PreLab 10: Securing workstations

Or: *ACLs really need to be planned out ahead of time*

What You Will Do:

1. Create ACLs to secure workstations for 3 different types of usage
2. [Optional] To maximize your success in lab, test some of the ACLs in PT or NetLab
3. [During your lab] You will actually deploy and test the ACL you have written to protect your workstation. The specific ACL will be assigned by the lab Professor.

Things that you will need to know or learn:

1. The skill of writing extended ACLs that you developed in the previous post-lab.

What you need to submit and when:

1. **TWO PRINTED COPIES** of your ACLs, submitted in person within 5 mins of the official start time of your lab session. Clearly separate the ACLs into three different sections.

This pre-lab is worth **36%** of this lab, even though the number of points may differ between the three parts.

References and Resources:

- Slide decks on ACLs
- Post-Lab 9 exercise on extended ACLs

Hints and Tips

– Some research may be required to determine specific allowed IP addresses.
– Completing the postlab 9 quiz will be of great help in composing the new ACLs.

(Continued on next page.)

Scenario

Your workplace needs to secure the workstations for three different uses. These are defined below. You need to submit the exact details of complete *named* ACLs (for Cisco devices) that will limit traffic to known applications and known destinations as defined below.

Your job is to (a) determine exactly which protocols and/or ports must be included in the set of ACEs for each ACL; then (b) compose the required ACL. Choose appropriate names!
Important: **State** if you designing your ACLs for traffic *inbound to* or *outbound from* the user?!

1. Ordinary user (think of a grandparent) – 9 protocols/ports
   - boot-up into windows (DHCP, DNS, NTP)
     Hint: one protocol isn't always be particularly noticeable, but check bottom right of screen!
   - surf the internet (HTTP, HTTPS)
   - use an email client of their preference (e.g. Thunderbird). You do **not** know what kind of server they will be connecting to, so allow access for all possible setups.
     (legacy & TLS SMTP, legacy and TLS POP3, or just legacy and TLS IMAP)
   - **ALL OTHER TRAFFIC IS BLOCKED** and must be monitored by a matching ACE

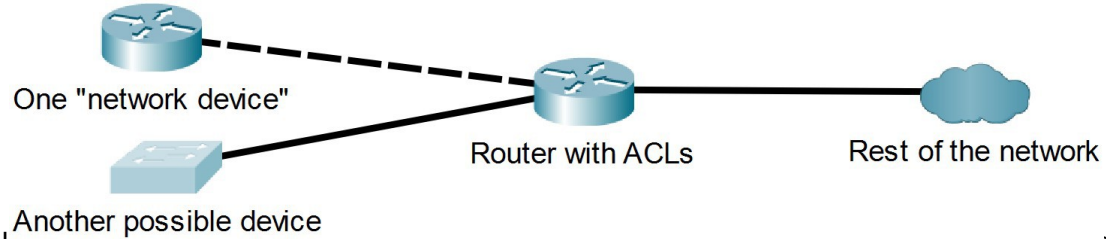
The only acceptable DNS servers are Google and CloudFlare's public servers.

2. Networking Student – 5 additional protocols/ports
   - all the same applications and specifications as an ordinary user
   - NetLab (Telnet, SSH)
   - Run the two (most common!) network troubleshooting tools (ICMP)
   - FTP (FTP control, data)
   - **ALL OTHER TRAFFIC IS BLOCKED** and must be monitored by a matching ACE

3. Network device (router, switch) – 6 protocols/ports
   - Factory-fresh (completely uninitialized) systems must be able to boot up from the network
   - Prepared configs must be retrieved from a TFTP server
   - Send log messages to an external server (Ref: read ENSA section 12.3.4!) (Syslog)
   - Run the two (most common!) network troubleshooting tools
   - All other traffic will be permitted

The purpose of the ACL(s) is to monitor the *number of packets* of each type that *exit* ("egress") and *enter* ("ingress") to/from the device. So even though all traffic is ultimately permitted, it must nonetheless be matched by individual ACEs.

Q. Consider whether you need *two separate* ACLs or whether a single ACL can be applied to both the input and output of the interface. Does that affect the design of your ACL?



Extra Refs: https://blog.certskills.com/cl661/ https://blog.certskills.com/cl661-answers/

Marking Rubric – 4 marks total
[1 mark] = handed something in, which showed reasonable effort
[1 mark] = ACL #1 about 9+ lines; ACL #2 about 14+ lines; ACL #3 about 6+ lines
[1 mark] = Many/most protocols correctly identified (by number or Cisco name)
[1 mark] = Overall quite correct

Note: Below are the three ACLs structured for filtering **in**bound traffic returning to the host. For the corresponding ACLs for filtering traffic coming FROM the host, simply swap the source and destination fields.

In the case of DHCP, the client sends requests to the server using the broadcast IP address 255.255.255.255, so that could be included in the ACE:

```
    10 permit udp any eq 68  255.255.255.255 eq 67 log
```

```
ip access-list extended SIMPLE_USER
    remark This ACL is for INBOUND on ext I/F - replies TO the client
    remark DHCP - Server port is 67, client port is 68
    10 permit udp any eq 67 any eq 68 log
    remark DNS - allow CloudFlare and Google
    20 permit udp host 1.1.1.1 eq 53 any log
    30 permit udp host 8.8.8.8 eq 53 any log
    remark NTP - Both server & client typically use the NTP port = 123
    40 permit udp any eq 123 any eq 123 log
    remark For ALL TCP rules, could also include the keyword 'established'
    remark HTTP/S - allow both styles
    50 permit tcp any eq 80 any log
    60 permit tcp any eq 443 any log
    remark Email - classic/secure options for SMTP, POP3, IMAP
    70 permit tcp any eq 25 any log
    remark secure SMTP has two alternatives for the port number: 465, 587
    80 permit tcp any eq 465 any log
    90 permit tcp any eq 587 any log
    100 permit tcp any eq 110 any log
    110 permit tcp any eq 995 any log
    120 permit tcp any eq 143 any log
    130 permit tcp any eq 993 any log
    remark Deny all other - explicitly set so we can count & log it
    140 deny ip any any log
```

(**Continued next page**)

```
ip access-list extended NETWORK_TECH
    remark This ACL is for INBOUND on ext I/F - replies TO the client
    remark DHCP - Server port is 67, client port is 68
    10 permit udp any eq 67 any eq 68 log
    remark DNS - allow CloudFlare and Google
    20 permit udp host 1.1.1.1 eq 53 any log
    30 permit udp host 8.8.8.8 eq 53 any log
    remark NTP - Both server & client typically use the NTP port = 123
    40 permit udp any eq 123 any eq 123 log
    remark HTTP/S - allow both styles
    50 permit tcp any eq 80 any log
    60 permit tcp any eq 443 any log
    remark For ALL TCP rules, could also include the keyword 'established'
    remark Email - classic/secure options for SMTP, POP3, IMAP
    70 permit tcp any eq 25 any log
    remark secure SMTP has two alternatives for the port number: 465, 587
    80 permit tcp any eq 465 any log
    90 permit tcp any eq 587 any log
    100 permit tcp any eq 110 any log
    110 permit tcp any eq 995 any log
    120 permit tcp any eq 143 any log
    130 permit tcp any eq 993 any log
    remark Allow ping, and in-order: FTP (data, command), SSH, Telnet
    140 permit icmp any any log
    150 permit tcp any eq 20 any log
    160 permit tcp any eq 21 any log
    170 permit tcp any eq 22 any log
    180 permit tcp any eq 23 any log
    remark Deny all other - explicitly set so we can count & log it
    190 deny ip any any log

ip access-list NETWORK_DEVICE
    remark This ACL is for INBOUND on ext I/F - replies TO the client
    remark DHCP - Server port is 67, client port is 68
    10 permit udp any eq 67 any eq 68 log
    remark DNS - allow CloudFlare and Google
    20 permit udp host 1.1.1.1 eq 53 any log
    30 permit udp host 8.8.8.8 eq 53 any log
    remark NTP - Both server & client typically use the NTP port = 123
    40 permit udp any eq 123 any eq 123 log
    remark TFTP - for downloading images; saving & restoring configs
    50 permit udp any eq 69 any log
    remark Syslog utility - status messages
    60 permit udp any eq 514 any log
    remark Ping
    70 permit icmp any any log
    remark Permit all other - packets passing through the router!
    80 permit ip any any
```