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
Туре	Subnet
IP/Netmask	192.168.1.0/24
Interface	any

2. Software Development

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

3. Game Design

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

4. Quality Assurance

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

5. <u>3D Modelling</u>

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

6. <u>3D Printing</u>

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

7. <u>Research</u>

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

8. <u>Innovate</u>

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

9. <u>Customer Support</u>

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

10. Marketing

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

11. VR Game Design

Field	Value
Name	VR_GAMEDESIGN_SUBENT
Туре	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

• <u>NETLAB Implementation:</u>

🛯 port3	-	
	-	This mewall policy will delive all packet
🖻 port1	-	with any protocols from reaching the
⊒ all +	×	HR_SUBNET. This policy is scheduled t
HR_SUBNET +	×	be in affect at all times when it is enabled.
o always	-	
ALL +	×	
ACCEPT Ø DENY		
	Port1 All HR_SUBNET All ALL ACCEPT O DENY	port1 all + HR_SUBNET + always ALL +

• <u>Traffic Flow Diagram:</u>



2. Block external access to the VR Department

• Address Group Creation:

Color Type 1 Members	Change Group Folder INNOVATE_SUBNET RESEARCH SUBNET	×	Before applying the firewall policy, we will create an Address Group to combin
Exclude members Static route configuration () Comments	+ Write a comment	<i>M</i> 0/255	the INNOVATE_SUBNET with the RESEARCH_SUBNET. We will call this VR DEPARTMENT.

• <u>Security Policy #1:</u>

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:

Name 🚺	VR_BLOCK		
Incoming Interface	im port3	•	
Outgoing Interface	port1	•	
Source	🔲 all	×	
Destination	唱 VR_DEPARTMENT	×	
Schedule	🖸 always	•	
Service	ALL	×	
Action	✓ ACCEPT Ø DENY		
C Las Vieleties Tes	46 -		

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.

• <u>Traffic Flow Diagram:</u>



• <u>Security Policy #2:</u>

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

• <u>NETLAB Implementation:</u>

	VR_ACCESS		
Incoming Interface	🗎 port3	•	This policy will ALLOW all traffic of
Outgoing Interface	🔳 port1	•	any protocol originating from the
Source	唱 VR_DEPARTMENT +	×	VR_DEPARTMENT, to any other
Destination	🗉 all +	×	subnet on the network. This policy is
Schedule	🖸 always	•	scheduled to be in affect at all times
Service	ALL +	×	when it is enabled.
Action	✓ ACCEPT Ø DENY		
Inspection Mode	Flow-based Proxy-based		

3. <u>Allow Internal Access Within The VR Department</u>

• <u>Security Policy #1:</u>

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

• <u>NETLAB Implementation:</u>

Name 🚺	RESEARCH_TO_INNOVATE_A	CCESS	
Incoming Interface	im port3	•	
Outgoing Interface	im port1	•	This policy will ALLOW all traffic of any
Source	RESEARCH_SUBNET +	×	protocol originating from the
Destination	INNOVATE_SUBNET +	×	RESEARCH_SUBNET , to the
Schedule	o always	•	INNOVATE_SUBIVET , nence providing
Service	🖬 ALL	×	internal access within the VR DEPARTME
Action	ACCEPT O DENY Flow-based Proxy-based		This policy is scheduled to be in affect at times when it is enabled.
Firewall / Network C	options		
NAT			

• <u>Traffic Flow Diagram:</u>



• <u>Security Policy #2:</u>

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

• <u>NETLAB Implementation:</u>

lame 🚯	INNOVATE_TO_RESEARCH_A	CCESS	
Incoming Interface	im port3	-	For traffic to flow both ways through a
Outgoing Interface	im port1	•	Tor traine to now both ways through a
Source	INNOVATE_SUBNET +	×	firewall, the firewall policy must be
Destination	RESEARCH_SUBNET +	×	configured to allow for traffic to flow in
Schedule	🐻 always	•	both directions . We will repeat the
Service	I ALL +	×	policy created above but this time, we
Action	✓ ACCEPT Ø DENY		will <i>switch</i> the <i>Source</i> and <i>Destination</i>
Inspection Mode	Flow-based Proxy-based		values.
Firewall / Network O	ptions		
NAT			

4. <u>Blocking all external access to VR Game Design (excluding the Game Design team)</u>

• <u>Security Policy #1:</u>

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

• NETLAB Implementation:



• <u>Traffic Flow Diagram:</u>



• <u>Security Policy #2:</u>

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

• <u>NETLAB Implementation:</u>

Name 🚯	VR_GAMEDESIGN_BLOCK		
Incoming Interface	im port3	•	
Outgoing Interface	im port1	•	DENY ALL subnets on the Tech Park
Source	🗐 all +	×	network from contacting the
Destination	VR_GAMEDESIGN_SUBNET +	×	protocol. This policy is scheduled to be in
Schedule	Co always	•	affect at all times when it is enabled.
Service	ALL	×	
	+		
Action	✓ ACCEPT Ø DENY		

• <u>Traffic Flow Diagram:</u>



5. <u>Allow the Game Design team to have access to external subnets</u>

• <u>Security Policy:</u>

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

• <u>NETLAB Implementation:</u>

Name 🚯	GAME_DESIGN_ACCESS		
Incoming Interface	🗎 port3	•	
Outgoing Interface	im port1	•	
Source	GAME_DESIGN_SUBNET +	×	ALLOW the GAME_DESIGN_SUBNET to
Destination	💷 all +	×	communicate with All subnets via any
Schedule	lo always	•	protocol. This policy is scheduled to be in
Service	₽ ALL +	×	affect at all times when it is enabled.
Action	✓ ACCEPT Ø DENY		
Inspection Mode	Flow-based Proxy-based		
Firewall / Network O	Options		
NAT			

• <u>Traffic Flow Diagram:</u>



6. Allowing Internet access to all departments

• Creating the TECH_PARK Address Object:

		Creating the TECH_PARK Address Object
n TECH_PARK	唱 ART 唱 DESIGN_AND_DEVELOPMENT 唱 HR	that contains all the department's subnets combined within one object.
	彊 PRODUCT 彊 VR	This makes it easier to manage and
		implement.

• <u>Security Policy:</u>

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

• <u>NETLAB Implementation:</u>

Name 🜖	INTERNET_ACCESS	
Incoming Interface	im port3	
Outgoing Interface	im port1	
Source	彊 TECH_PARK	
Destination	💷 all	
Schedule	Co always	
Service	ALL_ICMP	
	DNS	
	HTTP	
	HTTPS	
	SSH	
	+	
Action	✓ ACCEPT Ø DENY	
Inspection Mode	Flow-based Proxy-based	

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:

A Network Network Network Network Olicy & Objects AntWinus Web Filter Video Filter DNS Filter Application Control Intrusion Prevention	Create New SECURITYR SOCIAL_NE Vr5 SOCIAL_NE Vr5 VR_DEPAR1 W15 default W15 monitor-all W15 wifi-default	 1)Navigate to the <i>Security Profiles</i> tab on the left panel and click to expand it. 2)Select the <i>Web Filter</i> option highlighted in the screenshot. 3)Click the <i>Create New</i> icon shown on the top, right-side of the screenshot.
File Filter SSL/SSH Inspection		

New Web Filter Profile	
Name Comments Write a comment Feature set Flow-based	In the <i>Name</i> field, add a name for the web filter.
FortiGuard Category Based Filter	

2. <u>Choose the category you want to filter:</u>

Allow Monitor Q	Block A Warning Authenticate	1)Enable the FortiGuard Category Based Filter to view the categories
Potentially Liable Potentially Liable Potentially Liable Potentially Liable Potential Potential Discrimination Explicit Volence Extremist Groups Provay Avoidance Potential	Monitor Monitor Monitor Monitor Monitor Monitor Monitor Monitor Monitor Monitor	 2)Select a value under a category you want to filter. In the case of the screenshot, whave selected <i>Drug Abuse</i> under the <i>Potentially Liable</i> category. 3)Select the value you wish to filter, then select either the <i>Allow, Monitor, Block, Warning or Authenticate</i> options shown at the top of the screen shot.
] Potentially Liable 12 rug Abuse	Ø Block	If <i>Block</i> 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	Enable
Category	
Based Filter	
Security	Block all entries
Risk	
Potentially	Block all entries
Liable	
Unrated	Block all entries
Bandwidth	Block all entries
Consuming	

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

Security Risk 6		Potentially Liable 12		Bandwidth Consuming 6	
Malicious Websites	Ø Block	Drug Abuse	Ø Block	Freeware and Software Downloads	Ø Block
Phishing	Ø Block	Hacking	Ø Block	File Sharing and Storage	O Block
Spam URLs	Ø Block	Illegal or Unethical	Ø Block	Streaming Media and Download	Ø Block
Dynamic DNS	Ø Block	Discrimination	Ø Block	Peer-to-neer File Sharing	Ø Block
Newly Observed Domain	Ø Block	Explicit Violence	Ø Block	Internet Dadie and TV	O Block
Newly Registered Domain	Ø Block	Extremist Groups	Ø Block	Internet Radio and TV	Ø BIOCK
		🕞 Unrated 1			
		Unrated	O Block		

• <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:

A -+ 13 //	2	
Antivirus		
Web Filter	C VR_DEPARTMENT_RESTRICT V	1) Under the Security Profiles section in the Firewall Policy,
DNS Filter		enable Web Filter.
Application Con	ntrol 🕥	
IPS		2) Then show the VR DEPARTMENT RESTRICTIONS option
File Filter	0	from the drop down menu next to it.
SSL Inspection	ss. certificate-inspection 🝷 🖋	· · · · · · · · · · · · · · · · · · ·

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

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

• NETLAB Implementation:



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

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

• <u>Create Web Filter:</u>

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

• <u>NETLAB Implementation:</u>

Edit Web Filter Profile Name SOCIAL_NETW Comments Write a comme Feature set Flow-based P	/ORKING nt @ 0/255 Proxy-based	1)Enter the name of the Web Filter Profile
FortiGuard Category Based Filter Anow Monitor Block Name News and Media Social Networking Political Organizations	Warning Authenticate Action Allow Block Allow	2)Enable Fortiguard Category Based Filter 3)Block Social Networking under the General Interest – Personal category

• <u>Security Profile for Web Filtering</u>

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	Imp	lementation:
--	---	--------	-----	--------------

Name 🚯	ART_SOCIAL_NETWORKING_B	LOCK	Creating the
Incoming Interface	m port3	-	Creating the
Outgoing Interface	m port1	-	ART SOCIAL NETWORKING BLOCK pol
Source	碹 ART +	×	which will allow the ART Department to
Destination	⊒ all +	×	communicate with the internet. For Internet Ac
Schedule	lo always	-	we have defined ALL ICMP DNS HTTP H
Service	ALL_ICMP DNS HTTP HTTPS SSH	* * * * *	and <i>SSH</i> , which are web protocols that handle Internet traffic. This policy is scheduled to be i
Action	ACCEPT O DENY Flow-based Proxy-based		affect at all times when it is enabled
Security Profiles]
AntiVirus 🔾	WEB SOCIAL NETWORKING -		The SOCIAL_NETWORKING Web Filter, is

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

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	Enable
Category Based	
Filter	
Security Risk	Block all entries
Adult/Mature	Block all entries
Content	

• NETLAB Implementation:



Malicious Websites	Ø Block
Phishing	Ø Block
Spam URLs	Ø Block
Dynamic DNS	Ø Block
Newly Observed Domain	Ø Block
Newly Registered Domain	Ø Block

Alternative Beliefs	Ø Block
Abortion	Ø Block
Other Adult Materials	Ø Block
Advocacy Organizations	Ø Block
Gambling	Ø Block
Nudity and Risque	Ø Block
Pornography	Ø Block
Dating	Ø Block
	A B ()

• <u>Security Profile for Web Filtering</u>

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

• <u>NETLAB Implementation:</u>

Name 🚺	SECURITYRISK_AND_ADULTC	ONTEN
Incoming Interface	m port3	
Outgoing Interface	m port1	
Source	稽 TECH_PARK +	,
Destination	雪 all +	,
Schedule	Co always	,
Service	ALL_ICMP	,
	DNS DNS	,
	HTTP	,
	HTTPS	,
	SSH SSH	3
	+	
Action	ACCEPT Ø DENY	
Security Profiles	Storm Issent Brown bacad	
AntiVirus 🕥		

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.<u>Applying a Schedule for Social Networking Usage for all Departments</u> <u>excluding Art</u>

• 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:

New Polic	,				
Name 🚯		SOCIAL_N	ETWORK	ING_TIME_L	IMIT
Incoming I	nterface	port3			-
Outgoing	Interface	port1			-
Source			V_AND_D	EVELOPME	NTX
		PRODU	ІСТ		ŝ
		NR VR			×
			+		
Destinatio	n	💷 all			×
Cohodulo				DRING TIM	15.11
Schedule		Le SOCIAL		RKING_IIM	1E_LI ♥
Jervice		DNS	*11*		ŝ
		HTTP			×
		HTTPS			×
		SSH	_		×
			+	E2 12 4	
en senedare					
enocidate					
Type Recuri	ing One Time				
Type Recurr	ing One Time		LIMIT		
Type Recurr Name	SOCIAL_NET	WORKING_TIM	e_limit		
Type Recurr Name Color	SOCIAL_NET	WORKING_TIM	E_LIMIT		
Type Recurr Name Color Days	SOCIAL_NET		E_LIMIT Tuesday		Wednesday
Type Recurr Name Color Days	SOCIAL_NET		E_LIMIT Tuesday Friday		Nednesday Saturday
Type Recurr Name Color Days	SOCIAL_NET GChange Monday Thursday	WORKING_TIM	E_LIMIT Tuesday Friday	2	Nednesday Saturday
Type Recurr Name Color Days All day	SOCIAL_NET GChange Monday Thursday Sunday	WORKING_TIM	E_LIMIT Tuesday Friday	01	Wednesday Saturday
Type Recurn Name Color Days All day Start Time 3	SOCIAL_NET C Change Monday Thursday Sunday O1:00:00.0		E_LIMIT Tuesday Friday	0	Wednesday Saturday
Type Recurn Name Color Days All day Start Time 1	SOCIAL_NET SOCIAL_NET C Change Monday Thursday Sunday Ol: 00:00.0 01: 30:00.0		E_LIMIT Tuesday Friday	20 v 20 s	Wednesday Saturday
Type Recurr Name Color Days All day itart Time 3 itop Time	SOCIAL_NET SOCIAL_NET Change Monday Thursday Sunday O1:00:00.0 01:30:00.0	WORKING_TIM 2000 PM 2000 PM	E_LIMIT Tuesday Friday	2 v 19 s	Wednesday Saturday
Type Recurr Name Color Days All day Start Time 1	SOCIAL_NET Change Monday Thursday Sunday O1:00:00.0 01:30:00.0	WORKING_TIM 200 PM 200 PM	E_LIMIT Tuesday Friday	2 v 2 s	Wednesday Saturday
Type Recurr Name Color Days All day Start Time 9 Stop Time	ing One Time SOCIAL_NET G Change Monday Thursday Sunday 01:00:00.0	WORKING_TIM 200 PM 200 PM	E_LIMIT Tuesday Friday	20	Wednesday Saturday
Type Recurr Name Color Days All day Start Time 1 Stop Time	Ing One Time SOCIAL_NET Change Monday Thursday Thursday 01:00:00.0 01:30:00.0	WORKING_TIM	E_LIMIT Tuesday Friday Cance		Wednesday aaturday
Type Recurr Name Color Days All day Start Time 1 Stop Time	ing One Time SOCIAL_NET G Change C Monday C Thursday C Sunday O 01:00:00.0 (01:30:00.0	WORKING_TIMI	E_LIMIT Tuesday Friday Cance	2 L 2 S	Wednesday Saturday
Type Recurr Name Color Days All day Start Time 9 Stop Time	Ing One Time SOCIAL_NET Change Monday Thursday Sunday 01:00:00.0	WORKING_TIMI	E_LIMIT Tuesday Friday Cance	2 1 2 5	Wednesday Saturday
Type Recurr Name Color Days All day Start Time 1 Stop Time	ing One Time SOCIAL_NET G Change Ø Monday Ø Thursday Ø 1:00:00.0 01:00:00.0	WORKING_TIMI	E_LIMIT Tuesday Friday Cance	2 M 2 S	Wednesday Saturday
Type Recurr Name Color Days All day Start Time ① Stop Time	ing One Time SOCIAL_NET G Change Monday Thursday O1:00:00.0 01:30:00.0	WORKING_TIM	E_LIMIT Tuesday Friday Cance	2 1 2 2	Wednesday Saturday
Type Recurr Name Color Days Start Time I Stop Time	ing One Time SOCIAL_NET G Change Ø Monday Ø Thursday Ø Sunday Ø 1:00:00.0	WORKING_TIMI	E_LIMIT Tuesday Friday Cance	2 1 2 2	Wednesday Saturday
Type Recurr Name Color Days All day Start Time I Stop Time Security Prof AntiVirus	ing One Time SOCIAL_NET G Change Monday Thursday O 1: 00: 00, 0 01: 30: 00, 0 iles		E_LIMIT Tuesday Friday Cance	2 1 2 2	Wednesday Saturday

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.<u>Creating a Traffic Shaper to Guarantee Bandwidth Originating from</u> <u>the VR Department</u>

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

• NETLAB Implementation:

↔ WiFi Controller > Feature Visibility ✿ System ① Policy Disclaimer	We must first enable Traffic Shaping on our firewall
Administrators Policy-based IPsec VPN	GUI. On the left-side panel, go to:
Admin Profiles	
Firmware Fabric Management 1 SD-WAN Interface	1)System
Settings SSL-VPN Personal Bookmark	
HA SNMD SSL-VPN Realms	2)Feature Visibility
Replacement Threat Weight Tracking	
Messages FortiGuard Image: Contraction of the second secon	Then Enable Traffic Shaping under Additional
Feature Visibility 🏠 💽 VoIP	Features
Certificates Wireless Open Security	
Dashboard > Edit Traffic Shaper Anternark	To create a new Traffic Shaper Profile, go to:
Policy & Objects Vigner Per IP Shaper	
Firewall Policy GUARANTEE 1000_MBPS	1)Policy & Objects
IPv4 DoS Policy Quality of Service	2)Traffic Shaping
Addresses Traffic priority High •	3)Create New
Internet Service Bandwidth unit Mbps	4)Name: GUARANTEE 1000 MRPS
Services Maximum bandwidth C 2000 🔅 Mbps	5) Traffia Driarity: High
Schedules DSCP O	C) D = 1 : 1.1 II : Mhar
Virtual IPs	o)Banawiath Unit: Mops
IP Pools	7)Maximum Bandwidth: 2000
Protocol Options	8)Guaranteed Bandwidth: 1000
CLIConsole(1) Lecal-fortiGate d config firewall shaper traffic-shaper Lecal-fortiGate (traffic-shaper) d edit "CUMDATEE_1000_MEDS" Lecal-fortiGate (CUMDATEE_1000_MEDS) d show config firewall haper traffic-shaper edit "CUMDATEE_1000_MEDS" Let Guardeed Sundation 1000	Once the profile is created, right-click it and select <i>Edit in CLI</i> . Alternatively, we can log into the Local-FortiGate CLI in NETLAB. Enter the following
set maximum-bandwigth 2000 set bandwidth-unit mbps next	command to enable traffic shaping to occur per
end	policy:
Local-FortiSate (GUARANTEE_1000_NDF3) # set per-pointy endoire	
Local-FortiGate #	set per-policy enable
Edit Traffic Shaping Policy	Then we created a new <i>Traffic Shaping Policy</i> that
Name VR_BANDWIDTH	will be applied to the VR Department:
Status Comments Write a comment	and to applied to the FR Department.
Virte a commence. // 0/255	1)Name: VR_BANDWIDTH
If Traffic Matches:	
Destination I all X	2)Status: Enabled
Schedule	3) Source: all
Jonedure Lo always	
Service 🛛 ALL 🗶	<i>5)50uce. uu</i>
Service ALL ×	4)Schedule: alwavs
Service Q ALL * Application • URL Category +	4)Schedule: always

Then:			6)Outgoing Interface: port1
Outgoing interface	<pre>port1 +</pre>	×	7)Apply Shaper: Enabled
Apply shaper			
Shared shaper	GUARANTEE_1000_MBPS	•	8)Shared Shaper: GUARANTEE_1000_MBPS
Reverse shaper	C GUARANTEE_1000_MBPS	•	9) Reverse Shaper: GUARANTEE_1000_MBPS
Per-IP shaper			
Assign shaping class I	D 🕽		

٦

SNAT:

l-FortiGate (settin ot enable central-) l-FortiGate (settin l-FortiGate (settin l-FortiGate (settin	ngs) # set central-nat enable nat with firewall policy using vip (id=15). ngs) # ngs) # set central-nat enable ngs) # end
 Policy & Objects Firewall Policy IPv4 DoS Policy Addresses Internet Service Database Services Schedules Virtual IPs IP Pools Protocol Options 	Name INTERNAL-HOST-EXT-IP Comments Write a comment @ 0/255 Type Overload One-to-One Fixed Port Range Port Block Allocation External IP address/range 10.200.1.100-10.200.1.100 NAT64 Image: Comment of the second seco
Traffic Shaping Security Profiles VPN	OK Cancel
 Network Policy & Objects Firewall Policy Central SNAT IPv4 DoS Policy Addresses Internet Service Database Services 	New Policy Incoming Interface
Schedules	NAT

DNAT:

Policy & Objects DNAT & VIP type IPv4 DNAT Name CENTRAL_DNAT Comments Write a comment O/255 Color Change Status Status Image: Status Image: Status
Firewall Policy Name CENTRAL_DNAT Central SNAT Comments Write a comment IPv4 DoS Policy Color Change Addresses Status Image
Central SNAT Comments Write a comment 0/255 IPv4 DoS Policy Color Change Addresses Status Image: Change
IPv4 DoS Policy Color Color Color Color Addresses Status Color Color Color
Addresses Status O
Internet Service Database Network
Services Interface m port1
Schedules Type Static NAT FQDN
DNAT & Virtual IPs 🚓 Source interface filter 💿
IP Pools External IP address/range 1 0.200.1.150
Protocol Options Map to
Traffic Shaping IPv4 address/range 10.0.1.10