Case Study

Fully Unreal Reality (FUR) is a growing enterprise in need of a new design for their network. FUR now specialises in virtual reality headsets and is an industry leader in this field. Along with this, FUR has branched out further into VR games, becoming an industry leader in using haptic feedback to imitate human touch in games. They have excelled in creating cheap, but high quality, virtual reality headsets and haptic suits for gaming consoles and PC gamers.

FUR have decided to move their headquarters, opting for a more modern and liveable location: Mawson Lakes Technology Park (Tech Park). This has put them in the difficult position of needing a network built for their new headquarters and their branch offices to be upgraded. FUR's previous head office in Sydney will become a branch office. Their Adelaide CBD branch office will move to Tech Park and will require significant upgrades to support the number of staff and devices.

FUR currently has the following staffing requirements for each department:

Sydney (the current HQ)

Department	Team	Staff	Expected Growth in 5 Years
Human Resources & Finance	-	25	Limited.
Design and Development	Software Engineering	53	At least 30%.
	Game Design	11	At least 30%.
	VR Game Design	15	At least 50%.
	Quality Assurance	5	Limited.
	Research	2	Limited.
Art	Concept Art	5	At least 10%.
	3D Modelling	13	At least 15%.
	3D Printing	14	At least 40%.
Virtual Reality	Research	41	At least 50%.
	Innovate	33	At least 30%.
	Prototype	12	At least 50%.
Product	Custom Support	120	At least 25%.
	Marketing	22	At least 10%.

Melbourne Branch Office

Department	Team	Staff	Expected Growth in 5 Years
Human Resources & Finance	-	5	Limited.
Design and Development	Software Engineering	23	Limited.
	Game Design	5	At least 10%.
Art	Concept Art	3	At least 30%.
	3D Modelling	7	At least 10%.
Product	Custom Support	15	At least 40%.
	Training	2	At least 10%.

Adelaide

Department	Team	Staff	Expected Growth in 5 Years
Human Resources & Finance	-	2	At least 20%.
Design and Development	Game Design	11	At least 30%.
	VR Game Design	2	At least 40%
	Quality Assurance	1	At least 20%
Art	3D Modelling	4	Limited.
	3D Printing	10	Limited.
Virtual Reality	Research	11	Limited.
	Innovate	15	Limited.
Product	Marketing	5	At least 10%.

FUR has a few servers at each company location: Web, File and Email. Servers should all have externally accessible IP addresses. Servers should be in a DMZ zone; this means that a server should not be able to ping/access internal devices unless the internal device initiates the connection. You are not required to provide any IP addressing for devices, simply referring to them by their name ("Sydney Concept Art PC", "Melbourne Product Customer Support PC") is sufficient.

Certain teams should also not be able to contact other teams. A list of general security policies (not business policies, firewall policies) include:

- HR should not be accessible by any team.
- The entire Virtual Reality (VR) department should not be contactable from any other team.
    - Teams inside the VR department should be able to contact each other.
- VR Game Design team should be accessible to only the Game Design team.
    - The Game Design team should still have access to everything else.
- All departments should have access to the Internet. Certain limitations apply:
    - The VR department should have no access to Bandwidth Consuming, Potentially Liable, Security Risk, and Unrated web filter categories.
    - The Art department should have no access to Social Networking.
    - The entire company should have no access to: Adult/Mature Content, Security Risk categories.
    - Social networking should be restricted to 30 minutes a day for every department except Art.

- Virtual Reality is high-bandwidth capable and as a result, traffic from the Virtual Reality department to anywhere should be guaranteed 1000Mbps.

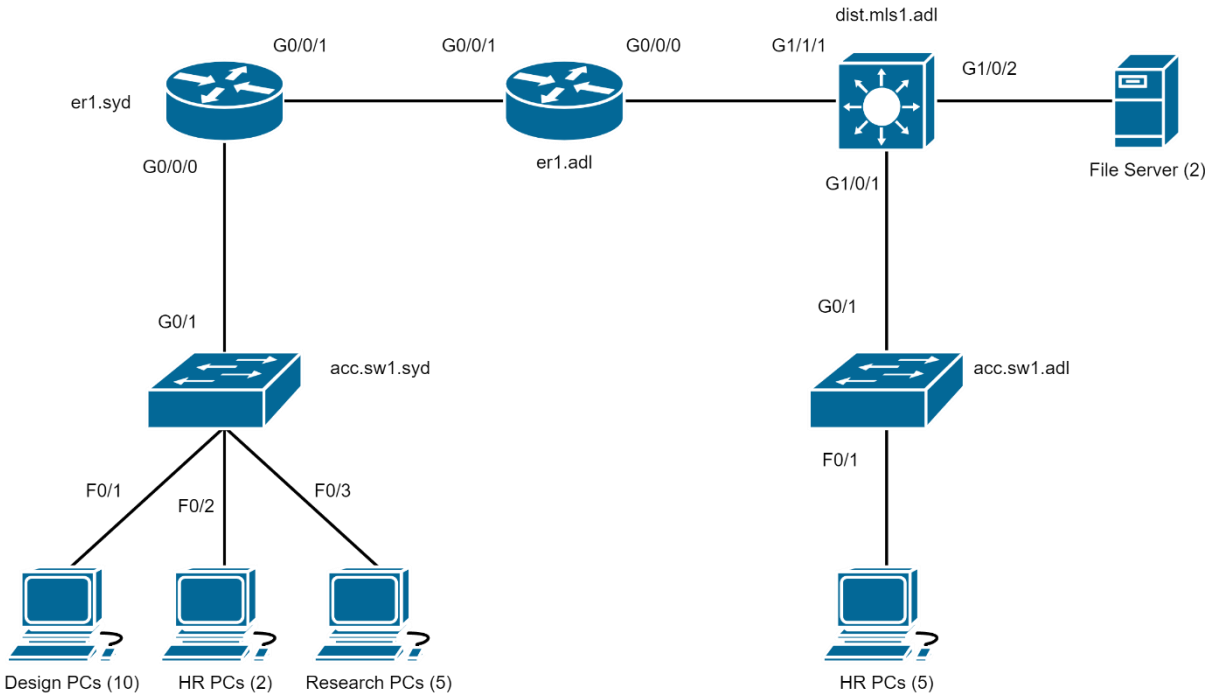
Your role in this is to be the network consultant, providing a new network design, equipment list, security policies and traffic flow diagrams. This new design should support the expected growth in 5 years, as shown above. You need to calculate the new headquarter staff numbers. Staff are not expected to be made redundant in the transition to Tech Park. You are free to base the Sydney branch office staffing levels off Adelaide/Melbourne's current staffing levels.

Network Design

You are required to create a logical network diagram for the entire new network. This means that Sydney will be a branch office in your diagram and Tech Park will exist.

This course does not have a pre-requisite that contains information on network design, as such, it is not expected of you to include any IP addressing in your logical network diagram. It is however expected that you include some aspects of network design, such as a two-tier or three-tier system and give reason as to why you chose one over the other. An example of a logical diagram without IP addressing is shown below.

This diagram SHOULD NOT be used as a complete diagram. This diagram also does NOT contain firewalls. Your final diagram SHOULD contain firewalls.



Remember, you are marked on completeness, suitability, scalability, security, redundancy. If you are not familiar with network design, please find the video titled "Network Design" on the Assignment tab to assist you.

Your logical diagram should be drawn using Draw.IO (https://app.diagrams.net/). You may opt to use Lucidcharts or Visio, you will probably find Draw.IO the easiest.

You are given significant freedom in what you choose to do in terms of design, link speeds and hostnames. Keep all decisions appropriate to the case study, include justifications and assumptions.

Draft Security Policies & Traffic Flow for Tech Park Headquarters (~500 words[2])

After you have decided on your new design it is time to write your draft security policies and illustrate how the network will work with the draft security policies implemented. **You only need to create these policies, use cases, and traffic flow diagrams for the new Tech Park Headquarters.**

Your draft security policies should be written like how you would write a firewall policy (they will be implemented as firewall policies in Part 3). These draft security policies should take the form of a table. The format of the table is up to you to decide on and make. All policies should use the same table format.

Traffic flow diagrams should clearly illustrate how traffic will move throughout the network in different use cases. At the very least a traffic flow diagram should show:

- Who initiated the connection in the use case (Concept Art? Product Customer Support?),
- Where the traffic flow is allowed to go,
- Where the traffic flow is not allowed to go.

You will need to create more than one traffic flow diagram. You may find it easiest to write several use cases to show network activity ("HR connects to the Internet", "VR connects to the Art department") and then draw traffic flow diagrams based off the use cases. Ensure the use cases are included in your traffic flow supporting document.

Equipment List (~250 words[3])

The second task in this part is to create an equipment list. This may take the form of paragraphs for each device or a table which cleanly outlines the equipment that has been chosen for the new network design.

Equipment for this new network should include:

- Networking devices (NOT consumer-based devices, enterprise vendors only):
    - Routers,
    - Layer 3 switches,
    - Layer 2 switches.
- Firewall appliances (these MUST be Fortinet).
- Prices for the above
    - Licensing
    - Hardware

[2] **Note:** word count is a guide, do not treat it as a maximum or required number. You may go over or under this word count as much as you wish.

[3] **Note:** word count is a guide, do not treat it as a maximum or required number. You may go over or under this word count as much as you wish.

The equipment list **should not include**:

- Printers,
- Servers,
- Other end devices.

All equipment choices should be justified and compared to other potential solutions. All choices should also be researched, particular attention should be paid to the port speeds, density, and compatibility with Fortinet. It is not appropriate to state, “Because it will work well for this company”.

Your equipment list should include references, you might find footnotes to be particularly suitable. A footnote should include a link to the website/resource and the date you viewed it.

Implementation using Netlab/Remotelab

As a part of the new design FUR wants to see the implementation of your security policies on a simulated environment. For this we will use Netlab/Remotelab which you have all used for your practicals. Your implementation will be different depending on your design you have created above. You will be marked by the consistency between your security policies (firewall policies) that you have implemented on Netlab and the listed policies in Part 2 of the assignment.

Netlab has a standardised pod design that cannot be changed. As a result of this, you are not required to create a complete, functioning network. You will, however, implement certain aspects of your design. You should use the Local-FortiGate device (access through the Local-Client machine) to implement the following:

- The security policies you have create
- Web filter profile(s) – these should be applied to the appropriate firewall policy as well,
- App control profile(s) – these should be applied to the appropriate firewall policy as well,
- Traffic shaping profile(s),
- Relevant IP address objects – **IP addresses are not marked, but you will need to create IP address objects identifying the devices to use in your policies,**
- SNAT/DNAT.

You are required to create screenshots of your implementation (GUI and/or CLI) and organise them in a Word document for submission. Be careful to include all details in your screenshots, you may need to take more than one screenshot for the feature implemented. A short description for each screenshot or section should clearly tell the reader what part is being implemented.