

## Table des matières

Mise en place fortigate.....	1
Firewall et règles .....	7
Mise en place d'une regle DNAT .....	11
Mise en place de RIP .....	16
Approfondissement de la CLI .....	18
Voir les groupes de services .....	19
Création d'un service group WEB_ONLY.....	21
Créer un service et l'ajouter à un groupe de services.....	22
Créer une règle.....	23
Afficher contenu d'une règle.....	23
Configuration du DHCP sur le LAN .....	24
Activer le serveur.....	25
Mise en place d'une règle de DNAT .....	27
Resultat.....	30
Interface virtuelle pour routage intervlan.....	31

## Mise en place fortigate

Je vais explorer fortigate via GNS3 j'ai installé une version sur GNS3 la 7.2.12

Mdp par défaut

Admin / blank

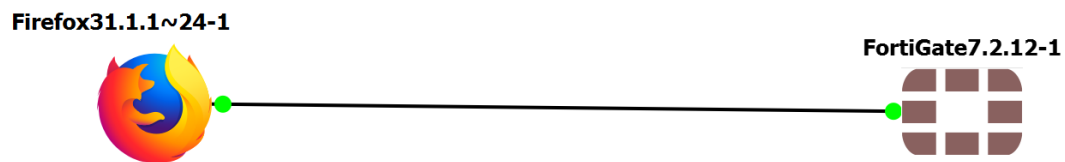
Il faut modifier le mdp à la première connexion il faut modifier le mdp la première connexion se fait en ligne de commande

Le config system est un peu comme le conf t de cisco

```
FortiFirewall-VM64-KVM # config system interface
FortiFirewall-VM64-KVM (interface) # edit port2
FortiFirewall-VM64-KVM (port2) # set ip 10.0.0.254 255.255.255.0
FortiFirewall-VM64-KVM (port2) # set allowaccess https http ssh ping
FortiFirewall-VM64-KVM (port2) # end
```

Je configure le port 2 je mets une ip et j'autorise l'accès en https http ssh et ping pour parametre ma machine

J'ai une machine firefox sur GNS3 que je relie au port 2



Le reseau pour l'instant c'est 10.0.0.0/24

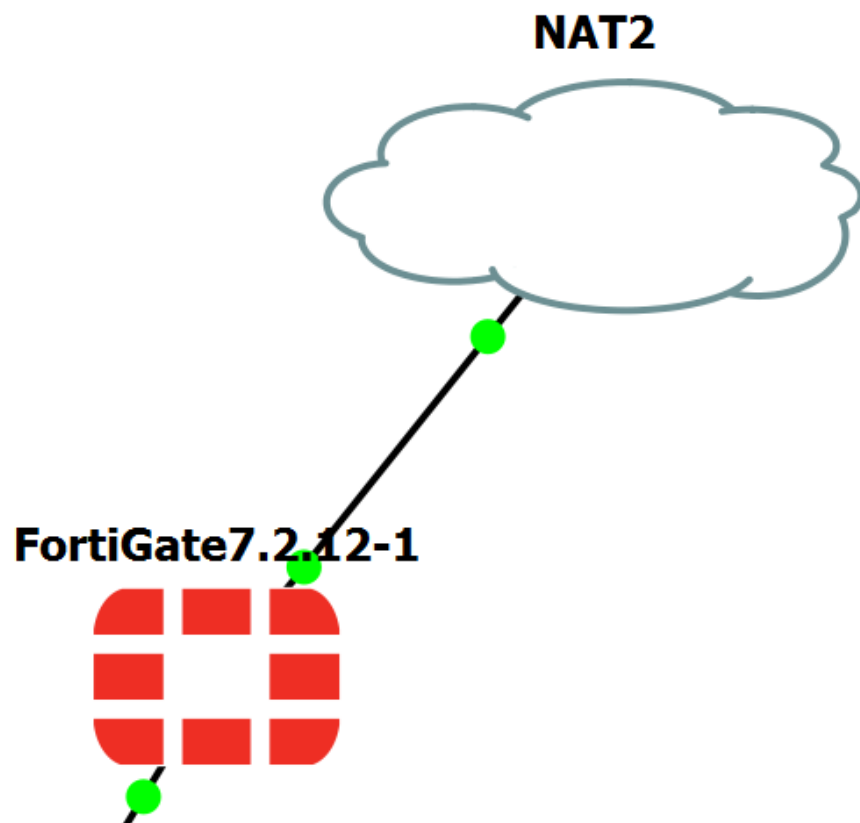
L'ip de mon client firefox : 10.0.0.1

On va d'abord tester le ping pour voir la conenctivité entre les deux machines

```
gns3@box:~$ ping 10.0.0.254
PING 10.0.0.254 (10.0.0.254): 56 data bytes
64 bytes from 10.0.0.254: seq=0 ttl=255 time=2.456 ms
64 bytes from 10.0.0.254: seq=1 ttl=255 time=0.697 ms
64 bytes from 10.0.0.254: seq=2 ttl=255 time=0.649 ms
64 bytes from 10.0.0.254: seq=3 ttl=255 time=0.855 ms
^C
--- 10.0.0.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.649/1.164/2.456 ms
gns3@box:~$ █
```

<https://10.0.0.254>

Il faut mettre une licence pour utiliser la version evaluation il faut mettre un nat à connecter au port 1 pour avoir de la connexion via internet



Je passe sur hyper-v GNS3 c'est trop compliqué

oici le **bloc de commandes FortiGate** (router + DNS) prêt à coller dans ta doc.  
Adapte l'interface et les IP si besoin.

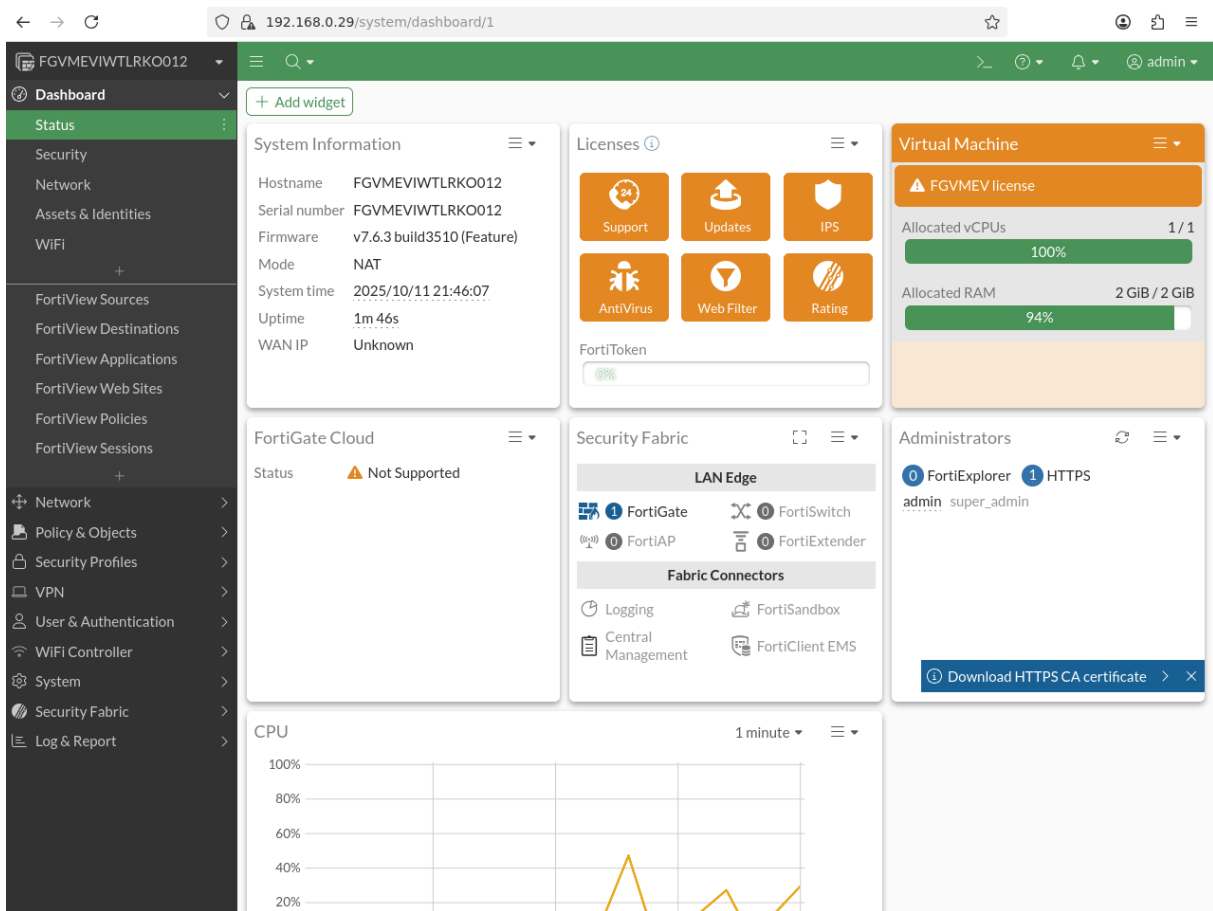
```
# --- DNS publics ---
config system dns
    set primary 8.8.8.8
    set secondary 1.1.1.1
end

# --- Route par défaut via la passerelle du WAN (ex: port1) ---
config router static
    edit 1
        set gateway 192.168.0.254
        set device port1
    next
end

# (Optionnel) Autoriser les accès d'admin utiles sur le WAN
config system interface
    edit port1
        set allowaccess ping https http ssh
    next
end

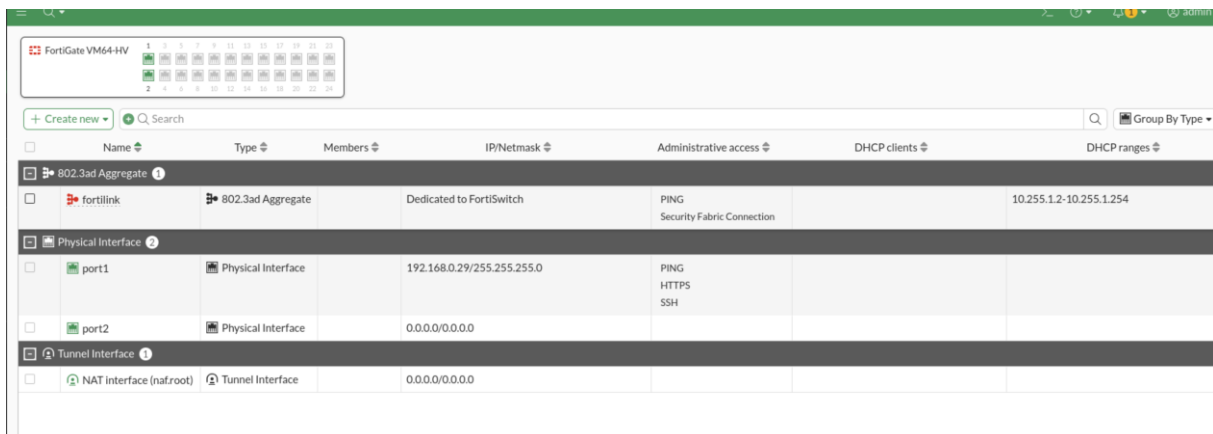
# --- Vérifications rapides ---
get system dns
get router info routing-table all
execute ping 8.8.8.8
execute ping google.com
```

Me voila enfin sur l'interface web



Je vais configurer la seconde interface pour avoir un client debian dans un commutateur interne et tout les tests se feront avec lui

Je créer une interface supplémentaire sur la machine hyper-V



Je vois port 2 ici je clique dessus

## Ensuite Edit

### Address

Addressing mode: **Manual** IPAM DHCP PPPoE One-Arm Sniffer

IP/Netmask: 10.0.0.254/255.255.255.0

Create address object matching subnet

Name: port2 address

Destination: 10.0.0.0/24

Secondary IP address:

### Administrative Access

IPv4

<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> HTTP ⓘ	<input checked="" type="checkbox"/> PING
<input type="checkbox"/> FMG-Access	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP
<input type="checkbox"/> FTM	<input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> Security Fabric Connection ⓘ
<input type="checkbox"/> Speed Test	<input type="checkbox"/> SCIM	

Receive LLDP ⓘ: Use VDOM Setting **Enable** Disable

Transmit LLDP ⓘ: Use VDOM Setting **Enable** Disable

J'active le serveur DHCP

### DHCP Server

DHCP status: **Enabled** Disabled

Address range: 10.0.0.2-10.0.0.254

Netmask: 255.255.255.0

Default gateway: **Same as Interface IP** Specify

DNS server: **Same as System DNS** Same as Interface IP Specify

Lease time ⓘ  604800 second(s)

Advanced

J'ai mis mes aliases etc

802.3ad Aggregate						
<input type="checkbox"/>	fortilink	802.3ad Aggregate	Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254
Physical Interface						
<input type="checkbox"/>	LAN (port2)	Physical Interface	10.0.0.254/255.255.255.0	PING HTTPS SSH HTTP	1	10.0.0.2-10.0.0.250
<input type="checkbox"/>	WAN (port1)	Physical Interface	192.168.0.29/255.255.255.0	PING HTTPS SSH		

```
(root@kali)-[~]
└─# dhclient -v
Internet Systems Consortium DHCP Client 4.4.3
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:15:5d:60:01:06
Sending on   LPF/eth0/00:15:5d:60:01:06
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPOFFER of 10.0.0.3 from 10.0.0.254
DHCPREQUEST for 10.0.0.3 on eth0 to 255.255.255.255 port 67
DHCPCACK of 10.0.0.3 from 10.0.0.254
bound to 10.0.0.3 -- renewal in 256838 seconds.

(root@kali)-[~]
└─#
```

## Firewall et règles

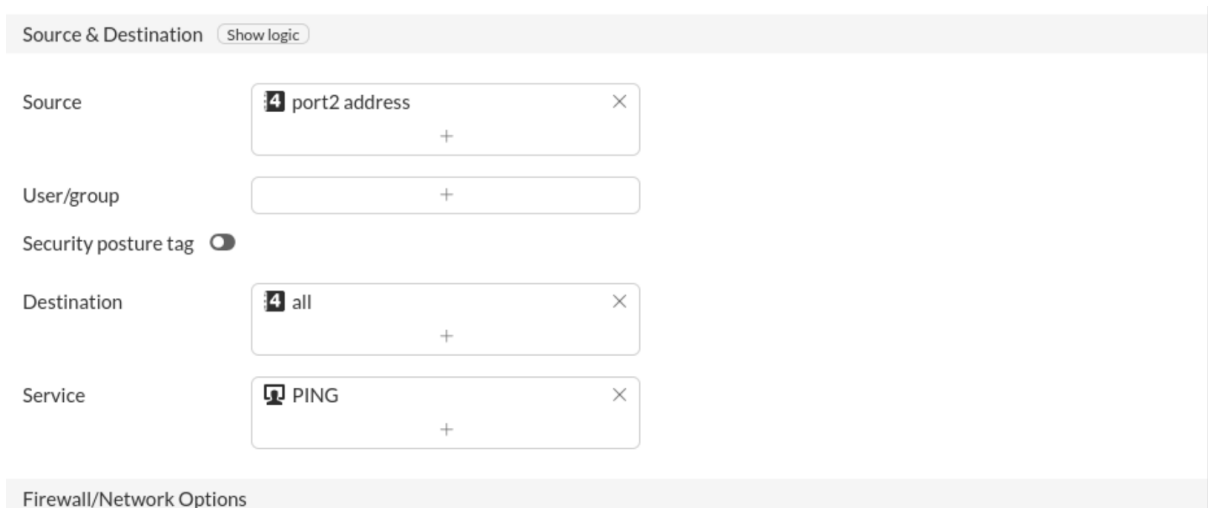
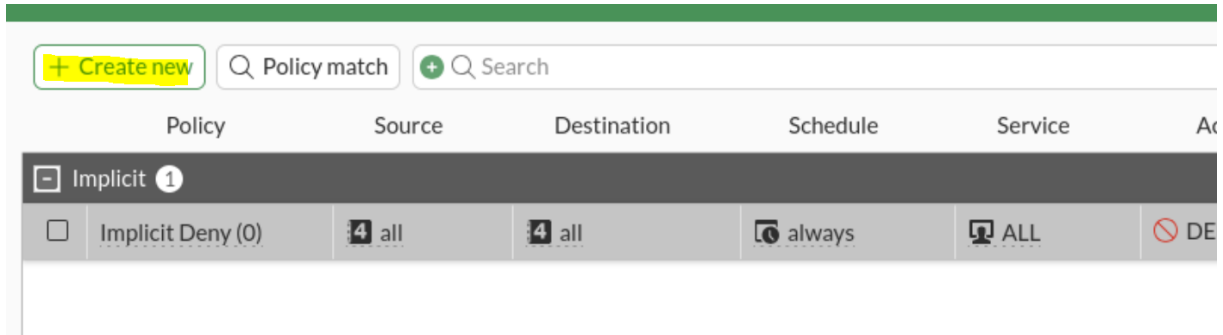
Nous allons configurer notre première règle de firewall

Effectivement depuis le client nous ne pouvons pas émettre de ping vers l'extérieur en l'occurrence 1.1.1.1

```
(root@kali)-[~]
└─# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
^C
 1.1.1.1 ping statistics:
 2 packets transmitted, 0 received, 100% packet loss, time 1002ms

(root@kali)-[~]
└─#
```

Il faut ce rendre dans Policy & Objects > Firewall Policy > Create new



On voit que le NAT se configure directement dans la règle

Firewall/Network Options

Inspection mode:  Flow-based  Proxy-based

NAT:

IP pool configuration:  Use Outgoing Interface Address  Use Dynamic IP Pool

Source port translation:  Always  When port conflicts  Never

Protocol options:  PROT default

---

Security Profiles

AntiVirus:

Web filter:

DNS filter:

Application control:

IPS:

File filter:

## Résultat

Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles	Log	Bytes
LAN (port2) → WAN (port1)	PING (1)	port2.address	all	always	PING	ACCEPT	NAT	Standard	no-inspection	UTM	0B
Implicit											

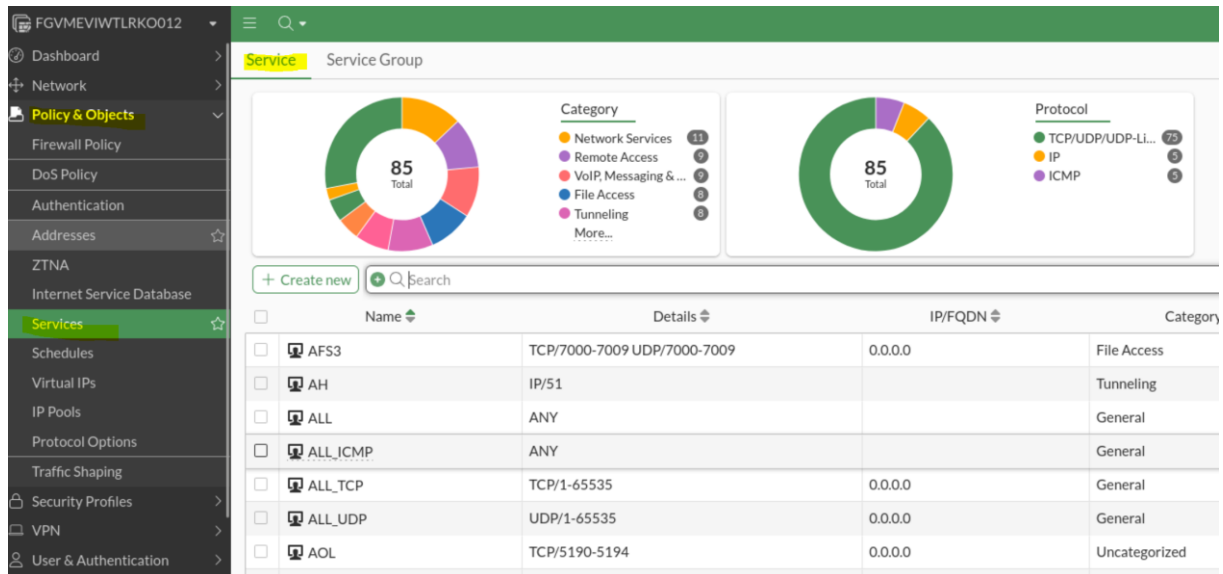
Maintenant le ping passe

```
(root@kali)-[~]
└─# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data:
64 bytes from 1.1.1.1: icmp_seq=1 ttl=53 time=4.44 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=53 time=3.13 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=53 time=4.30 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=53 time=3.97 ms

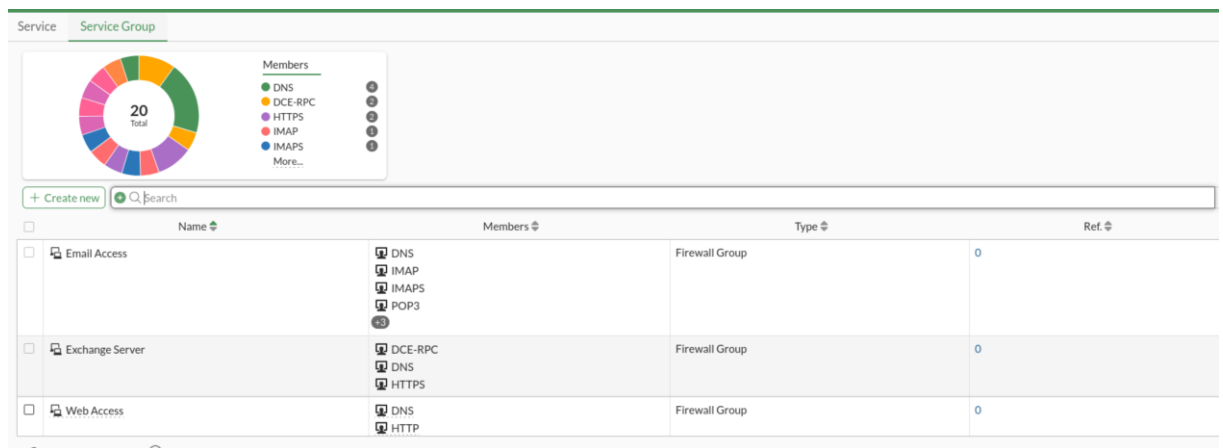
```

Le firewall fonctionne avec des objets

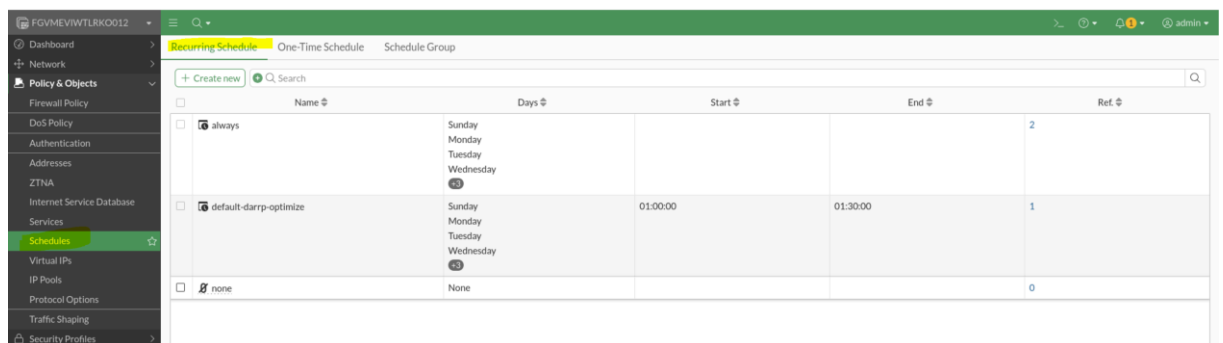
Chaque service est un objet



Et nous avons des groupes de services déjà configuré



Dans schedule on peut aussi mettre nos règles en fonction du temps




## Mise en place d'une règle DNAT

Il faut d'abord aller dans Policy object > Virtual IP

Je veux rediriger le port 22 de mon IP dans le WAN vers le port 22 de ma machine KALI

Les paramètres dans le screen sont assez simple pas besoin de m'étaler dessus

Edit Virtual IP

Name	<input type="text" value="SSH-KALI"/>
Comments	<input type="text" value="SSH-KALI"/> 8/255
Color	 <input type="button" value="Change"/>

Network

Interface	<input type="text" value="WAN (port1)"/>
Type	Static NAT
External IP address/range ⓘ	<input type="text" value="192.168.0.29"/>
Map to	
IPv4 address/range	<input type="text" value="10.0.0.3"/>

Optional filters & restrictions

Port Forwarding

Protocol	<input checked="" type="button" value="TCP"/> <input type="button" value="UDP"/> <input type="button" value="SCTP"/> <input type="button" value="ICMP"/>
Port Mapping Type	<input checked="" type="button" value="One to one"/> <input type="button" value="Many to many"/>
External service port ⓘ	<input type="text" value="22"/>
Map to IPv4 port	<input type="text" value="22"/>

Le plus important est dans les règles de firewall il faut créer une règle pour autoriser ce flux

Name ⓘ SSH-KALI  
 Schedule always  
 Action  ACCEPT  DENY  
 Type Standard ZTNA  
 Incoming interface WAN (port1)  
 Outgoing interface LAN (port2)

Source & Destination Show logic

Source all  
 User/group  
 Security posture tag   
 Destination SSH-KALI  
 Service SSH

Firewall/Network Options  
 Inspection mode  Flow-based  Proxy-based

Généralement le trafic entrant viendra de la l'interface WAN et ira vers une interface LAN dans la source je mets ANY mais je peux restreindre sur une ip ou range ensuite au niveau service je peux meme mettre ALL si je veux dans tout les cas le tout sera rediriger vers le port 22 mais pour garder une continuité je mets « SSH »

Je mets nat ici pour pas avoir un probleme de route ou autre

Firewall/Network Options

Inspection mode  Flow-based  Proxy-based

NAT

IP pool configuration  Use Outgoing Interface Address  Use Dynamic IP Pool

Source port translation  Always  When port conflicts  Never

Protocol options  PROT default

---

Security Profiles

AntiVirus

Web filter

DNS filter

Application control

IPS

File filter

SSL inspection  SSL  no-inspection

---

Logging Options

Log allowed traffic

Je lance un test

```

root@dedier:~# ssh -p 22 root@192.168.0.29
root@192.168.0.29's password:
Linux kali 5.10.0-kali2-amd64 #1 SMP Debian 5.10.9-1kali1 (2021-01-22) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have no mail.
Last login: Sun Oct 12 06:41:39 2025 from 10.0.0.254
(Message from Kali developers)

We have kept /usr/bin/python pointing to Python 2 for backwards
compatibility. Learn how to change this and avoid this message:
⇒ https://www.kali.org/docs/general-use/python3-transition/

(Run: "touch ~/.hushlogin" to hide this message)
root@kali:~#

```


C'est parfait sa fonctionne

Maintenant je change le port extérieur de 22 à 2222

**Edit Virtual IP**

Name

Comments  8/255

Color 

---

**Network**

Interface

Type

External IP address/range

Map to

IPv4 address/range

---

Optional filters & restrictions

---

Port Forwarding

Protocol

Port Mapping Type

External service port

Map to IPv4 port

Dans la règle de pare-feu il faut que j'autorise le port 2222 et 22 pour être sûr que rien ne bloque

J'ai créé un objet ssh-bis avec le port 2222 en tcp

## Edit Policy

Name ⓘ	SSH-KALI
Schedule	always
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Type	Standard ZTNA
Incoming interface	WAN (port1)
Outgoing interface	LAN (port2)

Source & Destination Show logic

Source	all
User/group	
Security posture tag	<input type="checkbox"/>
Destination	SSH-KALI
Service	SSH SSH-bis

Ça fonctionne

```
root@dedier:~# ssh -p 2222 root@192.168.0.29
root@192.168.0.29's password:
Linux kali 5.10.0-kali2-amd64 #1 SMP Debian 5.10.9-1kali1 (2021-01-22) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have no mail.
Last login: Sun Oct 12 06:47:50 2025 from 10.0.0.254
(Message from Kali developers)

We have kept /usr/bin/python pointing to Python 2 for backwards
compatibility. Learn how to change this and avoid this message:
=> https://www.kali.org/docs/general-use/python3-transition/

(Run: "touch ~/.hushlogin" to hide this message)
(root@kali)-[~]
#
```

C'est parfait

# Mise en place de RIP

J'ai déjà plusieurs nœuds rip

Je vais dans network > RIP

RIP

Version **1** **2**

Networks

IP/Netmask

Interfaces

[+ Create New](#) [Edit](#) [Delete](#)

Interface	Version	Passive	Authentication
WAN (port1)	Send: 2 Receive: 2	<span style="color: red;">●</span> Disabled	<span style="color: red;">●</span> Disabled
LAN (port2)	Send: 2 Receive: 2	<span style="color: green;">●</span> Enabled	<span style="color: red;">●</span> Disabled

Advanced Options

Default Metric

Inject Default Route

Timers

Inject Default Route ⓘ

Timers

Update: 30 seconds

Timeout: 180 seconds

Garbage: 120 seconds

Redistribute

Connected:  Auto Metric  
 All Filter

Static:  Auto Metric  
 All Filter

OSPF:  Auto Metric  
 All Filter

BGP:  Auto Metric  
 All Filter

ISIS:  Auto Metric  
 All Filter

Apply

Avec la commande `get router info protocols` je vais avoir des informations sur les protocoles de routage utiliser

```

Default version control: send version 2, receive version 2
Interface      Send Recv  Key-chain
port1          2      2
Routing for Networks:
192.168.0.0/24
Routing Information Sources:
Gateway        Distance  Last Update  Bad Packets  Bad Routes  TUN-ID
192.168.0.200    120      00:00:15     0             11          0.0.0.0
192.168.0.254    120      00:00:04     0             13          0.0.0.0
Distance: (default is 120)

Routing Protocol is "ospf 0", VRF 0
Invalid after 0 seconds, hold down 0, flushed after 0
Outgoing update filter list for all interfaces is
Incoming update filter list for all interfaces is
Redistributing:
Routing for Networks:
Routing Information Sources:
Gateway        Distance     Last Update
Distance: (default is 110)
Address        Mask          Distance List

OSPF interfaces with fast link failover enabled (vdom): 0
OSPF interfaces with fast link failover enabled (global): 0

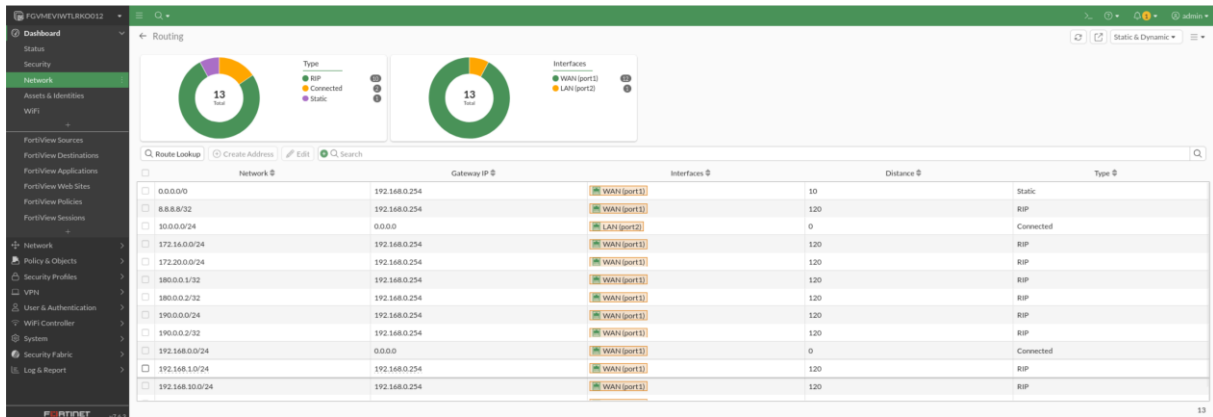
Routing Protocol is "isis"
System ID: 0000.0000.0000
Area addr: Non-configured
IS type: level-1-2
Number of Neighbors: 0

VR auto router ID is 192.168.0.29

```

Et si on part dans Dashboard > Network

Si tout est bien configuré on verra toutes nos routes ajoutées



## Approfondissement de la CLI

On va découvrir un peu plus en profondeur la CLI qui nous permet de réaliser des opérations lourdes simplement efficacement en tant qu'admin sys il ne faut jamais avoir peur de la CLI.

A mon avis pour les opérations lourdes vaut mieux passer en CLI et les opérations légères vaut mieux passer par la WEBUI

## Voir les groupes de services

Show firewall service group

```
FGVMEVIWTLRK0012 # show firewall service group
config firewall service group
  edit "Email Access"
    set uuid 09b62126-a723-51f0-73a3-afe893be3d73
    set member "DNS" "IMAP" "IMAPS" "POP3" "POP3S" "SMTP" "SMTPS"
  next
  edit "Web Access"
    set uuid 09b629be-a723-51f0-3e70-2c36679c1ff6
    set member "DNS" "HTTP" "HTTPS"
  next
  edit "Windows AD"
    set uuid 09b62d88-a723-51f0-f505-ae6590dd4750
    set member "DCE-RPC" "DNS" "KERBEROS" "LDAP" "LDAP_UDP" "SAMBA" "SMB"
  next
  edit "Exchange Server"
    set uuid 09b632ec-a723-51f0-b192-3b52a2e53fa2
    set member "DCE-RPC" "DNS" "HTTPS"
  next
end
```

Show firewall service custom sa nous permet d'afficher tout les services individuellement

```
FGVMEVIWTLRK0012 # show firewall service custom
config firewall service custom
edit "ALL"
    set uuid 091e6cdc-a723-51f0-d6a4-506bd552f350
    set category "General"
    set protocol IP
next
edit "ALL_TCP"
    set uuid 091e70ce-a723-51f0-b13d-939748c6cd01
    set category "General"
    set tcp-portrange 1-65535
next
edit "ALL_UDP"
    set uuid 091e71f0-a723-51f0-abdc-203695ce8a7a
    set category "General"
    set udp-portrange 1-65535
next
edit "ALL_ICMP"
    set uuid 091e72f4-a723-51f0-b74c-deaac10c0fd1
    set category "General"
    set protocol ICMP
    unset icmptype
next
edit "ALL_ICMP6"
    set uuid 091e7510-a723-51f0-1bb9-a9f9c0cd72af
    set category "General"
    set protocol ICMP6
    unset icmptype
next
edit "GRE"
    set uuid 091e765a-a723-51f0-2812-e3d1d5252574
    set category "Tunneling"
    set protocol IP
    set protocol-number 47
--More-- [
```

On peut aussi pour les groupe effectuer

Config firewall service grou

Show

End

```

FGVMEVIWTLRK0012 # config firewall service group

FGVMEVIWTLRK0012 (group) # show
config firewall service group
  edit "Email Access"
    set uuid 09b62126-a723-51f0-73a3-afe893be3d73
    set member "DNS" "IMAP" "IMAPS" "POP3" "POP3S" "SMTP" "SMTPS"
  next
  edit "Web Access"
    set uuid 09b629be-a723-51f0-3e70-2c36679c1ff6
    set member "DNS" "HTTP" "HTTPS"
  next
  edit "Windows AD"
    set uuid 09b62d88-a723-51f0-f505-ae6590dd4750
    set member "DCE-RPC" "DNS" "KERBEROS" "LDAP" "LDAP_UDP" "SAMBA" "SMB"
  next
  edit "Exchange Server"
    set uuid 09b632ec-a723-51f0-b192-3b52a2e53fa2
    set member "DCE-RPC" "DNS" "HTTPS"
  next
end

FGVMEVIWTLRK0012 (group) # end

```

## Création d'un service group WEB\_ONLY

```

FGVMEVIWTLRK0012 # config firewall service group

FGVMEVIWTLRK0012 (group) # edit WEB_ONLY
new entry 'WEB_ONLY' added

FGVMEVIWTLRK0012 (WEB_ONLY) # set member HTTP HTTPS

FGVMEVIWTLRK0012 (WEB_ONLY) # next

FGVMEVIWTLRK0012 (group) # end

```

Toujours config firewall service group

Ensuite edit <NOM\_NOUVEAU\_GROUP>

Set member

Next

End

## Créer un service et l'ajouter à un groupe de services

Je créer le service custom comme ceci

```
FGVMEVIWTLRK0012 # config firewall service custom
FGVMEVIWTLRK0012 (custom) # edit TCP_8080
new entry 'TCP_8080' added
FGVMEVIWTLRK0012 (TCP_8080) # set tcp-portrange 8080
FGVMEVIWTLRK0012 (TCP_8080) # next
FGVMEVIWTLRK0012 (custom) # end
```

Et avec j'ajoute au service group avec la directive append

```
FGVMEVIWTLRK0012 # config firewall service group
FGVMEVIWTLRK0012 (group) # edit WEB_ONLY
FGVMEVIWTLRK0012 (WEB_ONLY) # append member TCP_8080
FGVMEVIWTLRK0012 (WEB_ONLY) # next
FGVMEVIWTLRK0012 (group) # end
```

## Créer une règle

```
FGVMEVIWTLRK0012 # config firewall policy
FGVMEVIWTLRK0012 (policy) # edit 10
new entry '10' added

FGVMEVIWTLRK0012 (10) # set name "LAN_TO_WAN_WEB"
FGVMEVIWTLRK0012 (10) # set srcintf "port2"
FGVMEVIWTLRK0012 (10) # set dstintf "port1"
FGVMEVIWTLRK0012 (10) # set srcaddr "all"
FGVMEVIWTLRK0012 (10) # set dstaddr "all"
FGVMEVIWTLRK0012 (10) # set action accept
FGVMEVIWTLRK0012 (10) # set schedule "always"
FGVMEVIWTLRK0012 (10) # set service "WEB_ONLY"
FGVMEVIWTLRK0012 (10) # set nat enable
FGVMEVIWTLRK0012 (10) # next
FGVMEVIWTLRK0012 (policy) # end
FGVMEVIWTLRK0012 # █
```

Voilà la base pour créer une règle dans le firewall

### [Afficher contenue d'une règle](#)

Show firewall policy <numero regle>

```
FGVMEVIWTLRK0012 # show firewall policy 10
config firewall policy
  edit 10
    set name "LAN_TO_WAN_WEB"
    set uuid 72acf156-a7c2-51f0-fada-9341f843e944
    set srcintf "port2"
    set dstintf "port1"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "WEB_ONLY"
    set nat enable
  next
end
```

## Configuration du DHCP sur le LAN

Normalement j'ai déjà un dhcp configuré

Show system dhcp server

```
edit 2
  set forticlient-on-net-status disable
  set dns-service default
  set default-gateway 10.0.0.254
  set netmask 255.255.255.0
  set interface "port2"
  config ip-range
    edit 1
      set start-ip 10.0.0.2
      set end-ip 10.0.0.250
    next
  end
next
end
```

J'ai reconfiguré le DHCP qui englobe l'interface LAN

```
FGVMEVIWTLRK0012 # config system dhcp server
FGVMEVIWTLRK0012 (server) # edit 2
FGVMEVIWTLRK0012 (2) # set interface "port2"
FGVMEVIWTLRK0012 (2) # set netmask 255.255.255.0
FGVMEVIWTLRK0012 (2) # set default-gateway 10.0.0.254
FGVMEVIWTLRK0012 (2) # set dns-service default
FGVMEVIWTLRK0012 (2) # config ip-range
FGVMEVIWTLRK0012 (ip-range) # delete 1
FGVMEVIWTLRK0012 (ip-range) # edit 1
new entry '1' added
FGVMEVIWTLRK0012 (1) # set start-ip 10.0.0.1
FGVMEVIWTLRK0012 (1) # set end-ip 10.0.0.253
FGVMEVIWTLRK0012 (1) # next
FGVMEVIWTLRK0012 (ip-range) # end
FGVMEVIWTLRK0012 (2) # next
FGVMEVIWTLRK0012 (server) # end
FGVMEVIWTLRK0012 # █
```

Activer le serveur

```
FGVMEVIWTLRK0012 # config system dhcp server
FGVMEVIWTLRK0012 (server) # edit 2
FGVMEVIWTLRK0012 (2) # set status enable
FGVMEVIWTLRK0012 (2) # next
FGVMEVIWTLRK0012 (server) # end
```

Il faut mettre set status enable et ensuite ne pas oublier « next »

Revenir en mode enabled et exécuter cette commande pour voir si le dhcp fonctionne bien

diagnose debug enable

diagnose debug application dhcps -1

Lancer une demande de bail depuis un client

```
FGVMEVIWTLRK0012 # diagnose debug application dhcpd -1
Debug messages will be on for 30 minutes.

FGVMEVIWTLRK0012 # [debug]locate_network prhtype(1) pihtype(1)
[debug]find_lease(): packet contains preferred client IP, cip.s_addr is 10.0.0.3
[debug]search through all subnets to find an ip lease (10.0.0.3)
[debug]found a new lease of ip 10.0.0.3
[debug]find_lease(): leaving function with lease set
[debug]find_lease(): the lease's IP is 10.0.0.3
[note]DHCPREQUEST for 10.0.0.3 from 00:15:5d:60:01:06 via port2(ethernet)
[debug]added ip 10.0.0.3 mac 00:15:5d:60:01:06 in vd root
[debug]packet length 300
[debug]op = 1 htype = 1 hlen = 6 hops = 0
[debug]xid = 68cb0d50 secs = 0 flags = 0
[debug]ciaddr = 0.0.0.0
[debug]yiaddr = 0.0.0.0
[debug]siaddr = 0.0.0.0
[debug]giaddr = 0.0.0.0
[debug]chaddr = 00:15:5d:60:01:06
[debug]filename =
[debug]server_name =
[debug] host-name = "kali"
[debug] dhcp-requested-address = 10.0.0.3
[debug] dhcp-message-type = 3
[debug] dhcp-parameter-request-list = 1,28,2,3,15,6,119,12,44,47,26,121,42
```

Ça marche c'est parfait

## Mise en place d'une règle de DNAT

Je veux publier le port 80 d'une machine sur le port 8080 du firewall

```
FGVMEVIWTLRK0012 # config firewall vip

FGVMEVIWTLRK0012 (vip) # edit "webserver"
new entry 'webserver' added

FGVMEVIWTLRK0012 (webserver) # set extinf "port1"

command parse error before 'extinf'
Command fail. Return code -61

FGVMEVIWTLRK0012 (webserver) # set extintf "port1"

FGVMEVIWTLRK0012 (webserver) # set extip 192.168.0.29

FGVMEVIWTLRK0012 (webserver) # set mappedip 10.0.0.3

FGVMEVIWTLRK0012 (webserver) # set portforward enable

FGVMEVIWTLRK0012 (webserver) # set extport 8080

FGVMEVIWTLRK0012 (webserver) # set mappedport 80

FGVMEVIWTLRK0012 (webserver) # next

FGVMEVIWTLRK0012 (vip) # end

FGVMEVIWTLRK0012 # █
```

Ensuite il faut faire une policy pour autoriser le flux comme on a deux ports ici le 80 et 8080 il faut bien autoriser les deux mais pas de panique les deux sont dans notre service group configurer plus tot

L'adresse de destination est bien l'ip virtual qu'on a créer plus tot fortigate fonctionne comme ça un fonctionnement un peu bizarre au début mais c'est comme ça

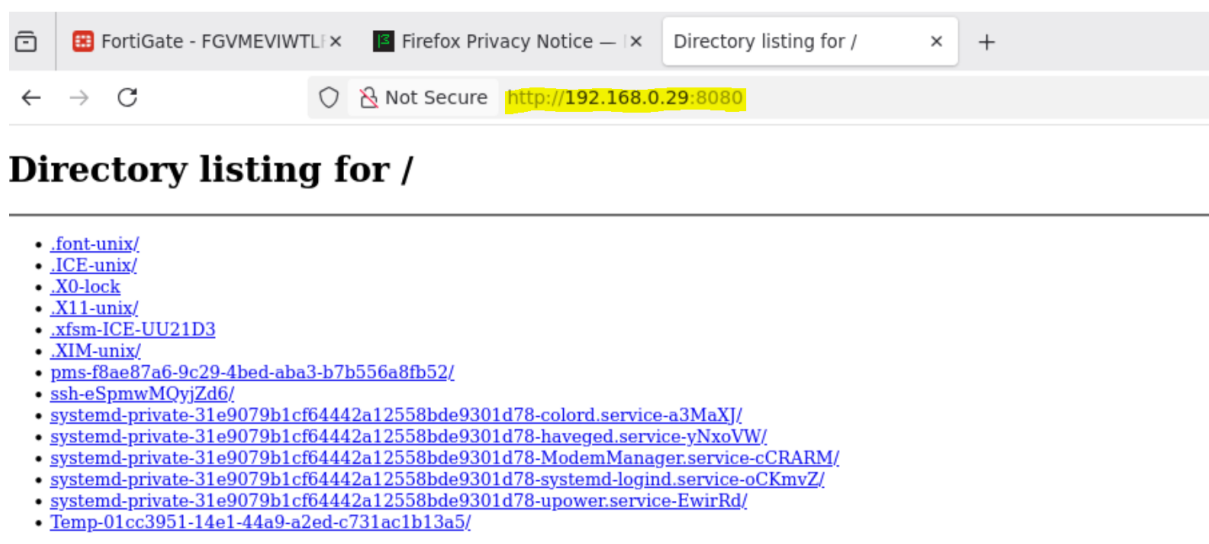
```
FGVMEVIWTLRK0012 # config firewall policy
FGVMEVIWTLRK0012 (policy) # edit 11
new entry '11' added
FGVMEVIWTLRK0012 (11) # set name "WAN_TO_WEBSERVER"
FGVMEVIWTLRK0012 (11) # set srcintf "port1"
FGVMEVIWTLRK0012 (11) # set dstintf "port2"
FGVMEVIWTLRK0012 (11) # set srcaddr "all"
FGVMEVIWTLRK0012 (11) # set dstaddr "webserver"
FGVMEVIWTLRK0012 (11) # set action accept
FGVMEVIWTLRK0012 (11) # set schedule "always"
FGVMEVIWTLRK0012 (11) # set service "WEB_ONLY"
FGVMEVIWTLRK0012 (11) # set nat enable
FGVMEVIWTLRK0012 (11) # next
FGVMEVIWTLRK0012 (policy) # end
FGVMEVIWTLRK0012 # █
```

Pour voir nos adresse virtuelles sois nos DNAT

Il faut faire show firewall vip

```
FGVMEVIWTLRK0012 # show firewall vip
config firewall vip
  edit "SSH-KALI"
    set uuid d2d6eca2-a72d-51f0-1e3c-7fb34c27ab15
    set comment "SSH-KALI"
    set extip 192.168.0.29
    set mappedip "10.0.0.3"
    set extintf "port1"
    set portforward enable
    set color 1
    set extport 2222
    set mappedport 22
  next
  edit "webserver"
    set uuid ae546560-a7c5-51f0-adf9-c7ab1878085d
    set extip 192.168.0.29
    set mappedip "10.0.0.3"
    set extintf "port1"
    set portforward enable
    set extport 8080
    set mappedport 80
  next
end
```

## Resultat



FortiGate - FGVMEVIWTLR... Firefox Privacy Notice — | x Directory listing for /

← → ↻ Not Secure http://192.168.0.29:8080

### Directory listing for /

---

- [.font-unix/](#)
- [.ICE-unix/](#)
- [.X0-lock](#)
- [.X11-unix/](#)
- [.xfsm-ICE-UU21D3](#)
- [.XIM-unix/](#)
- [pms-f8ae87a6-9c29-4bed-aba3-b7b556a8fb52/](#)
- [ssh-eSpmwMQyjZd6/](#)
- [systemd-private-31e9079b1cf64442a12558bde9301d78-colored.service-a3MaXJ/](#)
- [systemd-private-31e9079b1cf64442a12558bde9301d78-haveged.service-yNxoVW/](#)
- [systemd-private-31e9079b1cf64442a12558bde9301d78-ModemManager.service-cCRARM/](#)
- [systemd-private-31e9079b1cf64442a12558bde9301d78-systemd-logind.service-oCKmvZ/](#)
- [systemd-private-31e9079b1cf64442a12558bde9301d78-upower.service-EwirRd/](#)
- [Temp-01cc3951-14e1-44a9-a2ed-c731ac1b13a5/](#)

---

# Interface virtuelle pour routage intervlan

La premiere interface virtuelle

config system interface

```
FGVMEIWTLRK0012 (interface) # edit port2.10
new entry 'port2.10' added

FGVMEIWTLRK0012 (port2.10) # set vdom root

FGVMEIWTLRK0012 (port2.10) # set vlanid 10

FGVMEIWTLRK0012 (port2.10) # set ip 100.0.0.254/24

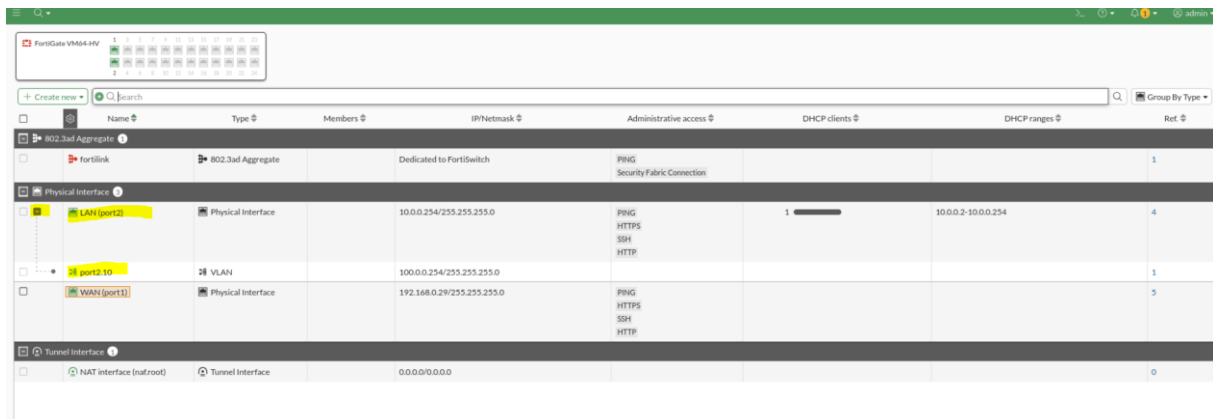
FGVMEIWTLRK0012 (port2.10) # set interface port2

FGVMEIWTLRK0012 (port2.10) # next

FGVMEIWTLRK0012 (interface) # end

FGVMEIWTLRK0012 #
```

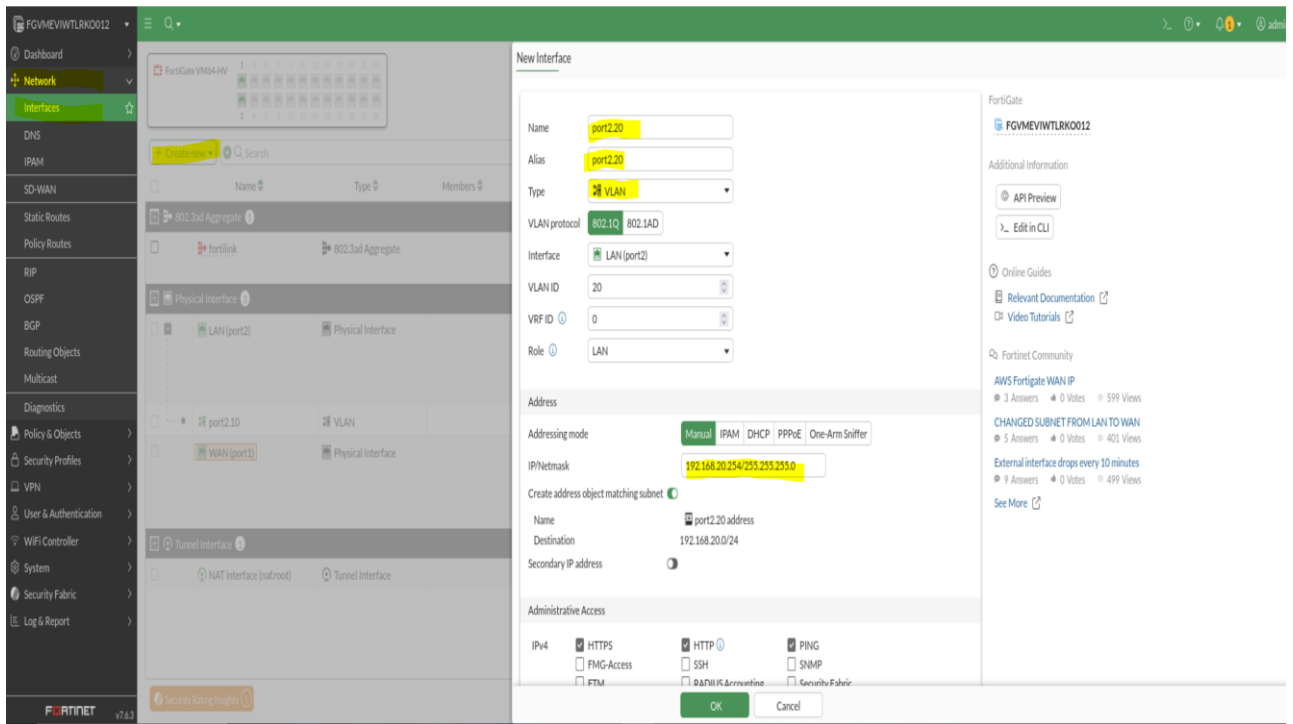
Dans l'interface graphique je vois l'interface virtuelle



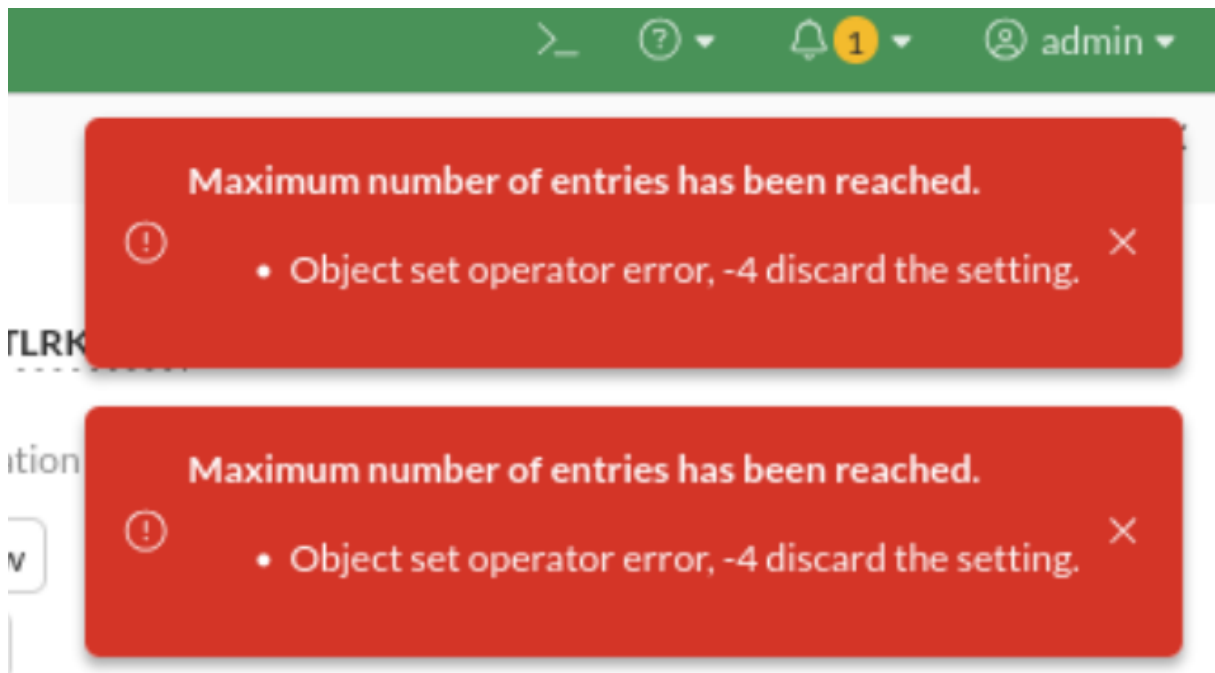
Name	Type	Members	IP/Netmask	Administrative access	DHCP clients	DHCP ranges	Ref
<b>Physical Interface</b>							
LAN (port2)	Physical Interface		10.0.0.254/255.255.255.0	PING HTTPS SSH HTTP	1	10.0.0.2-10.0.0.254	4
port2.10	VLAN		100.0.0.254/255.255.255.0				1
WAN (port1)	Physical Interface		192.168.0.29/255.255.255.0	PING HTTPS SSH HTTP			5
<b>Tunnel Interface</b>							
NAT interface (nat.root)	Tunnel Interface		0.0.0.0/0.0.0.0				0

Pour la seconde interface je passe en interface graphique mais erreur licence gratuite donc impossible

Car je fais face à une erreur bizarre



Erreur nombre maximum d'interface



[Documentation](#) ↗

Je repasse en CLI et configure le DHCP sur l'interface du VLAN 10

```
FGVMEVIWTLRK0012 # config system dhcp server
FGVMEVIWTLRK0012 (server) # edit 3
new entry '3' added
FGVMEVIWTLRK0012 (3) # set interface "port2.10"
FGVMEVIWTLRK0012 (3) # set netmask 255.255.255.0
FGVMEVIWTLRK0012 (3) # set default-gateway 100.0.0.254
FGVMEVIWTLRK0012 (3) # set dns-service default
FGVMEVIWTLRK0012 (3) # config ip-range
FGVMEVIWTLRK0012 (ip-range) # edit 1
new entry '1' added
FGVMEVIWTLRK0012 (1) # set start-ip 100.0.0.1
FGVMEVIWTLRK0012 (1) # set end-ip 100.0.0.250
FGVMEVIWTLRK0012 (1) # next
FGVMEVIWTLRK0012 (ip-range) # end
FGVMEVIWTLRK0012 (3) # next
FGVMEVIWTLRK0012 (server) # end
FGVMEVIWTLRK0012 # █
```

## Configurer l'interface hyper-v du forti en trunk

```
Set-VMNetworkAdapterVlan -VMName "forti" -Trunk -AllowedVlanIdList "10,20" -NativeVlanId 1
```

Je mets ma VM client dans le VLAN 10

C'est parfait ça fonctionne

```
(root@kali)-[~]
└─# dhclient -v
Internet Systems Consortium DHCP Client 4.4.3
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:15:5d:60:01:06
Sending on   LPF/eth0/00:15:5d:60:01:06
Sending on   Socket/fallback
DHCPREQUEST for 10.0.0.3 on eth0 to 255.255.255.255 port 67
DHCPNAK from 100.0.0.254
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 6
DHCPOFFER of 100.0.0.1 from 100.0.0.254
DHCPREQUEST for 100.0.0.1 on eth0 to 255.255.255.255 port 67
DHCPACK of 100.0.0.1 from 100.0.0.254
bound to 100.0.0.1 -- renewal in 241744 seconds.

(root@kali)-[~]
└─# █
```