A detailed Implementation Guide for the Network Security Policies created to support the relocation of the FUR Headquarters from Sydney to Tech Park.

Network Security Using Fortinet

By Saadullah Sajjad

Executive Summary

This document is an implementation guide for the network security policies developed for the new FUR infrastructure. In cohesion with the network design and equipment list, this document provides the application of Fortinet firewall policies, and a guideline on how they were installed on the NETLAB environment. This report addresses the Tech Park's network and its subnets.

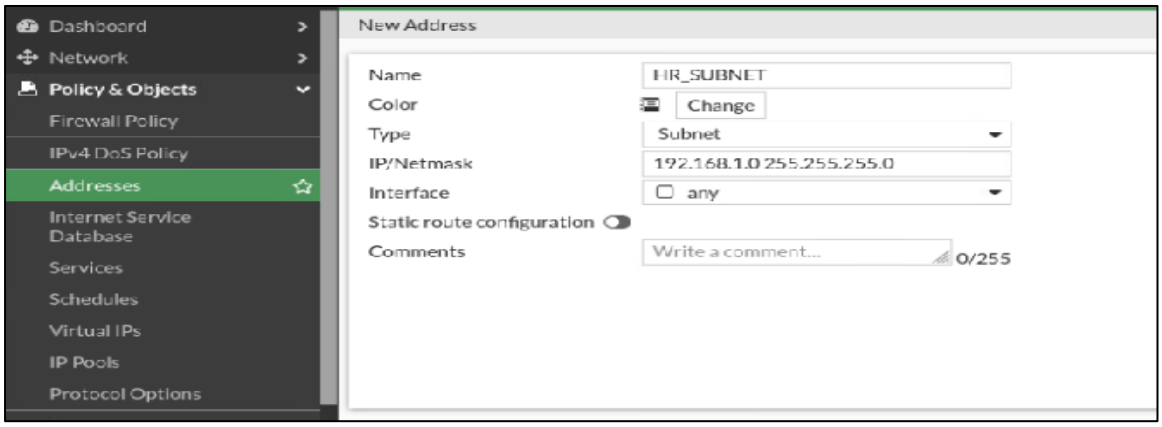
The document is structured as follows:

1. Creation of IP Address Objects of each team on the network using NETLAB.
2. Security Policy creation, which consists of 11 policies. Each policy may have one or more of the following sub-sections:
    a. Security Policy
    b. NETLAB Implementation
    c. Web Filter
    d. Traffic Flow Diagram
    e. Security Profile
    f. Web Filter Profile
3. The last section in the document contains the screenshots of the DNAT & SNAT configuration in NETLAB.

IP Address Object Creation

Below is a list of all departments in the new Tech Park headquarters. Each team in a department has been assigned an IP Address object that represents it on the network to other devices. The table under each heading defines the values of the object, accompanied by a screenshot of the required implementation on the Local-Fortinet device.

To avoid repetition, the screen shot below of the HR & Finance IP Address Object creation, will be referred to for all other IP Address Object creations listed. To access this webpage, click the *Policy & Objects* tab on the left side panel and then proceed to the *Addresses* tab highlighted in the screenshot.



From there, follow the data in each table as detailed below and enter the values in their respective fields. Don't forget to save each object by pressing the *OK* button at the bottom of the page.

1. **HR & Finance**

Field	Value
Name	HR_SUBNET
Type	Subnet
IP/Netmask	192.168.1.0/24
Interface	any

2. **Software Development**

Field	Value
Name	SOFTWARE_SUBNET
Type	Subnet
IP/Netmask	192.168.2.0/24
Interface	any

3. **Game Design**

Field	Value
Name	GAME_DESIGN_SUBNET
Type	Subnet
IP/Netmask	192.168.3.0
Interface	any

4. **Quality Assurance**

Field	Value
Name	QUALITY_ASSURANCE_SUBNET
Type	Subnet
IP/Netmask	192.168.4.0
Interface	any

5. **3D Modelling**

Field	Value
Name	3D_MODELLING_SUBENT
Type	Subnet
IP/Netmask	192.168.5.0
Interface	any

6. **3D Printing**

Field	Value
Name	3D_PRINTING_SUBNET
Type	Subnet
IP/Netmask	192.168.6.0
Interface	any

7. **Research**

Field	Value
Name	RESEARCH_SUBNET
Type	Subnet
IP/Netmask	192.168.7.0
Interface	any

8. **Innovate**

Field	Value
Name	INNOVATE_SUBNET
Type	Subnet
IP/Netmask	192.168.8.0
Interface	any

9. **Customer Support**

Field	Value
Name	CUSTOMER_SUPPORT_SUBNET
Type	Subnet
IP/Netmask	192.168.9.0
Interface	any

10. **Marketing**

Field	Value
Name	MARKETING_SUBENT
Type	Subnet
IP/Netmask	192.168.10.0
Interface	any

11. **VR Game Design**

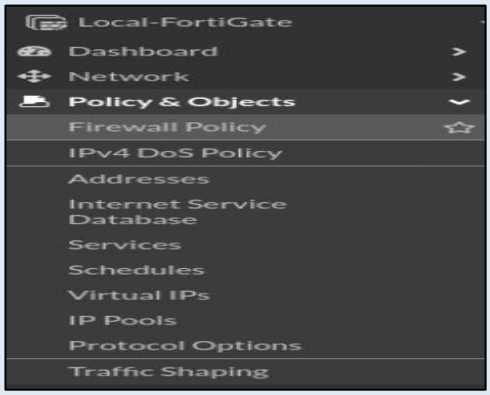
Field	Value
Name	VR_GAMEDESIGN_SUBENT
Type	Subnet
IP/Netmask	192.168.11.0
Interface	any

Security policies

Below are some security policy requirements provided to us by FUR, accompanied with screenshots of our implementation of them on the NETLAB environment. The example table below shows what each field value represents in this section. The screenshots of implementing these policies are added at the bottom of each table.

Field	Description
Name	*Name of firewall policy*
Incoming Interface	*Interface receiving traffic*
Outgoing Interface	*Interface sending traffic*
Source	*Source subnet*
Destination	*Destination subnet*
Schedule	*Determine the time policy will remain active*
Service	*Networking Protocols*
Action	*BLOCK or ALLOW policy*
NAT	*ON or OFF*

Additionally, a *Traffic Flow Diagram* is included for each security policy, along with a brief use case, to provide a visualisation of this policy in action.



ACCESSING THE FIREWALL POLICY TAB

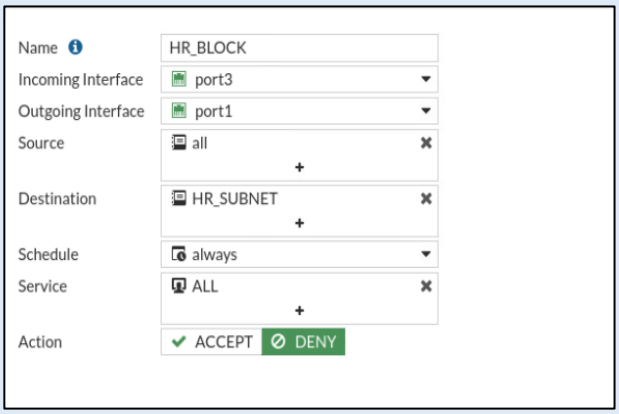
Select the ***Policy & Object*** tab located on the left side panel of the Local-FortiGate GUI to expand it. Then select the ***Firewall Policy*** tab.

1. Blocking Access to the HR & Finance Department

- Security Policy:

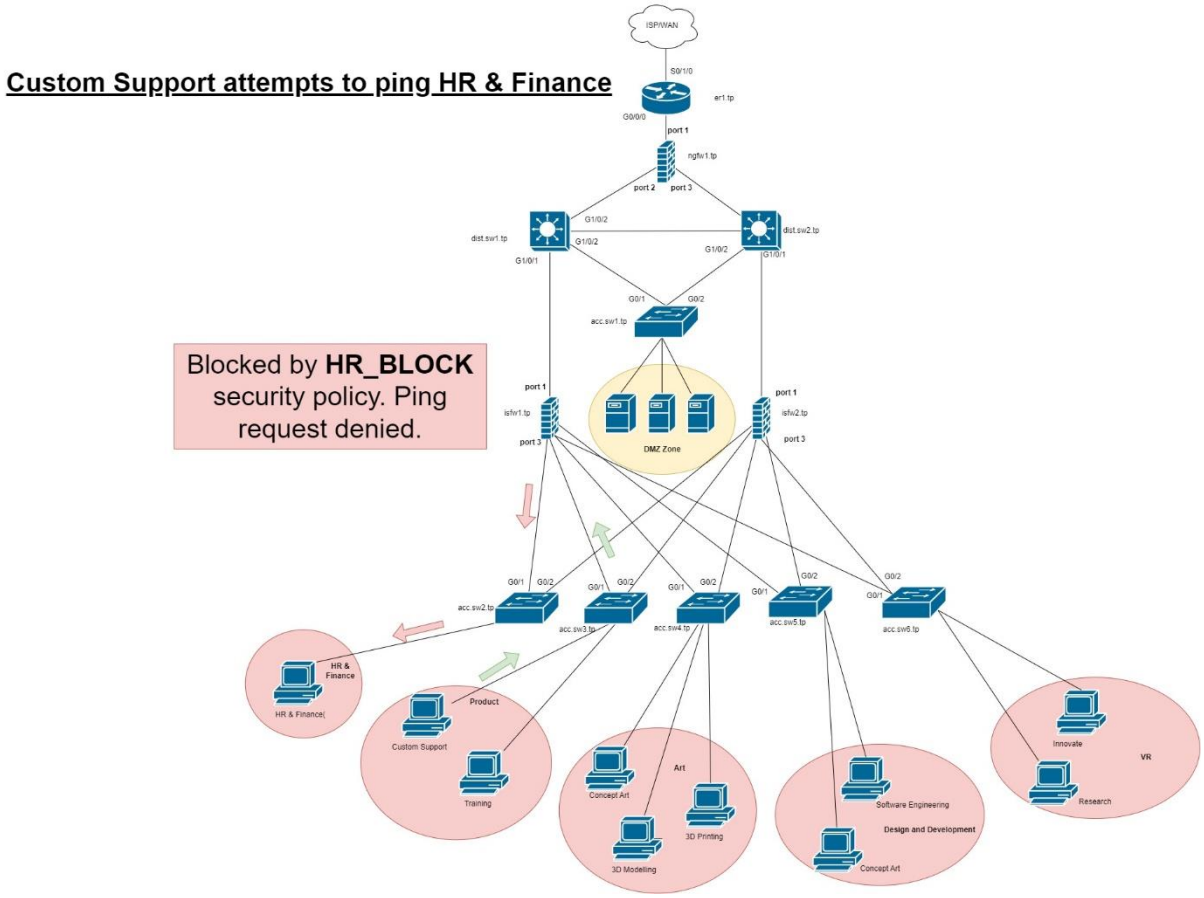
Field	Value
Name	**HR_BLOCK**
Incoming Interface	port3
Outgoing Interface	port1
Source	All
Destination	HR_SUBNET
Schedule	Always
Service	All
Action	DENY
NAT	Enable

- NETLAB Implementation:



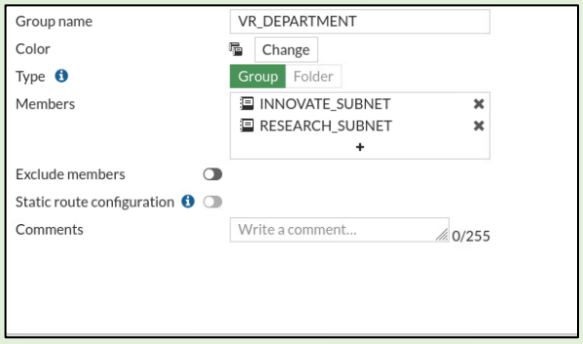
This firewall policy will deny all packets with any protocols from reaching the ***HR_SUBNET***. This policy is scheduled to be in affect at all times when it is enabled.

- Traffic Flow Diagram:



2. Block external access to the VR Department

- Address Group Creation:

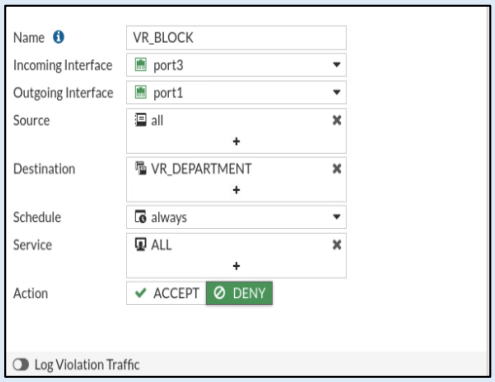


Before applying the firewall policy, we will create an ***Address Group*** to combine the ***INNOVATE_SUBNET*** with the ***RESEARCH_SUBNET.*** We will call this ***VR_DEPARTMENT.***

- Security Policy #1:

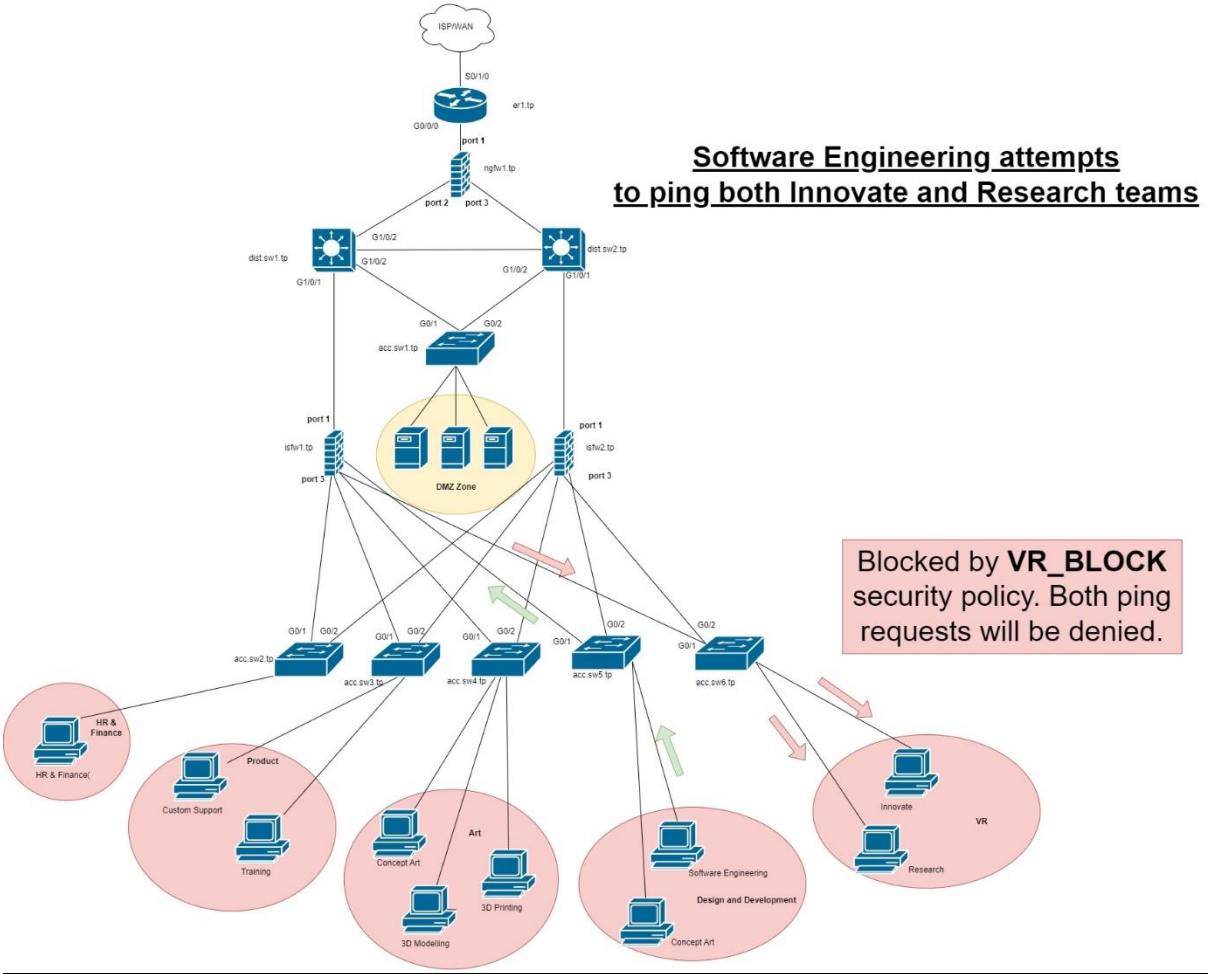
Field	Value
Name	**VR_BLOCK**
Incoming Interface	port3
Outgoing Interface	port1
Source	All
Destination	VR_DEPARTMENT
Schedule	Always
Service	All
Action	DENY
NAT	Enable

- NETLAB Implementation:



This policy will ***DENY*** all traffic of any protocol to the subnets present in the ***VR_DEPARTMENT.*** This policy is scheduled to be in affect at all times when it is enabled.

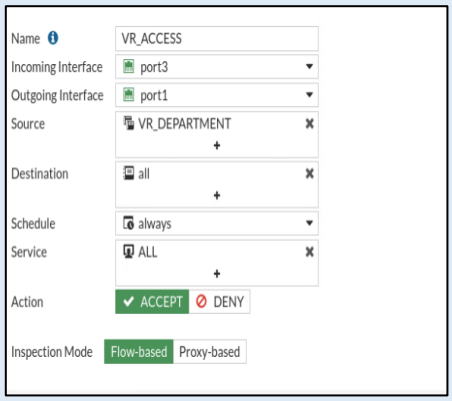
- Traffic Flow Diagram:



- Security Policy #2:

Field	Value
Name	**VR_ACCESS**
Incoming Interface	port3
Outgoing Interface	port1
Source	VR_DEPARTMENT
Destination	All
Schedule	Always
Service	All
Action	DENY
NAT	Enable

- NETLAB Implementation:



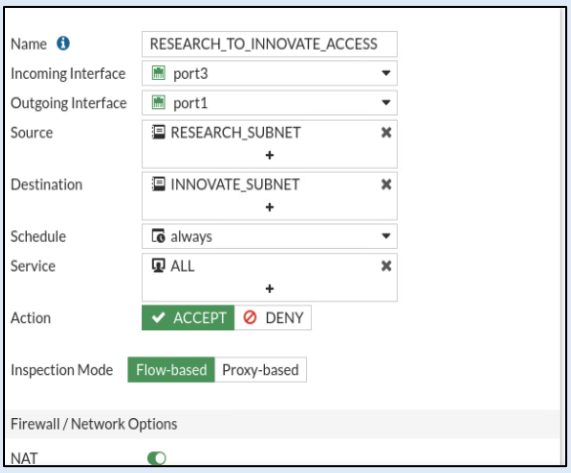
This policy will ***ALLOW*** all traffic of any protocol originating from the ***VR_DEPARTMENT***, to any other subnet on the network. This policy is scheduled to be in affect at all times when it is enabled.

3. Allow Internal Access Within The VR Department

- Security Policy #1:

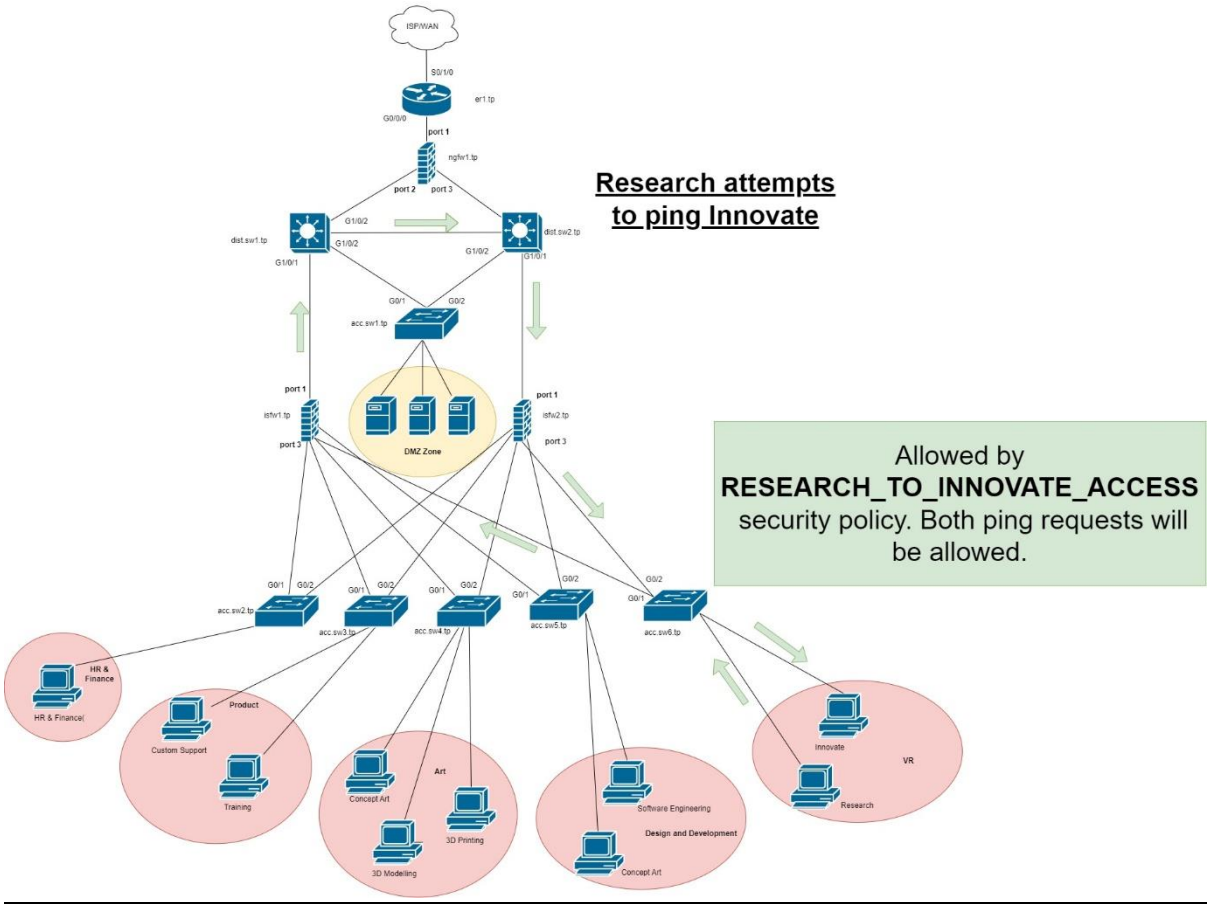
Field	Value
Name	**RESEARCH_TO_INNOVATE_ACCESS**
Incoming Interface	port3
Outgoing Interface	port1
Source	RESEARCH_SUBNET
Destination	INNOVATE_SUBNET
Schedule	Always
Service	All
Action	ACCEPT
NAT	Enable

- NETLAB Implementation:



This policy will ***ALLOW*** all traffic of any protocol originating from the ***RESEARCH_SUBNET***, to the ***INNOVATE_SUBNET***, hence providing internal access within the ***VR DEPARTMENT***. This policy is scheduled to be in affect at all times when it is enabled.

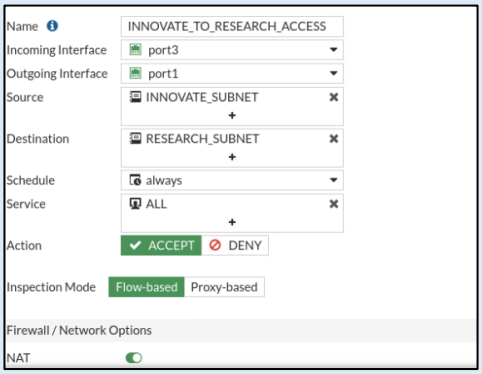
- Traffic Flow Diagram:



- Security Policy #2:

Field	Value
Name	**INNOVATE_TO_RESEARCH_ACCESS**
Incoming Interface	port3
Outgoing Interface	port1
Source	INNOVATE_SUBNET
Destination	RESEARCH_SUBNET
Schedule	Always
Service	All
Action	ACCEPT
NAT	Enable

- NETLAB Implementation:



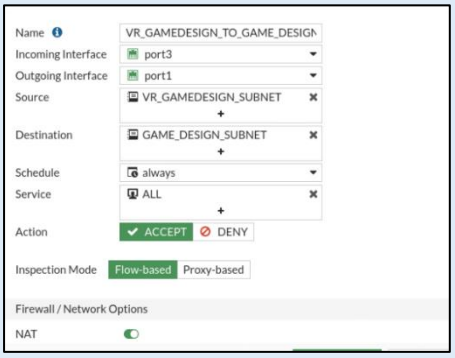
For traffic to flow both ways through a firewall, the firewall policy must be configured to allow for traffic to flow in ***both directions***. We will repeat the policy created above but this time, we will ***switch*** the ***Source*** and ***Destination*** values.

4. Blocking all external access to VR Game Design (excluding the Game Design team)

- Security Policy #1:

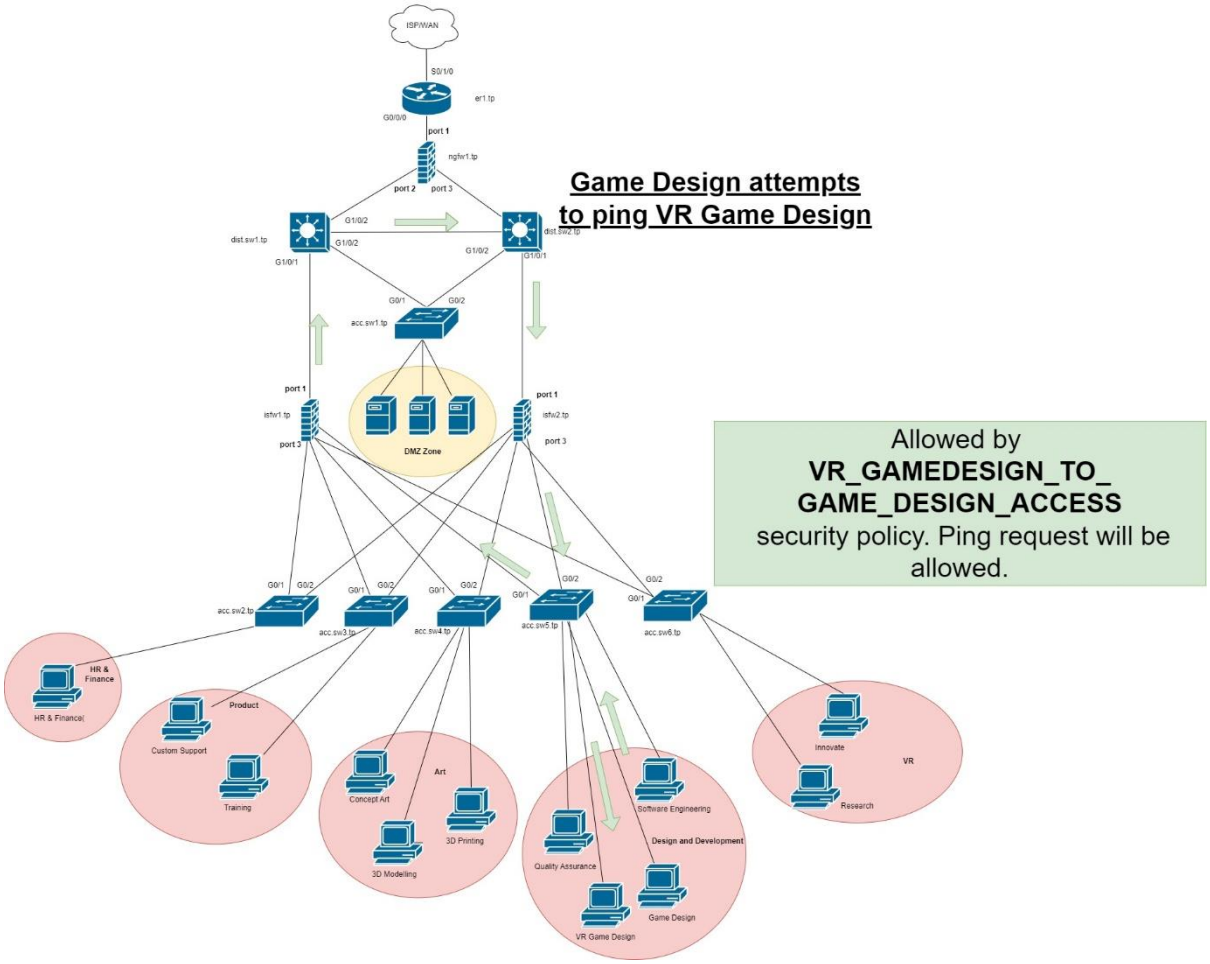
Field	Value
Name	**VR_GAMEDESIGN_TO_GAME_DESIGN_ACCESS**
Incoming Interface	port3
Outgoing Interface	port1
Source	VR_GAMEDESIGN_SUBNET
Destination	GAME_DESIGN_SUBNET
Schedule	Always
Service	All
Action	ACCEPT
NAT	Enable

- <u>NETLAB Implementation:</u>



Allow the ***GAME_DESIGN_SUBNET*** to contact the ***VR_GAMEDESIGN_SUBNET*** via any protocol. This policy is scheduled to be in affect at all times when it is enabled.

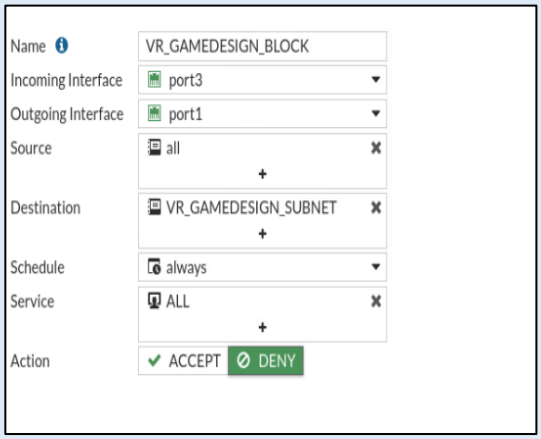
- <u>Traffic Flow Diagram:</u>



- Security Policy #2:

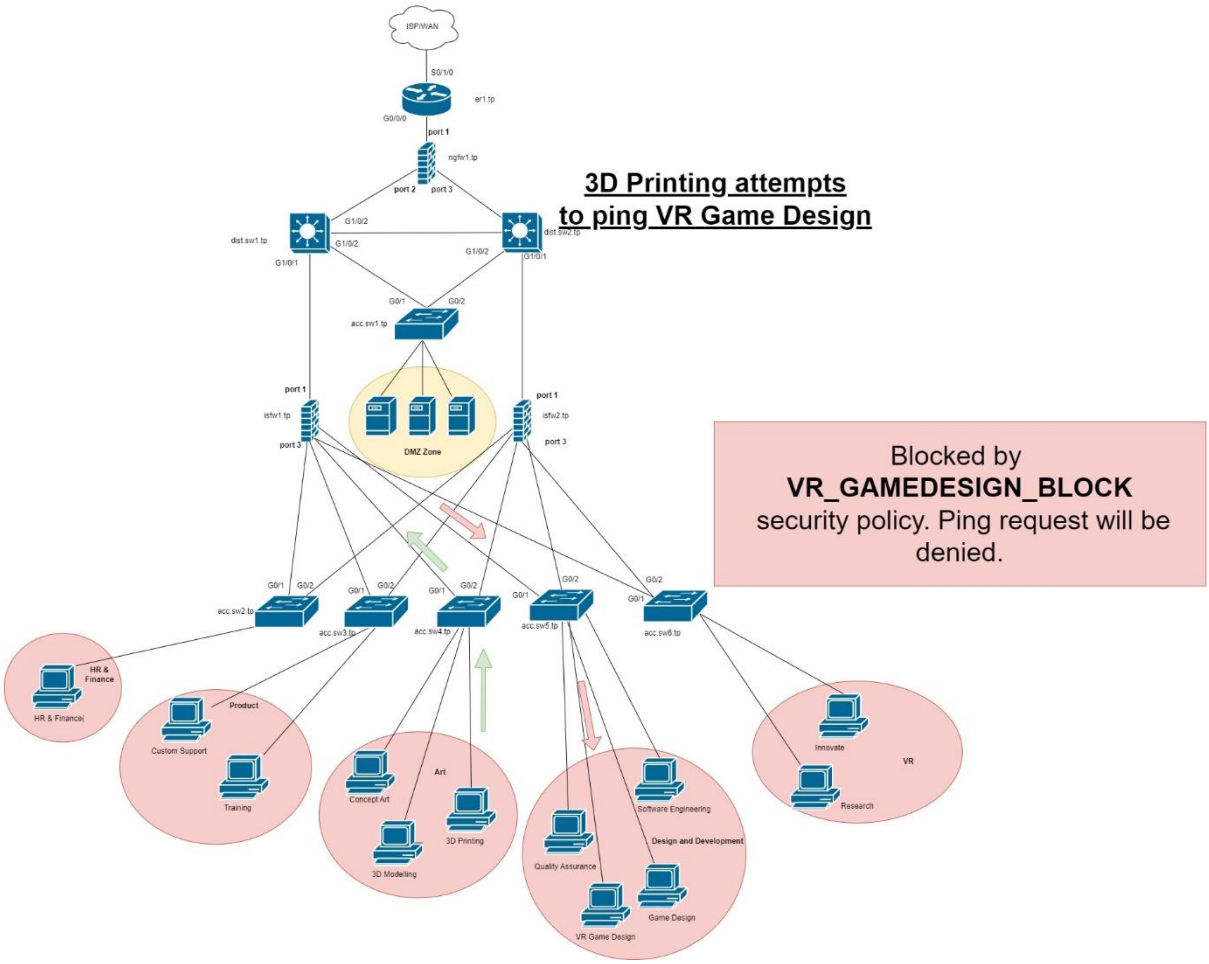
Field	Value
Name	**VR_GAMEDESIGN_BLOCK**
Incoming Interface	port3
Outgoing Interface	port1
Source	ALL
Destination	VR_GAMEDESIGN_SUBNET
Schedule	Always
Service	All
Action	DENY

- NETLAB Implementation:



DENY ALL subnets on the Tech Park network from contacting the ***VR_GAMEDESIGN_SUBNET*** via any protocol. This policy is scheduled to be in affect at all times when it is enabled.

- Traffic Flow Diagram:



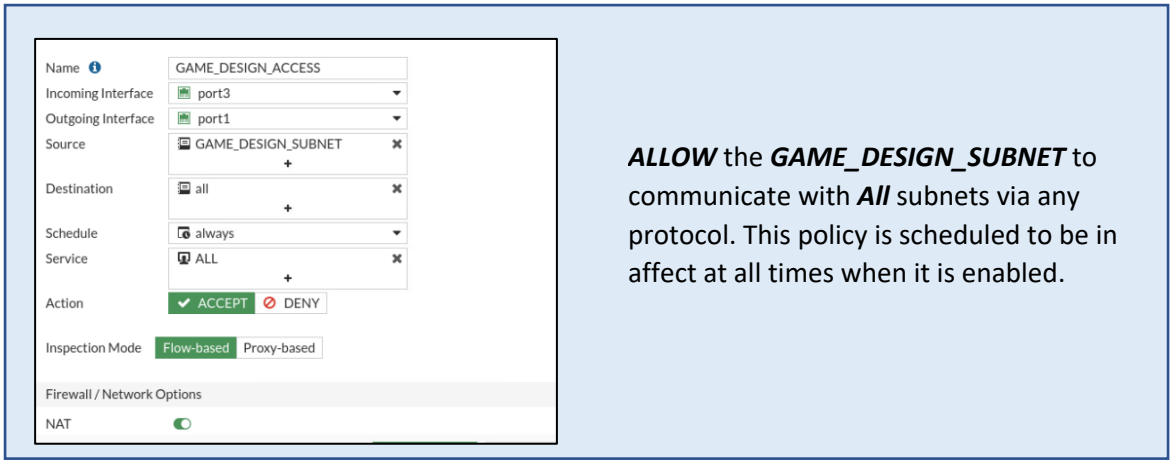
---

5. Allow the Game Design team to have access to external subnets

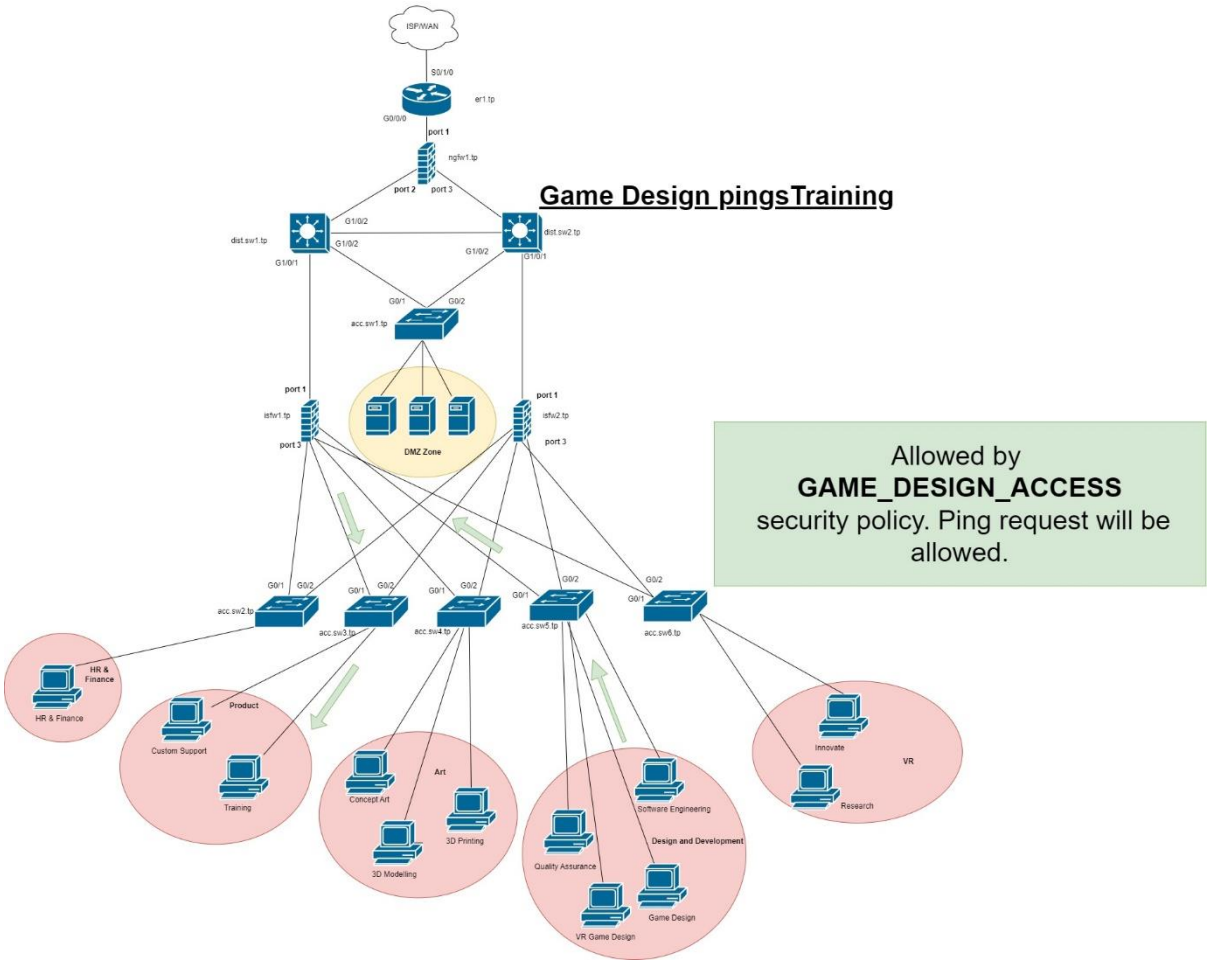
- Security Policy:

Field	Value
Name	GAME_DESIGN_ACCESS
Incoming Interface	port3
Outgoing Interface	port1
Source	GAME_DESIGN_SUBNET
Destination	All
Schedule	Always
Service	All
Action	ACCEPT
NAT	Enable

- NETLAB Implementation:

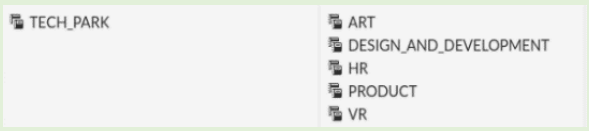


- Traffic Flow Diagram:



6. Allowing Internet access to all departments

- Creating the *TECH_PARK* Address Object:



Creating the ***TECH_PARK*** Address Object that contains all the department's subnets combined within one object. This makes it easier to manage and implement.

- Security Policy:

Field	Value
Name	INTERNET_ACCESS
Incoming Interface	port3
Outgoing Interface	port1
Source	TECH_PARK
Destination	All
Schedule	Always
Service	ALL_ICMP, HTTP, HTTPS, DNS, SSH
Action	ACCEPT
NAT	Enable

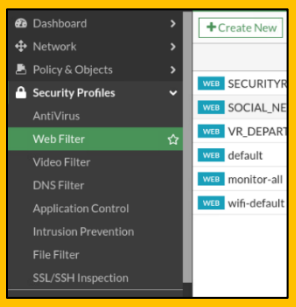
- NETLAB Implementation:

Creating the ***INTERNET_ACCESS*** policy which will allow ***TECH_PARK*** to communicate with all other networks, including the internet, which is connected to the outgoing ***Port1*** interface. For Internet Access, we have defined ***ALL_ICMP, DNS, HTTP, HTTPS*** and ***SSH***, which are web protocols that handle Internet traffic. This policy is scheduled to be in affect at all times when it is enabled.

7. Apply Web Filters to the VR Department

To apply web filters on a firewall policy, we must follow the process detailed below:

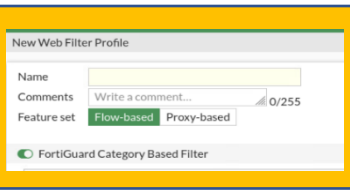
1. Create a new Web Filter:



1)Navigate to the *Security Profiles* tab on the left panel and click to expand it.

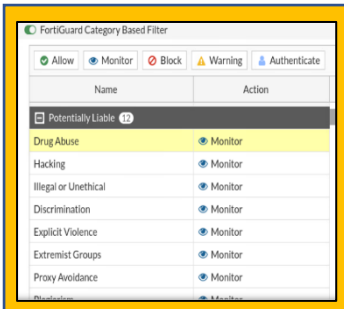
2)Select the *Web Filter* option highlighted in the screenshot.

3)Click the *Create New* icon shown on the top, right-side of the screenshot.



In the *Name* field, add a name for the web filter.

2. Choose the category you want to filter:



1)Enable the *FortiGuard Category Based Filter to view the categories*

2)Select a value under a category you want to filter. In the case of the screenshot, we have selected *Drug Abuse* under the *Potentially Liable* category.

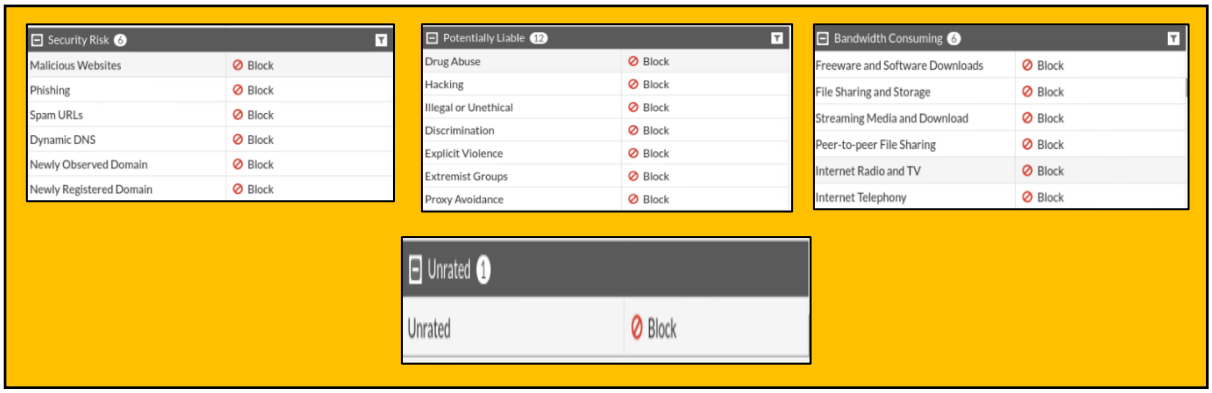
3)Select the value you wish to filter, then select either the *Allow, Monitor, Block, Warning or Authenticate* options shown at the top of the screen shot.

If *Block* is selected, the result will be visible as in the screenshot.

We have used the above steps to create the web filters for our policies. The table below outlines the values we entered to create our *VR_DEPARTMENT_RESTRICTIONS* web filter, for the implementation of our web filters

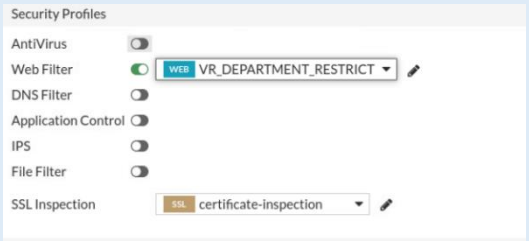
Field	Value
Name	VR_DEPARTMENT_RESTRICTIONS
FortiGuard Category Based Filter	Enable
Security Risk	Block all entries
Potentially Liable	Block all entries
Unrated	Block all entries
Bandwidth Consuming	Block all entries

Once the above table has been implemented, the *FortiGuard Category Based Filter*, will look like this:



- <u>Security Policy for Web Filtering:</u>

  We created a new Firewall Policy named *VR_DEPARTMENT_RESTRICTIONS*, that would implement the Web Filter policy created in the previous section. The implementation process is the same as those of the Firewall Policies created earlier. However, we must map the *Web Filter* we created to this policy, as shown below:



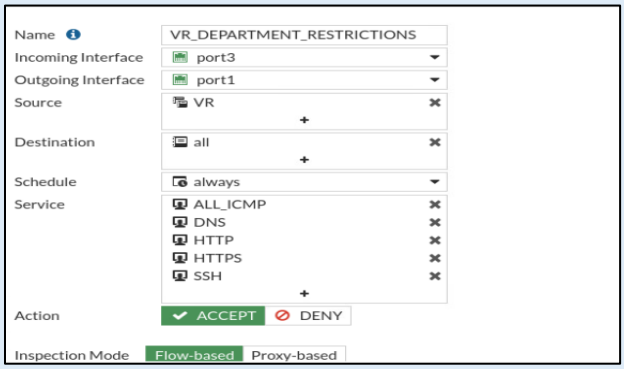
1)Under the *Security Profiles* section in the Firewall Policy, *enable Web Filter*.

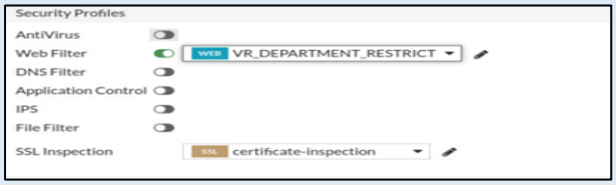
2)Then show the *VR_DEPARTMENT_RESTRICTIONS* option from the drop down menu next to it.

To finish creating the policy, enter the values from the following table:

Field	Value
Name	VR_DEPARTMENT_RESTRICTIONS
Incoming Interface	port3
Outgoing Interface	port1
Source	VR
Destination	All
Schedule	Always
Service	ALL_ICMP, HTTP, HTTPS, DNS, SSH
Action	ACCEPT
NAT	Enable
Web Filter	VR_DEPARTMENT_RESTRICTIONS

- NETLAB Implementation:





Creating the ***VR_DEPARTMENT_RESTRICTIONS*** policy, which will allow the ***VR*** Department to communicate with all other networks, including the internet. For Internet Access, we have defined ***ALL_ICMP, DNS, HTTP, HTTPS*** and ***SSH***, which are web protocols that handle Internet traffic. This policy is scheduled to be in affect at all times when it is enabled

Additionally, the ***VR_DEPARTMENT_RESTRICTIONS*** *Web Filter*, is also applied to restrict access to specific sites outlined by FUR.

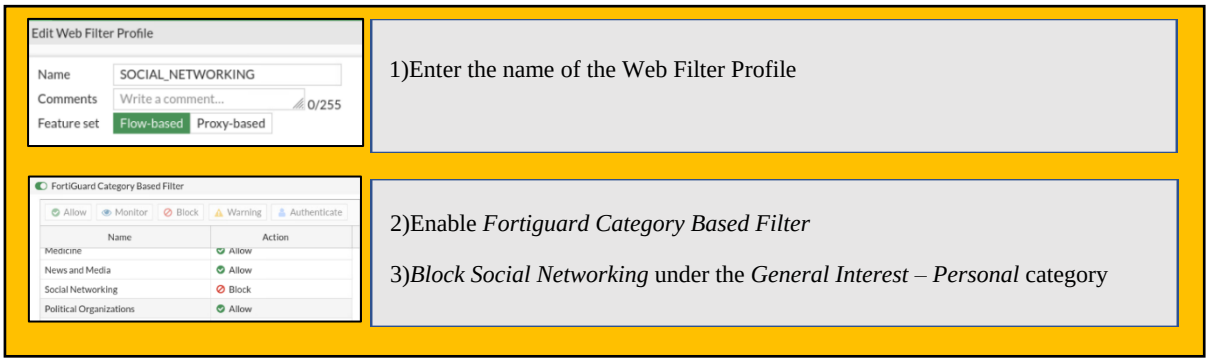
8. Block Social Networking Sites for the Art Department

- Create Web Filter:

We created a new Web Filter with the following values:

Field	Value
Name	SOCIAL_NETWORKING
FortiGuard Category Based Filter	Enable
General Interest -Personal	Social Networking - Block

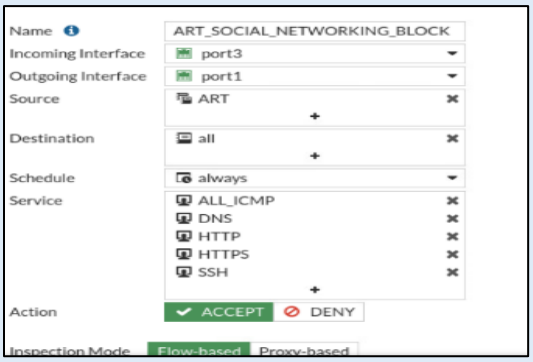
- NETLAB Implementation:



- Security Profile for Web Filtering

Field	Value
Name	ART_SOCIAL_NETWORKING_BLOCK
Incoming Interface	port3
Outgoing Interface	port1
Source	ART
Destination	All
Schedule	Always
Service	ALL_ICMP, HTTP, HTTPS, DNS, SSH
Action	ACCEPT
NAT	Enable
Web Filter	SOCIAL_NETWORKING

- NETLAB Implementation:



Creating the ***ART_SOCIAL_NETWORKING_BLOCK*** policy, which will allow the ***ART*** Department to communicate with the internet. For Internet Access, we have defined ***ALL_ICMP, DNS, HTTP, HTTPS*** and ***SSH***, which are web protocols that handle Internet traffic. This policy is scheduled to be in affect at all times when it is enabled

The ***SOCIAL_NETWORKING*** *Web Filter*, is also applied to restrict access to social networking sites.

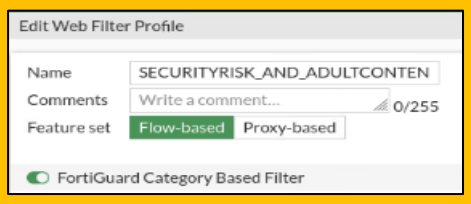
9. Block Tech Park Access to Adult/Mature Content and Security Risk categories.

To block access to restricted sites in all the departments at Tech Park, we will reuse the ***TECH_PARK*** Address Object that we created containing all its department's subnets.

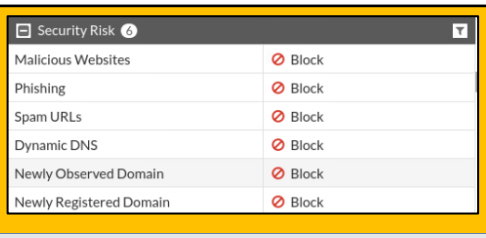
- Create Web Filter:

Field	Value
Name	SECURITYRISK_AND_ADULTCONTENT
FortiGuard Category Based Filter	Enable
Security Risk	Block all entries
Adult/Mature Content	Block all entries

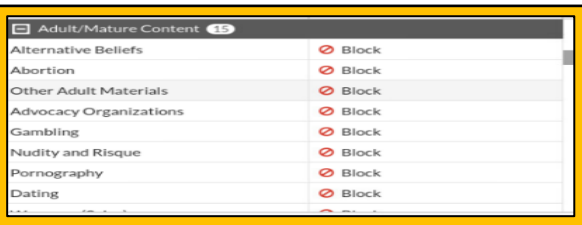
- NETLAB Implementation:



Enter the name of the *Web Filter* and enable the *FortiGuard Category Based Filter* as shown



Block all entries under the *Security Risk* Category



Block all entries under the *Adult/Mature Content* Category

- Security Profile for Web Filtering

Field	Value
Name	SECURITYRISK_AND_ADULTCONTENT_BLOCK
Incoming Interface	port3
Outgoing Interface	port1
Source	TECH_PARK
Destination	All
Schedule	Always
Service	ALL_ICMP, HTTP, HTTPS, DNS, SSH
Action	ACCEPT
NAT	Enable
Web Filter	SECURITYRISK_AND_ADULTCONTENT

- NETLAB Implementation:

Creating the ***SECURITYRISK_AND_ADULTCONTENT_BLOCK*** policy, which will allow all the departments under the ***TECH_PARK*** Address Group to communicate with the internet. For Internet Access, we have defined ***ALL_ICMP, DNS, HTTP, HTTPS*** and ***SSH***, which are web protocols that handle Internet traffic. This policy is scheduled to be in affect at all times when it is enabled.

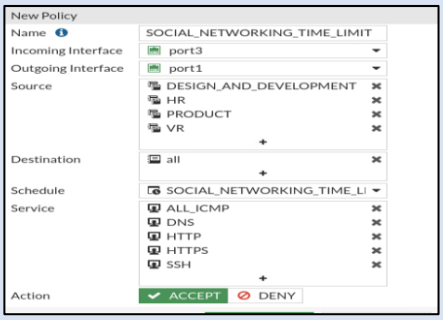
To apply the ***SECURITYRISK_AND_ADULTCONTENT*** Web Filter, we will enable the option on the left and select from the drop-down menu next to it.

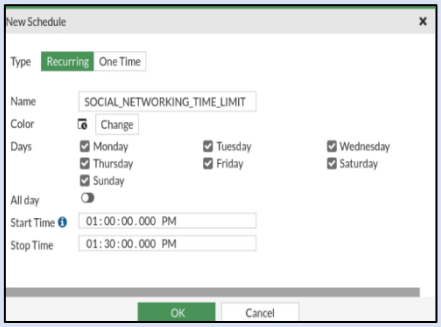
10. Applying a Schedule for Social Networking Usage for all Departments excluding Art

- Security Profile:

Field	Value
Name	SOCIAL_NETWORKING_TIME_LIMIT
Incoming Interface	port3
Outgoing Interface	port1
Source	VR PRODUCT HR DESIGN_AND_DEVELOPMENT
Destination	All
Schedule	Create a New Recurring Schedule
Service	ALL_ICMP, HTTP, HTTPS, DNS, SSH
Action	ACCEPT
NAT	Enable
Web Filter	SECURITYRISK_AND_ADULTCONTENT

- NETLAB Implementation:





Creating the ***SOCIAL_NETWORKING_TIME_LIMIT*** policy, which will allow all the departments, excluding ***Art***, to communicate with the internet. For Internet Access, we have defined ***ALL_ICMP, DNS, HTTP, HTTPS*** and ***SSH***, which are web protocols that handle Internet traffic. The scheduled of this policy is mapped to the ***SOCIAL_NETWORKING_TIME_LIMIT*** as created in the second screenshot on the left.

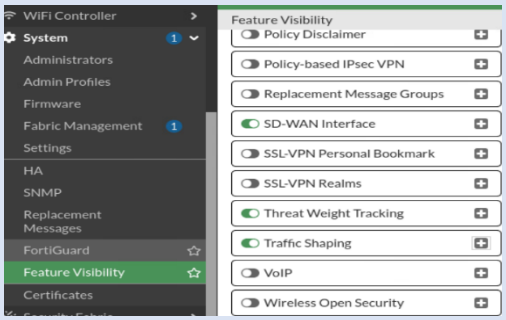
In the ***New Policy*** section, after selecting the ***Schedule*** drop-down menu, we hit ***Create,*** followed by the ***Recurring Schedule*** option. This brought us to the page shown on the screenshot towards the left. We then gave it the name ***SOCIAL_NETWORKING_TIME_LIMIT*** and we ticked all the ***Days***. We selected the ***Start Time*** as ***1:00 pm*** and ***End Time*** as ***1:30 pm***. As this is a ***Recurring Schedule,*** it will continue indefinitely as long as the policy is active.

To apply the ***SOCIAL_NETWORKING*** Web Filter that we had created earlier, we will enable the Web Filter option on the left and select from the drop-down menu next to it.

11. Creating a Traffic Shaper to Guarantee Bandwidth Originating from the VR Department

In order to set *Maximum* and *Guaranteed* bandwidth values, we created a *Traffic shaper* in *NETLAB* as shown below.

- NETLAB Implementation:

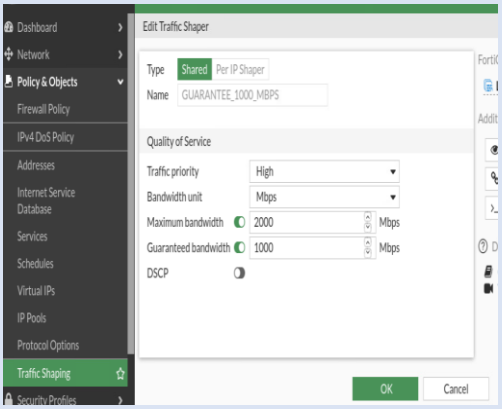


We must first enable Traffic Shaping on our firewall GUI. On the left-side panel, go to:

1)*System*

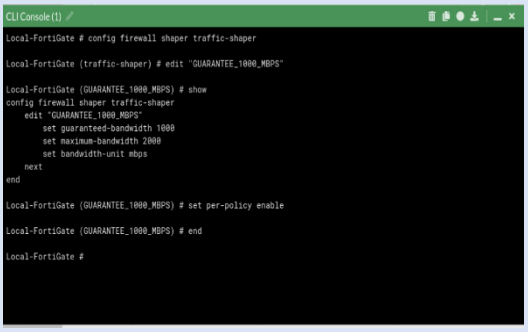
2)*Feature Visibility*

Then Enable *Traffic Shaping* under *Additional Features*



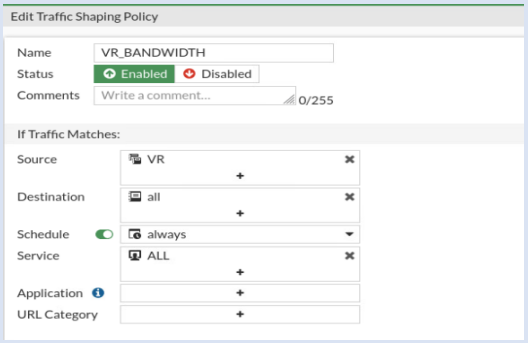
To create a new *Traffic Shaper Profile*, go to:

1)Policy & Objects
2)Traffic Shaping
3)Create New
4)Name: ***GUARANTEE_1000_MBPS***
5)Traffic Priority: ***High***
6)Bandwidth Unit: ***Mbps***
7)*Maximum Bandwidth:* ***2000***
8)*Guaranteed Bandwidth:* ***1000***



Once the profile is created, right-click it and select *Edit in CLI*. Alternatively, we can log into the Local-FortiGate CLI in NETLAB. Enter the following command to enable traffic shaping to occur per policy:

set per-policy enable



Then we created a new *Traffic Shaping Policy* that will be applied to the ***VR*** Department:

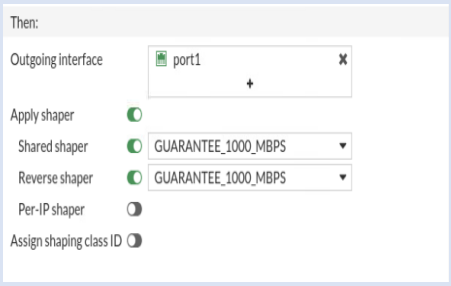
1)Name: ***VR_BANDWIDTH***

2)Status: ***Enabled***

3)Source: ***all***

4)Schedule: ***always***

5)Service: ***ALL***



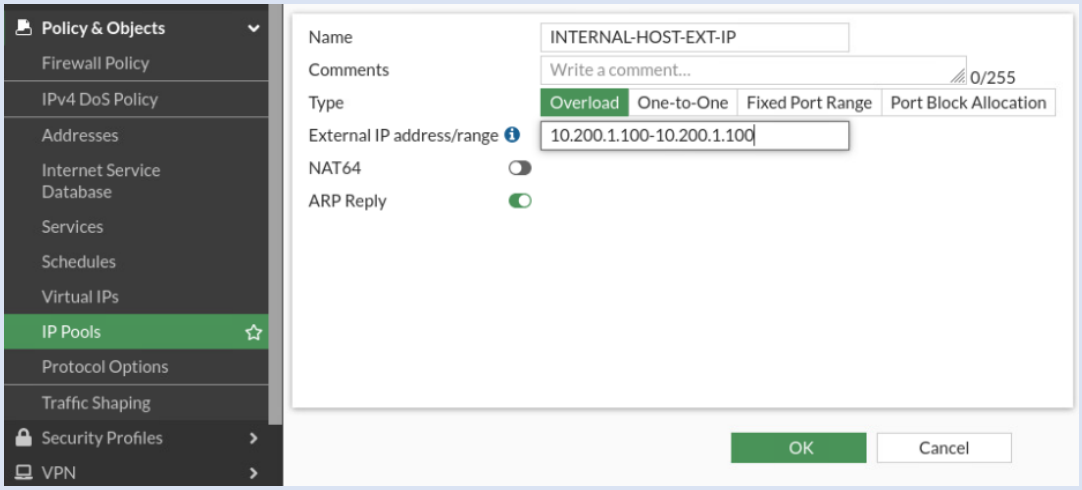
6)Outgoing Interface: ***port1***

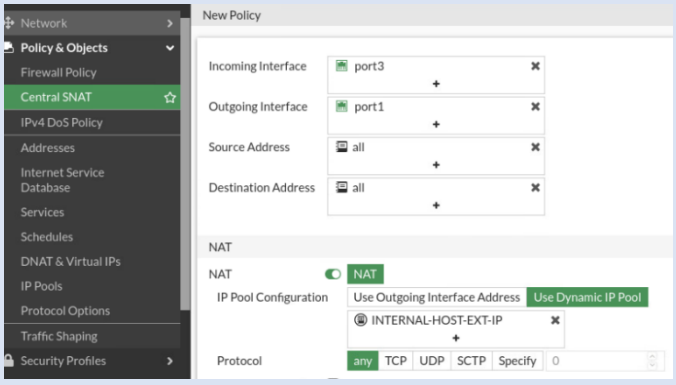
7)Apply Shaper: ***Enabled***

8)Shared Shaper: ***GUARANTEE_1000_MBPS***
9) Reverse Shaper: ***GUARANTEE_1000_MBPS***

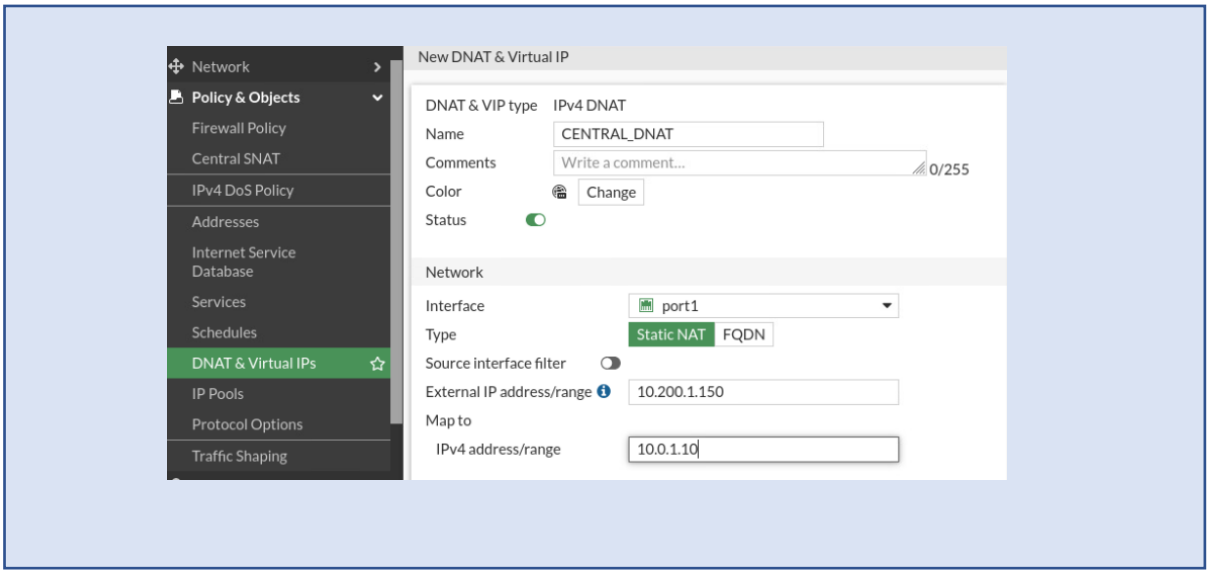
SNAT:

```
Local-FortiGate #
Local-FortiGate # config system settings

Local-FortiGate (settings) # set central-nat enable
Cannot enable central-nat with firewall policy using vip (id=15).

Local-FortiGate (settings) #
Local-FortiGate (settings) # set central-nat enable

Local-FortiGate (settings) # end
```





DNAT:


Network
Policy & Objects
Firewall Policy
Central SNAT
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
DNAT & Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
New DNAT & Virtual IP
DNAT & VIP type IPv4 DNAT
Name CENTRAL_DNAT
Comments Write a comment... 0/255
Color Change
Status
Network
Interface port1
Type Static NAT FQDN
Source interface filter
External IP address/range 10.200.1.150
Map to
IPv4 address/range 10.0.1.10