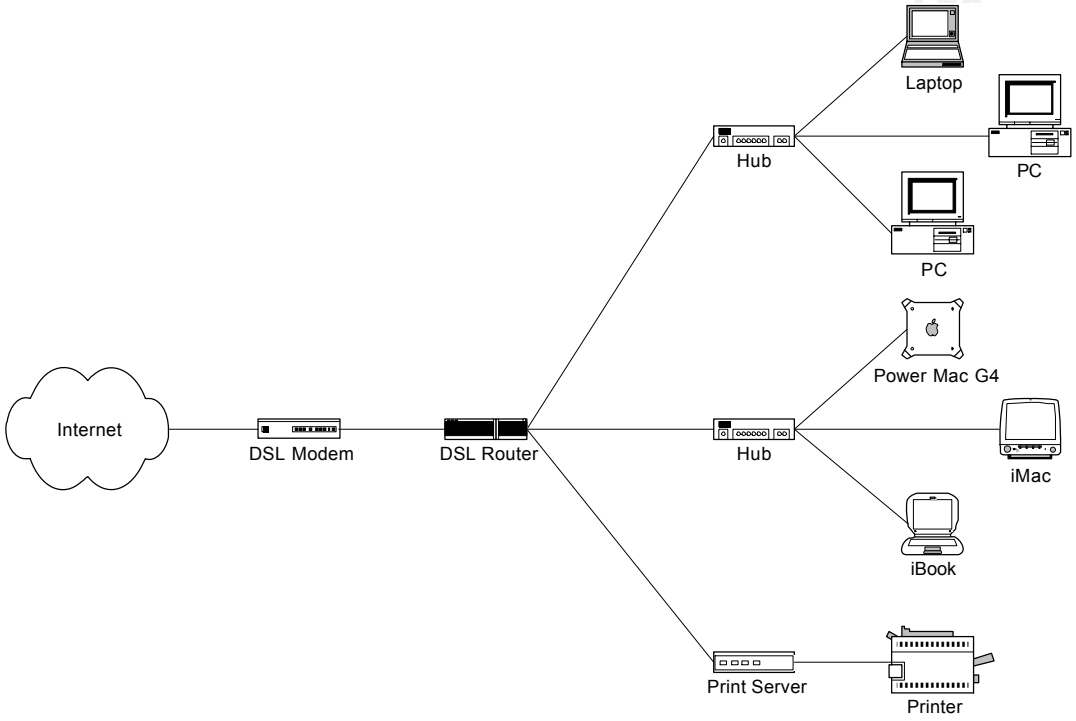


Figure 1 Example Network Diagram

IP Address Spaces

The NAT capability of the DSL router will be used to allow a private address space [3] to be used on the internal network. The DSL router will be a DHCP server with a scope of the private address space 192.168.10/24. This will provide an additional layer of security for the internal network [4].

The external network interface can have either a dynamically- or statically-assigned IP address since it will not be important to the firewall applications. For security consideration, a dynamically assigned address would provide a small measure of security since the hacker must determine the IP address of the DSL router as it changes with the DSL router leasing a new address every time it reconnects to the ISP.

Description of filtering router language

© SANS Institute 2000 - 2005 Author retains full rights.

The packet filtering capabilities of most DSL routers are limited but will provide an additional security layer. For this paper I will assume the generic DSL router allows for twelve filter sets that each contain six filter rules. Four filter sets can be cascaded together to screen a packet in a particular packet filter application. Thus, you can have a maximum of 24 rules that will screen a packet. The filter rules will be numbered by the combination of the filter set number and the rule number with in that set, for example, the fifth rule in the twelfth set would be 12-5.

Generic Filters

Each rule can be either a generic protocol independent filter or a TCP/IP filter. A generic filter allows specifying the bit pattern that the packet must match to be allowed or denied through the DSL router. For a generic filter rule you can specify the fields listed in Table 1.

Table 1 Generic Filter Fields

Offset	The point at which you want to begin the comparison. Range: 0-255. Default: 0.
Length	The number of bytes that should be used for comparison and masking. Range: 0-8. Default:0.
Mask	The hexadecimal value that will be logically ANDed with the data in the packet. The number of digits in the Mask should be two times the specified Length.
Value	The hexadecimal value that the router will compare with the masked packet data. The number of digits in the Value should be two times the specified Length
More	Specify whether the packet will pass through to the next filter rule. Options: • No (default) • Yes - Matched Action and Not Matched Action are N/A
Log	Set the logging for the each packet that attempts to pass the filter. Options are • None – no logging • Matched Action – log only if the packet matches the filter parameters • Not Matched Action – log only if the packet does not meet the filter parameters • Both – all packets are logged • Check Next Rule – the default • Forward – log only if the packet is forwarded • Drop – log only if the packet is dropped
Matched Action/ Not Matched Action	Specify what to do with the packet. • Check Next Rule • Forward • Drop

For example, a filter that would block packets that have the value 0xABCD beginning at the fourth byte of the packet would look like Table 2.

Table 2 Example Generic Filter

Filter Number:	12-1
Filter Type:	Generic

© SANS Institute 2000 - 2005 Author retains full rights.

```
Offset:          3
Length:          2
Mask:            FFFF
Value            ABCD
More:            No              Log:        None
Matched Action:          Drop
Not Matched Action       Check Next Rule
```

The abbreviated version of this rule would be

```
#     Type  Filter Rule                                  More  M     N
12-1  Gen   Off=3, Len=2, Mask=FFFF, Value=ABCD          No    D     CNR
```

where `M` is Matched Action, `NM` is not Matched Action. The actions are:

`CNR` is Check Next Rule
`D` is Drop
`F` is Forward.

Generic filters have been included in this paper for completeness of the discussion of the packet filtering capabilities of a DSL router. I will not use them in creating the filter rules for the SOHO example network.

TCP/IP Filters

For a TCP/IP rule, the fields listed in Table 3 can be specified for each filter.

Table 3 TCP/IP Filter Fields

IP Protocol	The IP-specific number of the protocol [5]. Range 0-255. ICMP is 1. TCP is 6. UDP is 17
Source Route	Specify whether to check if the source route bit of the packet.
Destination: IP Address Subnet Mask Port Port Comparison	 The IP address of the destination of the packet you want to filter. Default: 0.0.0.0 (0.0.0.0 implies any IP address.). The Subnet Mask of the destination IP address. Default: 0.0.0.0. The destination port of the packet. Range 0-65535. Default: 0. (0 implies any port.) Select the comparison operator that will be used with the Destination Port. The five options are: • None (default) • Less • Greater • Equal • Not Equal

© SANS Institute 2000 - 2005 Author retains full rights.

Source: IP Address Subnet Mask Port Port Comparison	 The IP address of the source of the packet you want to filter. Default: 0.0.0.0 (0.0.0.0 implies any IP address.). The Subnet Mask of the source IP address. Default: 0.0.0.0. The source port of the packet. Range 0-65535. Default: 0. (0 implies any port.) Select the comparison operator that will be used with the Source Port. The five options are: • None (default) • Less • Greater • Equal • Not Equal
TCP Established	This field is specific to IP protocol 6 (TCP). For other protocols, the field is ignored. • Yes – Filter will only matched established connections. • No – Filter will match both initial and established connections
More	Specify whether the packet will pass through to the next filter rule. Options: • No (default) • Yes - Matched Action and Not Matched Action are N/A
Log	Set the logging for the each packet that attempts to pass the filter. Options are • None – no logging • Matched Action – log only if the packet matches the filter parameters • Not Matched Action – log only if the packet does not meet the filter parameters • Both – all packets are logged • Check Next Rule – the default • Forward – log only if the packet is forwarded • Drop – log only if the packet is dropped
Matched Action/ Not Matched Action	Specify what to do with the packet. • Check Next Rule • Forward • Drop

For example, a filter that block incoming DNS queries is shown in Table 4.

Table 4 Example TCP/IP Filter

```
Filter Number:      9-1
Filter Type:        TCP/IP
             IP Protocol:    17              IP Source Route:  No
             Destination:    IP Address:     0.0.0.0
                             IP Mask:        0.0.0.0
                             Port Number:    53
                             Port
                             Comparison:     Equal
             Source:         IP Address:     0.0.0.0
                             IP Mask:        0.0.0.0
                             Port Number:    0
                             Port
                             Comparison:     None
```


© SANS Institute 2000 - 2005 Author retains full rights.

```
TCP
Established:    N/A
More:           No              Log:        None
Matched Action:         Drop
Not Matched Action      Check Next Rule
```

The abbreviated version of this rule would be

```
#     Type  Filter Rule                                    More  M     N
9-1   IP    Pr=17,SA=0.0.0.0, DA=0.0.0.0, DP=53            No    D     CNR
```

The filters can be assigned to the input or output of either the external interface or the internal interface. This allows the creation of four filter applications from cascaded filter sets. Figure 2 shows the four available filter applications.

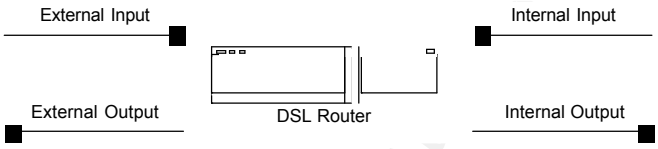


Figure 2 Filter Applications

Each filter application is built by specifying the filter sets in the order in which they should be applied. For example, if the filter sets 2, 5 and 7 will be used to filter the outbound packets on the internal interface then the internal input filter application is specified by:

```
Internal Incoming Filter Sets: 2,5,7
```

To make the filter application function correctly, each of the filter sets, except the last, must be modified to pass the packet to the next rule and not terminate. This means that the last filter rule in the set must have "`Check Next Rule`" specified for either Matched Action or Not Matched Action. The last filter set must terminate the application by specifying either "`Forward`" or "`Drop`" in both the "Matched Action" and the "Not Matched Action" fields for the last filter rule in the application.

Rule Set

For this paper I will assume that the internal network in this SOHO situation does not have any servers that must be reached from the external network. This may not be the case in all SOHO configurations. The addition of servers to the internal network that must be accessible from the external network would also require the configuration of the internal server publishing feature of the DSL router which will not be covered in this paper.

The list of ports and services that should be protected is extensive as discussed in Rick Thompson's paper.[1] In a normal firewall application, the recommended setup is to "deny all" and specifically allow the necessary ports to be open. In that case, the

© SANS Institute 2000 - 2005 Author retains full rights.

external input filter would look something like:

```
#     Type  Filter Rule                                    More  M     N
10-2  IP    Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP<1025         No    D     CNR
10-3  IP    Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP<1025          No    D     F
```

Of course, this filter set blocks will block any inbound connections to all "well-known" ports [5]. Any ports that need to be open to allow access to internal servers must be added *before* the "deny all" rules. For example, to allow access to an internal FTP server a filter rule similar to the following must be added.

```
#     Type  Filter Rule                                    More  M     N
10-1  IP    Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21            No    F     CNR
```

However, this will not show the concerns of the mixed OS SOHO environment that is the point of this paper. Therefore, I will not use the capability to block the well-known ports in this manner.

ICMP

The DSL router that has NAT capabilities appears as a single host to the external network. The external network should drop ICMP packets that are destined for the internal network since the internet router should not be configured to route packets addressed to a private address space. If a routable address space was being used on the internal network then, ICMP should be blocked by the external inbound filter application. The filter rule would be

```
#     Type  Filter Rule                                    More  M     N
10-4  IP    Pr=1, SA=0.0.0.0, DA=X.X.X.X, Mask=Y.Y.Y.Y     No    D     CNR
```

where `X.X.X.X` and `Y.Y.Y.Y` define the internal IP address space. This filter will break the "ping" and "tracert" commands since incoming responses from the external network will be dropped.

Source-Routed Packets

Source-routed packets are packets that specify the route that the packet will take going to its destination and also specifies the return path for responses. These packets can be used map or exploit the internal network.[6] To block source-routed packets the following filter rule would be used on the external input.

```
#     Type  Filter Rule                                    More  M     N
1-1   IP    Pr=0, Source Route = Y                         No    D     CNR
```

Private IP Address Spaces

The private address spaces specified by RFC 1918 [3] should not be routed across the network. However, a malicious user could attempt to send packets with a spoofed IP

© SANS Institute 2000 - 2005 Author retains full rights.

address that would appear to come from the internal network. The filter rules to block the private addresses at the external input would be

```
#     Type  Filter Rule                                          More  M     N
1-2   IP    Pr=0, SA=0.0.0.0, DA=10.0.0.0, Mask=255.0.0.0        No    D     CNR
1-3   IP    Pr=0, SA=0.0.0.0, DA=127.0.0.0,                      No    D     CNR
            Mask=255.0.0.0
1-4   IP    Pr=0, SA=0.0.0.0, DA=172.16.0.0,                     No    D     CNR
            Mask=255.255.0.0
1-5   IP    Pr=0, SA=0.0.0.0, DA=192.168.0.0,                    No    D     CNR
            Mask=255.255.0.0
```

Egress Filtering

The DSL router should filter out any outbound packets that have source addresses that do not match the internal network address space. Further information on egress filtering is available in Chris Brenton's paper.[7] The egress filter that would be applied to the inbound packets at the internal input interface should look like

```
#     Type  Filter Rule                                          More   M     N
7-1   IP    Pr=0, SA=192.168.10.0, DA=0.0.0.0,                   No     F     D
            Mask=255.255.0.
```

Common Ports

The following rules block inbound access the common services that are not published to the external network and are not specific to either OS in use on the internal network. The ports that will be blocked are:

- FTP (21)
- telnet (23)
- SMTP (25)
- DNS (53) on TCP and UDP
- HTTP (80)
- POP3 (110)
- IMAP (143) and
- HTTPS (443).

The "small services" ports (less than 20) will also be blocked. To minimize the number of rules the small services, FTP, telnet and SMTP ports will all be blocked by a single rule, number 1-6. This rule then also blocks port 22 and 24, neither has an assigned service [5]. Also, because a hardware print server is part of the example network, the LPD port (515) should be blocked.

```
#     Type  Filter Rule                                          More  M     N
1-6   IP    Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP<26                  No    D     CNR
2-1   IP    Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=53                  No    D     CNR
2-2   IP    Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=53                 No    D     CNR
2-3   IP    Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80                  No    D     CNR
2-4   IP    Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=110                 No    D     CNR
2-5   IP    Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=143                 No    D     CNR
2-6   IP    Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=443                 No    D     CNR
3-1   IP    Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=515                 No    D     CNR
```

Windows

© SANS Institute 2000 - 2005 Author retains full rights.

In an environment with Windows 2000/NT/9x, the blocking of NETBIOS ports (135, 136, 137, 138, 139, 445) is required both inbound and outbound on the external interface for both TCP and UDP. With a Windows 2000 domain, inbound LDAP (389) and LDAP over SSL (636) are also of concern and should be blocked.

Inbound Filter Rules

#	Type	Filter Rule	More	M	N
3-2	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP>134	Yes		
3-3	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP<140	No	D	CNR
3-4	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=445	No	D	CNR
3-5	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=636	No	D	CNR
3-6	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP>134	No	D	CNR
4-1	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP<140	No	D	CNR
4-2	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=445	No	D	CNR
4-3	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=636	No	D	CNR

Outbound Filter Rules

#	Type	Filter Rule	More	M	N
5-1	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP>134	Yes		
5-2	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP<140	No	D	CNR
5-3	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=445	No	D	CNR
5-4	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=636	No	D	CNR
5-5	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP>134	Yes		
5-6	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP<140	No	D	CNR
6-1	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=445	No	D	CNR
6-2	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=636	No	D	CNR
6-3	IP	Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53	No	D	CNR

Filter rule 6-3 in this last set prevents a Windows machine on the internal network from trying to resolve a NETBIOS name on the internal network by using an external DNS server.

Macintosh

For a Mac OS 9.x environment, the number of ports that must be protected is smaller. The two ports that should be blocked inbound and outbound are Apple File Protocol (AFP) (548) and Program Linking (3031) [8, 9]. There are additional ports in the Macintosh environment, although not as significant, that could be blocked if there were additional filter rules that could be added.

Inbound Filter Rules

#	Type	Filter Rule	More	M	N
4-4	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=548	No	D	CNR
4-5	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=3031	No	D	F

© SANS Institute 2000 - 2005 Author retains full rights.

Outbound Filter Rules

#	Type	Filter Rule	More	M	N
6-4	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=548	No	D	CNR
6-5	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=3031	No	D	F

With the release of Mac OS X, the list of ports of concern will need to be re-evaluated. Mac OS X has a Unix-based foundation (a BSD kernel) and brings along the some of the same security concerns as running a Unix machine.

Filter Applications

External Input

The filter application for the packets being sent to the DSL router from the DLS modem will consist of filter sets 1, 2, 3, and 4. This filter application consists of 23 rules.

External Output

The outbound packets on the external interface of the DSL router will consist of filter sets 5 and 6 with a total of 11 rules.

Internal Input

The internal input filter application consists of filter set 7 with one rule.

Internal Output

The internal output filter application has no filter rules.

Setup Verification

Once the DSL router has been configured with the filter rules and filter applications, the configuration must be tested. An actual scan of the DSL router from the Internet would be the best method of verifying the configuration. For this you would have to have another machine and connection to the Internet for the scanning machine, Figure 3. Figure 3 also shows an optional sniffer machine that would be used to monitor the scanning of the external interface of the DSL router. Scanning the DSL router may not be allowed or possible depending on the ISP and any restrictions in the user agreement.

© SANS Institute 2000 - 2005 Author retains full rights.

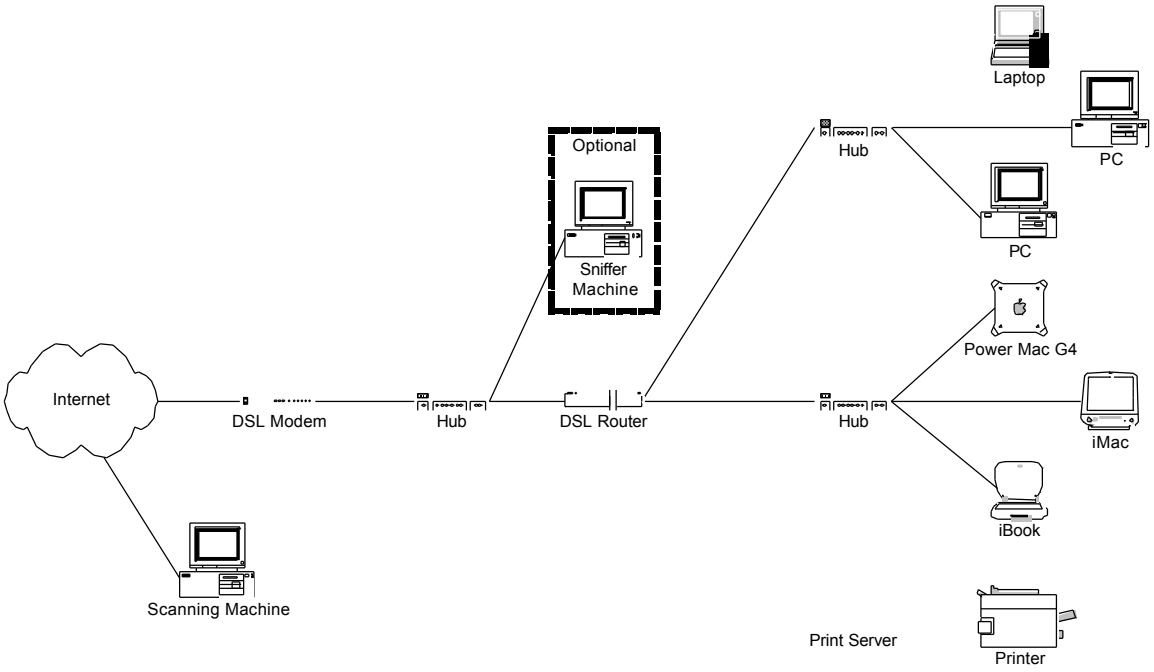


Figure 3 Example Network Diagram for Testing the DSL Router Configuration via the Internet

An alternative method is to modify the network and test the DSL router filter configuration from "in-house." To do this the connection between the DSL modem and the DSL router must be sent through a hub. For normal network operation, the DSL modem is connected to the hub through a crossover cable or to an uplink jack on the hub. The hub will have no effect on the network. During testing the DSL modem is disconnected from the hub and the scanning machine and an optional sniffer machine are connected as shown in Figure 4.

The scanning and sniffer machines and the DSL router must be configured to be on the same subnet. Prior to reconfiguring the DSL router, a backup of the router and filter configuration should be made. The DSL router reconfiguration will require shifting from DHCP to static IP addressing, unless either the scanning or sniffer machine is running a DHCP server. The reconfiguration will also require changing to standard Ethernet protocol from PPoE on the external interface..

Software for Verification Testing

The tests will be run from the scanning machine. There are several options for the automated scanning software. The short list of available commercial and freeware products is given here are mainly Windows-based and a couple that are Unix/Linux based. There are any number of commercial programs to choose from, ISS's Internet Scanner [10], eEye's Retina [11], Symantec's NetRecon [12] to name a few although these will probably be too expensive for the typical SOHO user.

© SANS Institute 2000 - 2005 Author retains full rights.

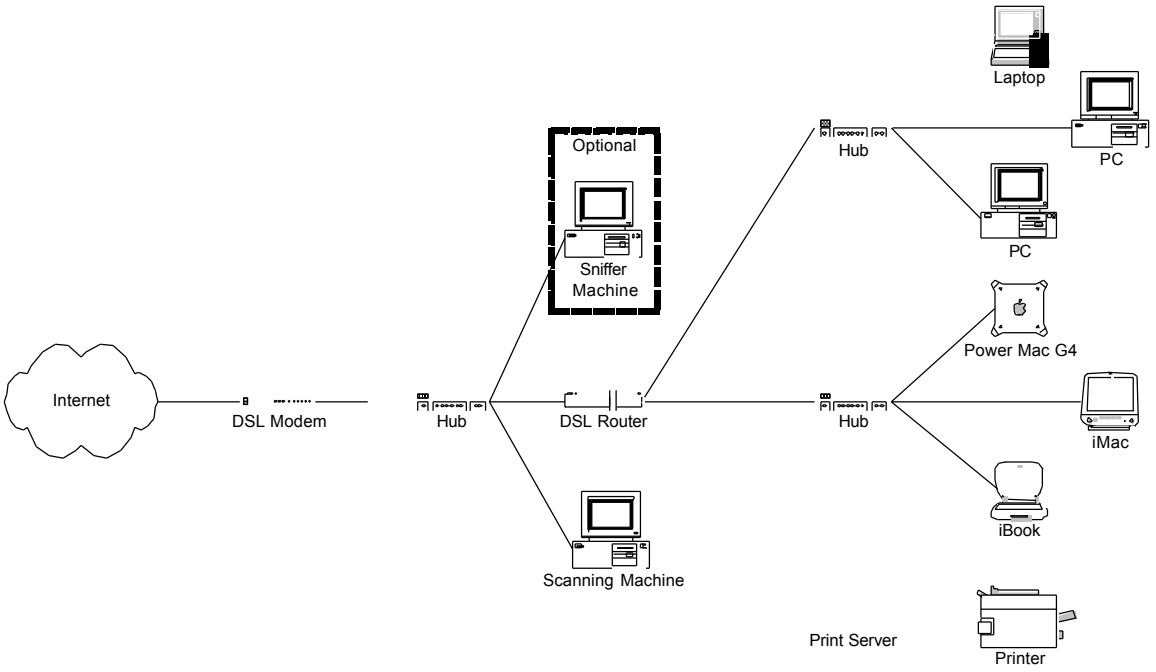


Figure 4 Example Network Diagram for Testing the DSL Router Configuration by Modifying the Network

For freeware, there are numerous options. NmapNT is the Windows port by eEye Digital Security [13] of the well-known nmap [14] originally written by fyodor. There are several others including, Foundstone's SuperScan (Win32) [15], WWDSI's SAINT (Unix/Linux) [16], and G-Lock Software's Advance Administrative Tools (Win32, not free but inexpensive) [17]. If testing a single port is required Netcat for NT can be used. Netcat was originally written by Hobbit [18] and ported to Windows by Weldpond [19].

The optional sniffer machine can be used to monitor the scanning of the DSL router's external interface. The sniffer software can be used to record the network traffic going to and from the DSL router. It can also be moved to the internal network to checking on any problems that are noted during the scanning. Possible commercial sniffers that can be used are Etherpeek [20], Microsoft's Network Monitor (the System Management Server version allows viewing all packets on the network) [21]. Freeware sniffers include Windump [22], and Ethereal [23]. Windump, a command line tool, provides complete details of the packets in text form. Ethereal provide a GUI interface and large number of protocol parsers.

The third alternative would be testing the configuration with a web-based scanner. Steve Gibson's "Shields Up" scanner [24] is free scanner test is designed for Windows machines. It checks for file sharing over NETBIOS and probes some of the common service ports. This is a convenient test to begin with it, however, it is not complete because it doesn't test for Macintosh related ports nor all Windows related ports.

© SANS Institute 2000 - 2005 Author retains full rights.

Another web-based scanner is WebSaint by World Wide Digital Security, Inc. (WWDSI) [25]. WebSAINT provides scanning over the Internet, for a fee, that is based on the SAINT product.

Conclusions

The limited number of packet filtering rules available on a DSL router prevents the DSL router from being a complete firewall. However, the packet filtering capability does allow the DSL router to be a significant contributor to the security of the internal network. The NAT capability provides additional security [4], which along with the packet filtering, provides a reasonable secure network.

For added security, more layers should be added to the layered defense. The DSL router supplies two layer: packet filtering and NAT. Additional layers that should be added, as a minimum, are personal firewalls and antivirus software on each machine on the internal network. A review of numerous personal firewalls for Windows can be found on the SecurityPortal.com site [26]. The SecurityPortal.com web site has a center on virus that contains a wealth of knowledge [27]. Patrick Harris's paper [2] list a number of Macintosh related firewall and antivirus products.

References

1. Thompson, R. (14 Aug. 2000) "**GIAC Firewall Practical: Implementation of Firewall Filters**." *SANS Institute*. http://www.sans.org/infosecFAQ/firewall/fw_filters.htm (6 Jan. 2001)

2. Harris P. **(15 Sep. 2000)** "**Macintosh Internet Security Basics." *SANS Institute*.** http://www.sans.org/infosecFAQ/mac/mac_sec.htm **(10 Jan. 2001)**

3. Rekhter, Y.; et al. (Feb. 1996) "Address Allocation for Private Internets." *The Internet Engineering Task Force.* http://www.ietf.org/rfc/rfc1918.txt?number=1918 (5 Jul. 2001)

4. Hassell, J. (6 Apr. 2001) "Using Network Address Translation to Secure Your SOHO's Web Connection." *Windows IT Security* http://www.windowsitsecurity.com/Articles/Print.cfm?ArticleID=20569 20 Jun. 2001)

5. Reynolds, J; Postel J. (Oct. 1994) "Assigned Numbers." *The Internet Engineering Task Force.* http://www.ietf.org/rfc/rfc1700.txt?number=1700 (5 Jul. 2001)

6. Microsoft Corporation. (20 Sep. 1999) "Microsoft Security program Frequently Asked Questions for Security Bulletin MS99-038." *Microsoft TechNet.* http://www.microsoft.com/technet/security/bulletin/fq99-038.asp (21 Jun. 2000)

© SANS Institute 2000 - 2005 Author retains full rights.

7. Brenton, C. (29 Feb. 2000) **"What is Egress Filtering and How Can I Implement It? Egress Filtering v 0.2."** ***SANS Institute*****. http://www.sans.org/infosecFAQ/firewall/egress.htm (1 Jul 2001)**

8. Open Door Networks, Inc. (Nov. 1999) "Understanding and Enhancing Mac OS Internet Security." *Open Door Networks*. http://www2.opendoor.com/doorstop/macossecurity.html (15 May 2001)

9. Open Door Networks, Inc. (Nov. 1999) "DoorStop Port List." *Open Door Networks*. http://www2.opendoor.com/doorstop/ports.html (15 May 2001)

10. Internet Security Systems. (Apr. 2001) Internet Scanner (v. 6.1). http://www.iss.net/securing_e-business/security_products/security_assessment/internet_scanner/ (6Jul. 2001)

11. eEye Digital Security. Retina (v. 4.0). (Jun 2001) http://www.eeye.com/html/Products/Retina/index.html (20 Jun. 2001)

12. Symantec Corporation. NetRecon (v. 3.0). (2001) http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=46&PID=6877199 (6 Jul. 2001)

13. eEye Digital Security, NmapNT (sp1). (13 Jul. 2001) http://www.eeye.com/html/Research/Tools/nmapNT.html (20 May 2001)

14. Insecure.Org. Nmap (v. 2.50). (28 Apr. 2000) http://www.insecure.org/nmap/ (20 May 2001)

15. Foundsone, Inc, SuperScan (v. 3.0). (2000) http://www.foundstone.com/rdlabs/proddesc/superscan.html (6 Jul. 2001)

16. World Wide Digital Security, Inc. SAINT (v.3.3.4) (3 Jul. 2001) http://www.wwdsi.com/saint/index.html (6 Jul. 2001)

17. G-Lock Software. Advanced Administrative Tools (v. 4.31) (6 Jul. 2001). http://www.glocksoft.com/ (6 Jul. 2001)

18. Hobbit, Avian Research. Netcat (v. 1.10). (1996) http://199.103.168.8:2030/web1/hak/netcat.html (7 Jul. 2001)

19. Weldpond, @stake Research Labs. Netcat for NT (v. 1.1). (2 Feb. 1998) http://www.atstake.com/research/tools/index.html (20 May 2001)

20. WildPacket, Inc. Etherpeek (v. 4.1 (Windows); v. 4.0.2 Macintosh).

© SANS Institute 2000 - 2005 Author retains full rights.

http://www.wildpackets.com/products/etherpeek (15 Jun. 2001)

21. Microsoft Corporation. System Management Server (SMS) (v. 2.0, SP 3). (13 Feb. 2001) http://www.microsoft.com/smsmgmt/default.asp (6 Jul. 2001)

22. Viano, P.; et al. WinDump (v. 3.5.2a). (6 Jun. 2001) http://netgroup-serv.polito.it/windump/ (18 May 2001)

23. Combs G. (17 May 2001) Ethereal (v. 0.8.18). http://www.ethereal.com (17 Jun. 2001)

24. Gibson, S. "Shields Up." *Gibson Research Corporation*. http://grc.com/default.htm (15 May 2001)

25. World Wide Digital Security, Inc. WebSAINT. http://www.wwdsi.com/websaint/index.html (6 Jul. 2001)

26. Personal Firewall Center. *SecurityPortal.com*. http://securityportal.com/firewalls/personal/ (7 Jul. 2001)

27. Virus Center. *SecurityPortal.com.* http://securityportal.com/virus/ (7 Jul. 2001)

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

© SANS Institute 2000 - 2005 Author retains full rights.