Global Information Assurance Certification Paper

GIAC Firewall and Perimeter Practical
Antoinette Binning

The following is a tutorial on how to eliminate the SANS ten most critical internet security threats on your perimeter defense. SANS recommends blocking these ports at a minimum. A better solution would be to block all unused ports. The instructions below are based on a Cisco 4500 series router running IOS 11.2 and a Checkpoint Firewall-1 version 4.0 service pack 7. The architecture for this tutorial is as follows. The internet router has two interfaces. The serial interface connects the router to the internet while the ethernet interface connects to the switch. Also connected to the switch is a firewall. The firewall has two more connections, one to the screened network (sometimes called the dmz) and another to an internal/private company network.

Internet ---Router----Switch---Firewall ---Company/Private Network
|
Screened Network

The first item on the list is to block spoofed packets from entering your network. These are the packets that will have the source address of your network or any private address including the 127 network. These packets should not be trying to enter your network. If they are it could mean someone is trying to exploit trust relationship between two machines in order to gain sensitive information such as the password file. Any application that uses the IP address as the basis of authentication could be in jeopardy. We will install this filter on the router. It is called an ingress filter. It is helpful in protecting against distributed denial of service attacks, ddos. For more information check out www.sans.org/dosstep/index.htm. Type the following:

access-list 20 deny 192.168.0.0 0.0.255.255
access-list 20 deny 172.16.0.0 0.15.255.255
access-list 20 deny 10.0.0.0 0.255.255.255
access-list 20 deny 127.0.0.0 0.255.255.255
access-list 20 deny <your internal network> <your network mask>
access-list 20 permit any

The first four statements in this filter are denying traffic with the source IP address of private addresses. The fifth statement is denying traffic from your company network. This filter will be applied to serial 0, as traffic is coming in to the router. You will first want to create all your access-list 20 statements than apply the statements as a group to the serial interface. The last statement permits any is because the default configuration of a router will be to allow all packets. As soon as you apply a filter, the router will now implicitly deny all unless told otherwise. Be careful not to get locked out of your router.

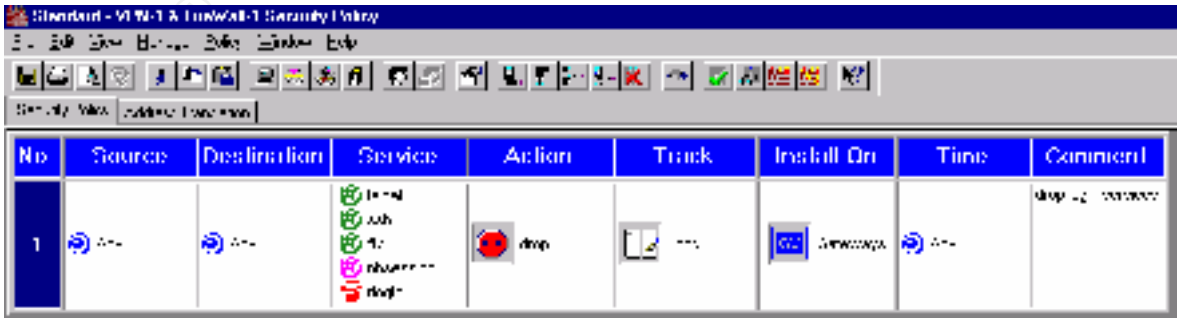
We are not yet finished with the first recommendation. We also need to block all source routed packets. A source routed packet is an IP option that allows the originator of the packet to specify what path the packet should take along with its return route. Source routing provides an avenue for a spoofed attack and will aid in emulating a trusted host relationship. The target host will

think it is taking to the trusted host but it is actually talking to an entirely different machine. Source routed packets can also by pass the firewall or other intrusion detection systems. This filter will be install on the router. This is a global command so you do not need to specify an interface or a direction, just type: no ip source-route .Now the router will drop any packet attempting to enter the network with the source address equal to an address that is part of the destination network.

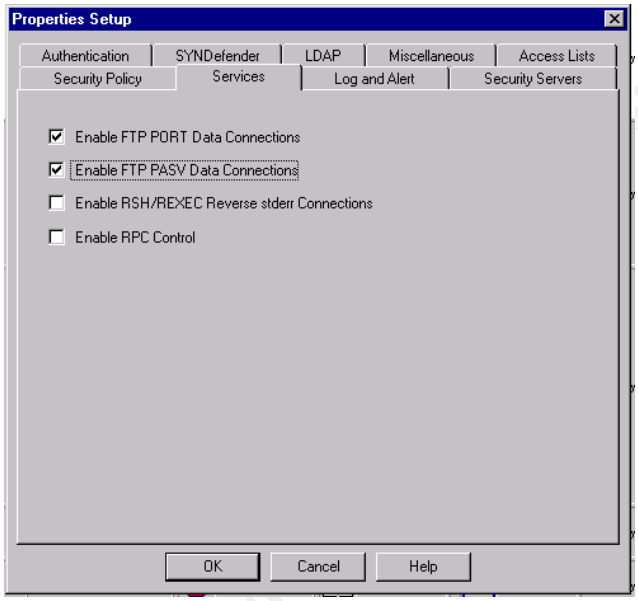
To test this rule put a sniffer on the switch (you will need to configure the switch for port mirroring) and see if any of these packets are getting through.

The second item on the list is to drop the following login services from entering your network, telnet, ssh, ftp, netbios and rlogin. Here are some reasons why. Both telnet and ftp transmit passwords in the clear. Telnet is useful in probing for the presence of various servers. It has numerous exploits ranging from gaining root access to denial of service attacks. Ftp is often abused to gain access to remote systems or store illegal files. Some ftp servers allow the user to transverse the entire directory structure or may have world writeable directories. NetBIOS is easily hacked and it too has many exploits. Rlogin is similar to telnet, though it may not require a password. If it is not properly configured, it will permit unauthorized access to accounts and commands. SSH is similar to telnet and rlogin but provides strong authentication. You shouldn't offer these services to the internet. If you have a business need send the traffic through an encrypted tunnel. For more information about exploits of these services, check out cve.mitre.org.

We will install this filter on the Checkpoint firewall. Checkpoint allows to you to configure which direction to apply the rules. For the purpose of the tutorial, the direction will always be inbound, in other words traffic coming from the router. The source for our filter is any. The destination is any and the services are the login services mentioned above. The action we want the firewall to take when it sees any of these services is to drop the packets. We will track these events long. Checkpoint has several methods of tracking to choose from. For the purpose here, I will always select long. I find long gives me the right amount of information. You can choose whichever tracking method you prefer or whichever is required by your security policy. The Rlogin service you see below is a group I created that includes the following resources: exec 512/tcp, login 513/tcp and shell 514/tcp. Creating a group is not necessary, you could just list each service individually. Nbsession is netbios port 139. Checkpoint has already created this service. The install on column enables you to specify more than one firewall and time allows to specify a time range for a rule. We only have one firewall and time will always be any.



A word of caution, if your webmaster needs to ftp files to your web server you will need a rule that allows this and it needs to be placed before the above mentioned rule. Also the default setting of the Checkpoint firewall allows for both the ftp data connection and passive ftp with only checks to a box. You will need to uncheck both options in the default properties page if you are not offering ftp services. The default properties page, otherwise know as rule zero, can be found under the properties option in the policy menu. Please note if you allow passive ftp it will not be logged.

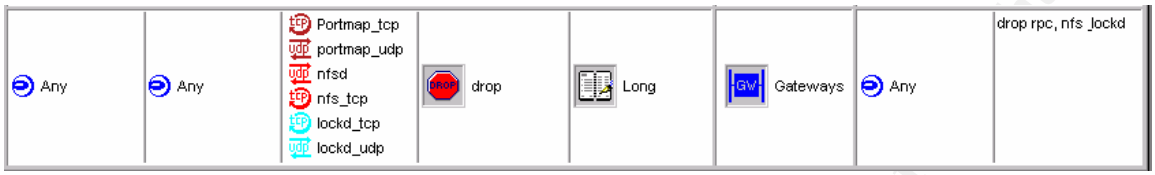


To confirm this rule is working and installed properly, try to ftp or telnet to a machine on the screened network or private company network from a connection outside the firewall. You could also use a port scanner such as nmap.

On to item three, block RPC portmap/rpcbind, NFS and lockd. RPC is difficult protocol to filter because the ports are randomly assigned at startup. The portmapper service maps rpc services to the assigned service numbers. Portmapper and rcpbind are the same thing just different names. NFS, network file system, is also a protocol. It allows a computer to access files over a network as if they were on its local disks. It is based on a trust model of network machines. The basis for allowing information exchange is the looking up the address of the accessing machine. This is how the system is most commonly exploited. Someone will impersonate a trusted host to obtain its rights to the file system. Lockd is a nfs process. Distributed file systems are historically vulnerable. RPC services can be easily fooled into allowing attackers to mount a remote file system. If you need it, use an encrypted tunnel. To get more information on these exploits, please check www.cert.org and cve.mitre.org.

This filter will be placed on the Checkpoint firewall. The source and destination are any. Create the rpc portmap service one for tcp the other udp. Nfsd is there by default. Be sure to check the

port number has not been changed. Create nfs_tcp and both the lockd services. Checkpoint allows you to create your own services. Try to use intuitive names so that the policy does not appear too complex. We are going to drop these services and track it long. I include a description of each rule. It helps explain what is going on.

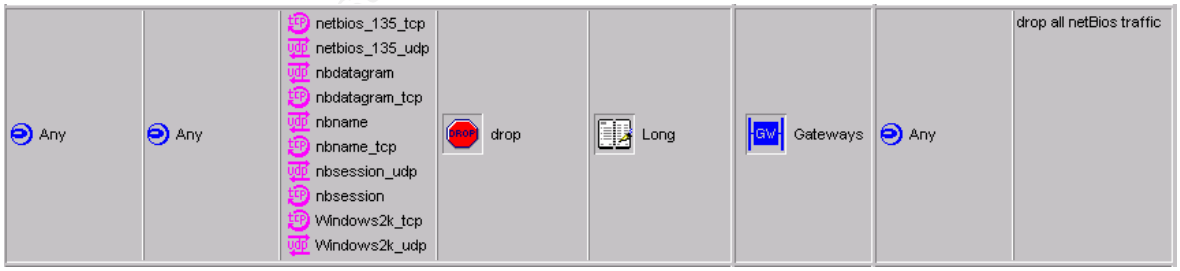


Word of caution, check the policy properties or the zero rule. Confirm the RSH/REXE reverse stederr connections and enable rpc control are not checked. These items will not be logged if they are allowed through the firewall.

If you would like to test this rule you can use Network Associate's Cyber Cop scanner.

Moving on to item number four. This recommendation is to block Windows NT netbios ports in addition to Windows 2000 port 445. Nearly everything pertaining to Microsoft networking occurs over netbios ports 135-139. It even provides supports for the older LAN manager authentication protocol. The Microsoft one account, one login environment is based on trust relationships. Many viruses are written to exploit these trusts. Netbios is easily hacked and has many exploits. If you need it, use an encrypted IP tunnel to connect LANs over the internet.

This filter will be created on the Checkpoint firewall. Source and destination will be any. I had to create a lot of the netbios services for this rule. I also confirmed any of the services already in the firewall had the correct port number and udp or tcp setting. All netbios traffic will be dropped and tracked long. Again I like to write comments about each of my rules, so that anyone looking at my company's firewall will be able to tell what is going on .



Another way to create this rule is to create a group. I called it NetBios_Win2k. You can call it whatever you like just try to keep it simple. I placed all the services you see in the example above in this group. To me this appears neater. Others prefer not to use groups so they can easily see what services are being targeted. This is just a personal preference.

There are few tools that will allow you to test this rule. One is l0pht (that is a zero not an o) crack. It will attempt to get username and passwords. The other tool called dump acl will attempt to enumerate Windows NT shares. Nmap, the port scanner will also work. Remember you need to test this from outside the firewall.

X-Windows is the next item on the list. X-Windows has been known to leak information from its displays including keystrokes. X-clients can kill windows, capture windows and display them elsewhere, capture the keystrokes of console user and even re-map the keyboard. It has week access control. Access control is determined by IP address. Check with your vendor for more information on the security concerns of X-Windows.

This filter will also be applied to the Checkpoint firewall. The source and destination are any. I had to create X-Windows service. The action will be drop and track long. I also include comments about what this rule does.

There is a tool called x-scan that will search an entire subnet looking for open x-server and log all keystrokes to a file. This would be a good test of this rule.

The next item number five on the SANS top ten list has a few parts. First we need to block dns queries to all machines that are not dns servers. Next we need to block zone transfers from all machines but our external secondary dns server and the last thing in this section is block ldap. The external dns server contains the names and IP addresses of all the services your company advertises on the internet, i.e. web servers. There are many well-known exploits of BIND, so you will need to check the version you are running. SANS reports that according to a mid-1999 survey, about 50% of all DNS servers connected to the internet are running a vulnerable version of BIND. The next item on our DNS to-do-list is to configure the external DNS server to only allow zone transfers from the secondary dns server. A zone transfer is a quick method of mapping an organizations network structure. This is usually the first sign of an attack. We will block zone transfers from the firewall but you can also configure this setting on the server itself. Check the documentation of the dns server software to find out more information. Some of the dns attacks are impersonation, man-in-the-middle, feed false information and being redirected elsewhere or to a black hole.

LDAP, light directory access protocol or if your are Microsoft you call it AD, active directory. It is a common way to implement a centralized account management system. It can be used by a single network, host or as an application login method. Active directory will contain more than just user account information. It will contain a logical representation of all the objects relevant to a company's infrastructure. Unfortunately this information can be leaked on to the internet and could provide the public valuable clues to the nature of your network and its users. If you need LDAP, consider a split implementation with only a limited set of information available publicly.

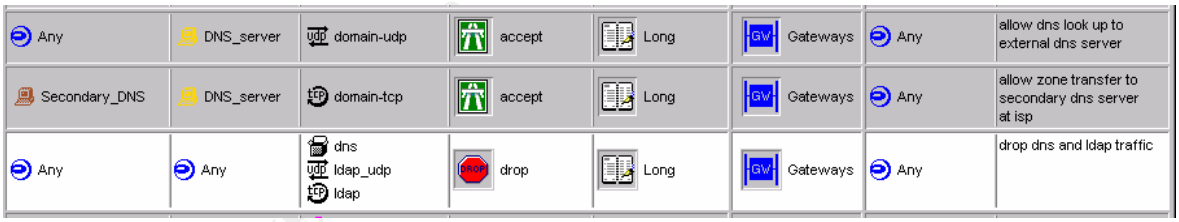
This filter will be installed on the Checkpoint firewall. The first thing we will do is allow dns queries to our external dns server. The source will be any and the destination is the dns server.

The service is domain-udp requests. We will accept this traffic. We will track it long and include information about the rule in the comment field.

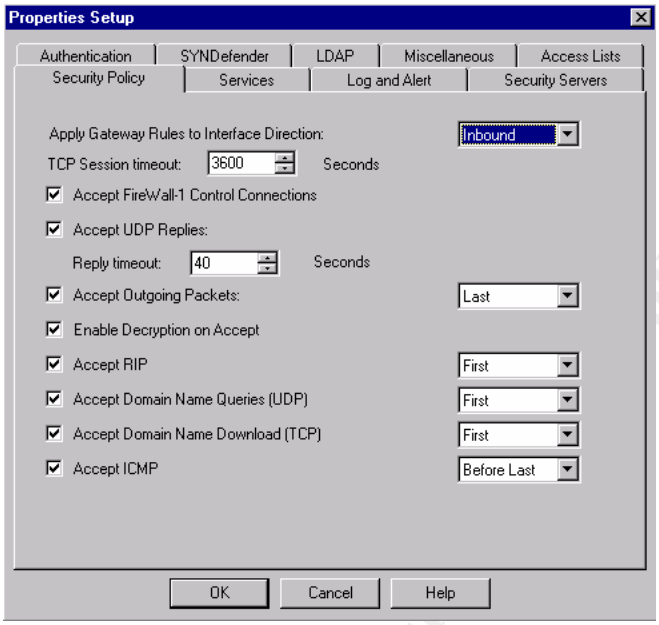
Next we need to allow zone transfers from the secondary dns server. It is common to have your internet service provider host your secondary dns server. The source for this rule will be the secondary dns server, the destination is the primary external dns server and the service is domain-tcp. We will allow this traffic and track it long.

Now we need to block all other dns traffic and ldap. The source and destination will be any. The dns service group and ldap_tcp were already created, just confirm on your Checkpoint box that the services and port numbers are correct. Create the ldap_udp service. Add the dns group, ldap and ldap_udp to the service box. The action will be drop and we will track it long. Add a description of the rule in the comment field.

Here is where firewall rule order can make a difference. This rule needs to go after the two rules we just created.



Just when you think you have everything covered in reference to dns. There is one more thing you need to do. Check the zero rule. The default settings for the Checkpoint firewall will allow for both udp domain queries and zone transfers before it will even look at the rules we have created. This is what *first* means on this screen. (See below.) Uncheck Accept Domain Name Queries and Accept Domain Name Download. Please note if these services are enabled, they will not be logged.



To confirm you have configured your filters correctly, try to do a zone transfer from outside your firewall. Type ls –d companydomain.com. Try to lookup a machine in your screened network or inside the company network. You can use nslookup or dig or sam spade.

Moving on the next item on the list. We need to drop all SMTP traffic to machines that are not an external mail relay along with dropping POP and IMAP services. SMTP will accept mail without checking authority or the identity of the sender. This leaves the server open to spam attacks and email flooding. The catch is if we want to receive internet mail we need to support SMTP. A client will use either POP or IMAP to connect to the mail server to retrieve their mail. This can be done over either the LAN or the internet. POP does not encrypt usernames or passwords, making these easy targets for packet sniffing. IMAP is more complex than POP and more secure. Passwords are not sent in the clear and mail can be retained on the mail server instead of being transferred to the client. In 1997 a CERT advisory was issued about some versions of the University of Washington's implementation of both POP and IMAP. The advisory warned of the possibility of remote users obtaining unauthorized root access with out access to an account on the system. The advisory recommended installing a patch or upgrading to the latest version of the product, that goes for any application on your network. Confirm there are no known security issues by checking with the vendor, CERT or bugtraq. Many sites have mail lists you can subscribe to for security updates. www.sans.org, has a great list of vendor related security mailing lists. It you need POP or IMAP be sure to limit its use to inside your company's network. If it must be offered through the internet use an encrypted tunnel. Also be certain to scan for viruses in mail attachments.

This filter is on the Checkpoint firewall. Source and destination are any. The service is SMTP, POP-2 (109/ tcp), POP-3 (110/tcp) and IMAP. The action is drop and we are tracking it long. The comment field describes what this rule does.

Any	Any	smtp pop-2 pop-3 imap	drop	Long	Gateways	Any	drop smtp, pop and imap traffic

The problem with the rule we just created is that it will prevent the mail server from getting mail. You will need a rule that allows any source to talk to the mail server via the SMTP service. We will track it long. This rule needs to be placed before the first rule we just created.

Any	mail_server	smtp	accept	Long	Gateways	Any	allow internet mail to mail server
Any	Any	smtp pop-2 pop-3 imap	drop	Long	Gateways	Any	drop smtp, pop and imap traffic

You will also need a rule that enables your users to retrieve their mail securely. This rule will depend on your network setup and security policy. The rule will need to be placed before the other two mail rules we just created.

To test this rule try to telnet to port 25 on your mail server or use a port scanner.

The next services on the blocking list are HTTP and SSL to all machines except external web servers along with some common high-order HTTP ports, 8000/tcp, 8080/tcp and 8888/tcp. The HTTP protocol transfers text, video, sound, and even programs over internet. The default port is 80. Exploiting this service will entail either having your web server hacked or a web site will contain malicious components such as active-x or java applets. Most web server application security holes are well known. Check with your vendor to confirm your product is secure. SSL, secure socket layer, provides encrypted communication through a web browser. This protocol is open and nonproprietary. It also provides server authentication and message integrity. It is a must in today's e-commerce. There are been CERT advisories in the recent past describing an issue with an internet browser and how it implements security and maintains a secure connection. Check with the vendor of your browser and confirm you have the latest patches. You can also check with CERT to get more information on the advisory.

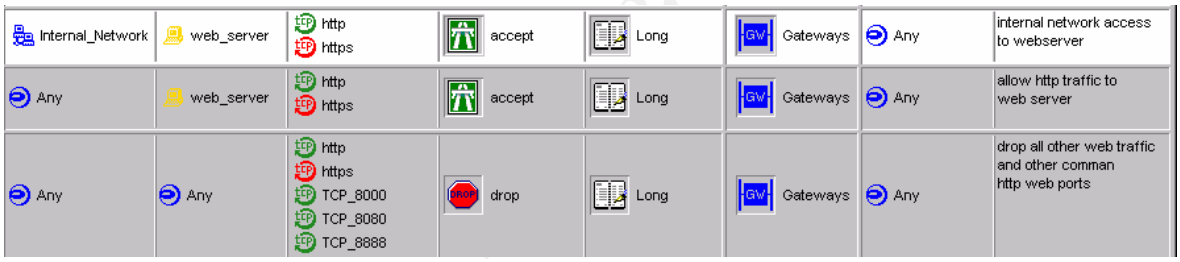
This filter will go on the Checkpoint firewall. Source and destination are any. Http, https and tcp ports 8000, 8080 and 8888. Https is another name for ssl port 443. I had to create the tcp 8000, 8080 and 8888 services. These services will be dropped and the information will be logged long. The comment field describes the rule.

Any	Any	http https TCP_8000 TCP_8080 TCP_8888	drop	Long	Gateways	Any	drop all other web traffic and other comman http web ports

Problem with this rule is if you have a web server no one will be able to reach it. You will need to have a rule that allows anyone to contact the web server using http and https, if you are need to encrypt web traffic. This traffic will be accepted and tracked long. This rule needs to go before the pervious.

Now your internal network can not reach the company's web server. This rule will allow the internal network to connect to the web server via the http and https service. We are going to track it long and describe the rule in the comment field. It needs to be placed before the last two rules created.

Here is a recap of the rule order.



Blocking all small services below port 20 for udp and tcp including the time protocol at port 37 udp/tcp is item number nine. The services we find below port 20 are echo, chargen and the daytime protocol. Echo is a protocol that will transmit back to the client whatever the client sent it. Chargen will continuously send out printable ASCII characters and the time protocols send out date or day and the time. These protocols are useful for debugging, testing networking connectivity and developing network tools. Even so, these protocols should be blocked. Echo and chargen can be used in tandem to flood a server with what is known as a udp bomb or udp packet storm. It is also possible to flood a target with redirected output of chargen data by using forged syn packets. As to the time protocols, there is a known vulnerability with a particular brand of routers. Check with cve.mitre.org for more information.

This filter will be applied to the router. To disable small services, echo, chargen and time type:

no service tcp-small-servers
no service udp-small-servers

These are global commands. You do not need to specify an interface or a direction. Now to disable the time protocol, you will need to first create the extended access list statements such as:

access-list 101 deny tcp any any eq 37
access-list 101 deny udp any any eq 37

An extended access list is used because we need to filter on something other than the source address. In this example it is port number 37. The router knows it is an extended access list by the use of the number 101. The access list range needs to be between 100-199. In this filter we are denying traffic in both of these statements, one denies tcp the other udp. The source and destination for both is any and the port is equal to 37. We will apply the filter to the serial interface as traffic is coming in.

To ensure we have set up this filter correctly, run nmap or any other port scanning utility.

The catchall category, miscellaneous, is our next block. TFTP is the first service we will discuss. This service is used for booting diskless workstations, terminal servers and routers. Hacker tools have been developed to use unprotected TFTP servers as pirated software dumping ground. In addition most routers support TFTP and use it for backing up and restoring configuration files. There is a wealth of information a hacker could obtain if they are able to download your router's configuration file. This is why I am putting this filter on the router. The format for this filter is access-list 101 deny udp any any eq 69 log. This will deny any source to any destination for udp port 69, TFTP and log it. This filter will be applied to the serial interface as traffic is coming in to the router.

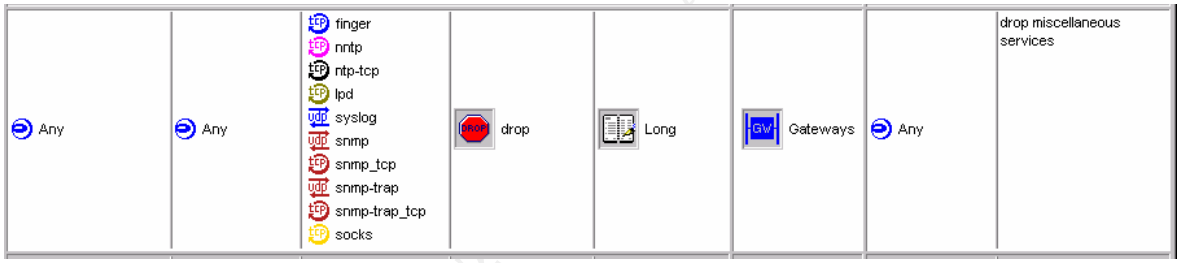
Border Gateway Protocol or BGP, will be another service we will block at the router. The filter is access-list 101 deny tcp any any eq 179. What we are doing here is deny tpc traffic from any source to any destination and port equals 179. We could have just typed bgp instead of the port number. Either will work. Bgp is commonly used on networks that have more than one internet connection. Apply this rule going in to at least the serial interface of your router. Blocking this traffic is a good idea because of the havoc a hacker could do if they got control of the network router and/or its routing table. Routers direct packets based on their routing tables. Often a hacker will isolate parts or your network or direct traffic elsewhere thus creating a denial of service attack.

The remaining services will be blocked using the Checkpoint firewall. Finger was designed to help network users communicate by providing a of system information such as when the last time someone checked their e-mail, a person's office hours, telephone numbers, and current projects. This information is a gold mine for hackers looking for account names and passwords, hence the reason for the block.

NNTP, network news transfer protocol, is used to access and read network news on the internet. I just did a search on www.cert.org and the first item I pulled up describes large scale attacks on NNTP servers. Check this above mentioned web site for more information.

NTP, LDP, syslog, SNMP and socks are all services that should not initiated by the internet nor offered to the internet. The NTP, network time protocol, assures us we are have an accurate local timekeeping with references to radio, atomic or other clocks located on the internet. LPD, line printer daemon, is used for remote printing. If you need to do remote printing, it should be initiated from inside your network. Syslog is a system's logging utility. You will not want a would-be hacker modifying your system logs or using that port to carry out some exploit. SNMP, simple network management protocol is a useful tool to remotely manage network devices such as routers, servers, hub and clients. What makes this protocol a security threat is most administrators leave the default passwords and community string or use easily guessed passwords. Unless you want a hacker to watch every aspect of data flow on your network. Block this protocol at the firewall. Socks is the last of the miscellaneous services we will be blocking here. This protocol is used to proxy allowed traffic out of the network but does not have specific security proxy software. Again, none of these services should be offered to the internet. They could provide a gold mine of information to an attacker.

This filter will be install on the Checkpoint firewall. Source and destination are any. The services we are blocking are finger, nntp, ntp-tcp, ldp, syslog, snmp, snmp_tcp, snmp-trap, snmp-trap_tcp, and socks. I had to create ldp, snmp_tcp, and socks. The action will be drop. Tracking is long.



To confirm the filter is set up correctly, you can again use nmap or a utility called IP network browser found at wwww.solarwinds.net.

Blocking icmp incoming echo requests, outgoing echo replies, time exceeded, and unreachable messages is the final item. These four filters will all be applied to the router. Icmp has no port numbers, no perceived client/server relationship or a reliable delivery guarantee. It is capable of being broadcast. Echo requests and echo replies are otherwise known as ping. Echo requests is one of the most common mapping techniques. It is used for initial reconnaissance. This is why we do not want hosts to reply. The router will response if the host can not. This is why we will turn off unreachable messages. Valuable information can be gleaned from many icmp unreachable messages. Next we will block time exceeded messages. This is a different issue, an issue that has yet to be resolved. Before the change of the millenium a flood of icmp time exceeded messages began popping up everywhere. It appears as if the router's IP addresses were spoofed since the source never sent out the message. We will block this service as a precaution. Icmp is vulnerable to several attacks, smurf attack, tribe flood network and loki. For more information check out www.sans.org.

The first filter will be applied to the serial interface as traffic is coming into the router. Here is what the filter would look like:

Access-list 101 deny icmp any any echo

Again this is an extended access list. We are denying the traffic. The protocol is icmp and echo means echo request. The next series of filters will be applied as a group on the ethernet interface of the router as traffic is coming in.

Access list 102 deny icmp any any echo-reply
Access list 102 deny icmp any any time exceeded
Access list 102 deny icmp any any unreachable

The first filter in this series denies icmp echo-replies from all sources and all destinations. The last two filters will prevent icmp time exceeded and unreachable messages from any source to any destination including the router.

To test this filter try pinging or doing a NT tracert to a host on the screened or private company network

In conclusion, I would like to reiterate that the SANS top ten list is a bare minimum. It would be best to block all unused ports and adopt a default "deny all" security policy. This is a better and more secure approach.

Sources

www.sans.org

cve.mitre.org

www.cert.org

GIAC Firewall and Perimeter Protection course material, July 2000

Firewalls 24 seven by Matthew Strebe, Charles Perkins, Sybex, ISBN:0-7821-2529-8

Hacking Exposed by Stuart McClure, Joel Scambray, George Kurtz, Osborne/McGraw Hill, ISBN:0-07-212127-0

Firewalls, A Complete Guide by Marcus Goncalves, McGraw Hill, 0-07-135639-9