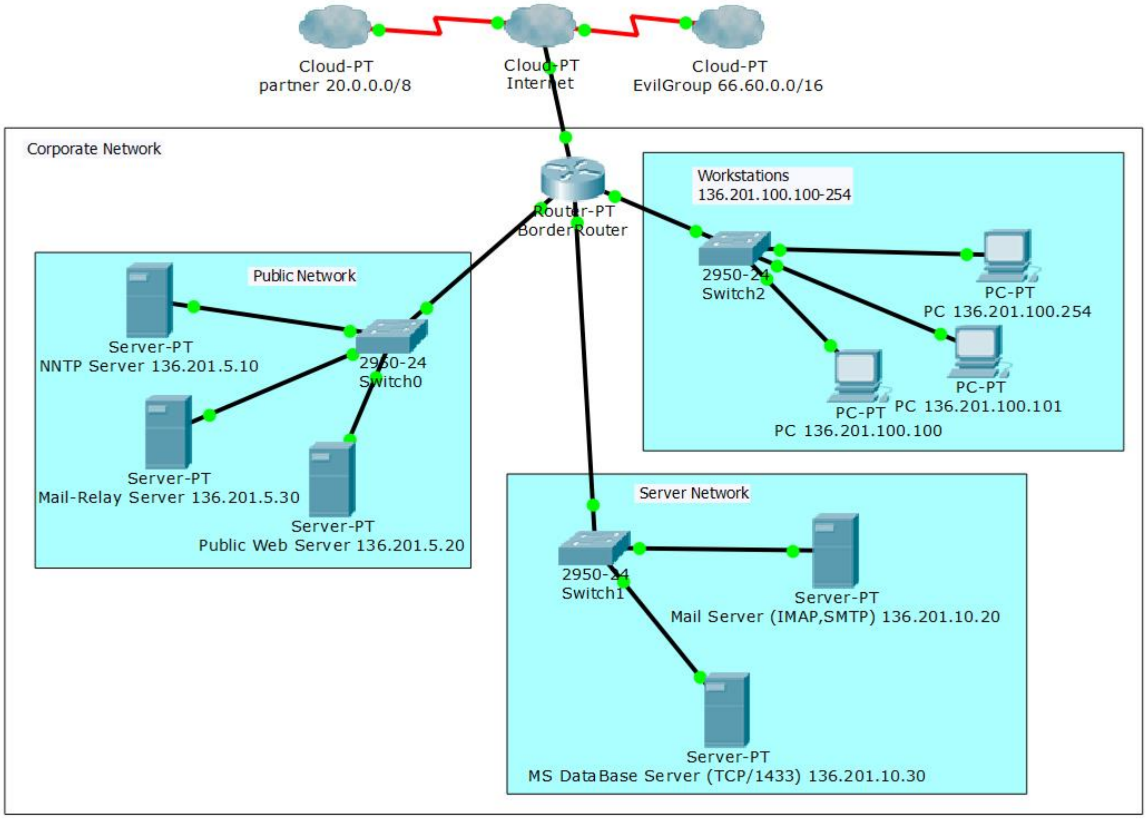
EE6042/ET4028 Host & Network Security
Project I – Cisco Access Control Lists

In this project you are asked to configure ACLs for a Cisco Packet Filter Firewall.

1. Task

Consider the following network:



This network has the following components:

- The Internet: any machine.
- Partner (class A network 20.0.0.0/8): a business partner with privileged access rights.
- Evil Group (class B network 66.60.0.0/16): known to have malicious intent.
- Your own corporate network (class B network 136.201.0.0/16), which has the following subnets:
    - 136.201.5.0/24 Public Servers
    - 136.201.10.0/24 Internal Servers
    - 136.201.100.0/24 Workstations

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

- GigabitEthernet 0/0: Connected to the ISP (Internet), IP address 10.10.10.10
- FastEthernet 1/0: Connected to the Public Network, IP address 136.201.5.100
- FastEthernet 2/0: Connected to the Workstation Network, IP address 136.201.100.1
- FastEthernet 3/0: Connected to the Server Network, IP address 136.201.10.100

Your task is to configure the router to implement the following security policy (only IPv4 needs to be considered) - use reflexive ACLs where appropriate:

- Perform sensible ingress and egress filtering (as discussed in the lecture).
- All devices from EvilGroup are denied access to any machine in the corporate network (in the following items “everybody”/”any” excludes devices from EvilGroup).
- Any outside machine can access Mail Relay server 136.201.65.30 via SMTP (on port TCP/25).
- Relay Mail server 136.201.65.30 can access any (outside) machine and Mail Server (136.201.10.20) via SMTP (port TCP/25).
- Everybody can access the Web server 136.201.5.20 at port TCP/80 – make sure the client cannot use any server port (1-1023)
- Any outside machine can access the NNTP (Network News) server 136.201.5.10 on ports TCP/119 and TCP/433.
- NNTP server 136.201.5.10 can only initiate connections to other machine on port TCP/433.
- Web server can only initiate connections to the DataBase Server (136.201.10.30:1433). All other traffic from the web server must be return traffic to previous requests.
- Only machines in the workstation subnet can access Mail Server via IMAP (on port TCP/143).
- Mail server (136.201.10.20) can access Relay Mail server via SMTP (port TCP/25)
- DataBase Server (136.201.10.30) can only be accessed by Web server (136.201.5.20), your own workstations (136.201.100.0/24) and your business partner (20.0.0.0/8) using SQL queries (TCP/1433). It can only react to incoming requests and is not allowed to initiate any connections.
- Workstations (136.201.100.0/24) can access:
    - Any web server on ports TCP/80, TCP/8080 and TCP/443.
    - Your own DataBase server (136.201.10.30) for SQL queries (TCP/1433).
    - Only the business partner’s DNS server 20.1.1.1 for DNS queries (TCP/53 and UDP/53)
    - Mail server (136.201.10.20) for IMAP and SMTP.
    - NNTP (136.201.5.10) server on port TCP/119

  Make sure that only traffic that is a response to a request from any of the workstations can reach this sub-network! You **must use reflexive ACLs** for this purpose.
- Create your own policy for the ICMP protocol (as outlined below, you need to justify your ICMP policy).

- Allow some form of routing protocol (RIP, EGP, BGP or any other you like) to reach your router.
- All other connections should be denied!

2. Instructions

- Each student has to submit her/his own solution.
- Implement ACLs to achieve the behaviour as outlined above and assign the ACLs to the corresponding interfaces.

3. Deliverables

Submit a single (!) text file (please use a .txt extension) containing:

- Your name & student ID
- A section containing **the list of commands** you used to configure your Border Router (including configuration of interfaces, creating the ACLs and assigning them to interfaces). **Do not include** the networks partner, Internet or EvilGroup.
- A section explaining for each item in the security policy above how/where (i.e. which rule(s) at what interface(s)/direction) it is implemented.
- A section discussing your ICMP protocol policy (including a justification why your policy is a sensible policy) and how you implemented it.
- A section explaining what routing protocol you selected and what ACL rules you have added ensure that it works properly.

4. Deadline and Marking

Deadline for submission of this project is **5pm on Friday, 07.04.2017**. Please submit your solution via the module’s SULIS page. This project contributes 15% to the overall module mark. These marks are distributed as follows:

Configuration command syntax ok:	4
Security Policy fully implemented:	7
ICMP policy (implementation & justification):	2
Routing protocol implemented:	2
Total:	**15**

Please submit any questions/queries as a new thread to the Questions & Answers forum on the SULIS page.