

C2107 Tutorial 6 (Network Security+Access Control)

School of Computing, NUS

March 17, 2021

Background on port number. Some students haven't completed module on Networking and may not be familiar with the role of port numbers in server-client connection. In almost all connection, there is a server and a client. The server provides a service and waiting/listening for entities to connect, whereas the client is the one who initiates the connection and request for that service. The service offered by a server can be connected through some predefined port number. E.g. consider the email SMTP server. The server listens to port number 25. If a client wants to connect to the server for SMTP, the client will initiate a connection by sending packets to the server's ip address at port 25. The server responds by sending packets to the client's ip address at another port number (greater than 1023) selected by the client.

Hence, if the client sends a packet to the SMTP server, the destination port of that packet must be 25, but the source port can be any number greater than 1023 selected by the client. Conversely, packets sent by the SMTP server have source port 25, and the destination port is the one specified by the client.

The number "25" for SMTP server is an informal standard. A server can choose whatever port number, as long as its clients know about it. Since it is difficult to announce the port number, servers accessible to the public typically use the standard port number. Potentially, an entity can set up a SMTP server with port number 12332 (just some arbitrary number) and set up its own "private" network of email services. There are methods that attempt to use the port number as a form of secret key—only those who know the port number can connect. Such methods can achieve some form of secrecy but not fool-proof (there are many ways to get that port number).

1. You are the system administrator of a new secondary school and your first task is to design the network and the firewall. You have decided to have 2 to 3 firewalls.

The machines in the network include:

- (a) **Lab.** There is a total of around 100 machines in a few labs for students to prepare report, search for materials in the web, etc. There are network printers in the Lab.
- (b) **Teachers.** Every teacher has a PC in the teacher room. The teachers use the PC to enter students' grades, sending/receiving emails, preparing teaching materials, printing exam questions, web-search, etc. There are network printers in the teacher rooms.
- (c) **Web-server.** School's web server.
- (d) **Email-server.** School's SMTP email server.

- (e) **SQL-server**. This is a SQL-server which stores the students database. Some of the information can be accessed through a web-based application hosted in the Web-server (for e.g. allowing student to update their mobile phone number via web-based application). Some information can only be accessed by the teachers.

There is a list of multiple firewall rules in a table. Each rule occupies a row in the table. Ten entries in a row are:

<i>src ip</i>	<i>dest ip</i>	<i>src port</i>	<i>dest port</i>	<i>direction</i>	<i>action</i>
---------------	----------------	-----------------	------------------	------------------	---------------

- (a) *Action*. Either **Block** or **Allow**.
- (b) *src ip*. A set of source ip addresses. It can be specified using the above predefined names in a boolean expression. For e.g. “**Email-server**”. You are free to define other names, e.g. “**Internal**” to be all machines in the school.
- (c) *dest ip*. A set destination ip addresses. Similarly, it can also be a set of predefined names given above.
- (d) *source-port, destination-port*. The port number of the source and destination. Note that services use some predefined port numbers. The firewall recognises some fixed port number like **HTTP**, **SMTP**, **LPR**, **SQL**. (Note: **LPR** is a network printing protocol listening to port number 515.)
- (e) *direction*. This can be **IN** or **OUT**. The firewall divides the network into two sectors, say S_1 , and S_2 . The field indicate which direction the packet is moving, either from S_1 to S_2 or the other way. Your design has to indicate the meaning of **IN** and **OUT**.

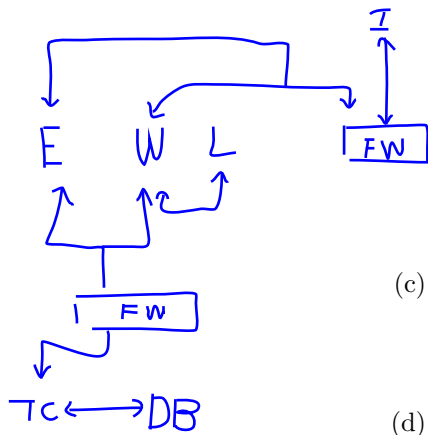
Same as the example in the lecture note, when a packet arrives, action of the first rule that matches the packet applies. For example, the three rules

<i>src ip</i>	<i>dest ip</i>	<i>src port</i>	<i>dest port</i>	<i>direction</i>	<i>action</i>
Web-Server	*	HTTP	*	OUT	Allow
*	Web-Server	*	HTTP	IN	Allow
*	*	*	*	*	Block

allows packets sent from the **Web-Server** to any other ip addresses, and block everything else. (Note that the symbol “*” matches to anything).

Remarks and Requirements.

- (a) It is important to prevent cases that exam questions get mistakenly printed in the Lab.
- (b) It is important to protect the SQL server.



- (c) We know that source ip addresses can be spoofed. The school is worry that some students are running some attack tools that generate spoofed ip-address. Hence they want to block outbound packets from the school that are not having legitimate source ip-addresses.
- (d) In this question, we ignore the issue on routing. So, we do not consider the gateway and Network Address Translation. For simplicity, just assume all are “public ip-addresses”.

What would be a reasonable partition of the networks and the rules of the firewalls?

2. Facebook has many users. There are many objects, including posts and images. Let’s use the images as example. **How does a user specify who can view the image uploaded by the user?** There is some form of “role-based” access control. **What is that?**

(As a computing students, even if you prefer not to have a Facebook account, it would be good to create a dummy account so as to know what’s happening there.)