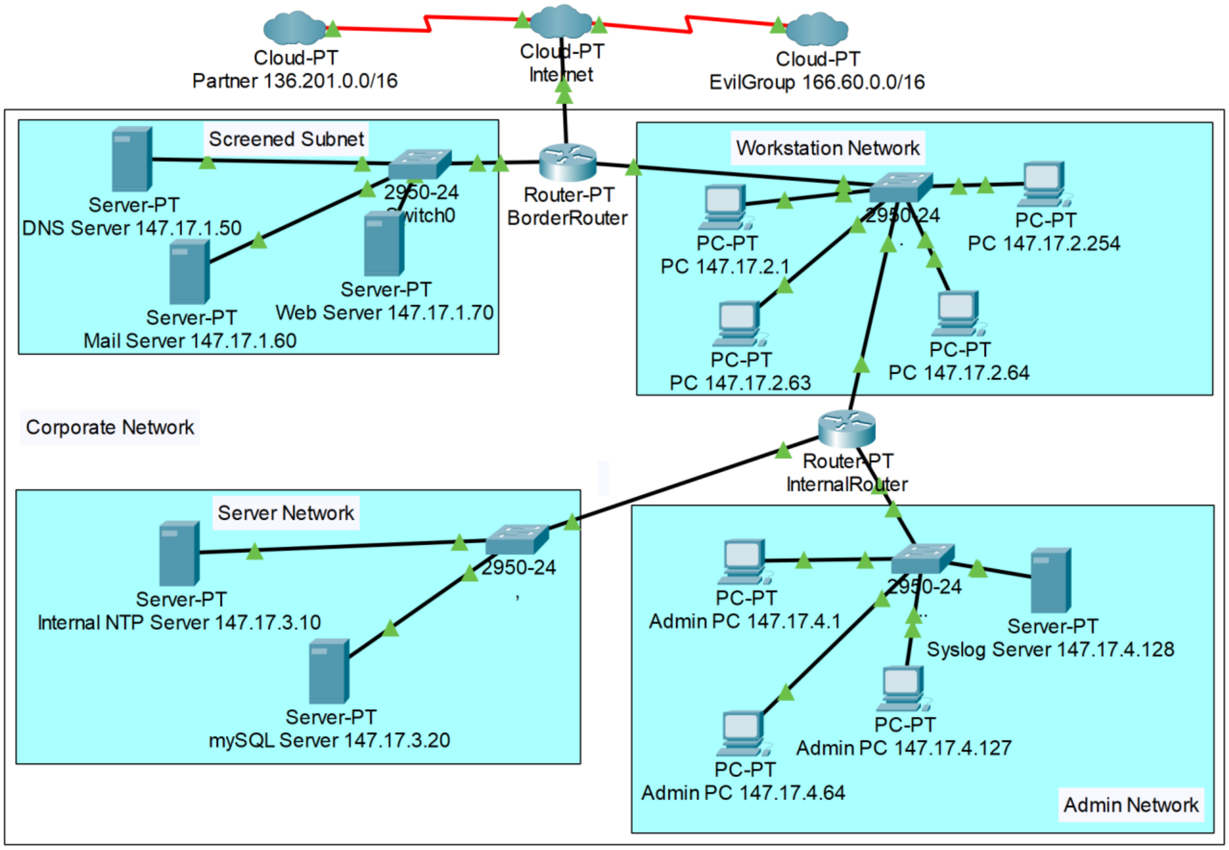
EE6042/ET4028 Host & Network Security
Firewall Assignment

1. Task

In this assignment you are asked to provide **named ACLs** for Cisco Packet Filter Firewalls. Each student must undertake their own assignment – any duplicate solutions will receive 0 marks. Please submit any questions/queries via email to reiner.dojen@ul.ie.

Consider the following network outline:

- Note: There is **no need to build this network !!!**
- Note: Not all PCs/Servers are displayed!



This network has the following components:

- The Internet: any machine/network range not mentioned elsewhere.
- Partner (class B network 136.201.0.0/16): a business partner with privileged access rights.
- Evil Group (class C network 6.6.60.0/C): known to have malicious intent.
- Your own corporate network (class B network 147.17.0.0/16), which has the subnets 147.17.1.0/24 Screened Subnet, 147.17.2.0/24 Workstation Network, 147.17.3/24 Server Network, and 147.17.4.0/24 Admin Network.

The Border Router in the Corporate Network has the following interfaces:

- FastEthernet 0/0: Connected to the ISP (Internet), IP address 10.10.10.10
- FastEthernet 1/0: Connected to the Screened Subnet, IP address 147.17.1.254
- FastEthernet 2/0: Connected to the Workstation Network, IP address 147.17.2.254

The Internal Router in the Corporate Network has the following interfaces:

- FastEthernet 0/0: Connected to the Workstation Network, IP address 147.17.2.254
- FastEthernet 1/0: Connected to the Server Network, IP address 147.17.3.254
- FastEthernet 2/0: Connected to the Admin Network, IP address 147.17.4.254

The Screened Subnet contains the following servers:

- DNS Server 147.17.1.50
- Mail Server 147.17.1.60
- Web Server 147.17.1.70

The Workstation Network contains the following machines:

- Internal PCs and Workstations 147.17.2.1-254 (even though 147.17.2.254/253 are the interfaces of the routers, treat them as if they were PCs)

The Internal Server Network contains the following servers:

- Internal NTP Server 147.17.3.10
- MySQL Database Server 147.17.3.20

The Admin Network contains the following machines:

- Admin PCs 147.17.4.1-127
- Syslog Server 147.17.4.128

Your task is to configure **named ACLs** in the two routers to implement the security policy outlined below (only IPv4 needs to be considered). Please note that some networking aspects that are usually required for the network to work might be missing – you can ignore these.

In this section, IP addresses are combined with ports in format ipaddress:port, where port indicates TCP (T) or UDP (U) as well as port number. Ranges are indicated as follows:

- Port in range x to y (both inclusive): Tx-y
- Any port greater than x: T>x
- Any port greater or equal to x: T>=x
- Any port less than x: T<x
- Any port less or equal to x: T<=x
- Selection of ports x,y,z: Tx,Uy,Tz

For example, if 192.168.10.100 connects from port 12345 to web server 192.168.1.2 on port 80 then the following notation is used: 192.168.10.100:T12345 connects to 192.168.1.2:T80

Security Policy:

- Perform sensible ingress and egress filtering (as discussed in the lecture).
- Any packets with a source IP address from EvilGroup are denied access to **<u>any</u>** machine in the corporate network (in the following items "everybody"/"any" excludes EvilGroup).
- All internal machines (all machines 147.17.0.0/16) can send log messages to the Syslog server (147.17.x.x:T>1023 to 147.17.4.128:T514) and can contact the NTP server (147.17.x.x:U>1023 to 147.17.3.10:U123).
- Business partner machines can connect to the Syslog Server via SSH (136.201.x.x:T>1023 to 147.17.4.128:T22), can send secure log message to the Syslog Server (136.201.x.x:T>1023 to 147.17.4.128:T514) and contact the NTP Server (136.201.x.x:U>1023 to 147.17.3.10:U123).
- Any machine (inside or outside - unless other policy rules forbid it) can access DNS Server 147.17.1.50:T53 (any:T>1023 to 147.17.1.50:53), Mail Server 147.17.1.60:T25 (any:T25 to 147.17.1.60:T25) and Web server 147.17.1.70:T443 (any:T>1023 to 147.17.1.70:443) – make sure the clients cannot use any server port (1 to 1023 – attention: SMTP is server to server).
- DNS Server can access any outside machine on TCP 53 (147.17.1.50:T>=1024 to any:T53). Only TCP requests are supported.
- Mail Server 147.17.1.60 can contact any outside machine on SMTP (147.17.1.60:T25 to any:T25).
- Web server can only initiate connections to the mySQL DataBase Server (147.17.1.70:T>=1024 to 147.17.3.20:T3360), NTP server (147.17.1.70:U>1023 to 147.17.3.10:U123) and Syslog Server (147.17.1.70:T>1023 to 147.17.4.128:T514). All other traffic originating in the web server **must be return traffic** to HTTPS requests.
- NTP server can only be accessed by internal machines and business partner machines.
- MySQL DataBase Server (147.17.3.20) can only be accessed by Web server (147.17.1.70), your own workstations (147.17.2.0/24) using SQL queries (machines:T>=1024 to 147.17.3.20:T3360). It can only react to requests (and send logs to the Syslog Server).
- Internal PCs and Workstations in the Workstation Network can only access:
  - Any web server (internal or external) via HTTPS (147.17.2.x:T>=1024 to any:T443).
  - DNS Server 147.17.1.50 (147.17.2.x:T>1023 to 147.17.1.50:T53)
  - Mail Server 147.17.1.60 for IMAP and SMTP (147.17.2.x:T>1023 to 147.17.1.60:T220,T25)
  - Your own mySQL DataBase Server (147.17.2.x:T>=1024 to 147.17.3.20:T3360).
  - Internal NTP Server (147.17.2.x:U>=1024 to 147.17.3.10:U123)
  - Syslog Server (147.17.2.x:T>1023 to 147.17.4.128:T514).
  - Workstations & PCs must use client ports (>1023) for all communication.
- Make sure that only traffic that is a response to a request from any of the workstations/internal PCs can reach machines in the Workstation Network (obviously some traffic must be permitted to reach Internal Router and machines in Server Network and

Admin Network)! You **must use reflexive ACLs** for this purpose. The only exception to this rule is remote access by admin PCs.

- Admin PCs (147.17.4.1-127) can remotely access any PC/Server in the Corporate Network via AnyDesk (147.17.4.1-127:T>=1024 to 147.17.x.x:T6568).
- Admin PCs cannot communicate with any outside machine.
- Syslog server cannot initiate communication to any machine outside the Admin Network. It can only receive Syslog messages and be contacted by business partner via SSH.
- Make sure to configure your ACLs such that some form of routing protocol (RIP, EGP, BGP or any other you like) can reach your routers.
- All other connections should be denied!

3. Deliverables

Submit a single (!) text file - please use a .txt extension and make sure it is a plain text file and not a word processor format. Your file should contain:

- Your name & student ID
- A **list of commands** you used to configure your Routers (creating the ACLs and assigning them to interfaces – no need to include interface setup). Please precede each line with a unique line-number for identification purposes (see point below) as outlined in the sample at the end of this project description. Make sure that you use a single, continuous set of line numbers – no line number should be repeated in your entire document!
- Please make sure to clearly indicate to which router the ACLs belong (Border Router or Internal Router).
- For each question in section “5. Firewall Evaluation Questions” detail which firewall rule(s) will be used to process the discussed traffic: If a packet is passed through a firewall, name all firewall rules (identified by their unique line number) that pass the packet. Similarly, if a packet is dropped by a firewall, name the firewall rule that drops the packet (add a comment the explains the reason for dropping). If a packet is processed by two or more ACLS, make sure to include all rules that process the packet. **For each passed** packet, name the firewall rule(s) that would process the corresponding return traffic (if any response is expected).

4. Deadline and Marking

Deadline for submission of your solution is **10:00h on Monday, 27th March**.

Where I have concerns about the originality of the submitted work, I reserve the right to conduct interviews (via MS Team or similar) with students, where marks will be adjusted correspondingly.

This project contributes 20% to the overall module mark.

These marks are distributed as follows:

Correct FW Evaluation: • evaluations that violate policy but are correct as per your ACL: half marks • ignoring return traffic: half marks	20 (1 mark each)
Penalties:	
ACL command syntax error	-10% each
Reflexive ACLs not used as requested	-30%
ACL not assigned to correct network interface	-2 mark each
Rule mistakes (e.g. rule order, policy violation not covered by evaluation questions, etc.)	Up to -50% per mistake (depending on severity)
No line numbers used	-50%
Line numbers not unique	-30%
Total:	20

5. Firewall Evaluation Questions

1. Machine 166.60.6.6:T4077 sends a HTTPS request to public web server 147.17.1.70:T443.
2. Machine 166.60.6.6 uses spoofed source IP address 147.17.2.10:T12345 to send a HTTPS request to Public Web Server 147.17.1.70:T443.
3. Machine 166.60.6.6 uses spoofed source IP address 172.16.1.1:T9834 to send a DNS request to DNS Server 147.17.1.50:T53.
4. Machine 4.14.54.33:T2233 sends a HTTP request to Web Server 147.17.1.70:T80.
5. Machine 123.5.4.3:T4321 sends a HTTPS request to Web Server 147.17.1.70:T443.
6. Machine 136.201.200.1:T6789 establishes a TCP connection to Syslog Server 147.17.4.128:T514.
7. Machine 136.201.200.1:T1023 establishes a TCP connection to Syslog Server 147.17.4.128:T514.
8. Router 4.4.4.4 uses your chosen routing protocol with suitable ports (if applicable) to send routing information to border router 10.10.10.10.
9. Web Server 147.17.1.70:T443 establishes a TCP connection to machine 211.4.3.2:T6789.
10. Web Server 147.17.1.20:T6789 establishes a TCP connection MySQL Database Server 147.17.3.20:T3360.
11. Web Server 147.17.1.20:T6789 establishes TCP connection to Syslog Server 147.17.4.128:T514.
12. Outside DNS Server 188.33.3.3:T10342 sends a DNS request to DNS Server 147.17.1.50:T53.
13. MySQL Database Server 147.17.3.20:T2233 sends a HTTPS request to Web Server 147.17.1.20:T443.

14. MySQL Database Server 147.17.3.20:T2233 establishes TCP connection to Syslog Server 147.17.4.128:T514.
15. PC 147.17.2.67:T1234 sends a HTTPS request to Web server 5.1.2.3:T443.
16. PC 147.17.2.201:T5555 establishes a connection to MySQL DataBase Server 147.17.3.20:T3360.
17. PC 147.17.2.123:T9237 contacts outside mail server 33.123.87.5:T25 on SMTP .
18. Machine 166.60.6.6 uses spoofed source IP address 20.1.1.1:T443 to send a HTTPS response to Internal PC 147.17.2.40:T9876 (without previous request).
19. Admin PC 147.17.50.10:T4408 establishes SSH session with DNS Server 147.17.1.50:T22.
20. Admin PC 147.17.50.60:8405 establishes AnyDesk Session with PC 147.17.2.121:T6568.

6. Sample List of Commands

```
(10) ip access-list extended inACL
(20) deny ip 1.0.0.0 0.255.255.255 any
(30) permit tcp 5.0.0.0 0.255.255.255 gt 1023 1.0.0.0 0.255.255.255 eq 22
(40) permit icmp 5.0.0.0 0.255.255.255 host 1.1.7.10 echo
(50) permit icmp any 1.0.0.0 0.255.255.255 echo-reply
(60) permit tcp any gt 1023 host 1.1.8.1 eq www
(70) permit tcp any eq www 1.0.0.0 0.255.255.255 gt 1023
(80) deny ip any any
(90) exit
(100) int FastEthernet0/0
(110) ip access-group inACL in
(120) exit
(130) ip access-list extended outACL
(140) permit …
```

Evaluation Question Samples:

Q: Machine 5.1.1.1:T9275 connects via ssh to PC 1.1.1.1:T22

A: Rule (30) on Border Router permits the packet to reach it's destination. Return traffic is permitted by (230)

Q: Outside machine 6.1.2.3 uses spoofed IP address 1.1.1.1:T2050 to connect to web server 1.1.8.1:T80.

A: Packet is denied by (20), which denies packets with source address from own range to enter network.