Global Information Assurance Certification Paper

SANS GIAC Firewall and Perimeter Protection Practical Assignment

Network Security 2000
Monterey, CA October 2000

Submitted by:

George Stanton

November, 2000

Assignment 1: Security Architecture

Define a security architecture using filtering routers, firewalls, VPNs and internal firewalls to rapidly implement the VISA "Ten Commandments" to the extent possible at a large and growing E-business startup that just completed a merger/acquisition and expects to earn 200 million per year in sales.

Produce a network diagram with explanatory text showing how to use perimeter defense technologies to implement as many of the VISA requirements as possible.

Assignment 2: Security Policy

For the purposes of this assignment, your security policy should be focused on implementation of VISA requirement number 1 "Install and maintain a working network firewall to protect data accessible via the Internet." For a baseline policy, use the filtering recommendations located at www.sans.org/topten.htm. Focus on ADDITIONAL filtering you would recommend and why. Your policy should implement your design above.

Write a tutorial on how to implement each additional recommended action in the filtering policy below on your firewall or perimeter defense solution. Be explicit about the brand and version of perimeter defense. Screenshots, network traffic traces, firewall log information and URLs to find further information should all be used. Be certain to include the following:

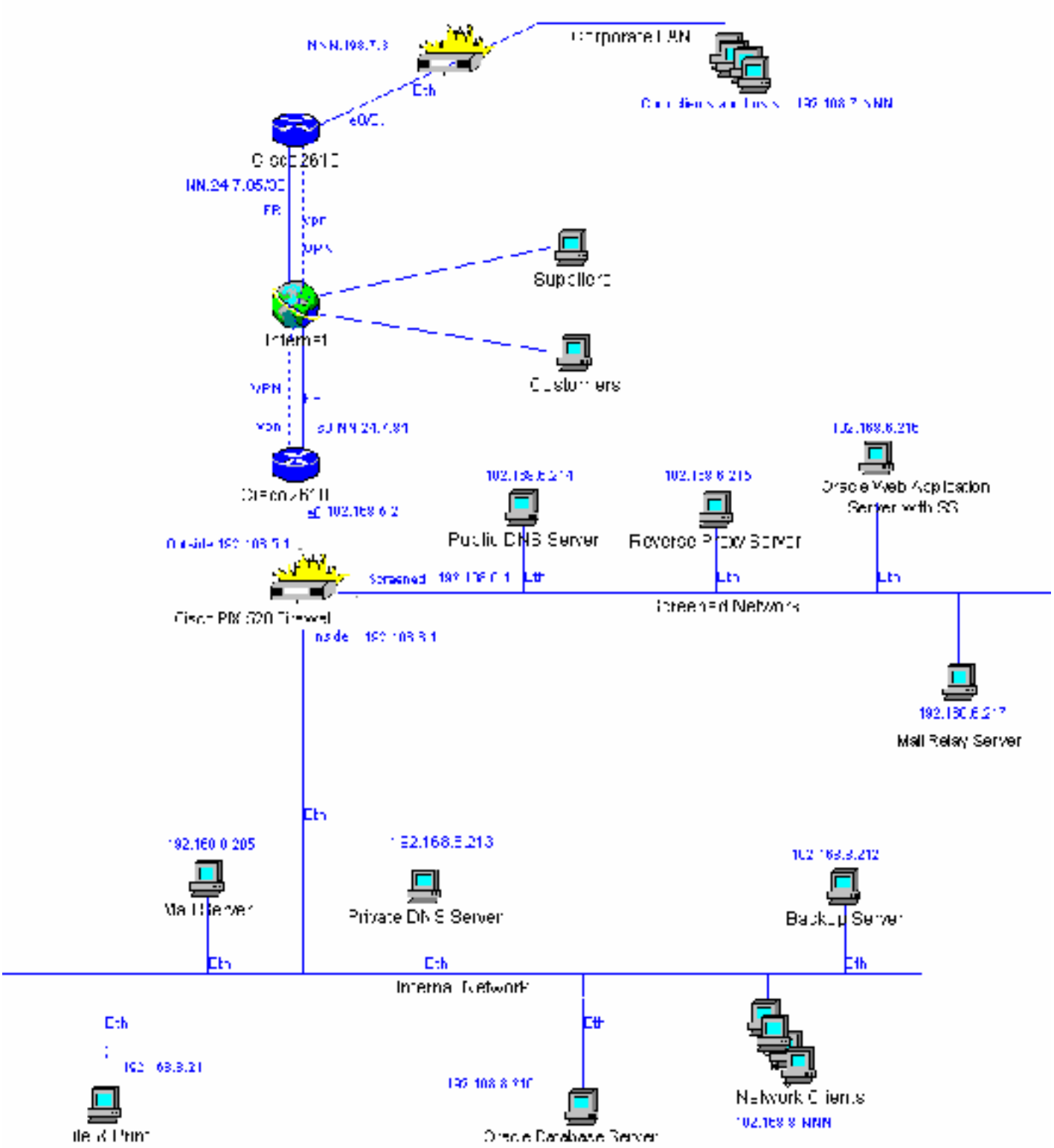
1. The reason these services might be considered a vulnerability
2. Relevant information about the behavior of the protocol or service on the network
3. Syntax of the filter
4. Description of each of the parts of the filter
5. Explain how to apply the filter
6. If this filter is order dependant, what other rules should this filter precede and follow.
7. Explain how to test the filter
8. Be certain to point out any tips, tricks, or gotcha's.

Assignment 3: Security Audit

For the purposes of this assignment please assume that you have been assigned to provide technical support for a comprehensive information systems audit of an electronic commerce facility The firewall analyst has set their firewall up according to their base + recommended enhancements security policy that happens to mirror your assignment 1 security policy exactly.

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
2. Implement the assessment. Validate that the firewall or perimeter router is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Screenshots when possible should be included in your report.
3. Perimeter analysis. Based on your assessment and referring to data from your assessment, analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Network Diagram for Assignment # 1



Network Description

The Network Diagram can be broken into three distinct areas of security considerations:

1. The internal network, which must be protected from outside threats.
2. A "trusted" Corporate Partner Network. Note that "Trusted" is used in business terms. Your network is only as secure as it's weakest link, which could be a trusted partner. Treat your own security policy accordingly. The local network must be protected from intentional or unintentional security risks from attached "trusted" networks.
3. The "un-trusted" Network consisting of Internet users, e-Business customers and suppliers.

The internal network is a Windows NT network and all hosts control access by distinct username/password logins. Best Practices for securing a Windows NT network as described in depth at http://www.sans.org/giactc/gcnt.htm are to be strictly adhered to.

Due to a corporate merger and a foray into the e-Commerce world, It is now necessary to quickly share information with corporate headquarters while making on-line shopping available to Internet customers. It is also necessary to share information with suppliers as well as delivery companies for the purpose of maintaining adequate inventory and expediting deliveries.

There is more than one possible solution for this problem but the one chosen is one that is relatively easy to implement, is moderate in cost of hardware/software, and can be accomplished in a reasonable time frame.

The plan consists of:

- Creating a VPN tunnel between existing Cisco 2610 routers at the internal network and the corporate network.
- Further access to resources by corporate users will be controlled at the network application level.
- The plan also calls for using two existing Cisco PIX 520 firewalls.
- The e-Commerce web server is an Oracle Application Server running SSL with 128bit encryption. All public access to the internal Oracle Database is via SQL*NET TCP/IP connect strings, which are routed through the Reverse Proxy Server.
- The network also deploys split DNS with public and private DNS servers placed on the screened and private network segments of the PIX firewall respectively.
- An external Sendmail server relays mail between the Internet and the internal email system.

Customers and suppliers will make SSL connections to the web server. For the exchange of sensitive private data. All queries to the database from un-trusted sources (customers and suppliers) will be routed to the internal Oracle Database via the Proxy Server using reverse proxy. This approach will hide the internal database from the outside. Database access will be controlled by Oracle Database security. Since all public servers reside on the screened network and have static routes translated to legal addresses, the backup server with a static legal address translation, backup and recovery operations can be performed through the firewall. This will be made possible by creating a conduit between the two computers through the firewall..

Security Policy for Assignment # 2

Note: Assume that the top ten base line policy, www.sans.org/topten.htm, is our base policy. Our policy will not go into detail for implementing the top ten. However, if you analyze this Security policy and it's implementation below you will see that the top ten list is covered to the extent possible.

For a good explanation of the top ten list of vulnerabilities and preventive measures see Adam Payne's practical paper at http://www.sans.org/y2k/practical/Adam_Payne.doc

The best rule for creating security policy is to keep it as simple as possible! The more rules you have the greater the opportunity to misconfigure your ACL. The best base security policy is to permit the minimum access to hosts from the minimum number of clients using only the essential protocols and ports to provide the required services. In other words, explicitly permit the services needed to run the site and then explicitly deny everything else. By permitting the services required and ending with deny any any, you effectively follow the "top ten" recommendation to the greatest degree possible while blocking all other traffic. Note that I said "to the greatest degree possible". This is because in reality, security policies are driven by business needs. There may be a need for exceptions to strict top ten policies in order for your company to do business. One of the rules for creating a security policy is to "know your weaknesses". In other words, you may be required to leave a hole open that has potential for exploitation as in the network diagram. The design has two holes going through the firewall – one to the database and one to the backup server. Knowing this weakness allows you to take every precaution through other means to protect your hosts and network. Following the approach described above the Security Policy for the above e-Commerce sight is as follows.

Note: Since we have a VPN connection, the packets coming from the corporate network are decrypted by the border router and forwarded to the firewall. This opens the possibility of an "inside" attack from anyone who gains access to the corporate side. Therefore, it is necessary to use the defensive layers of the perimeter defense to stop unwanted types of traffic from both the un-trusted and trusted networks.

Security Policy:

- Permit all internal users to connect to the internet for all purposes.
- Permit the corporate network to access the Oracle database.
- Permit Internet users to access the web server.
- Permit Internet users to send email to the public mail server.
- Permit customers and suppliers to access the Oracle database from the web server using reverse proxy.
- Drop all unnecessary inbound traffic.
- Prevent the use of the local network to launch attacks against other networks.

Applying the Rule Base

Perform the following filtering at the Border Router:

1. **Ingress Filtering** (Inbound Traffic) at serial interface 0
    a. Deny packets with private IP addresses. (rfc 1918 addresses)
    b. Deny packets with localhost, broadcast and multicast addresses.
    c. Deny packets without IP addresses
    d. Deny packets appearing to come from your internal address.
    e. Permit everything else
2. **Egress Filtering** (Outbound Traffic) "Good Neighbor Policy."

a. Permit only packets from legal internal IP addresses to be sent out through te router.
b. Establish network-to-network IPSec VPN to Corporate Network. Route all traffic bound for the corporate network through the VPN.

Perform the following filtering at the Firewall:

1. Permit inbound standard html traffic and SSL connections from any point to the Oracle Web Application Server located on the screened network.
2. Permit inbound DNS lookup on the public DNS Server, located on the screened network, from anywhere on the Internet.
3. Deny zone transfers.
4. Restrict use of ports above 1023 to established connections.
5. Permit inbound Internet SMTP traffic from anywhere to the external Sendmail Relay Server.
6. Permit inbound traffic from the Corporate Network via the IPSec tunnel to the internal Oracle Database Server. Allowing corporate access to the database directly via the VPN allows for granting the additional needed database rights without creating a possible exploit on the screened web server. The Oracle DBA will be responsible for overseeing privileges on the database. Sending corporate mail via the VPN rather than the Internet protects sensitive email documents from being intercepted on the Internet. Although we won't be covering the details in this writing, PKI authentication will also be required on email communications between employees. Rights to other areas of the internal network by trusted partners will be restricted unless/until a business need to reach other resources arises.

Deny all other traffic. **(Remember this denies everything not permitted above)**

Security Policy Implementation – Router – Cisco 2610 IOS version 12.0

Remember that the placement of rules in the access list can be crucial be careful not to place globally applied rules ahead of more select ones. For example placing a permit any any or a deny any any at the beginning of the list will cause all traffic to be permitted or denied respectively regardless of the rules that follow. The following rules are placed in the required order to enforce our security policy.

Bullets are used to make the commands more readable. If you were configuring your router or firewall, you would see the command prompt where the bullets are in the COMMAND column.

Some Basic Configurations

COMMANDS	**Comments**
▪ no ip source-route	▪ do not allow packets to be re-routed by rhe source. This can be used to bypass access lists.
▪ no service tcp-small-servers	▪ Small servers are disabled to prevent some undiscovered vulnerability.
▪ no service udp-small-servers	
▪ no service finger	▪ Finger can provide an intruder information about hosts that are logged in
▪ no ip http	▪ Server services (http, bootp) should be disabled.

▪ no ip bootp ▪ interface serial0.1 point-to-point ▪ description internet ▪ ip address NN.24.7.11 255.0.0.0 ▪ ip broadcast-address NN.24.7.84 ▪ frame-relay interface-dlci 103 broadcast ietf	▪ Create a point-to-point frame-relay connection to the ISP ▪ Broadcast the gateway external address. ▪ Dlci is provided by your !SP
▪ Interface serial0.2 point-to-point ▪ Description Corporate VPN ▪ Ip-address NN.24.7.85	▪ Create a point-to-point frame relay connection to the corporate border router. ▪ **We will create the VPN later in the tutorial.**
▪ Interface ethernet0 ▪ Ip address 192.168.5.2 255.255.255.0	▪ Configure the Ethernet card on the inside of the gateway router.

INGRESS FILTERING

COMMANDS	**Comments**

Purpose: You don't want to allow any packets to enter your network that can't be identified by the network as being foreign address. This is the first line of defense for preventing "Spoofing" attacks. Spoofing occurs when a hosts tries to look like another host on your network. Spoofing can be the cause of several different types of attacks, such as a smurf attack. A smurf attack occurs when a malicious host sends an ICMP echo request packet to the network broadcast address with the reply address as that of a victim's machine. All live machines then reply to the victim's machine, thus possibly causing, if there are enough live machines on the network, a DOS attack. You should never allow hosts with your internal IP addresses to come through your firewall.

```
Syntax - access-list {list#} permit/deny {source} {mask}
Standard access lists must be numbered 1 through 99.
```

▪ access-list 11 deny 192.168.0.0 0.0.255.255 any log ▪ access-list 11 deny 172.16.0.0 0.15.255.255 any log ▪ access-list 11 deny 10.0.0.0 0.255.255.255 any log	▪ Create a standard access list for incoming packets on serial 0 to enforce ingress filtering rules. ▪ Deny rfc 1918 addresses
▪ access-list 11 deny 127.0.0.0 0.255.255.255 any log ▪ access-list 11 deny 255.0.0.0 0.255.255.255 any log ▪ access-list 11 deny 224.0.0.0 7.255.255.255 any log	▪ Deny packets with localhost, broadcast and multicast addresses:
▪ access-list 11 deny 0.0.0.0 any log	▪ Deny packets without ip address.
▪ access-list 11 deny NNN.198.8.0 any log	▪ Deny packets that appear to come from your own registered domain.
▪ access-list 11 permit any	▪ Permit other traffic.
▪ interface Ethernet 0 ▪ ip access-group 11 in	▪ apply the ingress filter to the inbound side of the serial port.

Testing: To test the Ingress access list you can use a program such as Trash from outside your local network. Try sending packets to your network using source addresses that are within the ranges of the networks described above. If the filter is working packets will be dropped at the router and logged.

As an addition to the general ingress filtering, we want to be able to do some selective filtering of echo-requests and trace routes.

Purpose: We will want to be able to do some connection troubleshooting of the VPN that we will be creating later in this configuration.

Syntax for extended list – access-list {list#} {type} permit/deny {source} {destination} {port/name}
List numbers for extended lists must be between 100 and 199. Extended lists allow you to specify more filter criteria than standard lists. This requires more processing than standard lists which ony compare ip addresses. Thus, standard lists execute faster.

▪ access-list 101 permit icmp NNN.198.7.3 any echo-request	▪ Create an extended access list that will allow ping and tracert from Corporate to troubleshoot connections while denying echo requests from the public.
▪ access-list 101 deny icmp any any echo-request	▪ If this rule were to be placed first, then corporate traffic would be denied also. Be careful of placement.
▪ permit ip any any	▪ Permit all other traffic. Again, if this rule were placed above the previous rule then the deny filter would not be executed.
▪ interface Ethernet 0 ▪ ip access-group 101 out	▪ Apply the company-ping access group to the ethernet interface outbound (toward the local net). In other words, we are permitting hosts from corporate to ping us but preventing all others.

Testing: Testing this filter is simple. Just send some ping packets from the Internet and from the corporate network. The router should drop those from the Internet while permitting those from the corporate domain.

Egress Filtering

Purpose: The egress filter helps prevent intruders from using certain tools to map our network. It also prevents our network from being used to launch spoofing attacks against your Internet neighbor.

COMMANDS	**Comments**
▪ ip access-list 111 deny icmp any any echo-reply ▪ ip access-list 111 deny icmp any any time-exceeded ▪ ip access-list 111 deny icmp any any unreachable	▪ There are two purposes for egress filtering. 1. We want to prevent our hosts from unintentionally allowing bad guys from discovering anything about our network. 2. We want to be a good cyber neighbor by

	preventing the bad guys from using our address for evil purposes.
▪ ip access-list 111 permit ip NNN.198.8.0 0.0.0.255 any ▪ ip access-list 111 deny ip any any	▪ Permit local addresses to the Internet. ▪ Deny IP traffic with spoofed addresses from leaving the local network The placement of these two commands is very important. If they were reversed then no IP traffic would leave the network.
▪ Interface Serial 0 ▪ Ip access-list 111 out	▪ We apply this list to the outgoing serial port.

Configure IPSec Virtual Private Network

▪ Crypto isakmp policy 1 ▪ Group 1 ▪ Authentication pre-share ▪ Lifetime 3600 ▪ Exit ▪ Crypto isakmp key 52xy address NN.24.7.85	▪ Policy 1 identifies unique VPN. ▪ Group 1 means we will use a 768 bit key. ▪ Next, we tell the Security Association negotiation to update every hour. ▪ Return to global configuration mode. ▪ Define our shared secret "52xy" and external IP address of the router on the other end of our VPN
▪ Access list 110 permit NNN.198.8.0 0.0.0.255 NNN.198.7.0 0.0.0.255	▪ Access list 110 says all traffic from the local network (NNN.198.8.0) will be encrypted if it is heading for the corporate network (NNN.198.7.1).
▪ Crypto ipsec transform-set corpvpn ah-md5-hmac esp-des esp-md5-hmac ▪ Crypto map onemin 60 ipsec-isakmp	▪ Enable authentication headers and encapsulation and name this combination of protocols corpvpn. ▪ The configuration named onemin will generate a new key every minute.
▪ Set peer NN.24.7.85 ▪ Set transform-set corpvpn ▪ Match address 110	▪ Peer defines the external IP address of the remote router. ▪ Use this configuration on access-list 110
▪ Interface s0.2 ▪ Crypto map onemin	▪ Apply the configuration to the serial interface of the router.
▪ ip route NNN.198.7.0 255.255.255.0 NN.24.7.85	▪ Route traffic addressed to the corporate network to the remote VPN router
▪ ip route NNN.198.8.0 255.255.255.0 192.168.5.1	▪ Route all traffic bound for the local network to the firewall. We don't want traffic from the corporate VPN to end up on the Internet by default.
▪ Ip route 0.0.0.0 0.0.0.0 NN.24.7.NN	▪ Route all other traffic to the ISP Internet router.

Gotcha: It is important to make sure the time on the routers on both ends remain in sync or the security of the link will break.

Security Policy Implementation – Firewall Rules Cisco PIX 520

For instructional purposes, we will completely reconfigure the Cisco PIX Firewall 520.

First, we connect to the Firewall via Telnet, enter the password, type enable, enter the enable password, and arrive at the PIX prompt. Then we begin configuration

COMMANDS	Comments
▪ write floppy	▪ Save the current configuration do diskette.
▪ write erase	▪ This erases the current configuration ▪ Note: You will be asked to confirm.
▪ passwd "password-of-your-choice"	▪ Set password for telnet and PIX Firewall Manager access to the PIX (up to 16 characters in length)
▪ enable password "password-of-your-choice"	▪ Change the privileged password.
▪ names ▪ nameif ethernet0 outside security 0 ▪ nameif ethernet1 inside security 100 ▪ nameif ethernet2 screened 50	▪ Name the interfaces ▪ Ethernet 0 for outside interface ▪ Ethernet 1 for inside interface ▪ Ethernet 2,3 for subsequent perimeter interfaces ▪ Security numbers indicate levels of security in relationship to the interfaces. 0 is the lowest security. 100 is highest level of security.
▪ interface ethernet0 auto ▪ interface ethernet1 auto ▪ interface ethernet2 auto	▪ Use the interface command to set the speed and duplex of network cards.
▪ ip address outside 192.168.5.1 ▪ ip address inside 192.168.8.1 ▪ ip address protected 192.168.6.1	▪ Ip address assigns ip addresses to the respective network card.
▪ no failover ▪ failover ip address outside 0.0.0.0	▪ Disables the failover feature. Failover allows you to run two PIX boxes

▪ failover ip address inside 0.0.0.0 ▪ failover ip address screened 0.0.0.0	connected by a serial cable. If the main firewall fails, the failover takes control.
▪ fixup protocol ftp 21 ▪ fixup protocol http 80 ▪ fixup protocol h323 1720 ▪ fixup protocol rsh 514 ▪ fixup protocol smtp 25 ▪ fixup protocol sqlnet 1521	▪ These are default settings, which can be changed with the no fixup command. **Note: Users cannot access these protocols unless a conduit is created to the IP address where they are to be run. These are default ports but can be changed with caution. Changing them may break things if everything is not configured accordingly.**
▪ pager lines 24	▪ Sets the PIX to display 24 lines before prompting you to continue the listing
▪ logging on ▪ logging facility 16 ▪ logging trap debugging ▪ logging host inside 192.168.8.100	▪ Enable logging at debugging level and send logs to the internal host 192.168.8.100
▪ no arp timeout	▪ Sets the arp timer to default (4 hours).
▪ no rip outside passive ▪ no rip outside default ▪ no rip inside passive ▪ no rip inside default ▪ no rip screened passive ▪ no rip screened default	▪ Disable RIP listening and default rout broadcasting for all interfaces. ▪ We don't want the inherent routing capabilities to give out any information.
▪ no snmp-server location ▪ no snmp-server contact ▪ snmp-server community fubar ▪ no snm p-server enable traps	▪ Disable SNMP event trapping. ▪ Rename server community from default.
▪ global (outside) NNN.198.8.1-NNN.198.8.200 netmask 255.255.255.0	▪ Global creates a pool of addresses for outbound connections and for inbound connections resulting from outbound connections. We use hosts 1-200 here because we are reserving addresses above 200 for static address translations for hosts we want to be available to the outside. **You can't use a static address if it is being used by the global range.**
▪ nat (inside) 1 0 0	▪ Nat associates a network (our inside) with the global pool of addresses. The 1 is an arbitrary nat_id. The first 0

	represents the local_ip and allows all hosts to start outside connections. The second 0 represents the netmask and allows all outbound connections to translate with IP addresses from the global pool. Both zeros are abbreviations of 0.0.0.0.
▪ route outside 0 0 192.168.5.2 1	▪ This command creates a default route from the outside interface for ip_address 0.0.0.0 with netmask 0.0.0.0 (both abbreviated to 0) pointing to the perimeter router in the diagram. The trailing 1 denotes that the router is the first hop.
▪ write memory ▪ reload	▪ Save this configuration to flash memory and restart the PIX.

At this we have configured a firewall with 3 interfaces that allows everyone on the internal network to start an outbound connection with Network Address Translation and by default allows no one from the outside to access anything on the inside or screened interfaces. Let's continue.

COMMANDS	Comments
▪ conduit permit icmp any any echo-reply ▪ conduit permit icmp any any unreachable ▪ conduit permit icmp any any source-quench ▪ conduit permit icmp any any time-exceeded	▪ Permit replies to icmp queries initiated locally to be returned to the internal initiator.
▪ static (screened ,outside) NNN.198.6.214 192.168.6.214 netmask 255.255.255.255 0 0 ▪ conduit permit udp host NNN.198.6.214 eq 53 any	▪ Create a static address translation for the outside to the public DNS server. ▪ Allow DNS queries from outside sources.
▪ static (inside,screened) NNN.198.8.210 192.168.8.210 netmask 255.255.255.255 0 0 ▪ static (screened,inside) NNN.198.8.215 192.168.6.215 netmask 255.255.255.255 0 0 ▪ conduit permit tcp host NNN.198.8.210 eq 1521 NNN.198.8.215	▪ Create static address translations for the internal database server and proxy server so sql transactions can pass between the two on port 1521 and be relayed back and forth to the internet.
▪ static (inside,outside) NNN.198.8.210 192.168.8.210 netmask 255.255.255.255 0 0 ▪ conduit permit tcp host NNN.198.210 eq 1521 NNN.198.7.0	▪ Create a static address translation for the outside to the internal database. ▪ Pemit database queries to the database sever from corporate hosts.

- static (screened,outside) NNN.198.6.216 192.168.8.216 netmask 255.255.255.255 0 0
- conduit permit tcp host NNN.198.6.216 eq 80 any
- conduit permit tcp host NNN.198.6.216 eq 443 any

- Create static address translation for the outside to access the web server.
- Permit standard http to port 80.
- Permit SSL connections to port 443.

- static (screened,outside) NNN.198.6.217 192.168.8.217 netmask 255.255.255.255 0 0
- conduit permit tcp host NNN.198.6.217 eq 25 any

- Create a static address translation for the mail relay server
- Allow incoming smtp on port 25

- static (inside,outside) NNN.198.8.210 192.168.8.210 netmask 255.255.255.0 0 0
- conduit permit tcp NNN.198.8.210 255.255.255.0 eq 1521 NNN.198.7.3 1 255.255.255.0

- Create static address translation for the outside to access the database server
- Allow incoming traffic on port 1521 from the corporate network.

Assignment # 3 – Auditing a Firewall

Methodology:

Auditing a Firewall consists of two parts.

1. Auditing the integrity of the operating systems of the firewall. If an intruder can gain access to the computer that is running your firewall, he may be able to modify the firewall itself. Since the Firewall in this case is a Cisco PIX520, it is a hardware-based solution. We don't need to worry about the underlying operating system of the firewall computer. We simply need to verify that the telnet connection can be accessed from the local network for administration but not the accessed via the Internet.

2. Auditing the firewall rule base to make sure that the firewall is enforcing your security policy.

The tool of choice for our network auditing purpose is NmapNT network scanner from eeye.com, which is based on nmap from insecure.com. The following paragraph is eeye's description of the product.

"nmap is a the most customizable network scanner ever. It has various options to perform stealth scans, ping scans, UDP scans, as well as a handful of other scan types.

nmap also has the ability to remotely fingerprint an IP address. In other words, by sending various queries to a remote IP address and reading the responses, nmap can determine which operating system the remote IP address is running or whether it is a router, a network printer, etc. In all, nmap's database contains over 500 unique fingerprints.

All of the functionality found in the Unix version of nmap can now be taken advantage of on Windows NT platforms."

Since the firewall is being audited with permission of management, the audit will be performed during the middle of the day when the greatest number of computers will be turned on the local network. This allows for the most possible access points to the network to be active. An intruder might well choose a time when they are less likely to be detected by an alert administrator, or he might try different times of the day the audit will create volumes of audit trails, but since the intent is to audit, there is no need for stealth.

Note The output IP addresses on all of the following screen captures has been edited to protect the innocent.

Nmappnt scans, that do not include any –s switches use the default –sT TCP connect() scan type.

Links provided, are to SANS practical assignments and other sources that explain in detail some of the vulnerabilities associated with the various ports described in the SANS top ten vulnerabilities. The purpose of this practical assignment was not to re-invent the wheel. There are many papers written that already do an excellent job of describing many of the details.

Typing nmapnt at the command prompt gives you the entire list of available options. See below.

C:\nmapnt\>nmapnt

```
Starting nmapNT V. 2.53 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )
nmap V. 2.53 Usage: nmap [Scan Type(s)] [Options] <host or net list>


Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect() port scan (default)
* -sS TCP SYN stealth port scan (best all-around TCP scan)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)


Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oM <logfile> Output normal/machine parsable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

The MAN page referred to can be found at http://www.insecure.com/nmap/nmap_manpage.html.

Step 1: Verify administrative connectivity to the firewall from the local network.

Scan: To begin the audit, we will start by scanning the firewall from the inside. NmapNT will report the state of the ports scanned and tell us if they are open or closed (filtered).

C:\Nmapnt>nmapnt 192.168.8.1

Starting nmapNT V. 2.53 by ryan@eEye.com
eEye Digital Security (http://www.eEye.com)
based on nmap by fyodor@insecure.org (www.insecure.org/nmap/)

Interesting ports on (192.168.8.1):
(The 1521 ports scanned but not shown below are in state: closed)
Port State Service
23/tcp open telnet
1467/tcp open unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 1529 seconds

These are the two normal ports (tcp23,tcp1467) that are open on a PIX for Administrative Control Communications.

Step 2: Check to see if any login services are available from the Internet.

Scan: From the outside, perform a scan of Login Services ports.

Vulnerability: Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp are all vulnerable to attacks. Port 1467 was included because it was known to be open on the firewall to inside hosts from the previous internal firewall scan above. For a detailed description of some specific types of login service attacks, refer to http://www.sans.org/y2k/practical/Adam_Payne.doc.

C:\Nmapnt>nmapnt nnn.198.8.0/24 -p 21-23,139,512-514,1467 -oN logins.log

All 8 scanned ports on (nnn.198.8.214) are: closed
All 8 scanned ports on (nnn.198.8.216) are: closed
All 8 scanned ports on (nnn.198.8.217) are: closed

Recommendation: **None.**

Step 3: Scan for open RPC and NFS ports.

Vulnerability: RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp) rank high on SANS top ten list of ports to block. . For a detailed description of some specific types of attacks, refer to http://www.sans.org/y2k/practical/Adam_Payne.doc.

C:\Nmapnt>nmapnt -sU -p 111,2049,4045 nnn.198.8.0/24

Interesting ports on (nnn.198.8.214):
Port State Service
111/udp open sunrpc
2049/udp open nfs

Interesting ports (nnn.198.8.216):
Port State Service
111/udp open sunrpc
2049/udp open nfs
4045/udp open unknown

Interesting ports on (nnn.198.8.217):
Port State Service
111/udp open sunrpc
2049/udp open nfs

Recommendation: These computers are on the extranet and should not be running these services. Stop the services that use these ports on these computers and block traffic from the outside from using these ports.

Step 4: Scans for open netbios TCP and UDP ports on windows computers.

Vulnerability: Windows networking (NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 – all of the earlier ports plus 445(tcp and udp) rank high on the list of SANS top ten vulnerabilities. For a detailed description of some specific types of attacks on these services, refer to http://www.sans.org/y2k/practical/Adam_Payne.doc.

C:\Nmapnt>nmapnt -p 135,139,445 nnn.198.8.0/24

All 3 scanned ports on (nnn.198.8.214) are: closed
All 3 scanned ports on (nnn.198.8.216) are: closed
All 3 scanned ports on (nnn.198.8.217) are: closed

C:\Nmapnt>nmapnt -sU -p 135,137,138,445 nnn.198.8.0/24

Interesting ports on (nnn.198.8.214):

Port	State	Service
135/udp	open	unknown
137/udp	open	unknown
138/udp	open	unknown
445/udp	open	unknown

Interesting ports on (nnn.198.8.216):

Port	State	Service
135/udp	open	unknown
137/udp	open	unknown
138/udp	open	unknown
445/udp	open	unknown

Interesting ports on (nnn.198.8.217):

Port	State	Service
135/udp	open	unknown
137/udp	open	unknown
138/udp	open	unknown
445/udp	open	unknown\

Recommendation: Stop windows networking services on these extranet computers. Block all outside addresses from using these ports.

Step 5: Scan for open TCP ports used by X Windows.

Vulnerability: X Windows is a comparatively dangerous protocol. Any client that can access a server can potentially access and change any X communications that take place on that server. See Securing X Windows available at http://ciac.llnl.gov/ciac/documents/ciac2316.html.

C:\nmapNT\Nmapnt>nmapnt –p 6000-6255 nnn.198.8.216

Interesting ports on (nnn.198.8.216):
(The 255 ports scanned but not shown below are in state: closed)
Port State Service
6050/tcp open unknown

Recommendation: Close the service that is using port 6050 on this computer. Block all outside traffic from using this range of ports.

Step 6: Scan DNS and LDAP ports.

Vulnerability: Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp) all have identified vulnerabilities. For a detailed description of some specific types of attacks, refer to http://www.sans.org/y2k/practical/Adam_Payne.doc.

C:\Nmapnt>nmapnt -sU -p 53,389 nnn.198.8.0/24

Interesting ports on (nnn.198.8.214):
Port State Service
53/udp open domain
389/udp open unknown

C:\Nmapnt>nmapnt -p 53,389 nnn.198.8.0/24

Interesting ports on (nnn.198.8.214):
(The 1 port scanned but not shown below is in state: closed)
Port State Service
53/tcp open domain

Recommendation: Block 389UDP - It is not needed. Block 53TCP to prevent zone transfers from the DNS server. Zone transfers can help an intruder to map your network.

Step 7: Scan for open SMTP e-mail ports.

Vulnerability: Network Ice lists 18 common attacks against SMTP servers at:
http://advice.networkice.com/advice/exploits/services/smtp/default.htm

C:\Nmapnt>nmapnt -p 25,109,110,143 nnn.198.8.0/24

Interesting ports on (nnn.198.8.217):
(The 3 ports scanned but not shown below are in state: closed)
Port State Service
25/tcp open smtp

Recommendation: Port 25 is required to be open on the mail relay. However, be sure it is configured to prevent relaying by anyone other than your internal mail.

Step 8: Scan for open ports used by web servers.

Vulnerability: Web -- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers. You may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.). These services are vulnerable to attack by virtue of the fact that they are open. Only open them **when and where they are required**.

C:\Nmapnt>nmapnt -p 80,443,8000,8080,8888 nnn.198.8.0/24

Interesting ports on (nnn.198.8.216):
(The 3 ports scanned but not shown below are in state: closed)
Port State Service
80/tcp open http
443/tcp open unknown

Recommendation: These ports must be open on the web server for http and https connections. However, make sure the applications are configured correctly using SANS recommendations at http://www.sans.org/topten.htm.

Step 9: Scan for open "Small Services" ports.

Vulnerability: The so-called "small services" are simple daemons originally designed as a troubleshooting tool to verify a server's behavior and connectivity. However, they are almost never used and are vulnerable to certain attacks. For a detailed description of some specific types of attacks, refer to http://www.sans.org/y2k/practical/Adam_Payne.doc.

C:\Nmapnt>nmapnt -sU -p 1-20,37 nnn.198.8.0/24

All 21 scanned ports on (nnn.198.8.214) are: closed
All 21 scanned ports on (nnn.198.6.216) are: closed
All 21 scanned ports on (nnn.198.6.217) are: closed

C:\Nmapnt>nmapnt -p 1-20,37 nnn.198.8.0/24

All 21 scanned ports on (nnn.198.8.214) are: closed
All 21 scanned ports on (nnn.198.6.216) are: closed

All 21 scanned ports on (nnn.198.6.217) are: closed

Recommendation: None

Step 10: Scan for some miscellaneous ports. – TFTP, finger, NNTP, NTP, LPD, syslog, SNMP, BGP and SOCKS.

Vulnerability: Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp) all have known vulnerabilities. . For a detailed description of some specific types of attacks, refer to http://www.sans.org/y2k/practical/Adam_Payne.doc.

C:\Nmapnt>nmapnt -sU -p 69,514,161,162 nnn.198.8.0/24

All 4 scanned ports on (nnn.198.8.214) are: closed
All 4 scanned ports on (nnn.198.6.216) are: closed
All 4 scanned ports on (nnn.198.6.217) are: closed

C:\Nmapnt>nmapnt -p 79,119,123,515,161,162,179,1080 nnn.198.8.0/24

All 8 scanned ports on (nnn.198.8.214) are: closed
All 8 scanned ports on (nnn.198.6.216) are: closed
All 8 scanned ports on (nnn.198.6.217) are: closed

Recommendation: none

General Recommendations and Summary

Take a layered approach to network security

1. Make sure you use you border router to defend you border.
2. Use your firewall to filter out undesirable traffic.
3. Harden your operating systems.
4. Implement a virus detection scheme. (and keep your signatures current)
5. Be prepared for the worst with a solid backup/recovery plan.

Keep abreast of breaking security news by subscribing to SANS, CERT or other security organizations' advisories. Better yet attend SANS security training.

The recommendations so far, have referred mostly to closing ports on specific machines. This requires disabling services on public access machines that are not necessary. In fact, you should only run the necessary (bare bones) services required for the computers on the extranet to perform their functions. It is imperative to be aware that ports that are legitimately available to the public allow an intruder to use them for other purposes if the applications are not configured correctly. Security, like a chain, is only as strong as it's weakest link.

On the e-Commerce network design, for example, even though the only communication to the database is between the web server and the proxy server, it would be prudent to set up an encrypted link between these two computers. Another encrypted link could be established between the proxy server and the database server. This, along with SSL, would create a secure link for customers all the way from the customer PC to the database server. PPTP would be a nice choice for these links except that it would not be able to handle the number of connections required by an active e-Commerce site. You would have to use an alternative like a host-to-host IPSec connection.

In addition, even though ports are showing that they are closed, doesn't mean that they are being filtered by the firewall. Considering the previously opened conduits to computers/ports on the network required to do business over the Internet, apply the following filters to the firewall.

- Conduit deny tcp any any
- Conduit deny udp any any
- Conduit deny icmp any any

Note these statements need to be the last three rules in the list. If these were your first three rules, no one could access your site. **A VERY SECURE NETWORK INDEED**.

After applying these rules, all of the NmapNT commands from above were included in a batch file and run. The TCP port scans were modified using the –sS (syn) switch which is more stealthy than the default -sT. The results follow. Notice that the network, although the servers were up and accessible via conventional means (browser, mail, nslookup), appears to be invisible to the port scanner.

```
C:\Nmapnt>nmapnt -sS -p 21-23,139,512-514 nnn.198.8.0/24

Nmap run completed -- 0 IP addresses (0 hosts up) scanned in 0 seconds


C:\Nmapnt>nmapnt -sS -p 111,2049,4045 nnn.198.8.0/24 -oN log6.log

Nmap run completed -- 256 IP addresses (0 hosts up) scanned in 128 seconds


C:\Nmapnt>nmapnt -sS -p 135,139,445 nnn.198.8.0/24 -oN log8.log

Nmap run completed -- 256 IP addresses (0 hosts up) scanned in 129 seconds


C:\Nmapnt>nmapnt -sU -p 135,137,138,445 nnn.198.8.0/24 -oN log9.log

Nmap run completed -- 256 IP addresses (0 hosts up) scanned in 128 seconds


C:\Nmapnt>nmapnt -sS -p 6000-65255 -oN log10.log

Nmap run completed -- 0 IP addresses (0 hosts up) scanned in 0 seconds
```

```
C:\Nmapnt>nmapnt -sU -p 53,389 nnn.198.8.0/24 -oN log11.log

Nmap run completed -- 256 IP addresses (0 hosts up) scanned in 129 seconds


C:\Nmapnt>nmapnt  -sS -p 53,389 nnn.198.8.0/24 -oN log12.log

Nmap run completed -- 256 IP addresses (0 hosts up) scanned in 128 seconds


C:\Nmapnt>nmapnt  -sS -p 25,109,110,143 nnn.198.8.0/24 -oN log13.log

Nmap run completed -- 256 IP addresses (0 hosts up) scanned in 129 seconds


C:\Nmapnt>nmapnt -sS -p 80,443,8000,8080,8888 nnn.198.8.0/24 -oN log14.log

Nmap run completed -- 256 IP addresses (0 hosts up) scanned in 128 seconds

C:\Nmapnt>nmapnt -sU -p 1-20,37 nnn.198.8.0/24 -oN log15.log

Nmap run completed -- 256 IP addresses (0 hosts up) scanned in 129 seconds


C:\Nmapnt>nmapnt  -sS -p 1-20,37 nnn.198.8.0/24 -oN log16.log

Nmap run completed -- 256 IP addresses (0 hosts up) scanned in 129 seconds


C:\Nmapnt>nmapnt -sU -p 69,514,161,162 nnn.198.8.0/24 -oN log17.log

Nmap run completed -- 256 IP addresses (0 hosts up) scanned in 128 seconds


C:\Nmapnt>nmapnt -sS -p 79,119,123,515,161,162,179,1080 nnn.198.8.0/24 -oN log18.log

Nmap run completed -- 256 IP addresses (0 hosts up) scanned in 129 seconds
```

The following are some selected excerpts from the firewall logs generated during the batch scan.

```
Nov 14 2000 12:59:33  PIXIP192.168.8.1] Group ID[106010] Facility[16] Priority[3]  <131>%PIX-3-106010: Deny inbound
tcp src outside:nn.nn.86.125/33305 dst inside:nnn.198.8.215/80

Nov 14 2000 12:59:33  PIXIP[192.168.8.1] Group ID[107001] Facility[16] Priority[2]  <130>%PIX-2-107001: nn.nn.86.125
attempted to ping nnn.198.8.216 (192.168.6.216)

Nov 14 2000 12:59:34  PIXIP[192.168.8.1] Group ID[106010] Facility[16] Priority[3]  <131>%PIX-3-106010: Deny inbound
```

```
icmp src outside:nn.nn.86.125 dst inside:nnn.198.8.217 (type 8, code 0)
```

Notice that the firewall reports that the outside host nn.nn.86.125 is trying to ping the host but doesn't log that it is denying the connection as it does with 215 and 217. This is because the deny icmp any any doesn't allow the host to be pinged. However it will receive a connection on port 80 so no deny is issued.

The following log entries verify that connections were made on the http port 80 and https port 443 on the web server.

```
Nov 14 2000 12:07:09  PIXIP[192.168.8.1] Group ID[302001] Facility[16] Priority[6]
<134>%PIX-6-302001: Built TCP connection 549927 for faddr nn.nn.86.125/53831 gaddr
nnn.198.8.216/80 laddr 192.168.6.216/80

Nov 14 2000 12:08:23  PIXIP[192.168.8.1] Group ID[302002] Facility[16] Priority[6]
<134>%PIX-6-302002: Teardown TCP connection 549933 faddr nn.nn.86.125/53831 gaddr
nnn.198.8.216/443 laddr 192.168.6.216/443 duration 0:00:00 bytes 0
```

The following excerpts verify that the DNS server is allowing lookups but denying tcp zone transfers.

```
Nov 14 2000 12:00:30  PIXIP[192.158.8.1] Group ID[302006] Facility[16] Priority[6]
<134>%PIX-6-302006: Teardown UDP connection for faddr nn.nn.86.125/23636 gaddr
nnn.198.8.214/53 laddr 192.168.6.214/53

Nov 14 2000 12:07:32  PIXIP[192.158.8.1] Group ID[106001] Facility[16] Priority[2]
<130>%PIX-2-106001: Inbound TCP connection denied from nn.nn.86.125/53831 to
192.168.6.214/53 flags SYN
```

The next group of log entries verifies that the mail server is allowing connections only on port 25.

```
Nov 14 2000 19:56:37  PIXIP[192.168.8.1] Group ID[302001] Facility[16] Priority[6]
<134>%PIX-6-302001: Built TCP connection 549769 for faddr 206.66.12.234/8300 gaddr
192.168.6.217/25 laddr 192.168.6.217/25

Nov 14 2000 20:22:13  PIXIP[192.168.8.1] Group ID[106001] Facility[16] Priority[2]
<130>%PIX-2-106001: Inbound TCP connection denied from nn.nn.86.125/53831 to
192.168.6.217/109 flags SYN

Nov 14 2000 20:22:15  PIXIP[192.168.8.1] Group ID[106001] Facility[16] Priority[2]
<130>%PIX-2-106001: Inbound TCP connection denied from nn.nn.86.125/53831 to
192.168.6.217/110 flags SYN

Nov 14 2000 20:22:23  PIXIP[192.168.8.1] Group ID[106001] Facility[16] Priority[2]
<130>%PIX-2-106001: Inbound TCP connection denied from nn.nn.86.125/53831 to
192.168.6.217/1437 flags SYN
```

One final scan of the known hosts on the network yielded the following output. Note that all ports are filtered on the DNS server (214). That is because the –sS scan is a TCP scan and the only port not filtered is UDP53. The only other ports not filtered are the TCP http 80, https 443 and 25 smtp. This, along with the log files, including the excerpts above, verifies that the filtering is working as expected.

```
C:\Nmapnt>nmapnt –sS –P0 nnn.198.6.214

All 1523 scanned ports on (nnn.198.6.214) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 908 seconds



C:\Nmapnt>nmapnt -sS -P0 nnn.198.8.216

Interesting ports on (nnn.198.8.216):
(The 1521 ports scanned but not shown below are in state: filtered)

Port       State       Service
80/tcp     open        http
443/tcp    open        unknown

C:\Nmapnt>nmapnt -sS -P0 nnn.198.8.217

Interesting ports on (nnn.198.8.217):
(The 1522 ports scanned but not shown below are in state: filtered)

Port       State       Service
25/tcp     open        smtp
```

Although the scanning process generated about 4000 pages of log entries, I will spare the reader any more detail. Suffice it to say that if you are going to run these kind of scans against your network, be prepared to read through a lot of log entries to verify that the firewall is applying the filters as expected. It is also noteworthy to mention that an abnormally large firewall log should tip you off that something is going on.

One other word of caution: If you are going to launch a massive scan against your network, get management approval first.

References

Northcutt, Stephen, TCP/IP for Intrusion Detection and Firewalls, SANS Security 2000, Monterey CA

Spitzner, Lance, Advanced Perimeter Protection and Defense In-Depth, SANS Security 2000, Monterey CA

Spitzner, Lance, Firewalls 101: Perimeter Protection with Firewalls, SANS Security 2000, Monterey CA

Brenton, Chris, Introduction to VPNs, SANS Security 2000, Monterey CA

Brenton, Chris, VPNs and Remote Access, SANS Security 2000, Monterey CA

Brenton, Chris, Network Design and Performance, SANS Security 2000, Monterey CA

Stevens, W. Richard, TCP/IP Illustrated, Volume 1, Addison-Wesley Publishing

Spitzner, Lance, Auditing Your Firewall Setup, http://www.enteract.com/~lspitz/audit.html

Safeguarding the e-Business Network, Cisco Systems Inc.

Mcclure, Scambray & Kurtz, Hacking Exposed: Network Security and Solutions, Osborne/McGraw-Hill