Global Information Assurance Certification Paper

Raffaele Amendola
15 August 2000

GIAC Firewall and Perimeter Protection Practical Assignment

Section 1. Introduction

This paper is a tutorial on one method that can be used to enforce the filtering policy listed in section two of this document. As stated in the description of the practical assignment, this list represents the minimum requirement for perimeter security. A more effective technique for perimeter defense is to deny all ports/services that are not required by your organization's security policy. The perimeter defense solution should also utilize egress as well as ingress filtering. This paper will also provide a brief description of each service and its associated vulnerabilities.

Section 2. Filtering Policy

The following list represents the recommended perimeter defense actions in the SANS "Top Ten" document:

1. Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.
2. Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)
3. RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)
4. NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - earlier ports plus 445(tcp and udp)
5. X Windows -- 6000/tcp through 6255/tcp
6. Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)
7. Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)
8. Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)
9. "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)
10. Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)
11. ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and unreachable messages

Section 3. Perimeter Defense Solution and Filter Syntax

A Cisco router running IOS version 11.3 was used to filter packets in accordance with the filtering policy. Beginning with IOS 11.3, Cisco routers support three different types of access-lists: standard, extended, and reflexive (added in IOS 11.3). Extended access-lists were used for this practical.

Extended access-lists are capable of filtering packets based on: IP source and destination address, protocol, and protocol options. Access-lists are written while in "configuration mode". The following is the basic syntax used in this paper for an extended access-list:

access-list ***access list number*** **deny/permit** ***protocol source source-wildcard destination destination-wildcard (protocol-option)*** **(log)**

Description of the Filter Syntax

access-list	Literal statement
access-list number	For extended access-lists, numbers 100-199 (inclusively) must be used. The configuration parser uses this number to determine how the information in the filter rule should be interpreted.
deny/permit	Specifies what action to take if the packet matches the stated criteria.
protocol	Name or number of protocol
source	Source IP address
source-wildcard	32-bit quantity number in four-part, dotted-decimal format. This number is used to determine what part of the source IP address is used for matching. A "binary 1 bit" in a bit field indicates that the corresponding bit in the IP address is **not** tested for a match. For example, wildcard 255.255.255.255 doesn't care about any of the bits in the IP address. Wildcard 0.0.0.0, however, indicates that all bits in the IP address need to be matched.
destination	Destination IP address
destination-wildcard	Performs the same function as the source-wildcard, with the exception that it corresponds to the destination IP address.
protocol-option	Optional. Allows you to add criteria that is specific to the identified protocol. For example, when using TCP/UDP, an operator such as eq (equal), gt (greater than), range, etc. and then a port or port range can be specified. For ICMP, an example would be the specification of a particular ICMP type.
log	Optional. Enables logging to the system console when a match occurs (regardless of whether the packet was permitted or denied).

Before providing an extended access-list example, here are a few helpful tips that can facilitate the writing of access-lists:

-When specifying the protocol, the keyword "**ip**", can be used to indicate the matching of any Internet protocol.

-When specifying the source and source-wildcard or the destination and destination-wildcard, the keyword "**any**" can be used to represent the address wildcard pair of "0.0.0.0 255.255.255.255".

The keyword "**host**" can be used to represent the address wildcard pair of "IP address 0.0.0.0", where an exact match is required on the specified IP address.

Once the access-lists have been written, they may be assigned to a specific interface. Just as with writing access-lists, applying access-lists to an interface is performed while in configuration mode. In order to apply an access-list to an interface, the following interface configuration command is used,

ip access-group *access-list-number* in/out

Description of Syntax

ip access-group	Literal statement
access-list-number	Represents the number of the access-list being applied to the interface.
in/out	Specifies whether the access-list will be applied to inbound or outbound packets (direction is in relation to the interface).

Example (information between "/* */" are comments):

```
interface Ethernet1  /* External interface*/
 ip address 194.162.12.1 255.255.255.0
 ip access-group 100 in /*access-list 100 is being applied to packets coming into the
                         external interface*/

access-list 100 permit udp any host 194.162.15.2 eq 53 log
```

Explanation:

-"100" indicates that this is an extended access-list

-"permit" indicates that if the packet matches the stated criteria, it will be allowed into the network.

-"udp any host 194.162.15.2 eq 53" indicates all udp packets (from any IP address) destined specifically for 194.162.15.2 (possibly a DNS server) port 53 (DNS expected)

-"log" indicates to make a log entry if the packet matches all stated criteria

Section 3. Filter Implementation

The following router interface configuration was used for this practical:

```
---------------------------
version 11.3
!
hostname fwrouter
!
boot system zzzz-zzzz-zzz.000.T.bin
enable
enable password
!
no ip source-route
no ip finger
!
```

```
!
!
interface Ethernet0 /*Internal router interface*/
 ip address 193.250.89.113 255.255.255.0
!
interface Ethernet1 /*External router interface*/
 ip address 193.250.89.76 255.255.255.0
 ip access-group 101 in
 ip access-group 102 out
---------------------------
```

1. **Block "spoofed" addresses**-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.

The purpose of blocking inbound packets using your internal address, private address, or the loopback address as the source address is to help protect your network from inbound spoofed packets.

Filtering rules:

```
access-list 101 deny   ip 193.250.89.0 0.0.0.255 any log
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any log
```

***193.250.89.0 - Internal network**

Testing: These filter rules can be tested by crafting packets that use the above addresses as the source address and sending the packets to the external interface of the router (traveling inbound). The log option is set in order to view whether or not the packets were blocked at the router.

Source routed packets: Source routing is an IP option that allows an originator to specify the route that a packet must take, thereby preempting normal dynamic routing. There are two types of source routing: strict source routing and loose source routing. Strict source routing dictates the specific path that a packet must traverse between two hosts (up to the first 9 hops). Loose source routing specifies the IP addresses of nodes that the packet must traverse through; however, the packet may also travel through other routers between any two IP addresses on the list.

Possible vulnerabilities: The IP source routing option can be used maliciously. An attacker can send traffic to a victim host with the spoofed IP address of a trusted host (trust relationship exists between the victim host and the trusted host). Normally, the victim host would respond back to the actual trusted host; however, if source routing is used, the attacker can specify the return path from the victim host and exploit the trust relationship.

Filtering rule:

The global configuration command: **no ip source-route** can be used to block source routing.
Global configuration commands are used to specify parameters for the entire system.

Testing: Attempt to send traffic through the router with the source routing IP option enabled (Hex 83 for loose source routing and Hex 89 for strict source routing). One way to determine whether the packets were blocked is to place a sniffer on the opposite side of the router and view the logs.

2. Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)

Telnet: This is a remote access protocol that enables bi-directional communications between a "user" host and a "server" host who both appear to the other to be a network virtual terminal. Once a session is established and a valid user name and password has been submitted, keystrokes entered at the "user" host are sent to the "server" host, and output from the "server" host appear on the screen of the "user" host.

Possible vulnerabilities: Data, including the username and password, are sent in clear text. The information being passed is susceptible to interception and exposure. Telnet is also vulnerable to session hijacking.

Filtering rule:

```
access-list 101 deny   tcp any any eq telnet log
```

Testing: Use an external host to attempt to establish a telnet session with an internal host. The log option is set in order to view whether or not the packets were blocked at the router.

SSH: Secure Shell is intended to be a replacement for the Unix "r" commands (rlogin, rsh, rcp, and rdist). It can be used for remote logons, remote execution of commands, and remote copy. SSH enables authentication and confidentiality through the use of mechanisms such as certificates and encryption algorithms. SSH also enables the forwarding of TCP connections through the encrypted channel.

Possible vulnerabilities: Since the traffic is encrypted, it is difficult for network administrators to monitor what kind of traffic is being sent and received. TCP forwarding can be exploited to send possibly malicious traffic across the channel.

Filtering rule:

```
access-list 101 deny   tcp any any eq 22 log
```

Testing: Use an external host to attempt a connection to port 22 on an internal host. The log option is set in order to view whether or not the packets were blocked at the router.

FTP: The File Transfer Protocol is used to perform file transfers from one system to another system. The user can use either an account with a specific username and password, or if supported, the user name "anonymous", to login to the server.

Possible vulnerabilities: Packet filters may experience difficulty with FTP because it uses two different ports: port 21 as a control channel and port 20 as a data channel. The FTP session may be susceptible to session hijacking and the information, sent in clear text, may be susceptible to sniffing. If the attacker has or gains write access, malicious code can be placed on the server.

Filtering rule:

```
access-list 101 deny   tcp any any eq ftp log
```

Testing: Use an external host to attempt a connection to port 21 on an internal host. The log option is set in order to view whether or not the packets were blocked at the router.

NetBIOS: Covered in part 4 of this section.

rlogin et al: TCP ports 512-514 (exec, login, shell, respectively) are used for logging into systems across the network and executing commands on remote systems.

Possible vulnerabilities: Since data is transmitted in clear text, traffic is susceptible to sniffing. Vulnerable to unauthorized access.

Filtering rule:

```
access-list 101 deny   tcp any any range 512 514 log
```

Testing: Use an external host to attempt a connection to ports 512-514 on an internal host. The log option is set in order to view whether or not the packets were blocked at the router.

3. RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)

Portmap/rpcbind: Portmapper (rpcbind is the name of the portmapper on systems using TI-RPC) is an RPC server program that acts as a registrar that keeps track of which RPC programs are using which ephemeral ports. Servers use RPCs to register themselves with the portmapper. Clients use RPCs in order to query the portmapper.

Possible vulnerabilities: An attacker can use rpcinfo, which is a program that calls PMAPPROC_DUMP, to gather information about which port numbers are being used by

which RPC program. Also, earlier versions of portmapper permitted any program to register itself.

Filtering rules:

```
access-list 101 deny   tcp any any eq sunrpc log
access-list 101 deny   udp any any eq sunrpc log
```

Testing: Use an external host to attempt a connection to TCP port 111 and UDP port 111 on an internal host. The log option is set in order to view whether or not the packets were blocked at the router.

NFS: The Network File System is a client-server application based on Sun RPC. NFS enables clients to access files and file systems on a server. The NFS client is able to access files on an NFS server by transmitting RPC requests to the NFS server.

Possible vulnerabilities: NFS is vulnerable to IP spoofing attacks because it uses IP addresses for access control. It may also be vulnerable to attackers placing malicious programs on the system. Certain versions of NFS that place limits on the access control list may be susceptible to the disabling of access controls when the limit is surpassed.

Filtering rules:

```
access-list 101 deny   tcp any any eq 2049 log
access-list 101 deny   udp any any eq 2049 log
```

Testing: Use an external host to attempt a connection to TCP port 2049 and UDP port 2049 on an internal host. The log option is set in order to view whether or not the packets were blocked at the router.

lockd: Lockd is an RPC program that is used with NFS to handle file lock requests either locally from the kernel or remotely from another lock daemon.

Possible vulnerabilities: Lockd may be susceptible to a remote denial of service attack.

Filtering rules:

```
access-list 101 deny   tcp any any eq 4045 log
access-list 101 deny   udp any any eq 4045 log
```

Testing: Use an external host to attempt a connection to TCP port 4045 and UDP port 4045 on an internal host. The log option is set in order to view whether or not the packets were blocked at the router.

4. NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - earlier ports plus 445(tcp and udp)

NetBIOS: NetBIOS is an application programming interface that uses three types of services: the name service uses port 137 to send UDP broadcast packets; the datagram service uses port 138 to send UDP broadcast or directed broadcasts; and the session service uses port 139 to send TCP segments. The WINS manager uses tcp port 135 and the Common Internet File System (CIFS) uses tcp and udp ports 445. NetBIOS is mainly used in the Microsoft Windows environment. The default NetBIOS setting for Windows 95 and 98 is enabled.

Possible vulnerabilities: An attacker sending spoofed "Name Release" or "Name Conflict" messages to a victim host could force the victim to remove its own name from its name table; this would result in a denial-of-service attack because the victim host would be unable to initiate NetBIOS requests or respond to NetBIOS requests. User name and password traffic on a Windows NT network is vulnerable to sniffers and crackers. Also, the "one account/one login" scheme places multiple resources at risk when one account has been compromised. Trust relationships existing in a Microsoft network are susceptible to exploitation.

Filtering rules:

```
access-list 101 deny   tcp any any eq 135 log
access-list 101 deny   udp any any eq 135 log
access-list 101 deny   udp any any eq netbios-ns log
access-list 101 deny   udp any any eq netbios-dgm log
access-list 101 deny   tcp any any eq 139 log
access-list 101 deny   tcp any any eq 445 log
access-list 101 deny   udp any any eq 445 log
```

Testing: Use an external host to attempt a connection to TCP port 135, UDP port 135, UDP port 137, UDP port 138, TCP port 139, TCP port 445, and UDP port 445 on an internal host. The log option is set in order to view whether or not the packets were blocked at the router.

5. X Windows -- 6000/tcp through 6255/tcp

X Windows: The X Window System is a client-server application that can support multiple virtual user windows on a single display that is managed by a server. In this architecture, the client is an application that runs on either the same host as the server or on a different host. The server is responsible for managing the display, mouse, and keyboard. There are two basic protection functions used in the X Window System: xhost and xauth. Xhost uses specified host IP addresses to restrict which activities are allowed. Xauth provides a similar protection service through the use of a "magic cookie" text string.

Possible vulnerabilities: An attacker may be able to redirect window displays and keyboard and mouse entries in order to execute commands on the victim's host. An attacker may also be able to establish a remote window session in order to execute commands on the victim's host. Certain versions are also vulnerable to buffer overflow attacks.

Filtering rules:

```
access-list 101 deny   tcp any any range 6000 6255 log
```

Testing: Use an external host to attempt a connection to an internal host using TCP ports in the range of 6000-6255. The log option is set in order to view whether or not the packets were blocked at the router.

6. Naming services-- DNS (53/udp) to all machines that are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp).

DNS: The Domain Name System is a distributed database that is used to translate a host name to an IP address as well as an IP Address to a host name. It also provides electronic mail routing information. UDP port 53 is used for DNS queries and replies. TCP port 53 is used for zone transfers and for when the UDP DNS response is greater than 512 bytes.

Possible vulnerabilities: DNS traffic needs to be controlled for several reasons, including: hosts, other than the DNS server, that are running a DNS implementation, such as BIND, may be exploited using vulnerabilities within that particular implementation. If the network administrators are not aware that those services are running on a non-DNS server, then they are unable to maintain and secure that application. This imposes a risk on the entire network, not just the host. DNS may also be vulnerable to cache poisoning. An attacker could a remote DNS server to place erroneous DNS records into the cache of the victim DNS server. Zone transfers must be controlled in order to prevent unauthorized disclosure of the internal network.

Filtering rules:

```
access-list 101 deny   udp any any eq domain log
access-list 101 deny   tcp any any eq domain log
```

This network does not have a local DNS server; however, if, for example, a DNS server (and its secondary) was located on the internal network with an IP address of 202.43.4.1, the following access-lists could be applied:

access-list 101 permit udp any host 202.43.4.1 eq domain log

access-list 101 deny tcp any any eq domain log (this will also block UDP DNS responses greater than 512 bytes, but if there is no other way, it is important that zone transfers are controlled.)

Testing: Use an external host to attempt a connection to an internal host using TCP port 53 and UDP port 53. The log option is set in order to view whether or not the packets were blocked at the router.

LDAP: The Lightweight Directory Access Protocol is a set of protocols used to access the X.500 Directory.

Possible vulnerabilities: Directories implementing LDAP may contain private individual and organizational information. An attacker may attempt to exploit LDAP vulnerabilities that may provide unauthorized access to this information. There is also the concern of denial of service attacks and modification of records.

Filtering rules:

```
access-list 101 deny   tcp any any eq 389 log
access-list 101 deny   udp any any eq 389 log
```

Testing: Use an external host to attempt a connection to an internal host using TCP port 389 and UDP port 389. The log option is set in order to view whether or not the packets were blocked at the router.

7. Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)

SMTP: The Simple Mail Transfer Protocol specifies how two Message Transfer Agents (MTAs) exchange electronic mail over a TCP connection. SMTP uses NVT ASCII.

Possible vulnerabilities: SMTP does not provide confidentiality and authentication. SMTP is therefore vulnerable to sniffing and modification of host and user name. SMTP is also susceptible to denial of service attacks. An attacker may also be able to Telnet to port 25 and execute commands as root.

Filtering rule:

```
access-list 101 deny   tcp any any eq smtp log
```

Testing: Use an external host to attempt a connection to an internal host using TCP port 25. The log option is set in order to view whether or not the packets were blocked at the router.

POP: The Post Office Protocol enables users to download e-mail messages stored on a mail server. POP3 uses TCP port 110. POP2 and older versions use TCP port 109.

Possible vulnerabilities: POP is vulnerable to spoofing and denial of service attacks. Since POP transmits passwords in clear text, an attacker would be able to capture and use this information. POP also does not provide server authentication; therefore, an attacker would be able to transmit data to the client and the client would think this information was originating from the mail server.

Filtering rule:

```
access-list 101 deny   tcp any any eq pop2 log
access-list 101 deny   tcp any any eq pop3 log
```

Testing: Use an external host to attempt a connection to an internal host using TCP ports 109 and 110. The log option is set in order to view whether or not the packets were blocked at the router.

IMAP: The Internet Message Access Protocol enables users to access e-mail messages stored on a mail server. IMAP does support, but not require, authentication mechanisms.

Possible vulnerabilities: IMAP is vulnerable to network sniffing.

Filtering rule:

```
access-list 101 deny   tcp any any eq 143 log
```

Testing: Use an external host to attempt a connection to an internal host using TCP port 143. The log option is set in order to view whether or not the packets were blocked at the router.

8. Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)

HTTP: The Hypertext Transfer Protocol is used for distributed, hypermedia information systems and resides at the application layer. Although HTTP's well-known port is TCP port 80, it can be configured to other ports. HTTP over SSL uses TCP port 443. HTTP can also use other ports such as TCP port 8080.

Possible vulnerabilities: Vulnerabilities exist within certain applications that use HTTP; for example, the dissemination of malicious mobile code or the use of HTTP to tunnel other types of services.

Filtering rules:

```
access-list 101 deny   tcp any any eq www log
access-list 101 deny   tcp any any eq 443 log
access-list 101 deny   tcp any any eq 8000 log
access-list 101 deny   tcp any any eq 8080 log
access-list 101 deny   tcp any any eq 8888 log
```

Testing: Use an external host to attempt a connection to an internal host using TCP ports 80, 443, 8000, 8080, 8888. The log option is set in order to view whether or not the packets were blocked at the router.

9. "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)

TCP Small Services: TCP Small Services include echo, chargen, discard, and daytime. Echo - server replies back with whatever is typed. Chargen - server generates a stream of ASCII data. Discard - server drops whatever is typed. Daytime - server returns system date and time.

UDP Small Services: UDP Small Services include echo, discard, and chargen. Echo - server replies back with the payload of the datagram that was sent. Discard - server drops the datagram that was sent. Chargen - server discards the datagram that was sent and responds with a 72-character string of ASCII characters.

Time: Server returns the time as a 32-bit binary number.

Possible vulnerabilities: These services are rarely used and should be blocked in order to help prevent the possible exploitation of vulnerabilities.

Filtering rules:

```
access-list 101 deny   tcp any any eq 37 log
access-list 101 deny   udp any any eq time log
```

For the TCP and UDP small services, the following global configuration commands should be used:

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

Testing: Use an external host to attempt a connection to an internal host using TCP/UDP ports 37, 7, 9, 19, and TCP port 13. The log option is set in order to view whether or not the packets were blocked at the router. Another way to determine whether the packets were blocked is to place a sniffer on the opposite side of the router and view the logs.

10. Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)

TFTP: Trivial File Transfer Protocol is a version of FTP that was developed for use when bootstrapping diskless systems. It uses UDP instead of TCP in order to make it smaller and simpler.

Possible vulnerabilities: If not properly implemented, TFTP will allow a user to download any file from the host. It also does not support authentication.

Filtering rule:

```
access-list 101 deny   udp any any eq tftp log
```

Testing: Use an external host to attempt a connection to an internal host using UDP port 69. The log option is set in order to view whether or not the packets were blocked at the router.

Finger: This service is used to acquire information about users logged into a certain system.

Possible vulnerabilities: An attacker can use this information to help plan an attack. For example, what period of the day would be the most opportune time to attack or perhaps to identify rarely used accounts.

Filtering rule:

The global configuration command: **no service finger**

Testing: Use an external host to attempt a connection to an internal host using TCP port 79. Place a sniffer on the opposite side of the router and view the logs to determine whether the packets were blocked.

NNTP: Network News Transport Protocol is used to transfer Usenet news across the Internet.

Possible vulnerabilities: NNTP uses access control lists that are based on hostnames. This protocol is vulnerable to IP spoofing. An attacker may be able to gain access to an NNTP server and view private information.

Filtering rule:

```
access-list 101 deny   tcp any any eq nntp log
```

Testing: Use an external host to attempt a connection to an internal host using TCP port 119. The log option is set in order to view whether or not the packets were blocked at the router.

NTP: The Network Time Protocol is used to synchronize system times across the network.

Possible vulnerabilities: A replay attack could be used to modify system clocks. This would have an affect on services such as time-based authentication and time stamps.

Filtering rule:

```
access-list 101 deny   tcp any any eq 123 log
```

Testing: Use an external host to attempt a connection to an internal host using TCP port 123. The log option is set in order to view whether or not the packets were blocked at the router.

LPD: LPD is a Unix printing protocol. Its access control is based IP addresses.

Possible vulnerabilities: LPD is susceptible to IP spoofing and denial of service attacks through the use of false print requests.

Filtering rule:

```
access-list 101 deny   tcp any any eq lpd log
```

Testing: Use an external host to attempt a connection to an internal host using TCP port 515. The log option is set in order to view whether or not the packets were blocked at the router.

Syslog: Syslog provides generic logging services for system events.

Possible vulnerabilities: False messages can be used to generate a denial of service attack. Information about the network's hosts can be obtained from the syslog. Older versions may be vulnerable to buffer overflows.

Filtering rule:

```
access-list 101 deny   udp any any eq syslog log
```

Testing: Use an external host to attempt a connection to an internal host using UDP port 514. The log option is set in order to view whether or not the packets were blocked at the router.

SNMP: The Simple Network Management Protocol is used to centrally manage network elements. Management stations can be used to gather information about interfaces as well as control particular functions on those interfaces. Port 161 is used for commands and port 162 is used for network device alarms.

Possible vulnerabilities: An attacker can use spoofing and sniffing to gather network device configuration settings as well as modify those settings. An attacker can also use SNMP to gather other types of data about the internal network.

Filtering rule:

```
access-list 101 deny   tcp any any range 161 162 log
access-list 101 deny   udp any any range 161 162 log
```

Testing: Use an external host to attempt a connection to an internal host using TCP/UDP ports 161 and 162. The log option is set in order to view whether or not the packets were blocked at the router.

BGP: The Border Gateway Protocol is an Exterior Gateway Protocol that connects distinct Autonomous Systems and forms a single network. This routing protocol is used on the Internet backbone.

Possible vulnerabilities: The BGP server is vulnerable to SYN flooding attacks, session hijacking, and RST attacks that attempt to tear down the connection to the server.

Filtering rule:

```
access-list 101 deny   tcp any any eq bgp log
```

Testing: Use an external host to attempt a connection to TCP port 179. The log option is set in order to view whether or not the packets were blocked at the router.

SOCKS: Secure Sockets is a protocol that is used to support TCP traffic through a proxy server.

Possible vulnerabilities: SOCKS may be vulnerable to denial of service attacks as well as buffer overflow attacks.

Filtering rule:

```
access-list 101 deny   tcp any any eq 1080 log
```

Testing: Use an external host to attempt a connection to TCP port 1080. The log option is set in order to view whether or not the packets were blocked at the router.

11. ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and unreachable messages

ICMP: The Internet Control Message Protocol is used to transmit status and error messages. Some of the message types include: host unreachable, redirect, and time exceeded.

Possible vulnerabilities: With the possible exception of outbound echo requests, used for troubleshooting network connectivity, and inbound echo replies, in response to the authorized outbound echo requests, ICMP traffic should be blocked whenever possible. An attacker can obtain valuable information about the internal network from ICMP messages. ICMP can be used in a denial of service attack such as a Smurf attack. ICMP can also be used as a covert channel, such as in Loki.

Filtering rule:

```
access-list 101 permit icmp any host 193.250.89.82 echo-reply log
access-list 101 deny   icmp any any log
access-list 102 permit icmp host 193.250.89.82 any echo log
access-list 102 deny   icmp any any log
```

Testing: Use an external host to transmit ICMP traffic. This should include ICMP echo-reply to the specified host and then to some other host. Use an internal host (other than the specified host) to transmit ICMP traffic. Send ICMP traffic from the specified host IP address (echo as well as other ICMP message types). The log option is set in order to view whether or not the packets were blocked at the router.

Section 4. Filter Order

Rules are applied on a first fit basis. I have highlighted the rules that are sensitive to order. Please note that this list represents the order of the rules used to enforce the specified filter policy. This does not represent a complete listing of rules.

> The blue rules must come first. If the blue rules were further down the list; there is a chance that a packet with one of the specified IP addresses would be accepted before being matched.
>
> For the green rules, "**`access-list 101 deny   icmp any any log`**" must come after "**`access-list 101 permit icmp any host 193.250.89.82 echo-reply log`**" otherwise no ICMP echo-reply traffic will ever be accepted.
>
> For the bold rules, the same logic that applied to the green rules apply here.

It is important to know that once an access-control list is added, the router denies all traffic that is not explicitly permitted.

```
-----------------------------
access-list 101 deny   ip 193.250.89.0 0.0.0.255 any log
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny   tcp any any eq telnet log
access-list 101 deny   tcp any any eq 22 log
access-list 101 deny   tcp any any eq ftp log
access-list 101 deny   tcp any any range 512 514 log
access-list 101 deny   tcp any any eq sunrpc log
access-list 101 deny   udp any any eq sunrpc log
access-list 101 deny   tcp any any eq 2049 log
access-list 101 deny   udp any any eq 2049 log
access-list 101 deny   tcp any any eq 4045 log
access-list 101 deny   udp any any eq 4045 log
access-list 101 deny   tcp any any eq 135 log
access-list 101 deny   udp any any eq 135 log
access-list 101 deny   udp any any eq netbios-ns log
```

```
access-list 101 deny   udp any any eq netbios-dgm log
access-list 101 deny   tcp any any eq 139 log
access-list 101 deny   tcp any any eq 445 log
access-list 101 deny   udp any any eq 445 log
access-list 101 deny   tcp any any range 6000 6255 log
access-list 101 deny   udp any any eq domain log
access-list 101 deny   tcp any any eq domain log
access-list 101 deny   tcp any any eq 389 log
access-list 101 deny   udp any any eq 389 log
access-list 101 deny   tcp any any eq smtp log
access-list 101 deny   tcp any any eq pop2 log
access-list 101 deny   tcp any any eq pop3 log
access-list 101 deny   tcp any any eq 143 log
access-list 101 deny   tcp any any eq www log
access-list 101 deny   tcp any any eq 443 log
access-list 101 deny   tcp any any eq 8000 log
access-list 101 deny   tcp any any eq 8080 log
access-list 101 deny   tcp any any eq 8888 log
access-list 101 deny   tcp any any eq 37 log
access-list 101 deny   udp any any eq time log
access-list 101 deny   tcp any any range 161 162 log
access-list 101 deny   udp any any range 161 162 log
access-list 101 deny   udp any any eq tftp log
access-list 101 deny   tcp any any eq nntp log
access-list 101 deny   tcp any any eq 123 log
access-list 101 deny   tcp any any eq lpd log
access-list 101 deny   udp any any eq syslog log
access-list 101 deny   tcp any any eq bgp log
access-list 101 deny   tcp any any eq 1080 log
access-list 101 permit icmp any host 193.250.89.82 echo-reply log
access-list 101 deny   icmp any any log
access-list 102 permit icmp host 193.250.89.82 any echo log
access-list 102 deny   icmp any any log
-------------------------------
```

Section 5. Log

In Section 3, a testing comment was included with each protocol/service. There are different ways to execute the validation test, for example: port scanners are available to assist with this testing, the actual protocol or application can be used, Telnet can be used to attempt to connect to the various ports, etc. Here is an extract of the log that was created by the router during the testing of these access-lists.

Cisco Router Log

00:09:55: %SEC-6-IPACCESSLOGDP: list 101 denied icmp 223.15.1.5 -> 193.250.89.54 (8/0
), 1 packet
00:12:10: %SEC-6-IPACCESSLOGP: list 101 denied udp 10.4.1.8(137) -> 193.250.89.54
(137), 1 packet

00:14:49: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1026) ->
193.250.89.54 (8
0), 1 packet
00:15:04: %SEC-6-IPACCESSLOGDP: list 101 denied icmp 223.15.1.5 ->
193.250.89.54 (8/0
), 3 packets
00:15:04: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1027) ->
193.250.89.54
.9(80), 1 packet
00:15:10: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1028) ->
193.250.89.54
.96(80), 1 packet
00:17:27: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1029) ->
193.250.89.54
.96(23), 1 packet
00:20:04: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1026) ->
193.250.89.54 (8
0), 3 packets
00:21:04: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1027) ->
193.250.89.54(80), 3 packets
00:23:04: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1029) ->
193.250.89.54
.96(23), 3 packets
00:24:58: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1031) ->
193.250.89.54(21), 1 packet
00:26:34: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1033) ->
193.250.89.54(111), 1 packet
.00:29:04: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1030) ->
193.250.89.54(22), 3 packets
fwrouter#
00:30:04: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1031) ->
193.250.89.54(21), 3 packets
00:30:57: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1035) ->
193.250.89.54(143), 1 packet
00:31:03: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1036) ->
193.250.89.54 (23), 1 packet
00:31:23: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1037) ->
193.250.89.54 (1080), 1 packet
00:31:55: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1038) ->
193.250.89.54 (17), 1 packet
00:32:04: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1033) ->
193.250.89.54 (111), 3 packets
00:32:51: %SEC-6-IPACCESSLOGP: list 101 denied tcp 223.15.1.5(1039) ->
193.250.89.54 (8080), 1 packet

Section 6. Additional information

It is important to note that when working with access-lists, new lines are added at the end of the list. If changes to the list are required, the list will need to be deleted and then recreated with the changes in place. Using a text editor and TFTP may facilitate the process. Cisco's website provides information on this procedure.

http://www.cisco.com

Perimeter Protection For An Added Layer of Defense in Depth as well as the Ten Most Critical Internet Security Threats is located at:

http://www.sans.org/topten.htm