Global Information Assurance Certification Paper

Firewall and Perimeter Defense Practical Assignment

Shan-Liang Yin

The examples used to complete this assignment are implemented using cisco IOS router extended access control lists. They should work with any version of Cisco IOS 11.2 and higher with a basic IP feature set. I choose cisco router access control lists because ciscos are commonly used as the access router between a site and the Internet and extended access control lists are part of the basic functionality of IOS.

The basic syntax of an access list is:

access-list <num> <action> <prot> <src details> <dest details> [log]

<num> is some number between 100 and 199. This will give you the extended access list functionality. Each number represents a grouping of filter rules which are applied on an interface in a specific direction.

<action> is either permit or deny. traffic that matches this access list will either be permitted through the router or blocked and discarded by the router.

<prot> specifies either the IP protocol or the protocol type of the IP packet. it may be IP, UDP, TCP, ICMP or any valid value in the IP header protocol field.

<src details> contains at least the source IP address. if the protocol specified is either TCP or UDP, then the source port number/range may also be specified.

<dst details> contains at least the destination IP address. if the protocol specified is either TCP or UDP, then the destination port number/range may also be specified. if the protocol is TCP, the word "established" may also be used to indicate a match when the ACK bit is set.

please refer to the relavent Cisco technical documentation for further details about the syntax or usage. It may be found in the following URL <http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/112cg_cr/5rbook/5rip.htm#xtocid232732>

The application of these access lists should be placed on the interface facing outside, whether on the access router between the WAN connecting to the Internet and the inside network or on the router between the DMZ network and the inside network.

This is to give the router some small level of "protection" against the probes and attacks that these list afford, and also to prevent the routing/forwarding engine from accepting the traffic before it is filtered.

as mentioned in the assignment, a better policy would be to create access list that *only* permit specific traffic through the perimeter and to block *all* other traffic (not specifically permitted).

it is easy to overlook or miss out "bad" traffic during configuration, or for probes or attacks to come through on traffic not specifically blocked.

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.**

- "Spoofed" and other private address, at the minimum can be used to cause DoS attacks to internal systems. source routed packets or compromised network infrastructure, in conjunction with spoofed addresses may also be used to gain unauthorized access, especially on systems that authorize based on IP address(e.g. host security, tcp wrapper, ACCess lists etc.)

```
! disable source routing
no ip source-route

! private (RFC1918 and network 127 addresses)
access-list 101 deny   ip 10.0.0.0 0.0.0.255 any
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
! "spoofed" addresses, assuming public address space is A.B.C.0/24
access-list 101 deny   ip A.B.C.0 0.0.0.255 any
! some other "impossible" addresses
access-list 101 deny   ip host 255.255.255.255 0.0.0.0
access-list 101 deny   ip host 0.0.0.0

! private (RFC1918 and network 127 addresses)
access-list 102 deny   ip any 10.0.0.0 0.0.0.255
access-list 102 deny   ip any 172.16.0.0 0.15.255.255
access-list 102 deny   ip any 192.168.0.0 0.0.255.255
access-list 102 deny   ip any 127.0.0.0 0.255.255.255
! "spoofed" addresses, assuming public address space of
! protected network is A.B.C.0/24
access-list 102 deny   ip any A.B.C.0 0.0.0.255
! some other "impossible" addresses
access-list 102 deny   ip any host 255.255.255.255
access-list 102 deny   ip any host 0.0.0.0

interface serial0/0
description outside WAN interface
ip access-list 101 in
ip access-list 102 out
no ip directed-broadcast

interface ethernet0/0
description inside LAN interface
no ip directed-broadcast
```

- the filter works by preventing any ip packets that have a source ip address from the private address range or addresses from within the protected network from entering the router's outside interface.

- also, source routing is disable and both inside and outside interfaces of the router will not forward directed broadcast packets.

- in addition, a corresponding outbound filter may be applied. this would prevent hosts within the protected network from being used to "attack" other sites if they were compromised. also, there should be no reason for packets destined for the protected network to leave the outside interface of the router, thus the rule blocking any outbound packets destined for the protected network.

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

- Login services allow remote access to protected hosts for file transfers or command line access. if allowed, security of the site will not depend on the perimeter/friewall security, and would instead rest of the security of the passwords of the user accounts on the hosts, as well as the correct implementation of the application servers (telnetd, sshd, ftpd, etc..).

```
! Login services
access-list 101 deny   tcp any any eq telnet
access-list 101 deny   tcp any any eq 22
access-list 101 deny   tcp any any eq ftp
access-list 101 deny   tcp any any eq 139
access-list 101 deny   tcp any any range 512 514

interface serial0/0
description outside WAN interface
ip access-list 101 in
```

```
- the filter works by preventing any packets with a destination
port number that corresponds with the blocked service from
entering the outside interface of the router.

- by filtering these services, users from the outside will not
be able to access ftp servers within the protected netowrk. this
may not be desirable if that is a services that is needed.

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

- RPC and NFS services are usually used for file sharing. NFS/RPC
are commonly exploited as there have been many security bugs and
problems in older software versions. blocking these services
would prevent external users from accessing NFS/RPC ( like
ToolTalk, etc..) services within the protected network. this
should protect against NFS/RPC exploits and prevent leakage of
proprietary/confidential data via NFS file sharing services.

! RPC and NFS services (inbound)
access-list 101 deny   tcp any any eq sunrpc
access-list 101 deny   udp any any eq sunrpc
access-list 101 deny   tcp any any eq 2049
access-list 101 deny   udp any any eq 2049
access-list 101 deny   tcp any any eq 4045
access-list 101 deny   udp any any eq 4045

! RPC and NFS services (outbound)
access-list 102 deny   tcp any any eq sunrpc
access-list 102 deny   udp any any eq sunrpc
access-list 102 deny   tcp any any eq 2049
access-list 102 deny   udp any any eq 2049
access-list 102 deny   tcp any any eq 4045
access-list 102 deny   udp any any eq 4045

interface serial0/0
description outside WAN interface
ip access-list 101 in
ip access-list 102 out

- the filter works by preventing any packets with a destination
port number that corresponds with the blocked service from
entering the outside interface of the router.

- in addition, a corresponding outbound filter may be applied if
needed. this would protect hosts within the protected network from
any potential client side exploits, as well as prevent them from
being used to "attack" other sites if they become compromised.

    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 is used for nearly all microsoft networking
and file sharing applications. it is also probably easily
exploited. blocking these ports should effectively block
microsoft networking interaction between hosts within the
protected network and the outside, and prevent external users
from accessing microsoft file sharing services from within
the protected network. this should also prevent leakage of
proprietary/confidential data via microsoft file sharing services.


! NetBIOS in WinNT (inbound)
access-list 101 deny   tcp any any eq 135
access-list 101 deny   udp any any eq 135
access-list 101 deny   udp any any range 137 138
access-list 101 deny   tcp any any eq 139
! Win2000 (inbound)
access-list 101 deny   tcp any any eq 445
access-list 101 deny   udp any any eq 445
! NetBIOS in WinNT (outbound)
```

```
access-list 101 deny   tcp any any eq 135
access-list 101 deny   udp any any eq 135
access-list 101 deny   udp any any range 137 138
access-list 101 deny   tcp any any eq 139
! Win2000 (outbound)
access-list 101 deny   tcp any any eq 445
access-list 101 deny   udp any any eq 445

interface serial0/0
description outside WAN interface
ip access-list 101 in
ip access-list 102 out
```

- the filter works by preventing any packets with a destination port number that corresponds with the blocked service from entering the outside interface of the router.

- in addition, a corresponding outbound filter may be applied if needed. this would protect hosts within the protected network from any potential client side exploits, as well as prevent them from being used to "attack" other sites if they become compromised.

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

- X Windows traffic is used for the X client to communicate with the X server. each display on the server uses one port number, starting with Display 0 on port 6000 all the way to Display 255 on port 6255. Blocking incoming traffic to TCP ports 6000 to 6255 will prevent outside X clients to connect to X servers on hosts within the protected network. This will prevent attacks that try to capture keystrokes or access the users' display in the protected network.

```
! X Windows
access-list 101 deny   tcp any any range 6000 6255

! X Windows
access-list 102 deny   tcp any any range 6000 6255

interface serial0/0
description outside WAN interface
ip access-list 101 in
ip access-list 102 out
```

- the filter works by preventing any packets with a destination port number that corresponds with the blocked service from entering the outside interface of the router.

- in addition, a corresponding outbound filter may be applied if needed. this would protect hosts within the protected network from any potential client side exploits, as well as prevent them from being used to "attack" other sites if they become compromised.

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)

- Naming services may be used to aid a potential attacker to map the protected network, especially zone transfers, as well as to gain details revealing network topology, personal details and corporate structure. Additionally, the bind daemon, which is used to provide DNS service, is easily exploitable if older software with security bugs is used. blocking access to hosts that are not DNS servers but are running the DNS service will reduce exposure to DNS related exploits.

```
! Naming services (inbound)
access-list 101 permit udp any host dns-server-ip eq 53
access-list 101 deny   udp any any eq 53
access-list 101 permit tcp host external-dns-secondary host dns-server-ip eq 53
access-list 101 deny   tcp any any eq 53
access-list 101 deny   udp any any eq 389
access-list 101 deny   tcp any any eq 389
```

```
! Naming services (outbound)
access-list 102 permit udp host dns-server-ip any eq 53
access-list 102 deny   udp any any eq 53
access-list 102 deny   udp any any eq 389
access-list 102 deny   tcp any any eq 389

interface serial0/0
description outside WAN interface
ip access-list 101 in
ip access-list 102 out
```

- the filter works by preventing any packets with a destination port number that corresponds with the blocked service from entering the outside interface of the router.

- in addition, a corresponding outbound filter may be applied if needed. this would protect hosts within the protected network from any potential client side exploits, as well as prevent them from being used to "attack" other sites if they become compromised.

- this filter rule will prevent inside clients from directly resolving names, but that should be acceptable as most DNS clients in the protected network should be using the "inside" dns server to resolve all DNS queries.

- the filter rule to permit connections inbound (or outbound) to the DNS servers should preceed any other rule to block DNS as the permit rules are more specific and will allow the DNS servers to resolve names outside. if the deny rules were first, they would take precedence and will block all inbound (or outbound) DNS traffic, including DNS traffic between the DNS servers and the outside.

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

- Mail services are another commonly exploited services, again due to the security bugs and implementation problems present in some software. blocking mail services will prevent outside users from access the POP or IMAP mail retrieval services, as well as prevent access to hosts that may be running SMTP servers which are not supposed to be externally accessible mail relays. also, mail retrival services like POP or IMAP transmit the user's password and username in the clear. If users are retriving mail from the outside, the username and password may be picked up, and used to remotely login to the hosts within the protected network (see rule 2 above).

```
! Mail (inbound)
access-list 101 permit tcp any host external-mail-relay-ip eq 25
access-list 101 deny   tcp any any eq 25
access-list 101 deny   tcp any any range 109 110
access-list 101 deny   tcp any any eq 143

! Mail (outbound)
access-list 102 permit tcp host external-mail-relay-ip any eq 25
access-list 102 deny   tcp any any eq 25
access-list 102 deny   tcp any any range 109 110
access-list 102 deny   tcp any any eq 143

interface serial0/0
description outside WAN interface
ip access-list 101 in
```

- the filter works by preventing any packets with a destination port number that corresponds with the blocked service from entering the outside interface of the router.

- in addition, a corresponding outbound filter may be applied if needed. this would protect hosts within the protected network from any potential client side exploits, as well as prevent them from being used "attack" other sites if they become compromised.

- it should be noted that blocking outbound IMAP or POP traffic may prevent users within the protected network from using external mail accounts/services.

- blocking outbound SMTP traffic will also prevent hosts within the protected network from delivering mail directly to the recipient mail server. however most mail clients in the protected network using a mail relay to resolve/forward mail to external sites would not be disrupted by the outbound rule. for example, some vendors's sendmail configuration defaults to delivering mail directly to the receipiant mail server and not to use a mail relay. in these cases, blocking outbound smtp traffic may not be possible without reconfiguring the smtp clients affected.

- the filter rule to permit connections inbound (or outbound) to the mail relay should preceed any other rules that block mail related traffic. the permit rules are more specific and will allow the mail relays to send and receive mail with external sites. if the deny rules were first, they would take precedence and will always block all mail related traffic, preventing the mail relays from working.

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.)

- Web services allow outside users to access web servers within the protected network.also, it is common for hosts to come preconfigured as web servers for "intranet" file sharing, or for embedded appliances to come with web based management, both of which pose considerable security risk if exposed to the outside, for example, DoS attacks may be acomplished by reconfiguring a printer/network appliance, confidential data maybe read off an "intranet server", or remote access maybe gain from poorly implemented CGI scripts.

```
! Web
access-list 101 permit tcp any host external-web-server eq 80
access-list 101 permit tcp any host external-web-server eq 443
access-list 101 deny   tcp any any eq 80
access-list 101 deny   tcp any any eq 443
access-list 101 deny   tcp any any eq 8000
access-list 101 deny   tcp any any eq 8080
access-list 101 deny   tcp any any eq 8888

interface serial0/0
description outside WAN interface
ip access-list 101 in
```

- the filter works by preventing any packets with a destination port number that corresponds with the blocked service from entering the outside interface of the router.

- the filter rule to permit connections inbound to the externally accessible web servers should preceed any other rules blocking web traffic as the permit rules are more specific and will allow access to the externally accessible web servers. if the deny rules were first, they would take precedence and will block all inbound traffic, including any web traffic to the externally accessible web servers.

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

- Small services are generally used for debugging and other diagnostic purposes and should not need to be access from the outside as they may be used for DoS attack purposes, or be exploited to gain unauthorized priviledge access from poor implementation or security bugs in the software.

```
! turn off small services on router itself,
```

```
! this is the default on more recent versions of cisco IOS
no service udp-small-servers
no service tcp-small-servers

! small services (inbound)
access-list 101 deny   udp any any lt 20
access-list 101 deny   tcp any any lt 20
access-list 101 deny   udp any any eq time
access-list 101 deny   tcp any any eq time

! small services (outbound)
access-list 102 deny   udp any any lt 20
access-list 102 deny   tcp any any lt 20
access-list 102 deny   udp any any eq time
access-list 102 deny   tcp any any eq time

interface serial0/0
description outside WAN interface
ip access-list 101 in
ip access-list 102 out

- the filter works by preventing any packets with a destination
port number that corresponds with the blocked service from
entering the outside interface of the router.

- in addition, a corresponding outbound filter may be applied
if needed. this would protect hosts within the protected network
from any potential client side exploits, as well as prevent them
from being used "attack" other sites if they become compromised.
```

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)

```
- The miscellaneous services listed above are usually not
provided for "general public consumption", and if access to
these services are not blocked from the outside, they may be
exploited to reveal details such as user names and accounts,
machine types, operating system and versions, and maybe even
confidential data. DoS attacks may also be carried out against
these services if exposed to the outside.

! misc. services (inbound)
access-list 101 deny   udp any any tftp
access-list 101 deny   tcp any any finger
access-list 101 deny   tcp any any nntp
access-list 101 deny   tcp any any lpd
access-list 101 deny   udp any any syslog
access-list 101 deny   udp any range snmp snmptrap
access-list 101 deny   tcp any any 161
access-list 101 deny   tcp any any bgp
access-list 101 deny   tcp any any 1080

! misc. services (outbound)
access-list 102 deny   udp any any tftp
access-list 102 deny   tcp any any finger
access-list 102 deny   tcp any any lpd
access-list 102 deny   udp any any syslog
access-list 102 deny   udp any range snmp snmptrap
access-list 102 deny   tcp any any 161
access-list 102 deny   tcp any any bgp
access-list 102 deny   tcp any any 1080

interface serial0/0
description outside WAN interface
ip access-list 101 in
ip access-list 102 out

- the filter works by preventing any packets with a destination
port number that corresponds with the blocked service from
entering the outside interface of the router.
```



```
- in addition, a corresponding outbound filter may be applied
```

if needed. this would protect hosts within the protected network from any potential client side exploits, as well as prevent them from being used to "attack" other sites if they become compromised.

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

- ICMP packets are used for network control and diagnostics. they may be exploited to perform DoS attacks or may be used to map the network. DoS attacks may come in the form of flooding, or by exploiting poorly implemented ip/icmp protocol stacks. Specifically, echo request and replies, time exceeded and unreachables may all be used to map ip hosts in the protected network, as well as probe open ports or firewall filter configuration.

```
! ICMP (inbound)
access-list 101 deny   icmp any any echo

! ICMP (outbound)
access-list 102 deny   icmp any any echo-reply
access-list 102 deny   icmp any any unreachable
access-list 102 deny   icmp any any time-exceeded

interface serial0/0
description outside WAN interface
ip access-list 101 in
ip access-list 102 out
no ip unreachables
```

- the filter works by preventing any icmp echo packets from entering the outside interface of the router, and for any icmp echo replies, icmp unreachables or icmp time-exceeded messages generated by hosts within the protected network from leaving the outside interface of the rotuer.

- note that this filter will prevent outside hosts from ping'ing the router, which in general is good, but may prevent the ISP from monitoring the connection. also, since this whole assignment is not based on a stronger "allow specific services and deny all others" policy, this filter also will not prevent/block udp-based traceroute programs from reaching the router and eliciting an icmp time-exceeded response from the router.

12. Putting it all together.

- since cisco access control list rules are order sensitive, with the first matching rule taking precedence over all subsequent rules, more specific rules should be listed before less specific rules.

- to implement the security policy in this assignment, essentially allowing all inbound traffic except for the services explicitly blocked, the most restrictive rule, the one blocking spoofed and private addresses, must be first. this will prevent any packet with a "spoofed" or private source address from matching any of the permit rules in subsequent sections, thus by-passing the filter to block spoofed/private addresses.once that takes precedence, the order of all subsequent sections does not matter as the services do not overlap one another.

```
! disable source routing
no ip source-route

! turn off small services on router itself,
! this is the default on more recent versions of cisco IOS
no service udp-small-servers
no service tcp-small-servers
```

```
! private (RFC1918 and network 127 addresses)
access-list 101 deny   ip 10.0.0.0 0.0.0.255 any
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
! "spoofed" addresses, assuming public address space is A.B.C.0/24
access-list 101 deny   ip A.B.C.0 0.0.0.255 any
! Login services
access-list 101 deny   tcp any any eq telnet
access-list 101 deny   tcp any any eq 22
access-list 101 deny   tcp any any eq ftp
access-list 101 deny   tcp any any eq 139
access-list 101 deny   tcp any any range 512 514
! RPC and NFS services (inbound)
access-list 101 deny   tcp any any eq sunrpc
access-list 101 deny   udp any any eq sunrpc
access-list 101 deny   tcp any any eq 2049
access-list 101 deny   udp any any eq 2049
access-list 101 deny   tcp any any eq 4045
access-list 101 deny   udp any any eq 4045
! NetBIOS in WinNT (inbound)
access-list 101 deny   tcp any any eq 135
access-list 101 deny   udp any any eq 135
access-list 101 deny   udp any any range 137 138
access-list 101 deny   tcp any any eq 139
! Win2000 (inbound)
access-list 101 deny   tcp any any eq 445
access-list 101 deny   udp any any eq 445
! X Windows
access-list 101 deny   tcp any any range 6000 6255
! Naming services (inbound)
access-list 101 permit udp any host dns-server-ip eq 53
access-list 101 deny   udp any any eq 53
access-list 101 permit tcp host external-dns-secondary host dns-server-ip eq 53
access-list 101 deny   tcp any any eq 53
access-list 101 deny   udp any any eq 389
access-list 101 deny   tcp any any eq 389
! Mail (inbound)
access-list 101 permit tcp any host dns-server-ip eq 25
access-list 101 deny   tcp any any eq 25
access-list 101 deny   tcp any any range 109 110
access-list 101 deny   tcp any any eq 143
! Web
access-list 101 permit tcp any host external-web-server eq 80
access-list 101 permit tcp any host external-web-server eq 443
access-list 101 deny   tcp any any eq 80
access-list 101 deny   tcp any any eq 443
access-list 101 deny   tcp any any eq 8000
access-list 101 deny   tcp any any eq 8080
access-list 101 deny   tcp any any eq 8888
! small services (inbound)
access-list 101 deny   udp any any lt 20
access-list 101 deny   tcp any any lt 20
access-list 101 deny   udp any any eq time
access-list 101 deny   tcp any any eq time
! misc. services (inbound)
access-list 101 deny   udp any any tftp
access-list 101 deny   tcp any any finger
access-list 101 deny   tcp any any nntp
access-list 101 deny   tcp any any lpd
access-list 101 deny   udp any any syslog
access-list 101 deny   udp any range snmp snmptrap
access-list 101 deny   tcp any any 161
access-list 101 deny   tcp any any bgp
access-list 101 deny   tcp any any 1080
! ICMP (inbound)
access-list 101 deny   icmp any any echo

! private (RFC1918 and network 127 addresses)
access-list 102 deny   ip any 10.0.0.0 0.0.0.255
```

```
access-list 102 deny   ip any 172.16.0.0 0.15.255.255
access-list 102 deny   ip any 192.168.0.0 0.0.255.255
access-list 102 deny   ip any 127.0.0.0 0.255.255.255
! "spoofed" addresses, assuming public address space of
! protected network is A.B.C.0/24
access-list 102 deny   ip any A.B.C.0 0.0.0.255
! RPC and NFS services (outbound)
access-list 102 deny   tcp any any eq sunrpc
access-list 102 deny   udp any any eq sunrpc
access-list 102 deny   tcp any any eq 2049
access-list 102 deny   udp any any eq 2049
access-list 102 deny   tcp any any eq 4045
access-list 102 deny   udp any any eq 4045
! NetBIOS in WinNT (outbound)
access-list 102 deny   tcp any any eq 135
access-list 102 deny   udp any any eq 135
access-list 102 deny   udp any any range 137 138
access-list 102 deny   tcp any any eq 139
! Win2000 (outbound)
access-list 102 deny   tcp any any eq 445
access-list 102 deny   udp any any eq 445
! X Windows
access-list 102 deny   tcp any any range 6000 6255
! Naming services (outbound)
access-list 102 permit udp host dns-server-ip any eq 53
access-list 102 deny   udp any any eq 53
access-list 102 deny   udp any any eq 389
access-list 102 deny   tcp any any eq 389
! Mail (outbound)
access-list 102 permit tcp host dns-server-ip any eq 25
access-list 102 deny   tcp any any eq 25
access-list 102 deny   tcp any any range 109 110
access-list 102 deny   tcp any any eq 143
! small services (outbound)
access-list 102 deny   udp any any lt 20
access-list 102 deny   tcp any any lt 20
access-list 102 deny   udp any any eq time
access-list 102 deny   tcp any any eq time
! misc. services (outbound)
access-list 102 deny   udp any any tftp
access-list 102 deny   tcp any any finger
access-list 102 deny   tcp any any lpd
access-list 102 deny   udp any any syslog
access-list 102 deny   udp any range snmp snmptrap
access-list 102 deny   tcp any any 161
access-list 102 deny   tcp any any bgp
access-list 102 deny   tcp any any 1080
! ICMP (outbound)
access-list 102 deny   icmp any any echo-reply
access-list 102 deny   icmp any any unreachable
access-list 102 deny   icmp any any time-exceeded


interface serial0/0
description outside WAN interface
ip access-list 101 in
ip access-list 102 out
no ip unreachables
no ip directed-broadcast

interface ethernet0/0
description inside LAN interface
no ip directed-broadcast
```

13. Testing and verification.

- since this is a basic packet filter, to test the filter is operating as planned, we just need to generate traffic that the filter is supposed to block and send it across the router. to verify that the router is indeed blocking the traffic, we just need to run tcpdump on the opposite side of the interface and watch for packets to pass. if the generated packets do not pass

and the access list counters increment, we know what the filter blocked the traffic.

- to clear the access-list counters before viewing, initialize/zero them out with the "clear access-list counters" command. to view the access-lists (and counters), use the "show access-list" command.

- for the tcp-based traffic we want to test, we may use the following short-cut to generate tcp traffic which simulates a client request.

on a unix host.

telnet server service-port
telnet A.B.C.1 25 (to test if host A.B.C.1 has smtp (tcp/25) blocked).