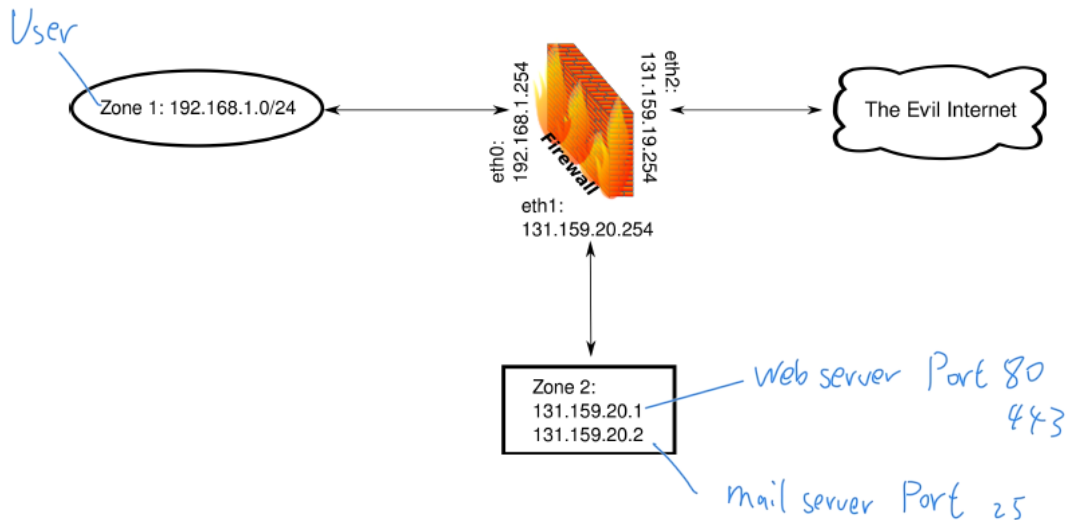# COMP9121 Week 12

1. We will practice firewall configuration in this task. The figure below shows the configuration you want to achieve. In Zone 2, you've got one Web server (131.159.20.1) on TCP ports 80 and 443, and one mail server (131.159.20.2) on TCP port 25. Your home users reside in Zone 1.

Your security policy is as follows:

1. Your home users may freely access any Web service, anywhere, on ports 80 and 443, but only if they initiate the connection themselves (i.e. they are allowed to browse the Web). No-one outside Zone 1 can initiate connections to Zone 1, on any port.

2. Everyone, including the Evil Internet, can access the web server (both ports) and mail server in Zone 2. However, no host in Zone 2 can initiate connections anywhere else.

To save you some writing, you can refer to the IP ranges (source and destination) by their 'zone names'. Use 'Ext' if you want to refer to the Evil Internet, 'Zone 1' if you want to refer to the IP range of Zone 1 etc.

Complete the table to define a stateless firewall configuration for the given scenario.

Interface	Source IP	Destination IP	Source Port	Destination Port	ACK	Action
Eth0	Zone1	*	*	80, 443	Any	allow
Eth1	Zone2	Zone1	80, 443	*	Set	allow
Eth2	Ext	Zone1	80, 443	*	Set	allow
Eth2	Ext	131.159.20.2	*	25 mail	Any	allow
Eth1	131.159.20.2	Ext	25 mail	*	Set	allow
Eth2	Ext	131.159.20.1	*	80,443 web	Any	allow
Eth1	131.159.20.1	Ext	80, 443 web	*	Set	allow
Eth0	Zone1	131.159.20.2	*	25 mail	Any	allow
Eth1	131.159.20.2	Zone1	25 mail	*	Set	allow
*	*	*	*	*	*	Deny

(handwritten annotations)

Web server Port 80 443
mail server Port 25

Z1 → Z2 & Ext
Z2 → Z1
Ext → Z1
Ext → Z2
Z2 → Ext
Ext → Z2
Z2 → Ext
Z1 → Z2
Z2 → Z1

Q1
Q2

Any: Can establish connection
Set: Cannot establish connection by itself, can only reply