

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.

GIAC Level Two
Practical Assignments for SANS Parliament Hill
August 21 - 24, 2000
Ottawa, Canada

© SANS Institute 2000 - 2002, Author retains full rights.

Submitted By
Blair Perry
Oct 16, 2000

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 1: Security Architecture

Design a secure network architecture for large and growing E-business that just completed a merger/acquisition considering the needs of customers, suppliers, and partners.

The objective of this section is to show how each of the following elements is used to design and implement a secure network architecture. Diagrams are included on pages 9 - 12

1. Security Policy
2. Planning
3. Filtering routers
4. External Firewalls
5. Internal Firewalls
6. Reverse Proxy
7. VPN (virtual Private Networks)
8. IDS (Intrusion Detection)
9. DNS
10. Mail
11. Physical security
12. Testing

1. Security Policy

Defining a security policy is the most important factor in designing a secure network architecture. Policy will determine the level of security that you wish to achieve which in turn defines the hardware, software and other requirements. Policy will determine how the internet will be used and ultimately our firewall rule sets. Without a Security policy you may end up with inappropriate hardware and software and there will be no guidelines to follow when changes are requested on the firewall and other security related devices.

Our Security Policy states the following with respect to Internet use

Use of Internet for Public Access (Consumers)

1.1 The external firewall will be configured to allow a minimal subset of TCP, UDP and ICMP from the Internet in order to provide the basic services that allow our customers to do business with us. This currently includes **incoming** connections for http, https, ftp, ntp and dns from the internet to selected hosts on the service network. The requirement for new protocols will be evaluated individually.

1.2 Incoming connections for Dns, smtp and http will also be permitted from the service network to the internal network to/from selected hosts.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Internet Use for Employees

2.1 Employees with no security clearance (green network) are permitted to use only HTTP for Internet use.

2.2 Employees with security clearance (blue network) are permitted to use all TCP protocols for Internet use, these few employees will be appropriately educated in security risks associated with Internet use.

Internet Use for remote access, branch office connection and Xtranets for Business Partners

Access to/from corporate resources via the internet will be limited to IPSEC VPN connections using Triple DES encryption. Pre-Shared keys will be used to set-up the Branch office tunnels which are to be used for Branch Office and Xtranet connections. Internet Security Association Key Management Protocol (ISAKMP) will be used to for remote access users. A firewall between the VPN server and the corporate network will ensure that access to corporate resources is sufficiently safe guarded.

Remote access users.

3.1 Employees working from home and while travelling will have access only to the Winframe server. This will provide access to email and other essential applications. Remote access VPN connections will be authenticated using SecureID.

Branch office connections.

3.2 Employees at remote branch offices will have full access to the servers on the low security (green) network. Branch offices will use the Nortel Instant Internet Firewall VPN appliance to establish a branch office tunnel to the Corporate Headquarters. Split Tunnelling at the remote VPN appliance will not be permitted. All the Internet access for the branch office will be provided via the Corporate LAN / Firewall.

3.3 Internet access will be limited to http and only via the Corporate LAN / Firewall

Xtranets.

3.4 In general services provided to business partners should be limited to only those services needed, and only to those devices (servers, routers etc) needed. Blanket access shall not be provided for anyone. The default stance will be to deny all access and then allow only those specific services that are needed. In no cases shall the Xtranet connection be used for internet access. (SANS Partner Connection Policy Draft)
http://www.sans.org/newlook/resources/policies/item8.pdf
The standard set of allowable services are ftp, smtp and http, however these will also be restricted to limited servers on our low security (green) network.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Our Security Policy states the following with respect to internal firewalls

> 4.1 Internal Firewalls will be used to limit access to confidential data. An internal secure network (Blue Network) will be configured behind a firewall protected from the office automation servers and general workstations.
>
> 4.2 The firewall will also serve to protect the secure (Blue) Network from the Xtranets and remote access users.
>
> 5.1 Exceptions may be made for additional protocols required for security and management.

2. Planning

Implementing a secure network architecture is a difficult task. You do not want to connect your firewall to the internet and then start thinking about how you are going to implement your security policy. Before configuring any hardware/software a detailed network diagram should be completed. This should include IP addresses and subnet masks, NAT translations (if they are used), hardware and software types and list the firewall rules you want to implement. The more time spent planning the less chance there will be for errors.

3. Screening Router

The screening router is an essential starting point for securing the perimeter. Before stateful inspection and proxy firewalls were readily available, many firewalls were simply routers with filters applied to the interface connected to the Internet. Screening routers basically rely on static rules to permit or deny IP packets. A screening router should never be considered a substitute for a Firewall even for a short period of time. It is expected that all traffic passed through the screening router will be subject to further inspection at the firewall. None the less a properly configured screening router does perform a valuable function.

The screening router in our example is a Cisco 2514 IOS 12.0 (5). Interface ether0 is connected to our ISP and ether1 is connected to the DMZ.

The screening router's primary function is to limit the potential for denial of service and other attacks by

- blocking packets with spoofed IP addresses from entering / leaving the network
- blocking packets with IP addresses from the Private address space from entering / leaving network
- tightly controlling ICMP traffic entering / leaving the router
- blocking source routed packets

The screening router in our example has been configured with two extended access-lists. One access-list blocks anomalous packets arriving from the Internet. The other access-list blocks anomalous packets from leaving our network.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4. External Firewalls

A firewall provides us with the best opportunity to validate traffic entering our network. How secure a firewall is depends on the method used to validate the incoming packets. Stateful inspection firewalls maintain a dynamic table of packet attributes to validate incoming packets and are much more secure than a packet filtering router. Proxy Firewalls are more secure than stateful inspection because they also validate the application data contained within the packet. For example if someone were trying to use a Telnet application on port 80 which is supposed to be HTTP, a proxy firewall would fail to see appropriate HTTP commands and block the packets. Stateful inspection firewalls have the benefit of being very secure and very fast, Proxy firewalls have the benefit of being most secure but may slow the network down depending on use.

A firewall will typically have three or more interfaces. One interface connects to the screening router, one interface connects to the internal network and one or more interfaces may connect to other networks called service networks. Hosts on these networks are generally for public access.

The external Firewall in our example is a Cisco PIX ver 4.4 (5) The PIX firewall operates on proprietary hardware and uses a micro kernel instead of a full-featured operating system. This eliminates the potential for operating system vulnerabilities that must be considered when deploying a firewall on NT, Unix etc. PIX uses Adaptive Security Algorithm (ASA) which is similar to stateful inspection and has limited proxy like characteristics for some applications like ftp and sequel. **PIX is not an Application Proxy Firewall**.

5. Internal Firewalls

Internal firewalls are often overlooked but should be implemented to restrict access within the corporate network. Internal firewalls should also be used to isolate connections to Xtranets and remote access users. Firewalls for these applications should be taken no less seriously than external firewalls.

The internal firewall in our example is a Cisco router with IOS IOS IP/FW 12.0.4T software. This firewall has been installed at the core of our internal network to provide firewall capabilities to several different networks at once. Cisco IOS firewall uses CBAC (Context Based Access Control). This is a stateful inspection process and is available as an optional feature set for Cisco IOS. CBAC dynamically updates access-lists and keeps a state table. CBAC can be applied to one or more interfaces and is configured with the familiar Access Control Lists (ACLs). In our example the Cisco router provides additional perimeter defence as well as an internal firewall.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

6. Reverse Proxy Web server

In our example the external web server provides the front end for customers and must be able to communicate securely with our internal database server. To do this we have implemented a reverse proxy server. All http is proxied from the external HTTP server to the internal HTTP server. Only the internal HTTP server interacts with the database.

7. VPN

The dangers of using the Internet to move unencrypted corporate data are so great that no organisation should even consider it. It would be best to assume that anything sent unencrypted across the Internet may appear on the front page of tomorrow's paper. Even if the data were not considered at risk, perimeter defence could be seriously compromised by allowing high risk protocols into the corporate network from un-authenticated sources. Since the formalisation of the IPSEC standard, VPN hardware and software is now widely available at relatively low cost across a wide variety of platforms.

The VPN in our example is a Nortel Contivity. The Nortel VPN appliance was selected because of its performance, reliability, ease of management and reliable IPSEC client. In our example the Contivity supports our Extranets, branch office and remote access users. Both the Cisco PIX firewall and the Cisco IOS firewall router could have been used for VPN connections, however it was decided to use a separate VPN appliance to off load the overhead of encryption from our firewalls.

8. IDS

Intrusion Detection is an essential part of the Network Security Architecture. Assuming that all efforts to protect our network resources are successful, we must still concern ourselves with identifying attempts to break our security. With the growing complexity of operating systems and applications, we must accept the fact that vulnerabilities will continue to be discovered. If we blind ourselves by ignoring unsuccessful attempts to break our security, we risk missing the signals that may alert us to something new on the horizon. The detection and analysis of the recent RingZero Trojan serves as a excellent example as to why we must all continue to monitor suspicious activity on our perimeters.

In our example both host based and network based Intrusion Detection systems have been used. There are advantages and disadvantages for each so the best solution is to use both. Axent Intruder Alert host based IDS has been installed on

- All servers on the Service Network
- All NT PDCs and BDCs
- All servers and desktops on the high security network

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

An Intruder Alert agent continually parses log files on each host that it is installed. ITA can parse many logs on each host if required. Flexible pattern matching rules are configured centrally and applied to the agents. Several actions are available on a match including:

- Logging the event back to the manager
- Sending an Email
- Logging the event back to another log file
- Sending an alarm to the ITA manager console
- Stopping a process

Axent ITA offers a simple and effective way to extract useful information from logs and take appropriate action. However in order to get the most out of Intruder Alert the administrator must have a very good understanding of the meaning of the log entries. It should also be noted that some o/s and application logs are more useful than others.

Axent Netprowler IDS monitors have been set-up to monitor traffic in three locations

- between the PIX firewall and the screening router
- between the high security network and the Internal firewall
- between the VPN and the internal firewall

NetProwler transparently examines network traffic and identifies, logs and terminates unauthorised use, misuse and abuse directed at our servers.

In addition to the IDS products discussed, the screening router, firewalls and Nortel VPN appliance each include a logging facility to provide further access-violations and other information. Each of these has been configured to log events to the syslog server where Axent ITA parses these logs.

9. DNS

A functional DNS is a critical component when designing a secure network architecture. Without functional name resolution doing business over the Internet is simply not going to work. While DNS is essential, it can be exploited and used to gain knowledge about our network topology, hosts and services. Care must be taken to limit the extent to which DNS may be used to our disadvantage.

In our example a split DNS with two distinct domains has been implemented to address some of the DNS vulnerabilities. The DNS servers on the internal network maintain the zone file for int.dm.com. These servers are recursive and do the name resolution for both internal hosts and external hosts.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The DNS servers on the service network maintain the zone file for ext.dm.com. To avoid possible DNS cache poisoning, these servers are not to be used for recursive lookups. Be aware that hosts on the service network must be configured to use the DNS servers on the internal network, which are recursive. The firewall must allow DNS queries from hosts on the DMZ to the internal DNS servers.

10. Mail

E-mail is an essential part of business. Simple Mail Transport Protocol (SMTP) which is used to move mail over the Internet has been plagued with vulnerabilities. Aside from vulnerabilities in the protocol itself, email is being used to propagate viruses and Trojans. Because a mail server has to be accessible by the entire Internet community, it is recommended to receive email on an external mail server, located on the service network. Mail is then checked for viruses etc and relayed from the external mail server to the internal mail server, where the intended recipient can retrieve it.

The mail servers in our example are MS Exchange. Both mail servers are equipped with Antigen Antivirus. Mail from the Internet is received on the external mail server where Antigen checks for viruses. Once the mail is checked it is forwarded to our internal MS Exchange server for delivery to individual mailboxes. The firewall permits SMTP from the external mail server to the internal mail server. The external MS Exchange server is configured to forward all email to the internal mail server. The internal mail server is configured so that it can't be used as a relay and checks all outgoing mail for viruses.

11. Physical Security

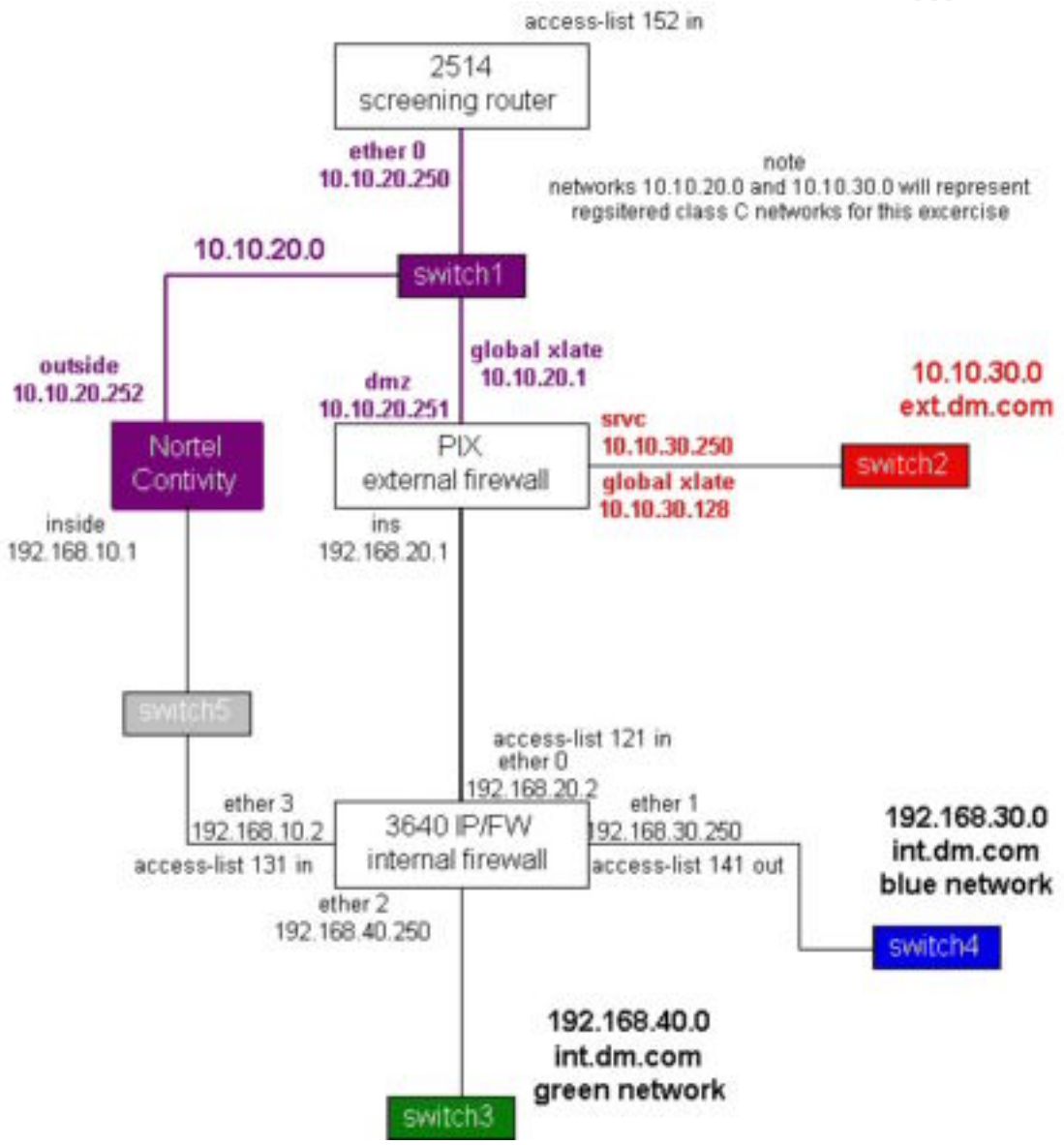
Physical security is often overlooked but all other efforts can be easily defeated if a critical server is located under someone's desk in a generally accessible area. In our example analysts with security clearance work in a secured area. Card locks are used to monitor access into the area. The only entry is highly visible from the work area and all visitors must sign in and display a visitor badge. All servers and core networking devices are located in a separate locked computer room located within the secure area. Card locks are also used to monitor access to the computer room, to which only a few analysts are allowed. Visitors to the computer room must be signed in and supervised at all times. Servers and network devices are locked in separate enclosed racks to further restrict access to authorised personnel only.

12. Testing

All firewall implementations should be tested on a regular basis to ensure that firewalls and other hardware is working the way we intended it to. Testing should be repeated when any changes are made to the firewall configuration.

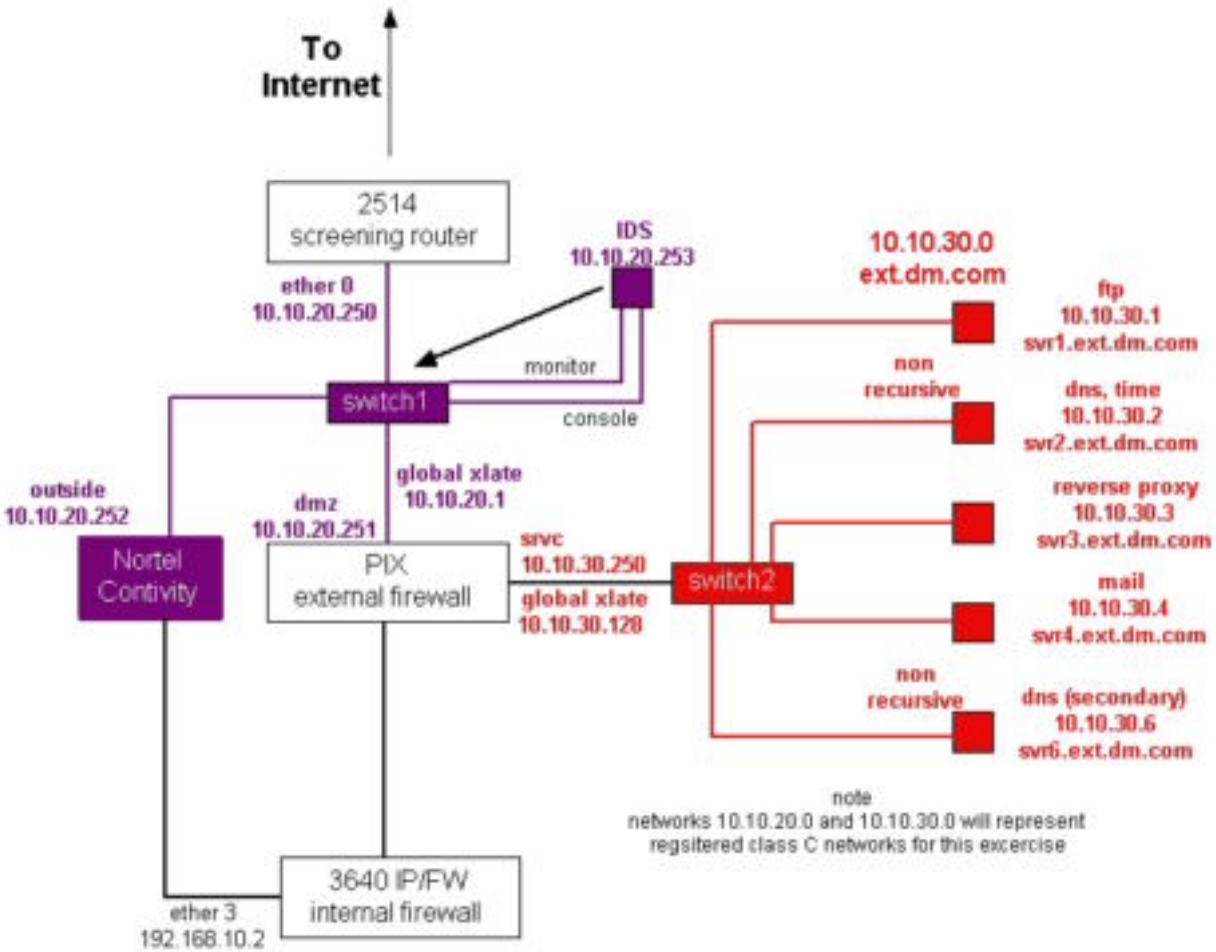
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Overview



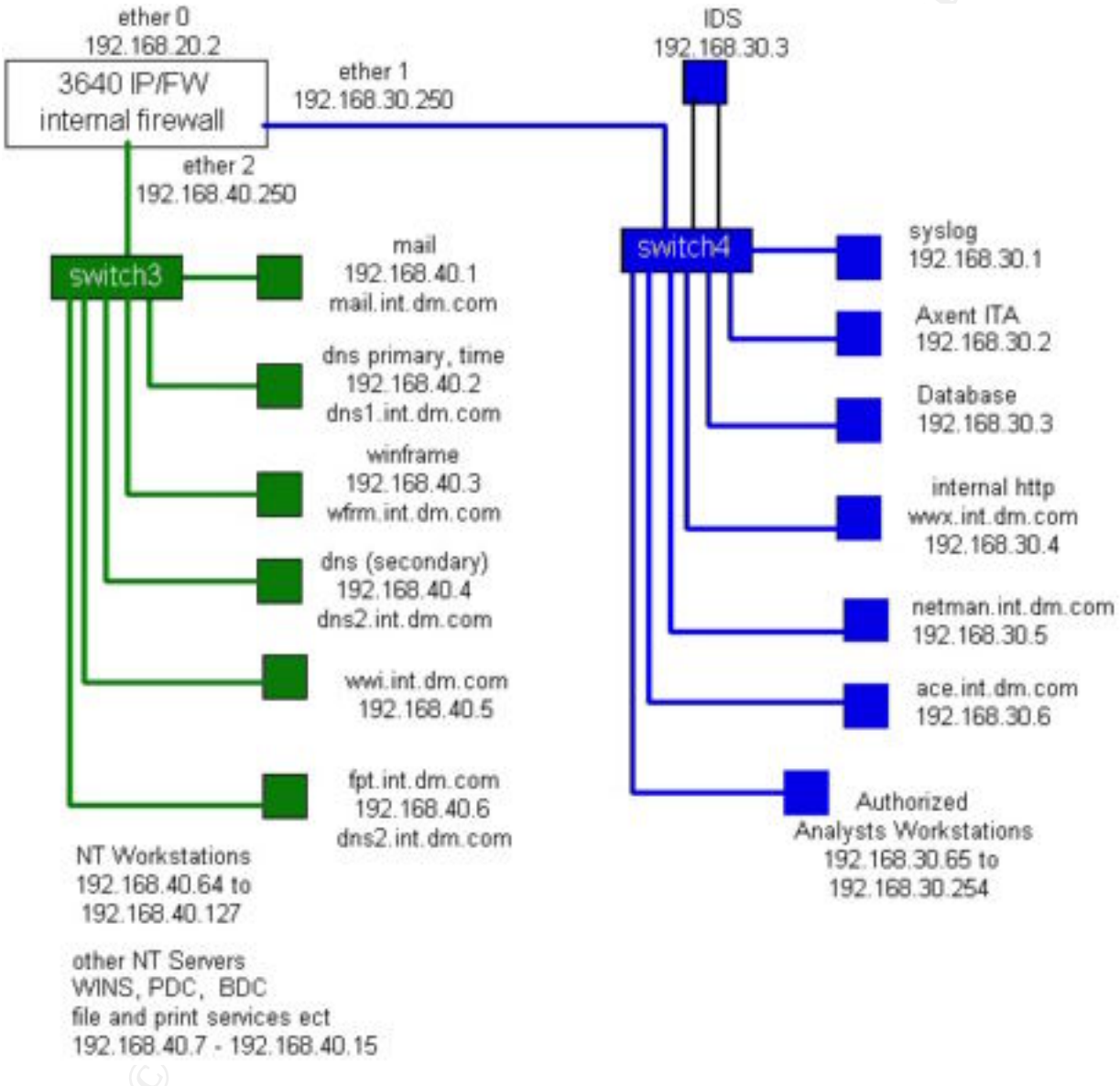
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

External Network

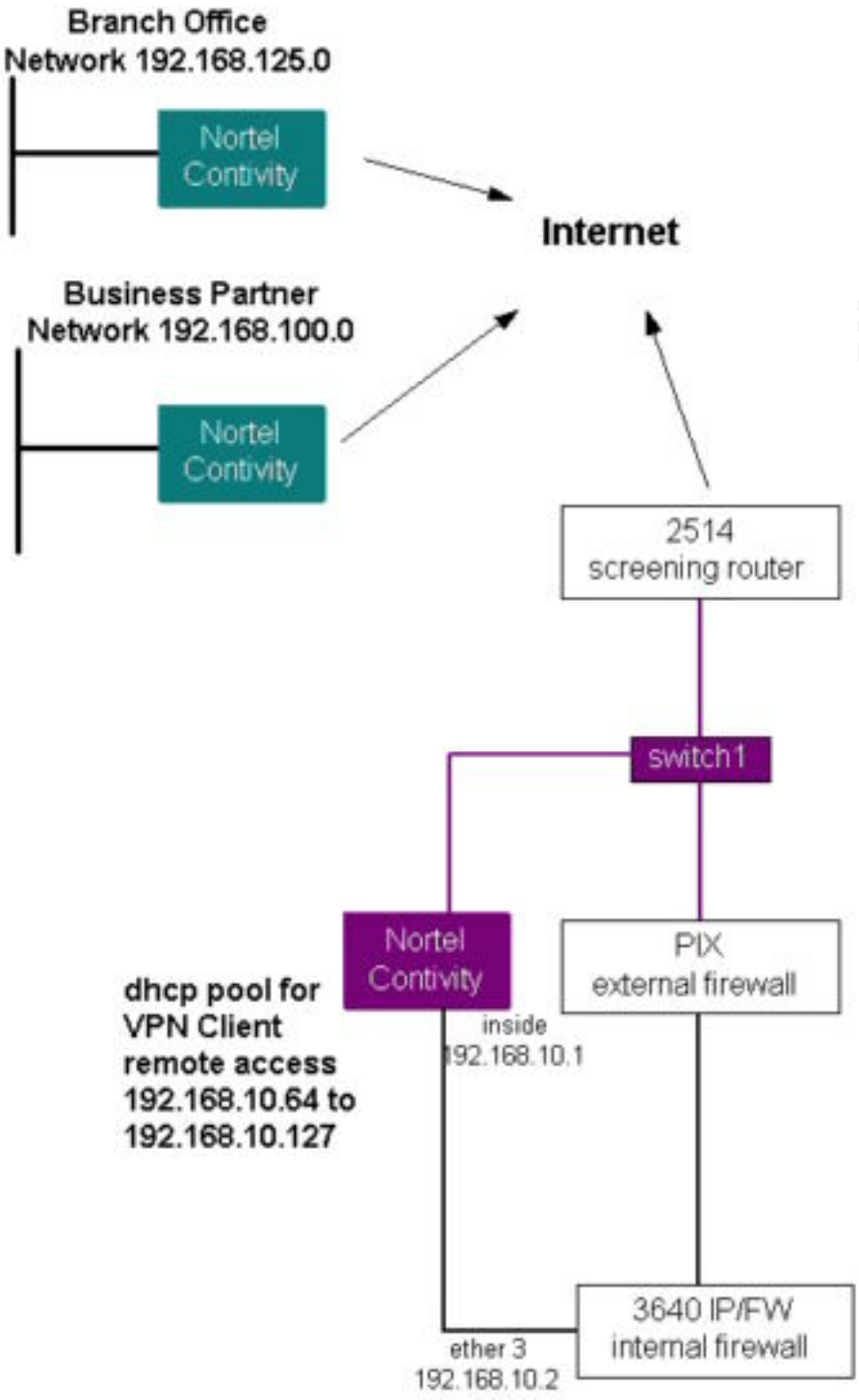


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Internal Network



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 2: Security Policy

Objective: Develop a security policy (implemented as a firewall filtering policy) to protect data accessible via the Internet"

For the exercise we refer to our Base security policy, which states the following

"*The external firewall will be configured to allow a minimal subset of TCP, UDP and ICMP from the Internet in order to provide the basic services that allow our* ***customers*** *to do business with us*"

"Access to/from corporate resources via the internet will be limited to IPSEC VPN connections using Triple DES encryption. A firewall between the VPN server and the corporate network will ensure that access to these resources is sufficiently safe guarded."

"In general services provided to business partners should be limited to only those services needed, and only to those devices (servers, routers etc) needed. Blanket access shall not be provided for anyone. The default stance will be to deny all access and then allow only those specific services that are needed. In no cases shall the Xtranet connection be used for internet access"

"Internal Firewalls will be used to limit access to confidential data. An internal secure network (Blue Network) will be configured behind a firewall protected from the office automation servers and general workstations. The internal firewall will also serve to protect the internal secure (Blue Network) from the Extranets and remote access users"

This section endeavours to show how our screening router, external and internal firewall have been configured in accordance with our Security Policy outlined in the previous section.

About Cisco Access-Lists

Much of the information that follows is based upon Cisco Access lists as they are used on the screening router and the internal Cisco 3640 firewall. Access-lists and have the same characteristics on both.

Access-lists are processed sequentially starting from the top and working down. Each packet arriving at an interface with an access-list applied is checked against each line (rule) in the list until a match is made. Once a packet matches a rule it is either denied (dropped) or permitted in which case it will be routed to the next interface where it may be subject to a new access-list. Only one access-list may be applied to an interface in each direction for a total of two per interface.

Every access-list implicitly denies all traffic that has not been matched in the access-list. This is the case whether you end the list with blanket deny statement or not. For example if you create an access-list with only one rule i.e. *deny icmp any any*, **all** IP traffic at this interface would be blocked because of the implicit deny characteristic.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

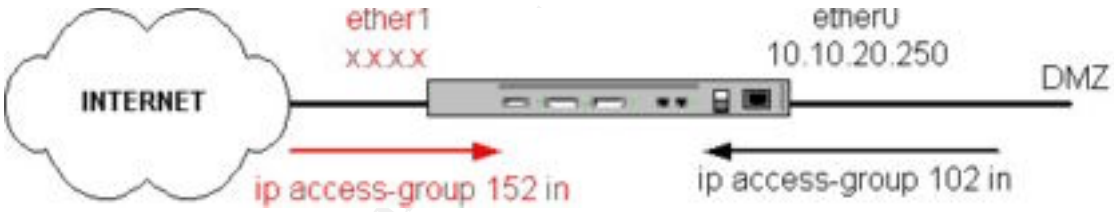
Be very careful when using permit or deny statements in a broad scope. For example if one of the first rules in an access-list were to *permit tcp any any* then all subsequent rules for tcp packets will be useless because all tcp packets will have already been forwarded. If your rules are very specific, the order of the rules may be less important. Sometimes rules that are most often matched are placed nearer the top of the list for efficiency, but it is more important that you do not defeat the intention of the overall rule set. Exceptions can be made to general rules by using a specific rule followed by one or more general rules. Use the "log" option for rules where matches are to be logged. All examples shown here use Cisco extended access-lists. If you are not familiar with Cisco Access-Lists it is highly recommended that you refer to Cisco's documentation for the IOS version you are running.

Screening Router

This section details the configuration of the Screening router, a Cisco 2514 router with IOS 12.0 (5) IP code. This router uses an access-list to block unwanted packets arriving from the internet and an access-list to prevent certain types of packets from leaving.

In our example access-list 152 is applied to inbound packets on interface ether1. This access-list provides our first defence to the Internet.

```
interface Ethernet1
 ip address x.x.x.x 255.255.255.0
 ip access-group 152 in
```



The following is a breakdown of rules from the screening router in our example. For clarity the deny statements are red and the permit statements are green.The first seven deny rules **must** appear first in the access-list otherwise the permit rules that follow would let these packets pass.

The rules that follow block packets with source addresses from private network space. Such packets should never be seen on the Internet because there are no routes back to these networks. This activity is either malicious or these packets have inadvertently leaked out from someone's network. In either event these should be dropped immediately.

```
access-list 152 deny  ip 10.0.0.0 0.255.255.255 any log
access-list 152 deny  ip 172.16.0.0 0.15.255.255 any log
access-list 152 deny  ip 192.168.0.0 0.0.255.255 any log
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The rules that follow block packets with source addresses that belong to our internal address space (spoofing). Obviously packets with our internal addresses as the source should never arrive from outside our network. This is usually malicious although I have seen network anomalies that will cause this. In either event these should be dropped immediately. *Remember that for our example these networks represent registered Class C networks.*

```
access-list 152 deny  ip 10.10.20.0 0.0.0.255 any log
access-list 152 deny  ip 10.10.30.0 0.0.0.255 any log
```

The rules that follow block additional invalid source addresses that could be used in a denial of service attack.

```
access-list 152 deny   ip host 0.0.0.0 any log
access-list 152 deny   ip host 127.0.0.1 any log
```

The rules that follow allow IP protocol 50 (IPSEC tunnel) and udp port 500 for ISAKMP destined for our VPN server

```
access-list 152 permit 50 any host 10.10.20.252
access-list 152 permit udp any host 10.10.20.252 eq 500
```

The rules that follow allow most TCP traffic destined for our registered Class C networks to pass to the firewall. Notice that only tcp for host 10.10.20.1 is allowed for network 10.10.20.0 This is because the only address ever visible on the internet for that network is our global translation address.

```
access-list 152 permit tcp any  host 10.10.20.1
access-list 152 permit tcp any  10.10.30.0 0.0.0.255
```

At this point we could also let all udp traffic pass to the PIX as well, but because we only need udp for DNS and NTP (time) we have decided to allow only the udp which is absolutely necessary. This is redundant to the firewall and is not required but it will off load a lot of udp junk from our Firewall.

The rules that follow allow our NTP and DNS servers to work. These allow **only** server to server communication for DNS and Time.

```
access-list 152 permit udp eq ntp any any eq ntp
access-list 152 permit udp any eq domain host 10.10.30.2 eq domain
access-list 152 permit udp any eq domain host 10.10.30.6 eq domain
access-list 152 permit udp any eq domain host 10.10.20.42 eq domain
access-list 152 permit udp any eq domain host 10.10.20.44 eq domain
```

Now we can block all the remaining udp. At this point you can choose to log the access-violations for udp or not. It is recommended to log everything but if you don't want to bother with UDP, you can choose not to log.

```
access-list 152 deny  udp any any log
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The rules that follow allow echo-reply (ping response) for our registered networks. This is optional and may depend on security policy.

```
access-list 152 permit icmp any  10.10.20.0 0.0.0.255 echo-reply
access-list 152 permit icmp any 10.10.30.0 0.0.0.255 echo-reply
```

The rules that follow block all remaining icmp. By having a separate rule for icmp echo we can choose not to log these access-violations. All remaining icmp access-violations are logged.

```
access-list 152 deny   icmp any any echo log
access-list 152 deny   icmp any any log
```

The rule that follow allows us to log all remaining blocked packets. These would have been denied anyway, but unless we include the deny any any rule, we can't log them.

```
access-list 152 deny ip any any log
```

This completes our access list. We have now

- blocked incoming all packets with invalid source addresses
- blocked all udp except for DNS and time, both are still subject to inspection by PIX
- Permitted all tcp to be handled by the PIX

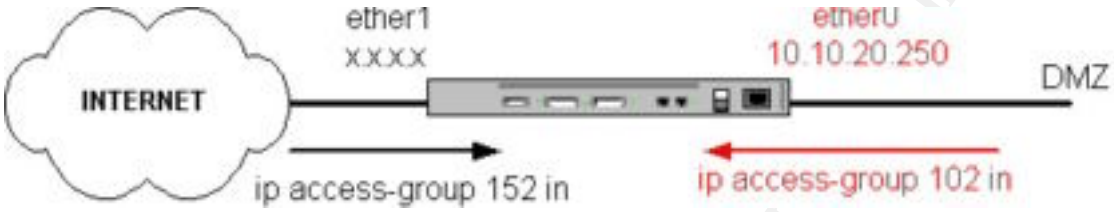
The rule set is show again below without the comments for clarity.

```
access-list 152 deny  ip 10.0.0.0 0.255.255.255 any log
access-list 152 deny  ip 172.16.0.0 0.15.255.255 any log
access-list 152 deny  ip 192.168.0.0 0.0.255.255 any log
access-list 152 deny  ip 10.10.20.0 0.0.0.255 any log
access-list 152 deny  ip 10.10.30.0 0.0.0.255 any log
access-list 152 deny   ip host 0.0.0.0 any log
access-list 152 deny   ip host 127.0.0.1 any log
access-list 152 permit 50 any host 10.10.20.252
access-list 152 permit udp any host 10.10.20.252 eq 500
access-list 152 permit tcp any  host 10.10.20.1
access-list 152 permit tcp any  10.10.30.0 0.0.0.255
access-list 152 permit udp eq ntp any any eq ntp
access-list 152 permit udp any eq domain host 10.10.30.2 eq domain
access-list 152 permit udp any eq domain host 10.10.30.6 eq domain
access-list 152 permit udp any eq domain host 10.10.20.42 eq domain
access-list 152 permit udp any eq domain host 10.10.20.44 eq domain
access-list 152 deny  udp any any log
access-list 152 permit icmp any  10.10.20.0 0.0.0.255 echo-reply
access-list 152 permit icmp any 10.10.30.0 0.0.0.255 echo-reply
access-list 152 deny   icmp any any echo
access-list 152 deny   icmp any any log
access-list 152 deny ip any any log
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Access-list 102 is applied to inbound packets on interface ether0 on the screening router. This access-list is intended to filter traffic leaving our network for the Internet. This helps to prevent and alert us to, anomalous network activity whether it is malicious or not.

```
interface Ethernet0
 ip address 10.10.20.250 255.255.255.0
 ip access-group 102 in
```



The first three rules must appear first in the access-list. If not the permit rules that follow would let these packets pass.

The rules that follow ensure that no packets destined for the private address space leave the network either intentionally or inadvertently.

```
access-list 102 deny   ip any 10.0.0.0 0.255.255.255 log
access-list 102 deny   ip any 172.16.0.0 0.15.255.255 log
access-list 102 deny   ip any 192.168.0.0 0.0.255.255 log
```

The rules that follow ensure that no unencrypted tcp or udp packets from the VPN server leave the network, except for udp protocol 500 required for ISAKMP. (VPN connections are authenticated internally with SecureID) Notice that we have used a specific permit rule as an exception to more general rules that follow. Order is important here!

```
access-list 102 permit udp host 10.10.20.252 any eq 500 (permits udp port 500 required)
access-list 102 deny   tcp host  10.10.20.252 any log
access-list 102 deny   udp host  10.10.20.252 any log (denys remaining udp)
```

The rules that follow rules ensure that only tcp and udp packets with source addresses from our registered address space leave the network. *Remember that for our example these networks represent registered Class C networks.*

```
access-list 102 permit tcp 10.10.20.0 0.0.0.255 any
access-list 102 permit udp 10.10.20.0 0.0.0.255 any
access-list 102 permit tcp 10.10.30.0 0.0.0.255 any
access-list 102 permit udp 10.10.30.0 0.0.0.255 any
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The rules that follow allow icmp echo-requests (ping) to leave the network (optional).

```
access-list 102 permit icmp 10.10.20.0 0.0.0.255 any echo
access-list 102 permit icmp 10.10.30.0 0.0.0.255 any echo
```

The rule that follows allows IP protocol 50 for IPSEC tunnels from our VPN server.

```
access-list 102 permit 50 host 10.10.20.252 any
```

The rule that follow blocks all remaining IP and logs these violations. This rule must be last. If this were first in our list it would have simply blocked everything.

```
access-list 102 deny   ip any any log
```

This completes our access lists. The screening router does not really address the internet use policy but it should now

- Block packets destined for private networks
- Ensured that only IP protocol 50 and UDP port 500 can be used by the VPN server
- Ensured that only packets from our registered address space leaves our network
- Allowed echo-requests (optional)

The rule set is show again below without the comments for clarity.

```
access-list 102 deny   ip any 10.0.0.0 0.255.255.255 log
access-list 102 deny   ip any 172.16.0.0 0.15.255.255 log
access-list 102 deny   ip any 192.168.0.0 0.0.255.255 log
access-list 102 permit udp host 10.10.20.252 any eq 500
access-list 102 deny   tcp host  10.10.20.252 any log
access-list 102 deny   udp host  10.10.20.252 any log
access-list 102 permit tcp 10.10.20.0 0.0.0.255 any
access-list 102 permit udp 10.10.20.0 0.0.0.255 any
access-list 102 permit tcp 10.10.30.0 0.0.0.255 any
access-list 102 permit udp 10.10.30.0 0.0.0.255 any
access-list 102 permit icmp 10.10.20.0 0.0.0.255 any echo
access-list 102 permit icmp 10.10.30.0 0.0.0.255 any echo
access-list 102 permit 50 host 10.10.20.252 any
access-list 102 deny   ip any any log
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Additional precautions for routers

Block icmp unreachables from being sent at the interface level. An access-list will not do this even if you deny all icmp. Access-lists only block icmp messages already in transit. Icmp messages that originate from the router bypass the access-list. There are a few specific icmp message types that can be blocked at the interface level.

interface Ethernet1
no ip unreachables

Prevent IP broadcasts from being propagated on all interfaces of your screening router, IP broadcasts are generally used maliciously for denial of service

interface Ethernet1
no ip directed-broadcast
interface Ethernet0
no ip directed-broadcast

Block source routed IP packets

interface Ethernet1
no ip source-route

Limit management access to the router from the network management station. The following lines ensure that only host 10.10.20.35 can access the router over the network.

access-class 10 in
access-list 10 permit 10.10.20.35

Limit snmp access to the router from the network management station. The following lines ensure that snmp packets will only be accepted from host 10.10.20.35

access-list 20 permit 10.10.20.35
snmp-server community xxxxxxxxx RW 20 (where 20 is the access-list and xxxx is the read write community string)

For further detailed information on securing a Cisco router see
http://www.cisco.com/warp/public/707/21.html

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

External Firewall

This section deals with the configuration of the Cisco PIX Firewall. Cisco has documentation that includes example configurations in great detail. The explanation that follows does not duplicate that effort. For more information about Cisco PIX see **http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v44/pix44cfg/pix44exs.htm**

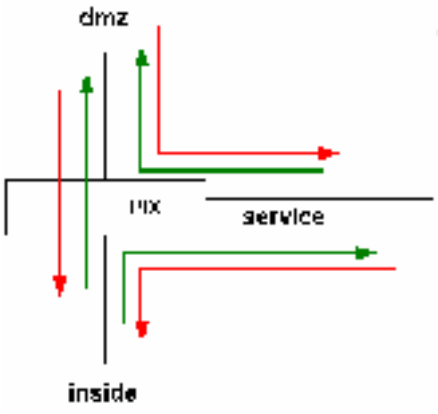
This section is intended to demonstrate the firewall rules but some other basic information is required.

When configuring the PIX, each interface is assigned a name and a security value between 0 and 100. Zero (0) represents the least secure network and 100 represents the most secure network. This is extremely important because unless otherwise configured, PIX will allow any outgoing connection from a high security interface to a lower security interface. Connections in the opposite direction require a conduit.

We have defined our inside network with 100 being the highest, the service network with 50 and the DMZ with a 0. This means that

- the inside network can start connections to the DMZ / Internet and the service network
- The service network can start connections to the DMZ / Internet
- Connections from the DMZ to either the service or inside network require conduits
- Connections from the service network to the inside network require conduits

In the following diagram the green arrows show where all outbound connections are permitted, the red arrows show where inbound conduits must be defined



The following lines configure the security on the interfaces

nameif ethernet0 dmz security0
nameif ethernet1 inside security100
nameif ethernet2 service security50

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Because of address translation for the inside network to the outside network and DMZ we have configured a number of static translations.

The following group of static translations are for hosts on the internal network which must be accessible form the service network. PIX allows us to create static translations which actually duplicate the inside IP address on both interfaces. These addresses can only be used by hosts on the service network. PIX routes packets received on the service network interface for these hosts to the internal network.

```
static (inside,service) 192.168.30.2 192.168.30.2 netmask 255.255.255.255 0 0
static (inside,service) 192.168.30.4 192.168.30.4 netmask 255.255.255.255 0 0
static (inside,service) 192.168.30.5 192.168.30.5 netmask 255.255.255.255 0 0
static (inside,service) 192.168.30.6 192.168.30.6 netmask 255.255.255.255 0 0
static (inside,service) 192.168.40.1 192.168.40.1 netmask 255.255.255.255 0 0
static (inside,service) 192.168.40.2 192.168.40.2 netmask 255.255.255.255 0 0
static (inside,service) 192.168.40.4 192.168.40.4 netmask 255.255.255.255 0 0
```

The following group of static translations are for internal hosts which must be accessed by hosts on the DMZ. These are for utility purposes and will be explained in the conduit section.

```
static (inside,dmz) 10.10.20.31 192.168.30.1 netmask 255.255.255.255 0 0
static (inside,dmz) 10.10.20.32 192.168.30.2 netmask 255.255.255.255 0 0
static (inside,dmz) 10.10.20.35 192.168.30.5 netmask 255.255.255.255 0 0
```

The following group of static translations are for internal DNS servers. Global address translation may however prevent our DNS from working properly so we have defined unique static translations.

```
static (inside,dmz) 10.10.20.42 192.168.40.2 netmask 255.255.255.255 0 0
static (inside,dmz) 10.10.20.44 192.168.40.4 netmask 255.255.255.255 0 0
```

As stated previously you must define conduits to allow connections from lower security interfaces to higher security interfaces. In this direction conduits are similar to access-lists.

The following conduits are for connections from the DMZ (internet) to hosts on the service network. Notice that these rules are **reverse from Cisco Access-Lists**. To the left is the destination address and port, to the right is the source address and port. These rules have been kept simple and explicit. Only the necessary services are configured for each server. In our case this includes ftp, http, https, smtp and DNS. Each server is accessible on the appropriate port by any host on the internet. See Policy 1.1

```
conduit permit tcp host 10.10.30.1 eq ftp any
conduit permit tcp host 10.10.30.3 eq www any
conduit permit tcp host 10.10.30.3 eq 443 any
conduit permit tcp host 10.10.30.4 eq smtp any
conduit permit udp host 10.10.30.2 eq domain any eq domain
conduit permit udp host 10.10.30.6 eq domain any eq domain
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The following conduits are for connections from the service network to hosts on the inside network. These are very limited and very explicit. See policy 1.2 and 5.1

The following line allows connections from the external mail server to the internal mail server.
conduit permit tcp host 192.168.40.1 eq smtp host 10.10.30.4

The following line allows the Axent Intruder alert logs from hosts on the DMZ to the IDS manager.
conduit permit tcp host 192.168.30.2 eq 5051 10.10.30.1 255.255.255.248

The following line allows http from our reverse HTTP proxy server to the internal HTTP server.
conduit permit tcp host 192.168.30.4 eq 80 host 10.10.30.3

The following line allows hosts on the service network to make DNS queries to our internal DNS servers.
conduit permit udp host 192.168.40.2 eq 53 10.10.30.1 255.255.255.248
conduit permit udp host 192.168.40.4 eq 53 10.10.30.1 255.255.255.248

The following conduits are for connections from the dmz to hosts on the inside network. These allow syslog from the screening router to the syslog server and allow ftp from the screening router to netman.int.dm.com for backup purposes. See policy 5.1

conduit permit udp host 10.10.20.31 eq syslog host 10.10.20.250
conduit permit udp host 10.10.20.35 eq ftp host 10.10.20.250

This line allows for echo replies. By default PIX will not allow these even if they are legitimate echo-replys. PIX will validate these against outgoing icmp echo requests.

conduit permit icmp any any echo-reply (optional)

The entire rule set is shown below without the comments to show how simple the rule set is. The rules are grouped for DMZ to Service, Service to inside and DMZ to inside. Notice that only permit statements are used.

conduit permit tcp host 10.10.30.1 eq ftp any
conduit permit tcp host 10.10.30.3 eq www any
conduit permit tcp host 10.10.30.3 eq 443 any
conduit permit tcp host 10.10.30.4 eq smtp any
conduit permit udp host eq domain 10.10.30.2 eq domain any
conduit permit udp host eq domain 10.10.30.6 eq domain any

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

conduit permit tcp host 192.168.40.1 eq smtp host 10.10.30.4
conduit permit tcp host 192.168.30.2 eq 5051 10.10.30.1 255.255.255.248
conduit permit tcp host 192.168.30.4 eq 80 host 10.10.30.3
conduit permit udp host 192.168.40.2 eq 53 10.10.30.1 255.255.255.248
conduit permit udp host 192.168.40.4 eq 53 10.10.30.1 255.255.255.248

conduit permit udp host 10.10.20.31 eq syslog host 10.10.20.250
conduit permit udp host 10.10.20.35 eq ftp host 10.10.20.250
conduit permit icmp any any echo-reply (optional)

This completes our rule set for the PIX Firewall.

- We have observed our Security Policy by allowing only **incoming** http, https, ftp, smtp and dns from the internet to our service network only. These are currently required to "*allow our **customers** to do business with us*".

- We have allowed limited access from the service network to the inside network for mail, http proxy, dns, security and management.

- We have allowed Syslog and FTP from our screening router (DMZ) for security and management.

Internal Firewall

This section deals with the configuration of the internal Firewall. With Cisco's firewall feature set a 3640 router can be used as Stateful inspection class of firewall. Cisco has a very good document that explains CBAC. The explanation that follows does not duplicate that effort. For more information about CBAC see http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt3/sccbac.htm#xtocid218832

To configure CBAC inspection for TCP or UDP, use one or both of the following global configuration commands. CBAC requires a separate list for each interface.

ip inspect name *inspection-name* tcp
ip inspect name *inspection-name* udp

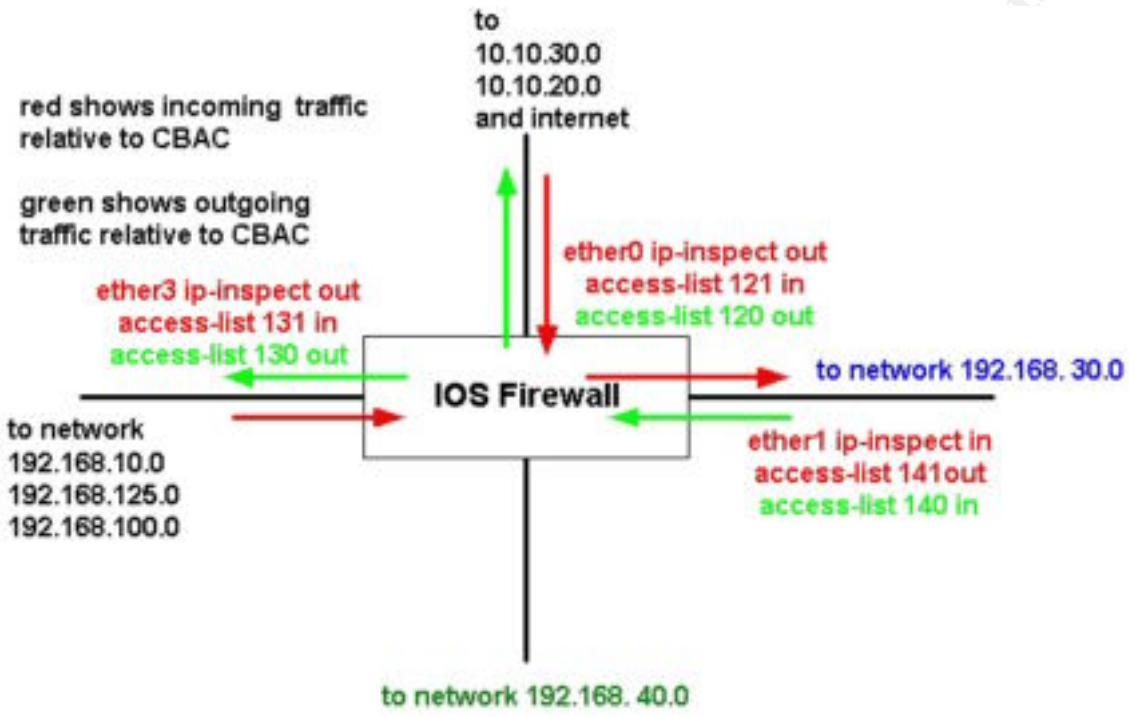
To configure CBAC inspection for specific applications, use the following global configuration commands. (This is a sample of supported applications)

ip inspect name *inspection-name* ftp
ip inspect name *inspection-name* smtp
ip inspect name *inspection-name* http

Ip-inspect is applied at the interface level, which is shown in the example for each interface.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

In our example CBAC works on three interfaces as shown below. Notice that interface ether1 is configured in the opposite manner as ether0 and ether3



Interface Ethernet 0 to PIX Firewall / Internet

Inter ether 0 is configured with CBAC to act as redundant firewall to the PIX. To apply CBAC to ether0

Global commands
ip inspect name *internet* tcp
ip inspect name *internet* udp
ip inspect name *internet* ftp
ip inspect name *internet* smtp
ip inspect name *internet* http

interface Ethernet0
 ip access-group 121 in
 ip access-group 120 out
 ip inspect internet out

Access-list 120 out (not intended to enforce any policy)

The rules that follow allow outbound udp and tcp from both internal networks.
access-list 120 permit tcp 192.168.30.0 0.0.0.255 any

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

access-list 120 permit udp 192.168.30.0 0.0.0.255 any
access-list 120 permit tcp 192.168.40.0 0.0.0.255 any
access-list 120 permit udp 192.168.40.0 0.0.0.255 any

The rule that follows allows outbound tcp from branch office connections
access-list 120 permit tcp 192.168.125.0 0.0.0.255 any

The rule that follows allows outbound tcp from remote access clients
access-list 120 permit tcp 192.168.10.64 0.0.0.15 any

Access-list 121 in

This access-list is for incoming connections from the DMZ and the service network. Many of these are for management and security. See policy 1.2 and 5.1

The rule that follows allows syslog output from the screening router to the syslog server
access-list 121 permit tcp host 10.10.20.250 host 192.168.30.1 eq syslog

The rule that follows allows ftp from the screening router to the management station
access-list 121 permit tcp host 10.10.20.250 host 192.168.30.5 eq ftp

The rule that follows allows syslog from the PIX firewall router to the syslog server
access-list 121 permit udp host 192.168.20.1 host 192.168.30.1 eq syslog

The rule that follows allows ftp from the PIX firewall router to the management station
access-list 121 permit tcp host 192.168.20.1 host 192.168.30.5 eq ftp

The rule that follows allows smtp from the external mail server to the internal mail server
access-list 121 permit tcp host 10.10.30.4 host 192.168.40.1 eq smtp

The rule that follows allows the IDS agent to report to the ITA management console
access-list 121 permit tcp 10.10.30.1 255.255.255.248 host 192.168.30.2 eq 5051

The rule that follows allows http from the external proxy web server to the internal server
access-list 121 permit tcp host 10.10.30.3 host 192.168.30.4 eq 80

The rules that follow allows servers on the service network to use the internal DNS
access-list 121 permit udp 10.10.30.1 255.255.255.248 host 192.168.40.2 eq 53
access-list 121 permit udp 10.10.30.1 255.255.255.248 host 192.168.40.4 eq 53

Allow icmp echo-replys (optional)
access-list 121 permit icmp any any echo-reply

Deny all remaining traffic and log
access-list 121 deny   tcp any any log
access-list 121 deny   udp any any log
access-list 121 deny   icmp any any log
access-list 121 deny   ip any any log

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Interface Ethernet 3 to VPN Extranet Server

This interface functions as the firewall to the VPN server and therefore is the point at which we enforce the policy for Xtranet (Business Partners), Branch office and employee remote access.

For this example our business partner has several requirements.

Email
It has been determined that since email could contain sensitive material, our internal mail servers would communicate via VPN rather than unencrypted over the Internet. This ensures that all mail is encrypted without burdening all our users with manual PGP encryption.

Bulk data transfer
There is a requirement for regular large transfers of data. These could be encrypted and moved via the internet to our external FTP server, but this would add too much overhead to the process. We have defined a single FTP server for access from our partner's FTP server.

Access to corporate Intranet
To allow our partners employees access to our Intranet, all hosts on the partner's network will have access to a virtual web server allowing them to see appropriate material about our company and employees.

Inter ether 0 is configured with CBAC to act as redundant firewall to the PIX. To apply CBAC to ether0

Global commands
ip inspect name *vpn* tcp
ip inspect name *vpn* udp
ip inspect name v*pn* ftp
ip inspect name v*pn* smtp
ip inspect name *vpn* http

interface Ethernet3
 ip access-group 131 in
 ip access-group 130 out
 ip inspect vpn out

Access-list 130 out (not intended to enforce any policy)

access-list 130 permit tcp 192.168.40.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 130 permit udp 192.168.40.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 130 permit tcp 192.168.40.0 0.0.0.255 192.168.125.0 0.0.0.255
access-list 130 permit udp 192.168.40.0 0.0.0.255 192.168.125.0 0.0.0.255
access-list 130 permit tcp 192.168.40.0 0.0.0.255 192.168.10.64 0.0.0.15 established
access-list 130 permit tcp any 192.168.125.0 0.0.0.255 established

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The following rules permit access as defined by our security policy for hosts on our Business partners network. See policy 3.4

Allows ftp (normal mode) from host 192.168.100.10 to access our internal FTP server
access-list 131 permit tcp host 192.168.100.10 host 192.168.40.5 eq 21

Allows smtp from host 192.168.100.11 to access our internal mail server
access-list 131 permit tcp host 192.168.100.11 host 192.168.40.1 eq 25

Allows http from hosts on network 192.168.100.0 to access our internal http server
access-list 131 permit tcp 192.168.100.0 0.0.0.255 host 192.168.40.6 eq 80

The following rules restrict the use of upd and tcp from branch office to servers on the green network. See policy 3.2
access-list 131 permit tcp 192.168.125.0 0.0.0.255 192.168.40.0 0.0.0.15
access-list 131 permit udp 192.168.125.0 0.0.0.255 192.168.40.0 0.0.0.15

The following rule allows all hosts from the branch office to use http to the internet but blocks all IP to networks 10.10.20.0 and 192.168.20.0 and 192.168.30.0 The order of these rules is important. See policy 3.3
Access-list 131 deny ip 192.168.125.0 0.0.0.255 10.10.20.0 0.0.0.255
Access-list 131 deny ip 192.168.125.0 0.0.0.255 192.168.20.0 0.0.0.255
Access-list 131 deny ip 192.168.125.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 131permit tcp 192.168.125.0 0.0.0.255 any eq http

The following rule allows the VPN server to communicate with the SecureID server.
Access-list 131 permit tcp host 192.168.10.1 host 192.168.30.6 eq xxxx

The following rule allows remote access-users to access the winframe server. See policy 3.1
access-list 131 permit tcp 192.168.10.64 0.0.0.15 host 192.168.40.3 eq xxx

The following rule denys all other access and logs
access-list 131 deny ip any any log

Interface Ethernet 1 to Secure Network

ip inspect name *bluenet* tcp
ip inspect name *bluenet* udp
ip inspect name *bluenet* ftp
ip inspect name *bluenet* smtp
ip inspect name *bluenet* http

interface Ethernet1
 ip access-group 141 out
 ip access-group 140 in
 ip inspect internet in

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Inter ether 1 is configured with CBAC to act as a firewall for the blue network. Two access-list are configured

Access-list 140 (not intended to enforce security policy)

access-list 140 permit tcp 192.168.30.1 any
access-list 140 permit udp 192.168.30.1 any

The following rules permit access as defined by our security policy for hosts on our Business partners network. See policy 3.4

allows http from our reverse HTTP proxy server to the internal HTTP server.
access-list 141 permit tcp host 10.10.30.3 host 192.168.30.3 eq 80

allows syslog from VPN server to syslog server
access-list 141 permit udp host 192.168.10.1 host 192.168.30.1 eq syslog

allows ftp from VPN server to network management server
access-list 141 permit tcp host 192.168.10.1 host 192.168.30.1 eq ftp

allows syslog from screening router to syslog server
access-list 141 permit udp host 10.10.20.250 host 192.168.30.1 eq syslog

allows ftp from screening router to network management server
access-list 141 permit tcp host 10.10.20.250 host 192.168.30.1 eq ftp

allows syslog from PIX firewall to syslog server
access-list 141 permit udp host 192.168.20.1 host 192.168.30.1 eq syslog

allows ftp from PIX firewall to network management
access-list 141 permit tcp host 192.168.20.1 host 192.168.30.2 eq ftp

allows SecureID from VPN server to SecureID server
Access-list 141 permit tcp host 192.168.10.1 host 192.168.30.6 eq xxxx

This completes the Internal Firewall Configuration

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 3: Audit your security architecture

For the purposes of this assignment please assume that you have been assigned to provide technical support for a comprehensive information systems audit.

Start-up meeting

1. Confirm the scope of the project
2. Agree upon hours for testing
3. Determine in house technical knowledge
4. Obtain existing documentation (firewall configuration, diagrams etc)
5. Review security policy with respect to firewall rules
6. Obtain list of contacts (names, after hours phone etc)

In the start-up meeting it was agreed that a complete perimeter assessment should include testing from the Internet, branch office, business partner and VPN client perspective. The client requested that we are to be as expedient as possible and it was agreed that we would limit our scans to ports listed in the nmap services file. The client provided hours for testing during off peak hours as the business is a 7x24 hour operation. The in house technical knowledge is good and we received up to date documentation. We were provided with a list of emergency contacts. The client has also asked that we do not to run any tests that would knowingly put the network at high risk, i.e. DOS attacks.

Post Start-up

1. review Firewall rule sets to ensure that the firewall is correctly configured to achieve the intended firewall policy
2. check with Cisco to determine if the firewall and router code has any known vulnerabilities
3. create a plan indicating what tests are to be conducted from what networks

The Plan

Use nmap to perform the following scans on the external firewall

1. from the service network to hosts on the service network.
2. from the internet towards hosts on our service network 10.10.30.0
3. from the internet towards addresses on DMZ 10.10.20.0
4. from the DMZ towards translated addresses on the PIX dmz interface.
5. from the DMZ towards hosts on our service network 10.10.30.0
6. from the service network to translated addresses on the PIX srvc interface (internal hosts)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Use nmap to perform the following scans on the internal firewall

1. From the network at the branch office to the blue and green network
2. From the network at the business partner office to the blue and green network
3. From a VPN client connection to the blue and green network
4. From the green network to the blue network
5. Check the services on internal router/firewall interfaces

Use nmap to check for services on the network devices

Screening router
PIX firewall
Internal Firewall
VPN server

Check the configurations on the DNS server

1. Ensure that the external zone file has only the required records
2. Ensure that the external server will not allow zone transfers from external servers
3. Ensure that the external DNS server is not recursive

About nmap

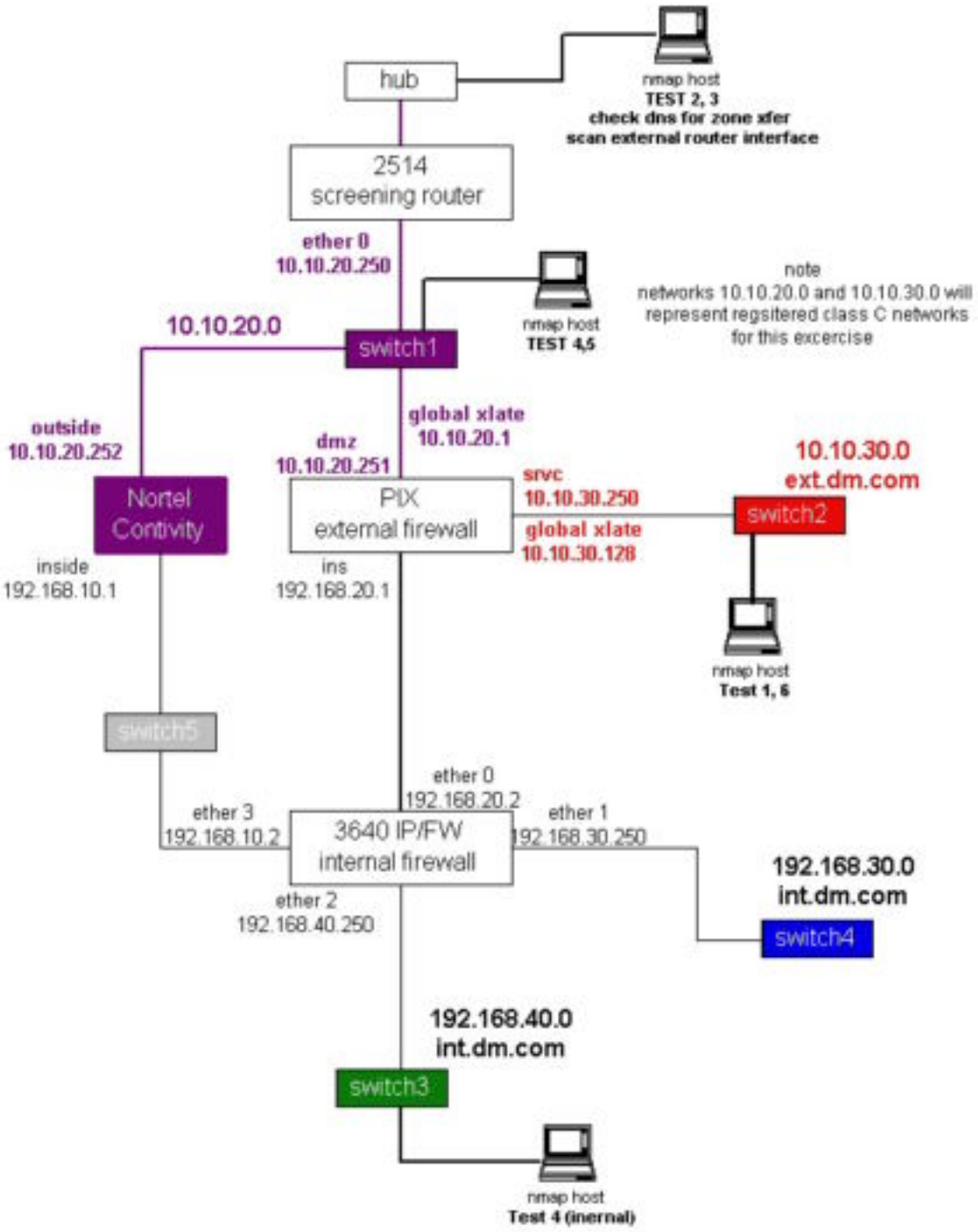
Nmap is a network scanning utility that can be installed on Linux and when run from root is very powerful. Nmap can perform a wide variety of scans designed to avoid detection and make log file analysis difficult. Since our intentions are legitimate we used the basic tcp SYN scan and the UDP scan. Nmap comes with a file of approximately 1060 tcp ports and 900 udp ports to scan. This can save time by not having to scan all possible 64000 ports and should be sufficient to verify firewall rule sets. Refer to the nmap documentation before you begin. I recommend you try this on your own network first if you have not used it before.

Examples

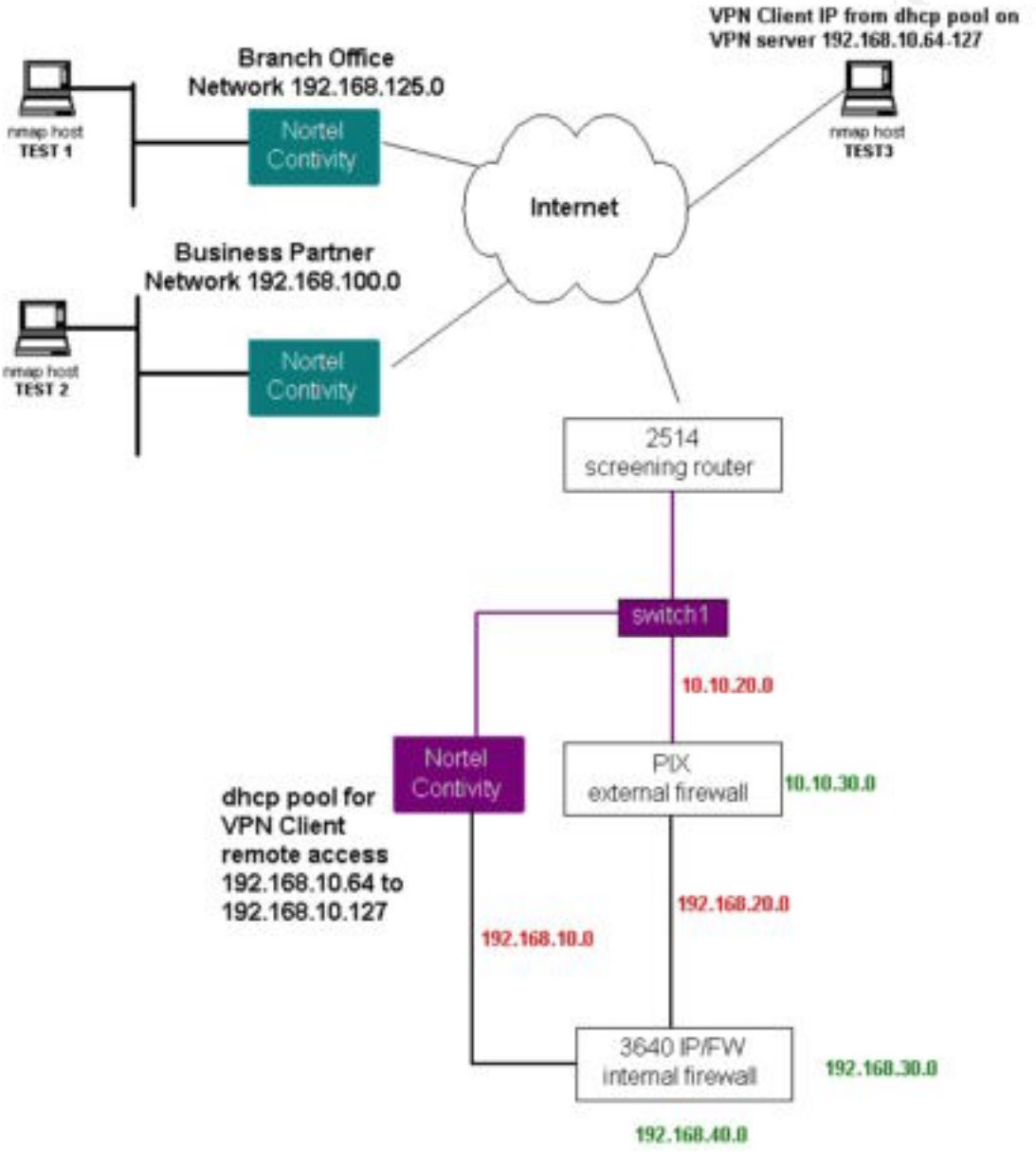
The network in our example does not really exist. The examples below are based upon actual output from scans of a similar nature. Where nmap output is included, it has been modified to represent the network in our example. A few examples of the output have been included, for the remaining scans I have summarised what was seen or what I would expect to see.

Refer to the following diagrams for the external and internal firewall verification

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

External Firewall Validation

For our example we will be using NMAP to perform network scans. **Remember that in our example networks 10.10.20.0 and 10.10.30.0 are representative of Registered Class C networks.**

1) from the service network to hosts on the service network

This is not intended to validate the firewall rules but simply to inventory the available ports on these servers. Assuming an unassigned address from network 10.10.30.0, we scanned all ports for each server on the service network. One example is shown below, the others were similar, as the base server configuration was the same.

The following command initiates the TCP connect port scan in verbose mode for ports 1-64000 in aggressive mode (T5) for host 10.10.30.1 The –P0 option does not use ping and the –oN option writes the results to a log file.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmap -sT -P0 –1-64000-T5 -v -n –oN scan1tcp
10.10.30.1
Interesting ports on  (10.10.30.1):
(The 63981 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
199/tcp    open        smux
1027/tcp   open        unknown
1034/tcp   open        unknown
1052/tcp   open        unknown
1059/tcp   open        nimreg
1987/tcp   open        tr-rsrb-p1
2301/tcp   open        compaqdiag
5052/tcp   open        unknown
6050/tcp   open        unknown
6055/tcp   open        unknown
41523/tcp  open        unknown
49400/tcp  open        unknown
49401/tcp  open        unknown
```

The following command initiates the UDP scan in verbose mode for ports 1-64000 for host 10.10.30.1

```
# Nmap (V. nmap) scan initiated 2.53 as: nmap -sU -P0 -v -p1-64000 -oN scan1udp
10.10.30.1
All 1024 scanned ports on (10.10.30.1) are: filtered
# Nmap run completed at Fri Sep 29 16:23:19 2000 -- 1 IP address (1 host up) scanned
in 1239 seconds
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2) From the internet towards hosts on our service network

A TCP SYN stealth port scan and a UDP scan will confirm what services are accessible on each server from the internet.

The following command initiates the TCP stealth port scan in verbose mode for tcp ports listed in the nmap services file (-F) for hosts 10.10.30.1 – 10.10.30.6. The –P0 option does not use ping and the –oN option writes the results to a log file. We use the –P0 option because ICMP is blocked at the screening router. Without the –P0 option, nmap will attempt to ping each host to see if it is reachable before starting the scan.

scan initiated 2.53 as: nmap -sS -v -F -P0 -oN scan2tcp 10.10.30.1-6

Interesting ports svr1.ext.dm.com(10.10.30.1):
(The 1061 ports scanned but not shown below are in state: filtered)
Port State Service
21/tcp open ftp

Interesting ports svr3.ext.dm.com (10.10.30.3):
(The 1060 ports scanned but not shown below are in state: filtered)
Port State Service
80/tcp open http
443/tcp open https

Interesting ports svr4.ext.dm.com (10.10.30.4):
(The 1061 ports scanned but not shown below are in state: filtered)
Port State Service
25/tcp open smtp

The following command initiates the UDP port scan in verbose mode for udp ports listed in the nmap services file (-F) for hosts 10.10.30.1 – 10.10.30.6. The –P0 option does not use ping and the –oN option writes the results to a log file. We use the –P0 option because ICMP is blocked.
Note UDP port scans can be extremely slow

scan initiated 2.53 as: nmap -sU -P0 -F -v -oN scan2udp 10.10.30.1-6

Interesting ports on svr2.ext.dm.com (10.10.30.2):
Port State Service
53/udp open domain
123/udp open ntp

Interesting ports on svr6.ext.dm.com (10.10.30.6):
Port State Service
53/udp open domain

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3 from the Internet towards addresses on the PIX dmz interface

A TCP SYN stealth port scan and a UDP scan will confirm what services are accessible for selected addresses on 10.10.20.0 Since these are translation addresses for internal hosts we only scanned the translations in use. We also scanned the outside address of the VPN server and the PIX. One example is shown below. **We should expect to see no services on any of the addresses we scanned for udp or tcp.** Syslog output from the screening router confirmed that udp was being blocked at the screening router.

```
nmap -sS -v -F -P0 -oN scan3atcp 10.10.20.1
nmap -sS -v -F -P0 -oN scan3btcp 10.10.20.31-35
nmap -sS -v -F -P0 -oN scan3ctcp 10.10.20.42-44
nmap -sS -v -F -P0 -oN scan3ctcp 10.10.20.250-254

nmap -sU -v -F -P0 -oN scan3audp 10.10.20.1
nmap -sU -v -F -P0 -oN scan3budp 10.10.20.31-35
nmap -sU -v -F -P0 -oN scan3cudp 10.10.20.42-44
nmap -sU -v -F -P0 -oN scan3cudp 10.10.20.250.254
```

4) from the DMZ towards addresses on the PIX dmz interface

This is a repeat of test 3 except the nmap host is located on the DMZ. The results duplicated test 3. This test was done to be sure that there was no advantage to using the DMZ network to attack the internal networks. We also added scans for hosts on our internal networks at this point. **We should expect to see no services on any of the addresses we scanned for udp or tcp.**

```
nmap -sS -v -F -P0 -oN scan4atcp 10.10.20.1
nmap -sS -v -F -P0 -oN scan4btcp 10.10.20.31-35
nmap -sS -v -F -P0 -oN scan4ctcp 10.10.20.42-44
nmap -sS -v -F -P0 -oN scan3dtcp 10.10.20.250-254
nmap -sS -v -F -P0 -oN scan4etcp 192.168.10.1-2
nmap -sS -v -F -P0 -oN scan4ftcp 192.168.20.1-2
nmap -sS -v -F -P0 -oN scan4gtcp 192.168.30.*
nmap -sS -v -F -P0 -oN scan4htcp 192.168.40.*

nmap -sU -v -F -P0 –oN scan4audp 10.10.20.1
nmap -sU -v -F -P0 -oN scan4budp 10.10.20.31-35
nmap -sU -v -F -P0 -oN scan4cudp 10.10.20.42-44
nmap -sU -v -F -P0 -oN scan4dudp 10.10.20.250.254
nmap -sU -v -F -P0 -oN scan4eudp 192.168.10.1-2
nmap -sU -v -F -P0 -oN scan4fudp 192.168.20.1-2
nmap -sU -v -F -P0 -oN scan4gudp 192.168.30.*
nmap -sU -v -F -P0 -oN scan4hudp 192.168.40.*
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5) from the DMZ towards hosts on our service network 10.10.30.0

This is a repeat of test 2 except the nmap host is located on the DMZ. The results duplicated test 2. This test was done to be sure that there was no advantage to using the DMZ network to attack hosts on the service network. **We should expect to see no deviation from test 2.**

```
nmap -sS -v -F -P0 -oN scan5tcp 10.10.30.1-6
nmap -sU -v -F -P0 -oN scan5udp 10.10.30.1-6
```

6) from the service network to internal addresses

With the nmap host located on the service network we scanned internal networks. We found no services with udp or tcp. We limited our scan of network 192.168.10.0 and 192.168.20.0 to the addresses that are in use. **We should expect to see no services on any of the addresses we scanned for udp or tcp.**

```
nmap -sS -v -F -P0 -oN scan6atcp 192.168.10.1-2
nmap -sS -v -F -P0 -oN scan6btcp 192.168.20.1-2
nmap -sS -v -F -P0 -oN scan6ctcp 192.168.30.*
nmap -sS -v -F -P0 -oN scan6dtcp 192.168.40.*

nmap -sU -v -F -P0 -oN scan6audp 192.168.10.1-2
nmap -sU -v -F -P0 -oN scan6budp 192.168.20.1-2
nmap -sU -v -F -P0 -oN scan6cudp 192.168.30.*
nmap -sU -v -F -P0 -oN scan6dudp 192.168.40.*
```

Tests from the service network were also repeated assuming the address of the mail server, the web server and the dns server to confirm that only the appropriate host pairs could communicate on the necessary ports for smtp, dns and http. This was confirmed.

Internal Firewall Validation

1. From the network at the branch office to the blue and green network
2. From the network at the business partner office to the blue and green network
3. From a VPN client connection to the blue and green network
4. From the green network to the blue network
5. Check the services on internal router/firewall interfaces

1) From Branch Office towards blue and green network

Hosts in the branch office have unrestricted access to servers in the green network only. Hosts in the branch office can use http to the Internet including our DMZ. Assuming an unused address from the branch office network we ran the following scans. Scans for both udp and tcp were used, only the nmap command for tcp is shown.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan8 192.168.10.1-2
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan6 192.168.20.1-2
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan5 192.168.30.*
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan7 10.10.20.*
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan7 10.10.30.1-6

We should expect to see no services on any of the addresses we scanned for udp or tcp except for port 80 on server 10.10.30.3

2) From our business partners network towards the blue and green network

In general, hosts in the business partners network have access only to the internal web server in the green network. Assuming an unused address from the business partners network we ran the following scans. Scans for both udp and tcp were used, only the nmap command for tcp is shown.

scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan8 192.168.10.1-2
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan6 192.168.20.1-2
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan5 192.168.30.*
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan5 192.168.40.*
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan5 10.10.20.*
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan5 10.10.30.1-6

We should expect to see no services on any of the addresses we scanned for udp or tcp except for port 80 on server 192.168.40.5

2a) added later

Additional access is permitted for the ftp and mail servers. For theses we were able to temporarily assume the IP address for the mail server and the ftp server. Obviously these servers had to be offline during testing. We repeated the scans above and observed that the ftp and mail servers could only see the appropriate services on our internal ftp and mail servers.

2b) added later

Hosts in the business partners network are not allowed to access the Internet via our network. By default, routing on the originating network would prevent this however we wanted to be sure. For this test we connected our NAMP host on the same network as the VPN server and configured our default gateway to point to VPN. This ensures that all of our packets go to the VPN. We then used a TCP SYN stealth scan and a udp scan to a range of address/ports on our business partners registered **external** network addresses. No services were seen. We confirmed that packets were being blocked at the internal firewall by checking the syslog.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3) From a VPN client session towards the blue and green network

scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan8 192.168.10.1-2
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan6 192.168.20.1-2
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan5 192.168.30.*
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan5 192.168.40.*
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan5 10.10.20.*
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan5 10.10.30.1-6

From a VPN client session the only connection allowed is to the winframe server. We expect to see a connection only to the winframe server on port xxx. We used a simple windows tcp scanner (Superscan) for this.

4) From the green network towards our blue network

Workstations and servers on the green network our not supposed to access hosts on networks 192.168.30.0. It was also noted that hosts on the green network should not have access to networks 192.168.10.0, 192.168.20.0 and 10.10.20.0 Workstations on the green network are permitted to use HTTP to the Internet, including our DMZ.

scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan8 192.168.10.1-2
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan6 192.168.20.1-2
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan5 192.168.30.*
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan7 10.10.20.*
scan initiated 2.53 as: nmap -sS -v –F -P0 -oN scan7 10.10.30.1-6
no services were found on any hosts for these scans except for port 80 on 10.10.30.3

scan initiated 2.53 as: nmap -sU -P0 –F-v -oN scan12 192.168.10.1-2
scan initiated 2.53 as: nmap -sU -P0 –F-v -oN scan10 192.168.20.1-2
scan initiated 2.53 as: nmap -sU -P0 –F-v -oN scan9 192.168.30.*
scan initiated 2.53 as: nmap -sU -P0 –F-v -oN scan11 10.10.20.*
scan initiated 2.53 as: nmap -sU -P0 –F-v -oN scan11 10.10.30.1-6
no services were found on any hosts for these scans

5) Check the services on internal router/firewall interfaces

This is not intended to test firewall rules. For each router the PIX firewall and the Nortel VPN server I performed a TCP and UDP scan from the internal network to verify what services are available on each. There are only two hosts that should be able to use telnet, snmp or http for management purposes. The nmap host was located on the blue network so no firewall rules would block any protocols. This ensures that all packets from the nmap host reach the routers, PIX firewall and VPN server. The IP address of

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the nmap host **was not** one which is allowed http snmp or telnet access. We expect to see no UDP or TCP services available.

Services on Screening router

Nmap (V. nmap) scan initiated 2.53 as: nmap -sS -P0 -F-v -oN screen 10.10.20.250
All 64000 scanned ports on (10.10.20.250) are: closed

Services on External Firewall
Nmap (V. nmap) scan initiated 2.53 as: nmap -sS -v -P0 -F-oN pix 192.168.20.1
Interesting ports on (192.168.20.1):
(The 63998 ports scanned but not shown below are in state: closed)
Port State Service
23/tcp open telnet
1467/tcp open csdmbase
Telnet access should be restricted
Csdmbase is unknown, follow up with Cisco TAC

Services on Internal Firewall

Nmap (V. nmap) scan initiated 2.53 as: nmap -sS -v -P0 -F-oN npp01 192.168.30.250
Interesting ports on (192.168.30.250):
All 64000 scanned ports on (192.168.30.250) are: closed

Services on VPN server

Nmap (V. nmap) scan initiated 2.53 as: nmap -sS -P0 –F-n -oN VPNin 192.168.10.1
Interesting ports on (192.168.10.1):
(The 63999 ports scanned but not shown below are in state: filtered)
Port State Service
80/tcp open http
HTTP management of this device should be restricted.

DNS

Our example has used a split DNS to hide all reference to our internal IP address and hostnames. The only records on our external DNS are for host names that must be resolved externally. We have limited our records to the following

SOA svr2.ext.dm.com
NS svr2.ext.dm.com
NS svr6.ext.dm.com
MX svr4.ext.dm.com
Svr1 A 10.10.30.1
Svr2 A 10.10.30.2
Svr3 A 10.10.30.3
Svr4 A 10.10.30.4
Svr6 A 10.10.30.6
www CNAME svr3

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

To confirm that zone transfers were not possible on the external DNS I used nslookup which uses TCP. From outside our network I was unable to successfully issue the **ls –d *zone_name*** command which would transfer all records for the domain.

Observations and Recommendations

Overall, the perimeter of this network has been well secured however there are a few items for consideration.

Telnet Access to the PIX

From the TCP scan, telnet appears to be available on the PIX firewall. Further investigation found that telnet sessions are restricted to the management station IP address specified in the PIX configuration. The following command restricts telnet access from host 192.168.30.5 only.

telnet 192.168.30.5 255.255.255.255

The PIX logged the following violation when we attempted to telnet from an unauthorised source
%PIX-3-307001: Denied Telnet login session from 192.168.30.65<010>

HTTP Management on the Nortel VPN server.

The Nortel VPN server appears to be accessible via http from any station. We confirmed that a host not otherwise prevented by firewall rules could access the http management. Currently hosts on the xtranet can use http to access the HTTP interface on the Nortel VPN server. We did not find any way to configure the Nortel Contivity (V02_51.07) to limit http connections from a specific host. We have asked the client to open a ticket with Nortel regarding this issue. As a work around, we advised that for each VPN group on the Nortel VPN server, filters should be configured so that none of the VPN networks/clients can access the HTTP port. HTTP access to the server is protected by a username and password, which we have been advised is sufficiently cryptic. The 3640 firewall does prevent access to the VPN server management from the internal networks.

Authentication on the Cisco routers and PIX firewall.

Cisco IOS and Cisco PIX can be configured to use radius authentication. We advised that the firewall and the routers in the network be configured to use the existing SecureID server for authentication.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Outgoing protocol restrictions

The analysts on the blue secure network only a few tcp protocols for internet use and no udp protocols. We recommend that only the required outgoing tcp protocols be permitted to the Internet and that udp is blocked. Incoming udp is blocked at the screening router already except as required for DNS and NTP.

The service network has no restrictions on outgoing protocols. Since very few or no protocols are required to start outgoing connections from servers on the service network, the majority of protocols should be blocked.

Available services on the servers connected to the service network

The servers on the service network are NT and have many tcp and udp ports open. Serious consideration should be given to the necessity of these ports/services. While the firewall blocks all but the required protocols, unnecessary services should still be disabled in case someone manages to gain access to the service network.

Screening Router Configuration

The screening router is fairly well secured however additional measures can be taken to prevent denial of service attacks. Follow the recommendations from the SANS institute.
http://www.sans.org/dosstep/index.htm
http://www.sans.org/ddos_roadmap.htm

Software Vulnerabilities

The software Version 4.4 (5) on the Cisco PIX Firewall has a known vulnerability.
http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-pub.shtml

The Cisco Secure PIX firewall feature "mailguard," which limits SMTP commands to a specified minimum set of commands, can be bypassed. We recommend that the Cisco PIX software is upgraded to Version 4.4 (7) as soon as possible.

The software Version IOS 12.0 (5) on the screening router and 12.0 (4) on the Internal firewall has a known vulnerability.
http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml

A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled and browsing to "`http://<router-ip>/%%`" is attempted. We recommend that the IOS software on the screening router be upgraded to 12.0 (12) as soon as possible. A patch for IOS 3640 IP/FW may not available yet. Cisco recommends the following workaround

disable the HTTP server using the command **no ip http server**

Limit http access to the router from the management station with an access-list i.e.
access-list 1 permit *10.1.2.3 where 10.1.2.3 is the address of the management station*
ip http access-class 1 *where 1 is the access-list*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Visa 10 Commandments

We were asked to rate the company's compliance with the Visa 10 commandments. To do this we obtained permission from management to

- review the Corporate Security Policy
- review position descriptions as necessary
- conduct interviews with staff as necessary
- look at server configurations with the assistance of an administrator
- attempt to break passwords on one or more servers

1) Our assessment of the perimeter defence concluded that the requirement to install and maintain a working network firewall to protect data accessible via the Internet, was met.

2) As stated in the network security policy, O/S and application patches are to be kept current. According to the position description, it is the responsibility of the senior network administrator to ensure this task is done. We observed that this individual subscribes to appropriate security mailing lists and a log is kept for each server. If patches are not applied for any reason this is also documented in the logs.

3) As stated in the network security policy, no corporate data is stored where it may be accessible from the Internet. The external FTP server is used on occasion but never for confidential data. There is no anonymous ftp and only a few analysts have accounts. We have advised that they re-evaluate the need for this ftp server and remove it if at all possible.

4) All data between the Corporate LAN and branch office, business partners and remote users, is encrypted. IPSEC is used to authenticate and encrypt with triple DES encryption. The screening router rules allow only IP protocol 50 and UDP port 500 in/out of the VPN server to the internet.

5) As stated in the network security policy, anti-virus software is used and updated regularly. According to the position description it is the responsibility of the senior network administrator to ensure this task is done. We found that virus updates are received regularly and made available on the network. Every ½ hour each workstation and server will check to see if the virus signature file has changed and will update the local file as required.

6) As stated in the network security policy, access to confidential data is restricted on a need to know basis. We observed that confidential data is kept on servers that are located in the high security network. Access to this network is limited by the internal firewall. We also observed that file and directory permissions were well organised with few accounts. Only a few analysts with security clearance had access to this data at the server level.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7) As stated in the network security policy, all persons shall have a unique ID. Under no circumstances are IDs (accounts) to be shared. We were able to verify that there were enough active accounts for each employee to have a unique ID. Interviews with a number of employees seemed to substantiate this requirement.

8) As stated in the network security policy, access to confidential data is tracked by user ID. We observed that for the servers with confidential data, the NT audit log was fully enabled. There is a procedure in place to back up the log files daily so it is possible to audit the previous years activity. The remaining servers did not log the same level of activity and these logs were not backed up.

9) As stated in the network security policy, vendor-supplied defaults for system passwords and other security parameters are not to be used. In an interview with the senior network administrator we determined that not only are default passwords not used, but that administrative passwords exceed the minimum password requirements set on the servers. In general administrator passwords were said to have a minimum of 10 characters, upper and lower case, one special character and must contain no apparent words. We ran LOPHT crack against the password file on the primary domain controller in the secure network. The password attack found no passwords and the brute force attack did not find any passwords after several hours.

10) As stated in the network security policy, security systems and processes are to be regularly tested. This external audit was the first thorough security audit. It is the intention of management to have in house staff competently trained to perform internal audits on a regular basis. Throughout this audit the senior network administrator was to observe and learn the skills required to carry on this work. Management is committed to provide money for the training that will be required to maintain a secure environment.

As a result of our audit we felt that at this time, this company had achieved the VISA Ten commandments. However, many of these are a matter of practice and policy. It is difficult to determine how well this or any company will measure up once the auditor has completed his report and left the premises. A change in staff or management and this status could rapidly break down. Security has to be a Corporate Mindset in order for it to have a lasting effect.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

WWW Links effective Oct 6, 2000-10-06

Cisco Documentation

PIX firewall vulnerability, public release 2000 October 5
http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-pub.shtml

Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks
http://www.cisco.com/warp/public/707/newsflash.html

Improving Security on Cisco Routers
http://www.cisco.com/warp/public/707/21.html

Internet Security Advisories
http://www.cisco.com/warp/public/707/advisory.html

Security Products Field Notices
http://www.cisco.com/warp/public/770/52.html

Cisco IOS Field Notices
http://www.cisco.com/warp/public/770/45.html

Configuration Guide for the PIX Firewall Version 4.4
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v44/pix44cfg/index.htm

Cisco CBAC explained
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt3/sccbac.htm#3974

Configuring Cisco Access Control Lists
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scacls.htm

Nortel

Nortel Contiviy VPN Documentation
http://www12.nortelnetworks.com/cgi-bin/cnss/library/liLibrary.jsp

Tools

SuperScan a windows gui port scanner
http://www.tlsecurity.net/windows/portscanner/superscan.htm

WS_Ping ProPack 2.3
http://www.ipswitch.com/Products/WS_Ping/index.html

nmap
http://www.insecure.org/nmap/

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Kiwi's Syslog Daemon Version 6.2.1
http://www.kiwi-enterprises.com/

L0phtCrack 2.52 for Win95/NT
http://www.l0pht.com/l0phtcrack/

Security Links

ICSA
http://www.icsa.net/

SANS Institute
http://www.sans.org/newlook/home.htm

CERT (Computer Emergency Response Team) Co-ordination Center
http://www.cert.org

CANCERT
http://www.gov.ab.ca/internal/security/

References

Chapman & Zwicky ; Building Internet Firewalls. O'Reilly Publishing 1995

Albitz & Liu ; DNS and Bind. O'Reilly Publishing 1997

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.