EE6042/ET4028 Host & Network Security

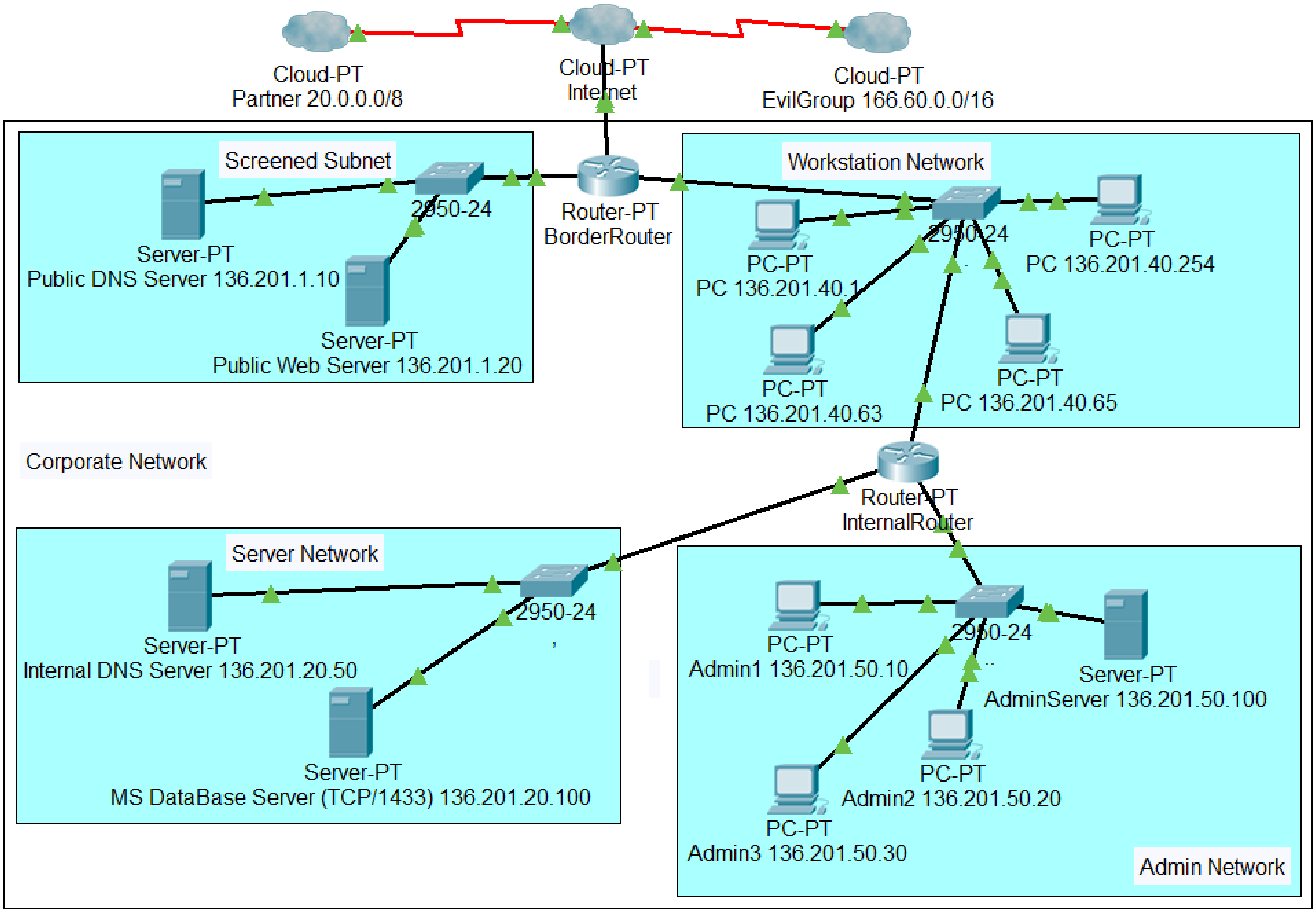
Firewall Assignment

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 as a new thread to the Firewall Assignment Questions & Answers forum on the SULIS page.

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 not mentioned in any other network.
- Partner (class A network 20.0.0.0/8): a business partner with privileged access rights.
- Evil Group (class B network 166.60.0.0/16): known to have malicious intent.
- Your own corporate network (class B network 136.201.0.0/16), which has the subnets 136.201.1.0/24 Screened Subnet, 136.201.20.0/24 Server Network, 136.201.40.0/24 Workstation Network and 136.201.50.0/24 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 136.201.1.200
- FastEthernet 2/0: Connected to the Workstation Network, IP address 136.201.40.200

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

- FastEthernet 0/0: Connected to the Workstation Network, IP address 136.201.40.201
- FastEthernet 1/0: Connected to the Server Network, IP address 136.201.20.200
- FastEthernet 2/0: Connected to the Admin Network, IP address 136.201.50.200

The Screened Subnet contains the following servers:

- Public DNS Server 136.201.1.10
- Public Web Server (HTTPS only) 136.201.1.20

The Workstation Network contains the following machines:

- Internal PCs and Workstations 136.201.40.1-254 (even though 136.201.40.200/201 are the interfaces of the routers, treat them as if they were PCs)

The Internal Server Network contains the following servers:

- Public DNS Server 136.201.20.50
- MS DataBase Server (MSSQL) 136.201.20.100

The Admin Network contains the following machines:

- Admin PCs 136.201.50.1-63.
- Admin Server 136.201.50.100

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 **any** machine in the corporate network (in the following items “everybody”/”any” excludes EvilGroup).
- Any outside machine can access Public DNS Server 136.201.1.10:T53. Machines are expected to use source port >= 1024 to connect to the Public DNS Server (any:T>=1024 to 136.201.1.10:T53).
- Public DNS Server can access any outside machine on TCP 53 (136.201.1.10:T>=1024 to any:T53) and also Internal DNS Server (136.201.1.10:T>=1024 to 136.201.20.50:T53). Only TCP requests are supported.
- Everybody (unless explicitly denied by other policy rules) can access the Web server 136.201.1.20 via HTTPS (TCP/443) only – make sure the client cannot use any server port (1-1023) (any:T>=1024 to 136.201.1.20:T443).
- Web server can only initiate connections to the DataBase Server (136.201.1.20:T>=1024 to 136.201.20.100:T1433). All other traffic originating in the web server **must be return traffic** to HTTPS requests.
- DataBase Server (136.201.20.100) can only be accessed by Web server (136.201.1.20), your own workstations (136.201.40.0/24) and your business partner (20.0.0.0/8) using MS SQL queries (machines:T>=1024 to 136.201.20.100:T1433). It can only react to requests and is not allowed to initiate any connections.
- Internal DNS Server 136.201.20.50 can only initiate connections to Public DNS Server (136.201.20.50:T>=1024 to 136.201.1.10:T53), receive (and respond to) requests from Public DNS Server (DNS, 136.201.1.10:T>=1024 to 136.201.20.50:T53) and from Workstations (136.201.40.x:T>=1024 to 136.201.20.50:T53).
- Internal PCs and Workstations in the Workstation Network can only access:
    - Any web server (including Public Web Server 136.201.1.20) via HTTPS (136.201.40.x:T>=1024 to any:T443).
    - Your own DataBase Server (136.201.20.100) for MS SQL queries (136.201.40.x:T>=1024 to 136.201.20.100:T1433).
    - Internal DNS Server (136.201.40.x:T>=1024 to 136.201.20.50:T53)
    - 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 (136.201.50.1-63) can remotely access any PC/Server in the Corporate Network via SSH (136.201.50.1-63:>=1024 to 136.201.x.x:T22) and Remote Desktop (136.201.50.1-63:T>=1024 to 136.201.x.x:T3389).
- Admin PCs cannot communicate with any outside machine.
- Admin Server (136.201.50.100) can only be accessed by Admin PCs. They cannot communicate with any machine outside the Admin Network.
- 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 next point) 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!
- 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. F**or 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 **17:00h (Irish Time!) on Wednesday, 6th April**.

Where I have concerns about the originality of the submitted work, I reserve the right to conduct interviews (via Skype, Zoom 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	-1 mark 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 136.201.11.20:T443.
2. Machine 166.60.6.6 uses spoofed source IP address 136.201.40.10:T12345 to send a HTTPS request to Public Web Server 136.201.1.20:T443.
3. Machine 166.60.6.6 uses spoofed source IP address 172.16.1.1:T53 to send a DNS request to Public DNS Server 136.201.1.10:T53.
4. Machine 4.14.54.33:T2233 sends a HTTP request to Web Server 136.201.1.20:T80.
5. Machine 123.5.4.3:T4321 sends a HTTPS request to Web Server 136.201.1.20:T443.
6. Machine 20.200.200.1:T6789 establishes a TCP connection to MS Database Server 136.201.20.100:T1433.
7. Machine 20.200.200.1:T1023 establishes connection MS Database Server 136.201.20.100:T1433.
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 136.201.1.20:T443 establishes a TCP connection to machine 211.4.3.2:T6789.
10. Web Server 136.201.1.20:T6789 establishes a TCP connection MS Database Server 136.201.20.100:T1433.
11. Public DNS Server 136.201.1.10:T5555 sends DNS request to outside DNS server 155.43.22.121:T53.
12. Public DNS Server 136.201.1.10:T1425 establishes TCP connection to MS Database Server 136.201.20.100:T1433.

13. Outside DNS Server 188.33.3.3:T10342 sends a DNS request to public DNS Server 136.201.1.10:T53.
14. Internal DNS Server 136.201.20.50:T20432 sends a DNS request to Public DNS Server 136.201.1.10:T53.
15. MS Database Server 136.201.20.100:T2233 sends a HTTPS request to Web Server 136.201.1.20:T443.
16. PC 136.201.40.10:T1234 sends a HTTPS request to Web server 5.1.2.3:T443.
17. PC 136.201.40.201:T5555 establishes a connection to DataBase Server 136.201.20.100:T1433.
18. Machine 166.60.6.6 uses spoofed source IP address 20.1.1.1:T443 to send a HTTPS response to Internal PC 136.201.40.40:T9876 (without previous request).
19. Admin PC 136.201.50.10:T4408 establishes SSH session with Public Web Server 136.201.1.20:T22.
20. Admin PC 136.201.50.60:8405 establishes Remote Desktop Session with PC 136.201.40.121:T3389.

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 …
```

7. Sample Answers:

Question x: Packet will be dropped by (80), as policy requests client to use port >=1024 as shown in rule (30).

Question y: Packet permitted by (60) and (170). Return packet permitted by (250) and (310).