Table des matières

Mise en place fortigate

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

Mdp par défaut

Admin / blank

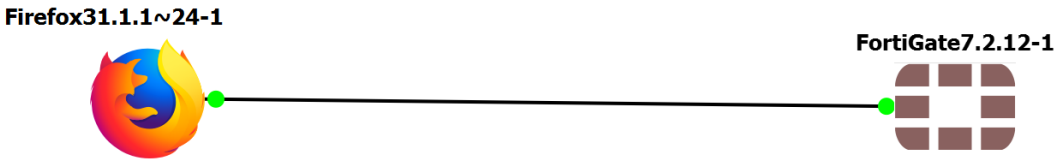
Il faut modifier le mdp à la premiere connexion il faut modifier le mdp la premiere connexion se fait en ligne de commande

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

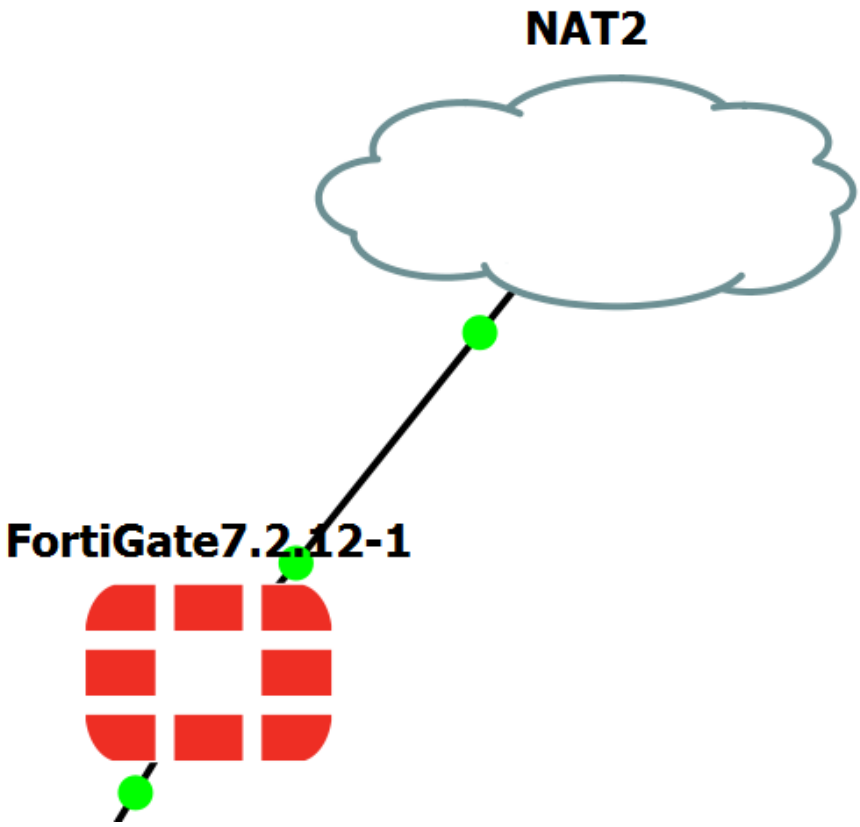
L'ip de mon client firefox : 10.0.0.1

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

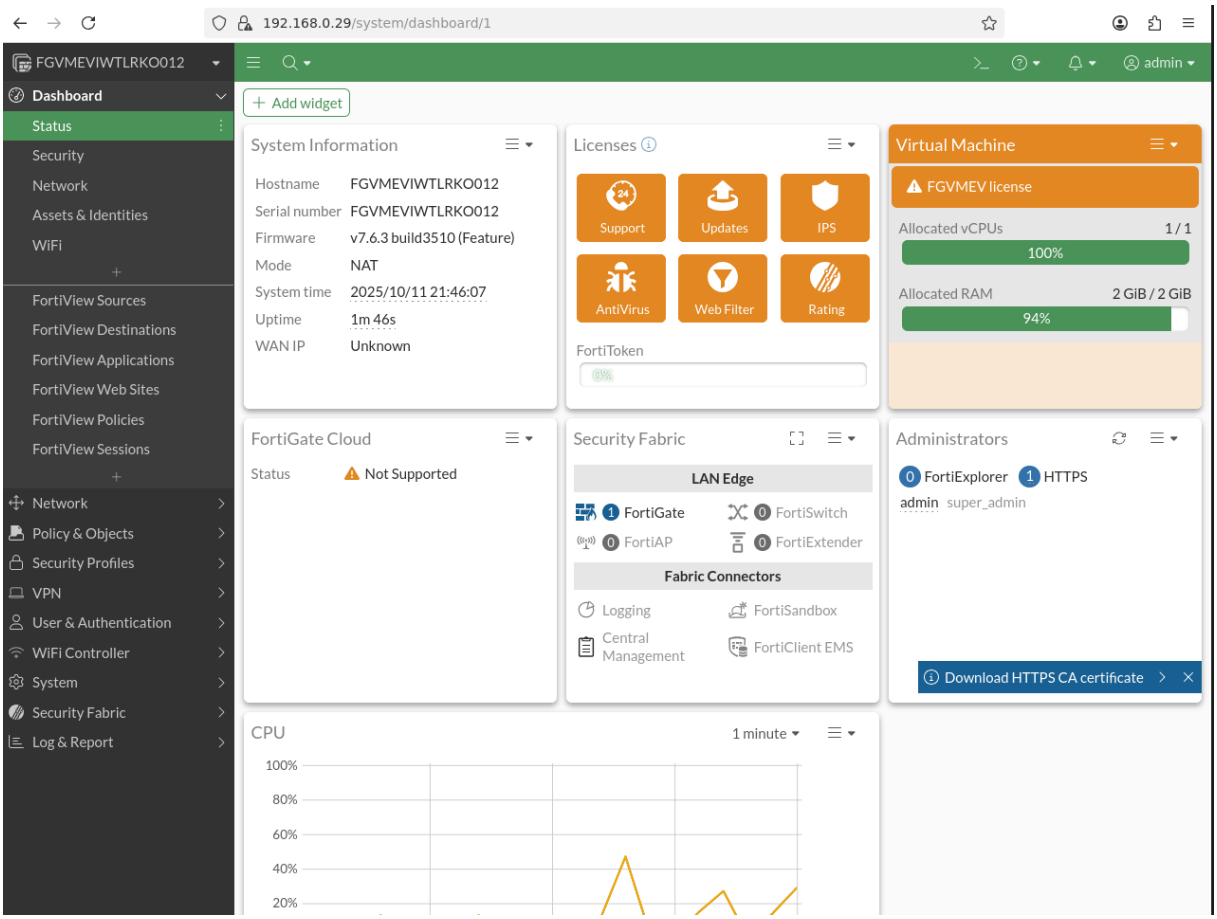


Je passe sur hyper-v GNS3 c’est trop compliqué

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

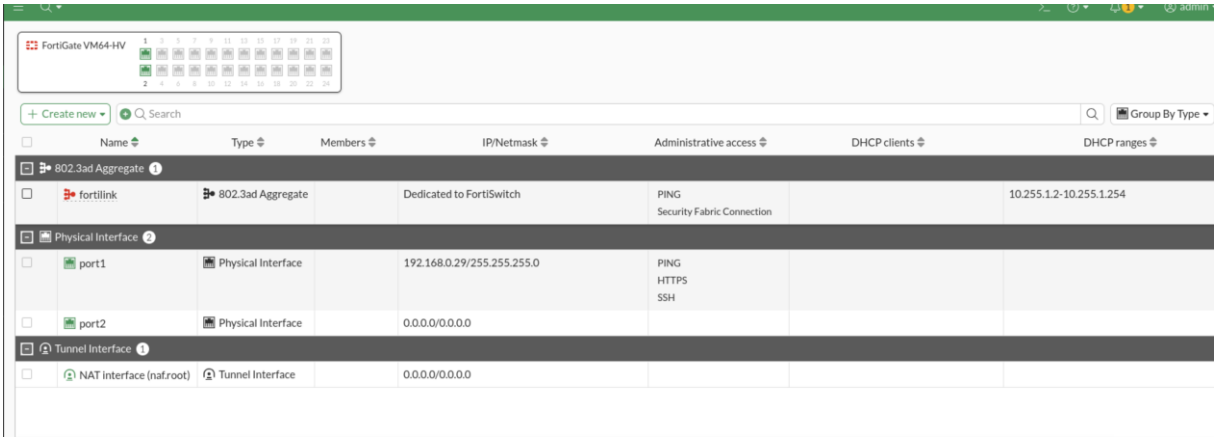
```
# --- DNS publics ---
config system dns
    set primary 8.8.8.8
    set secondary 1.1.1.1
end

# --- 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



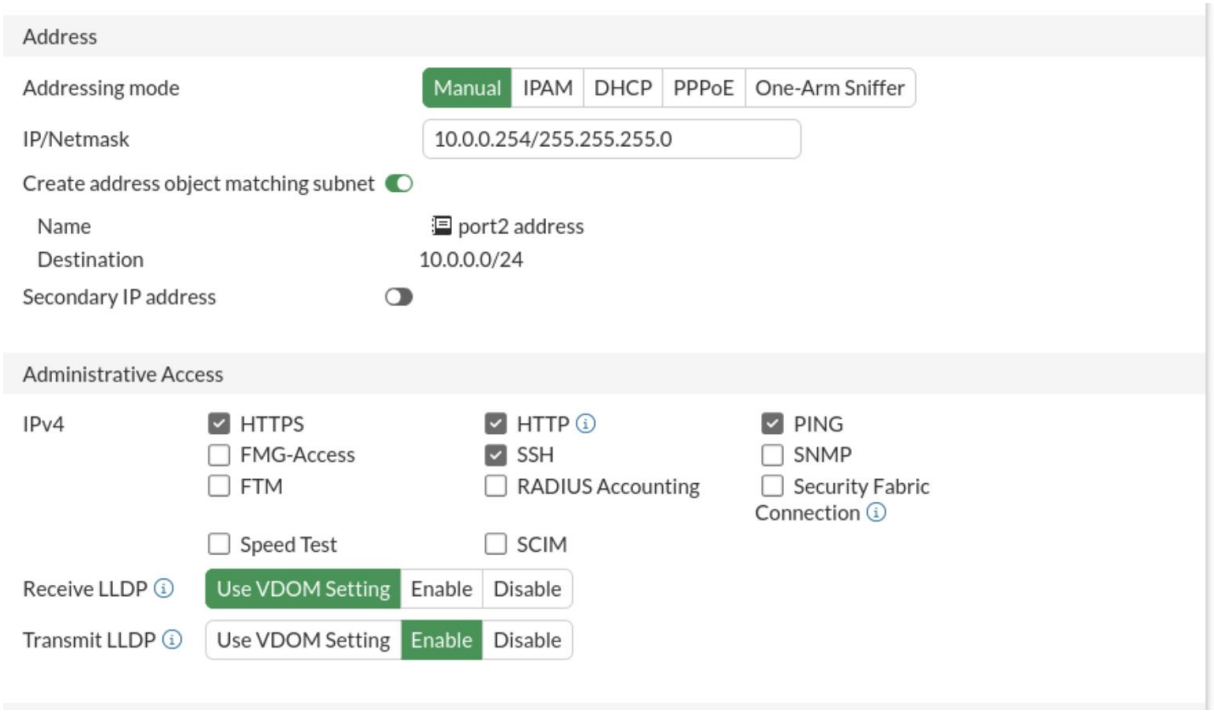
Je vais configurer la seconde interface pour avoir un client debian dans un commutateur interne et tout les tests se feront avec lui

Je créer une interface supplémentaire sur la machine hyper-V

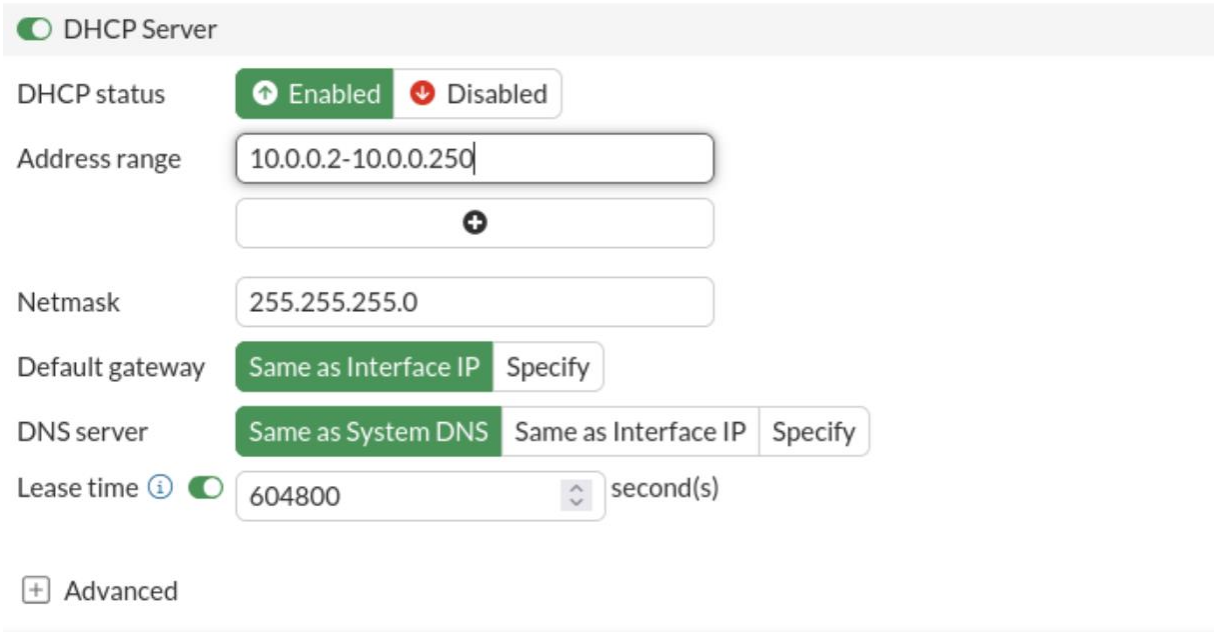


Je vois port 2 ici je clique dessus

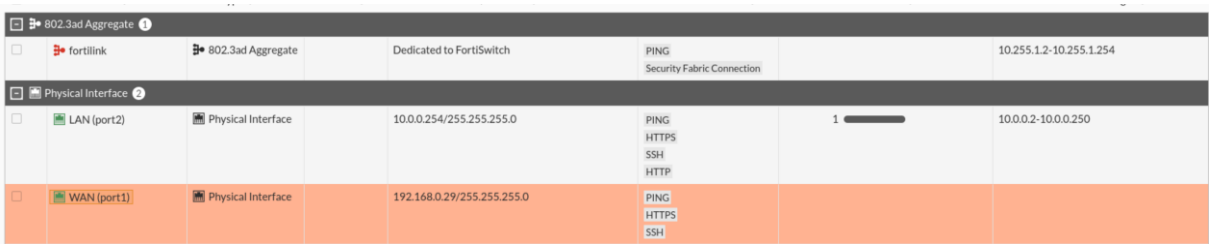
Ensuite Edit



J’active le serveur DHCP



J’ai mis mes alliases etc




```
┌──(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
DHCPACK of 10.0.0.3 from 10.0.0.254
bound to 10.0.0.3 -- renewal in 256838 seconds.

┌──(root㉿kali)-[~]
└─#
```

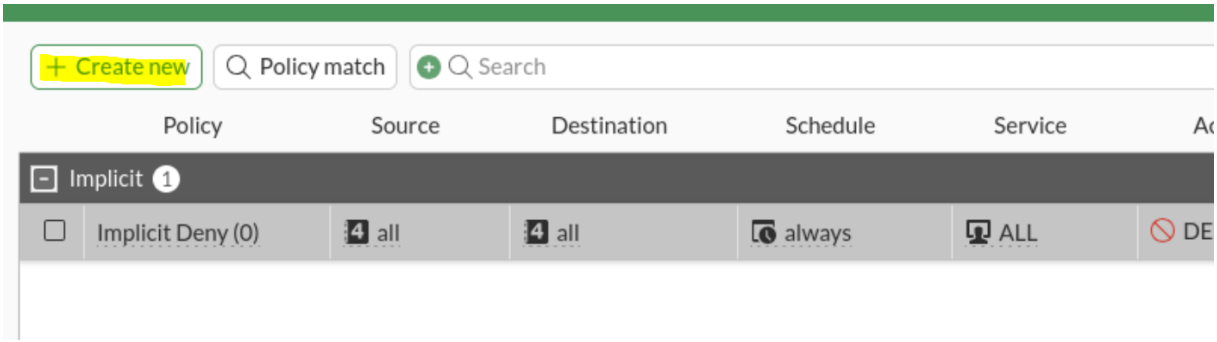
Firewall et règles

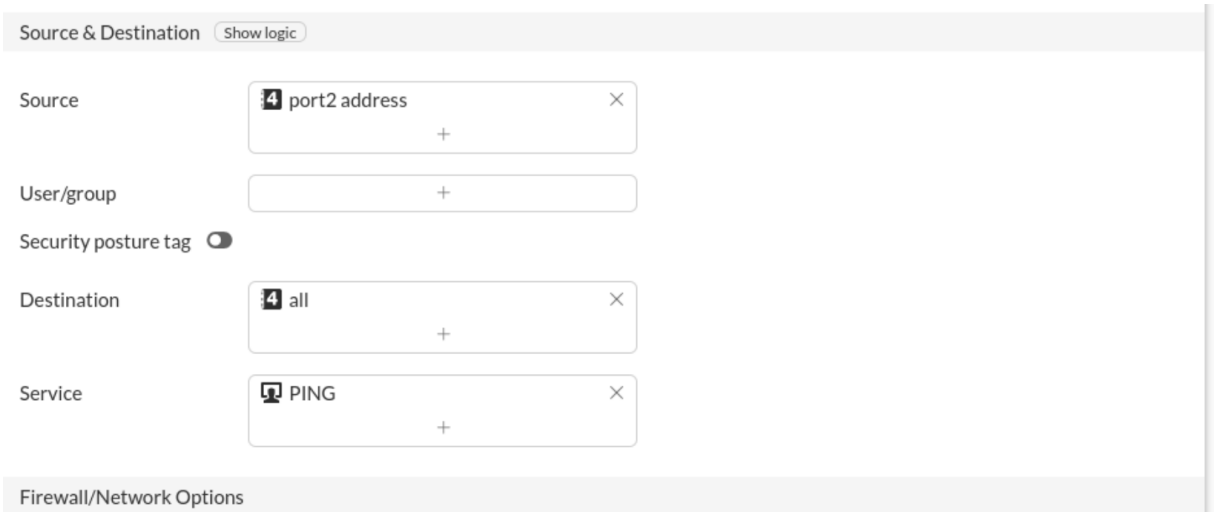
Nous allons configurer notre première règle de firewall

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

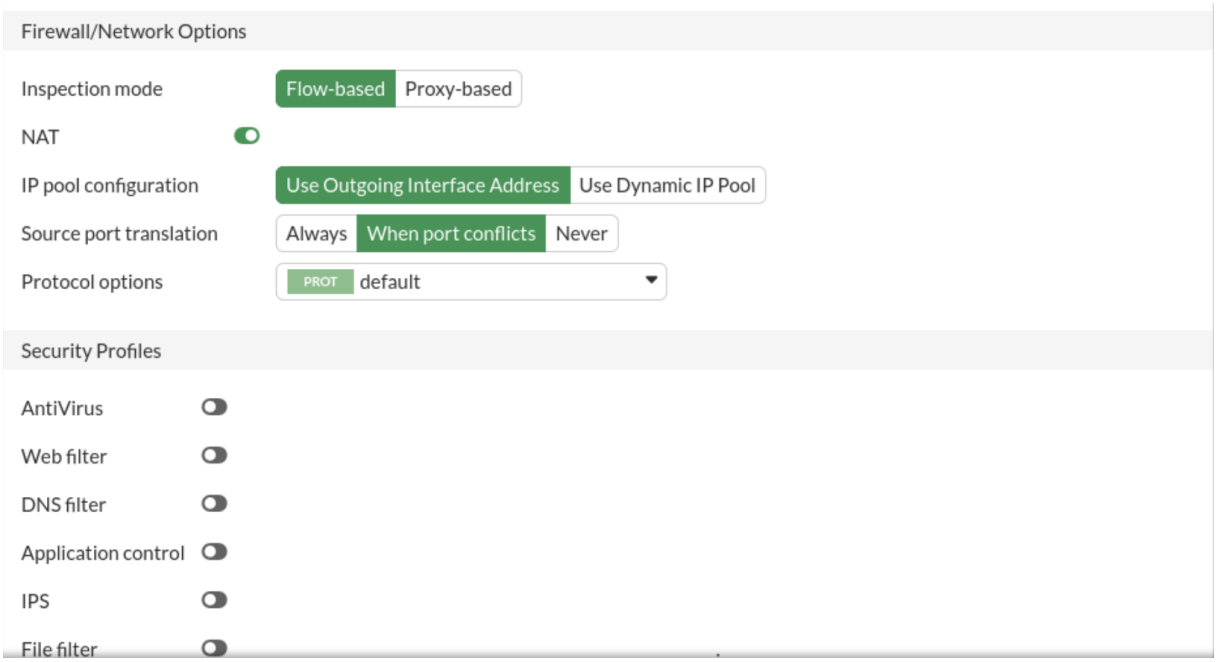
```
┌──(root㉿kali)-[~]
└─# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
^C
--- 1.1.1.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1002ms


┌──(root㉿kali)-[~]
└─#
```

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



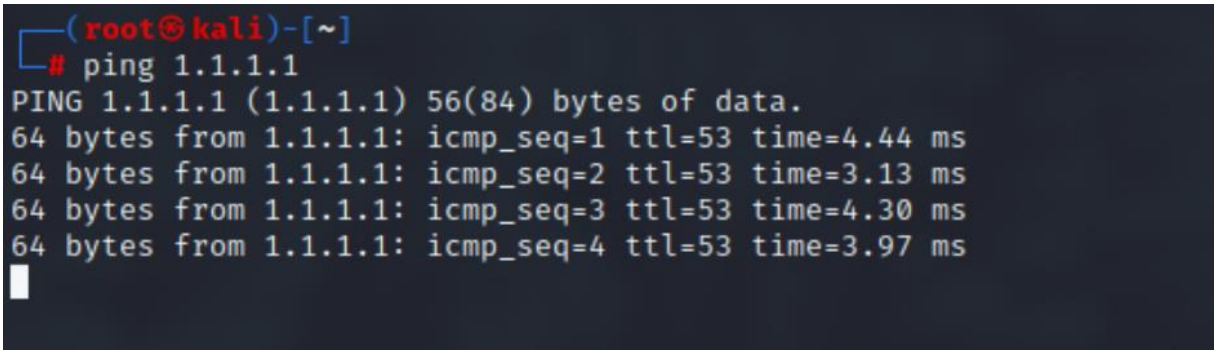


On voit que le NAT se configure directement dans la règle



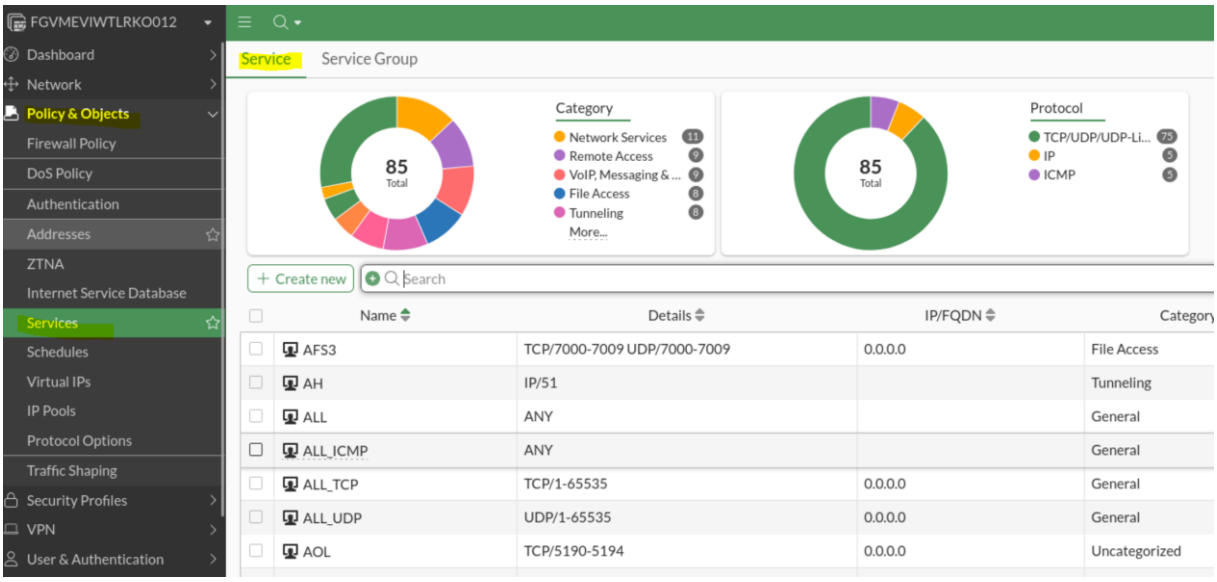
Résultat

Maintenant le ping passe

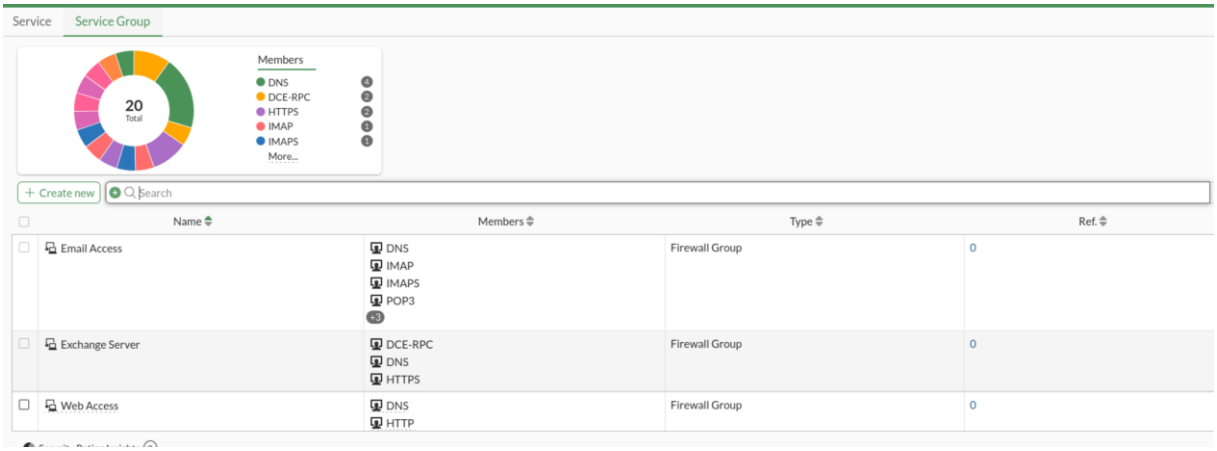


Le firewall fonctionne avec des objets

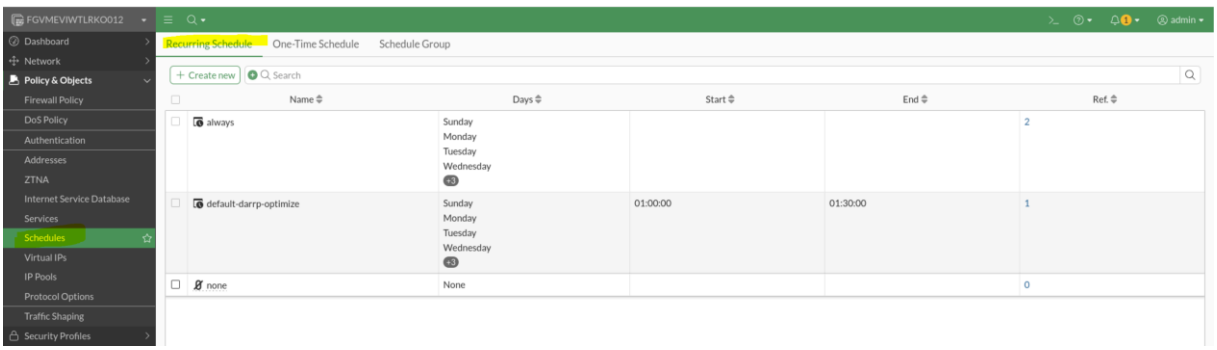
Chaque service est un objet



Et nous avons des groupes de services déjà configuré



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

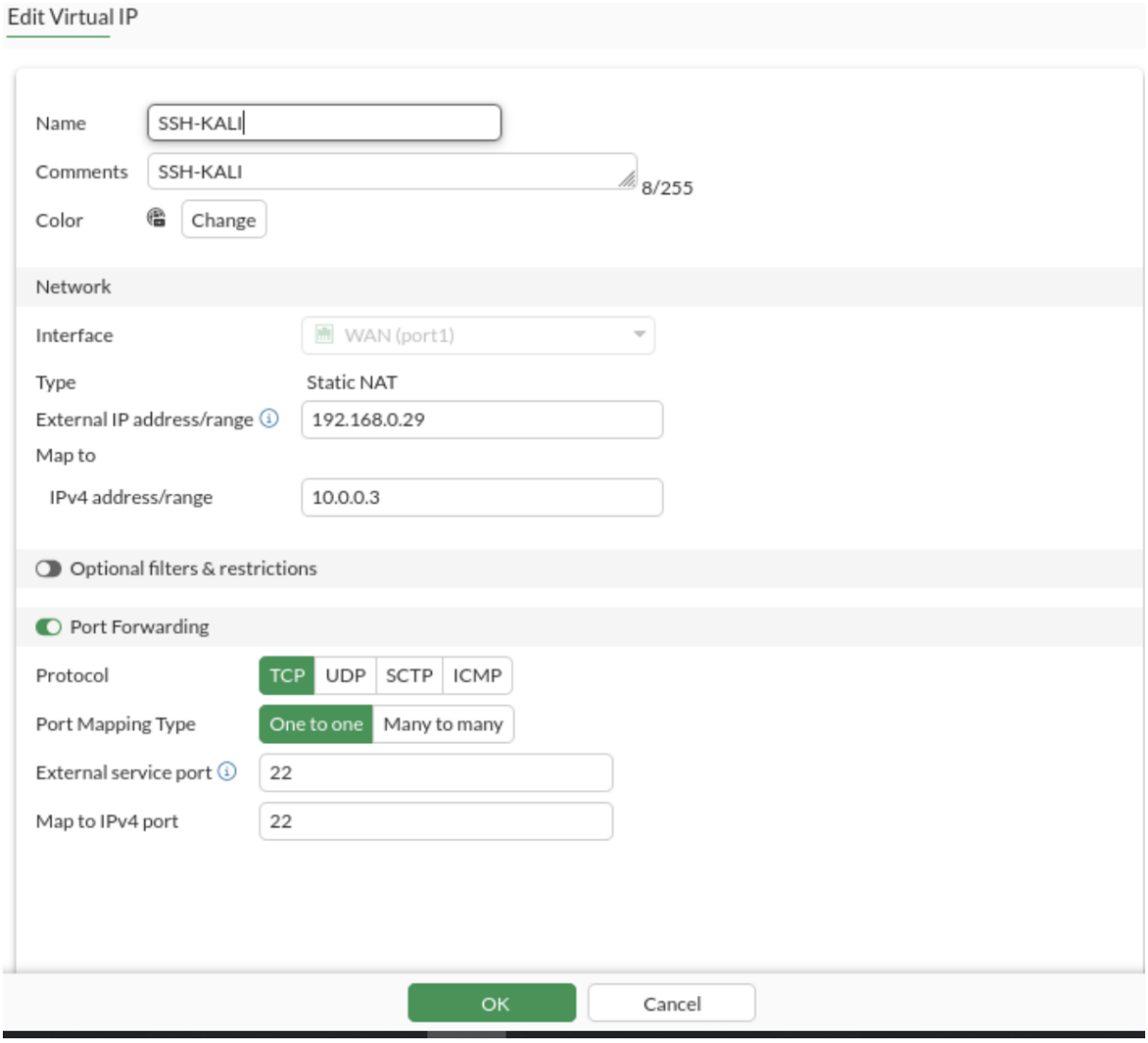


Mise en place d’une regle DNAT

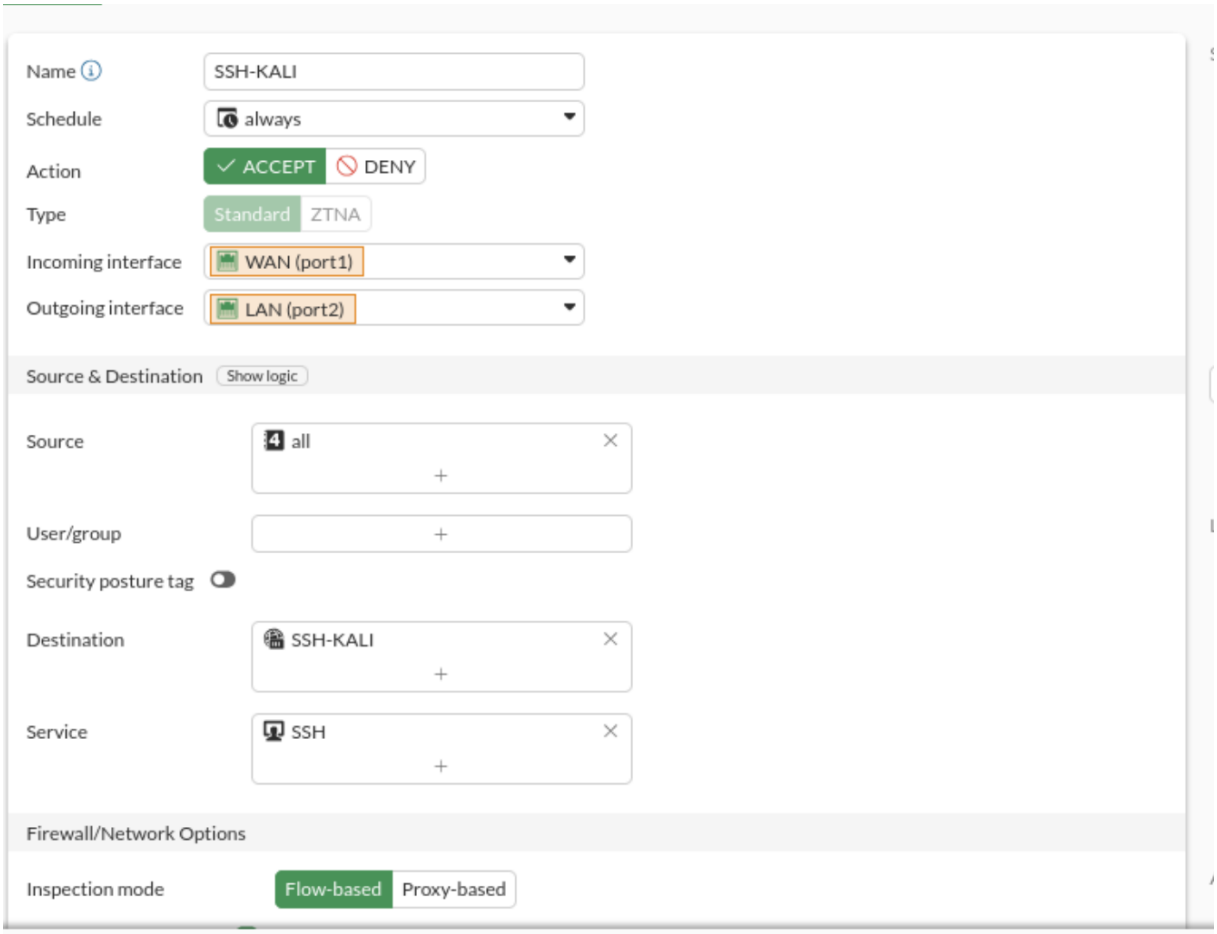
Il faut d’abord aller dans Policy object > Virtual IP

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’etaler dessus

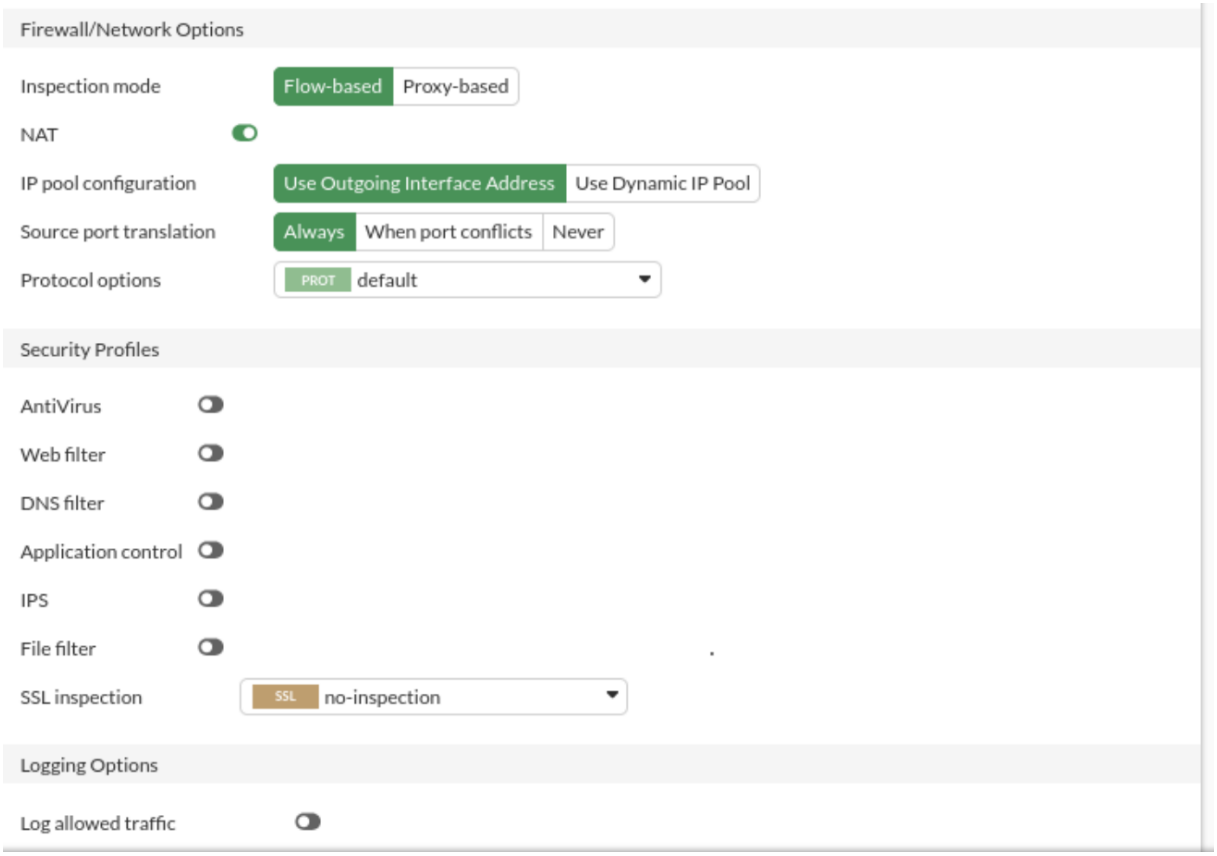


Le plus important est dans les règles de firewall il faut créer une règle pour autoriser ce flux



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

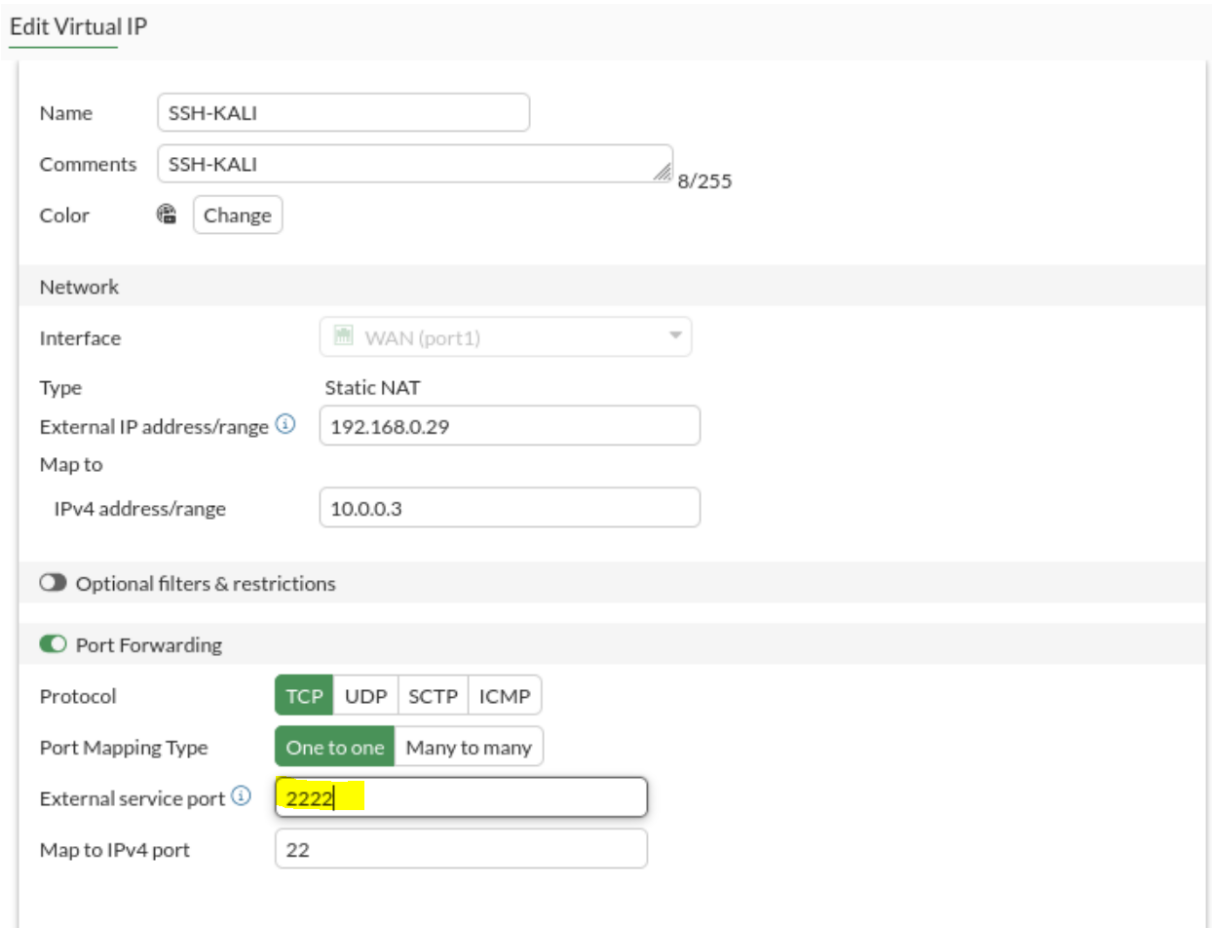


Je lance un test

```
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)-[~]
└─#
```

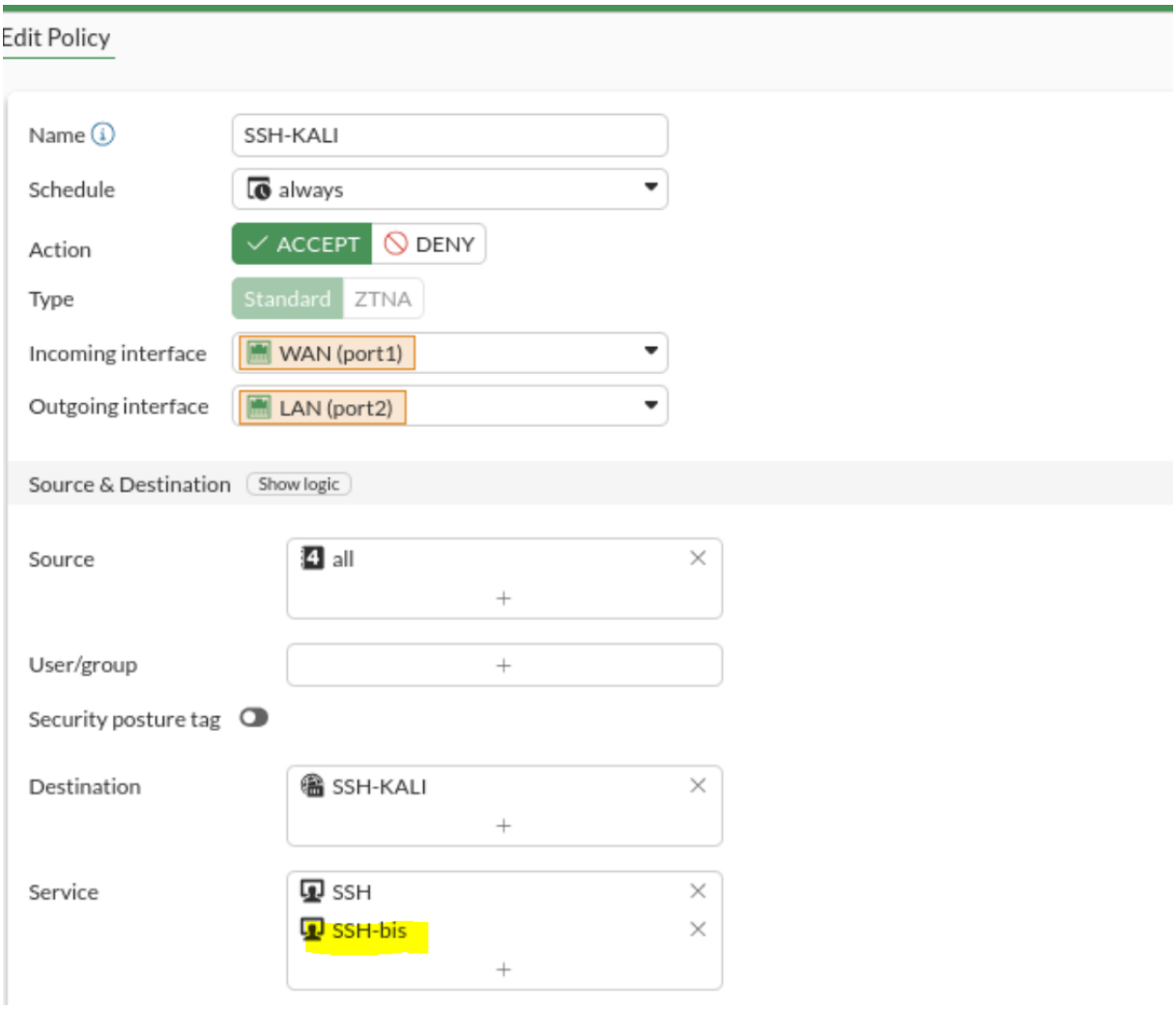
C'est parfait sa fonctionne

Maintenant je change le port exterieur de 22 à 2222



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

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



Ça fonctionne

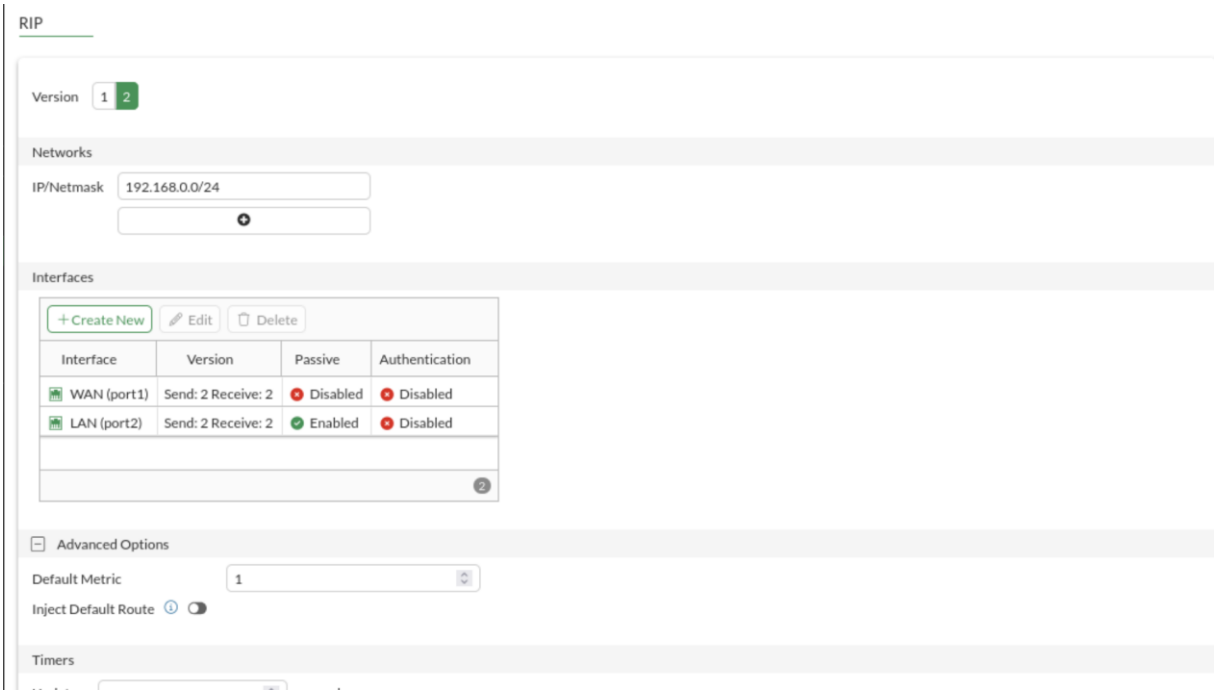
```
root@dedier:~# ssh -p 2222 root@192.168.0.29
root@192.168.0.29's password:
Linux kali 5.10.0-kali2-amd64 #1 SMP Debian 5.10.9-1kali1 (2021-01-22) x86_64

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)-[~]
└─#
```

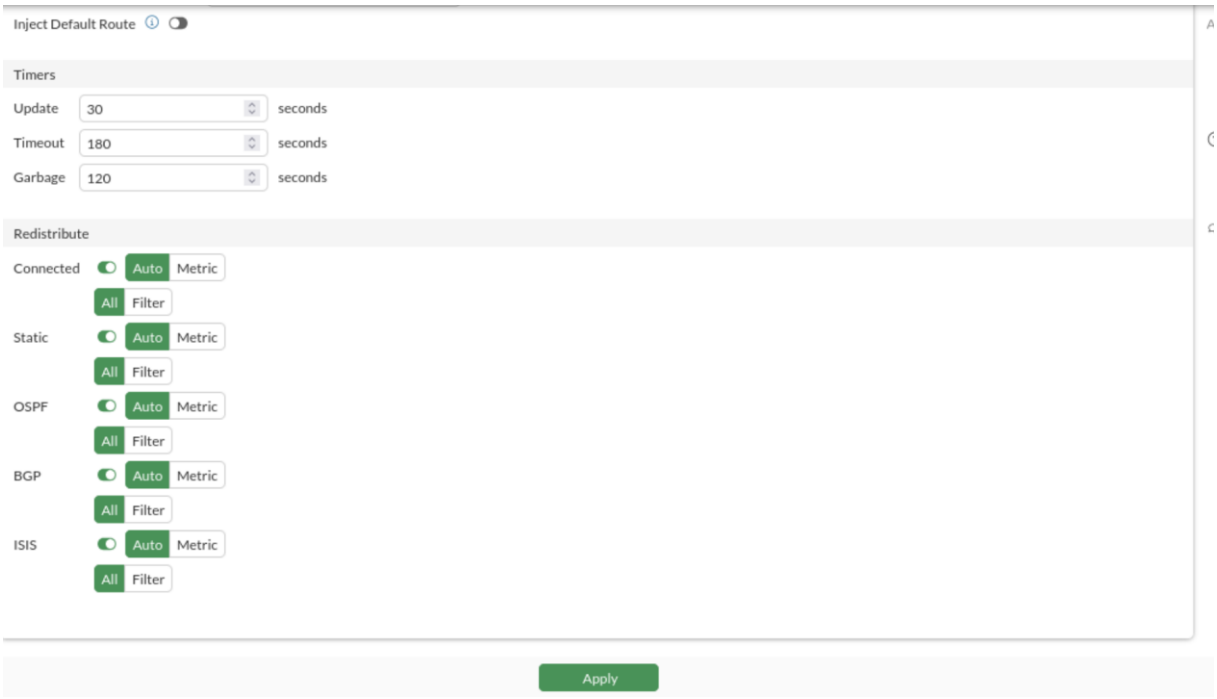
C'est parfait

Mise en place de RIP

J’ai déjà plusieurs nœuds rip

Je vais dans network > RIP



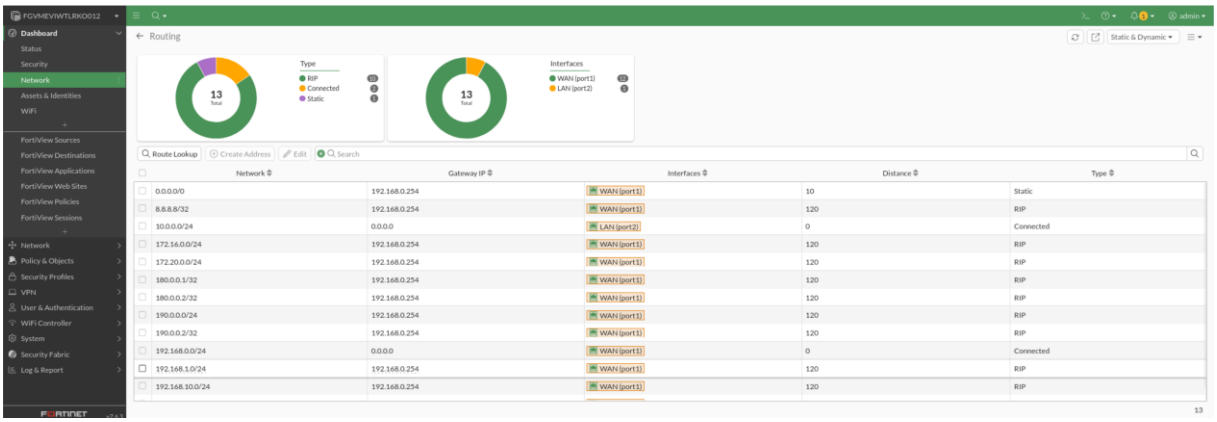


Avec la commande get router info protocols je vais avoir des informations sur les protocoles de routage utiliser

```
  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 operations lourdes simplement efficacement en tant qu'admin sys il ne faut jamais avoir peur de la CLI.

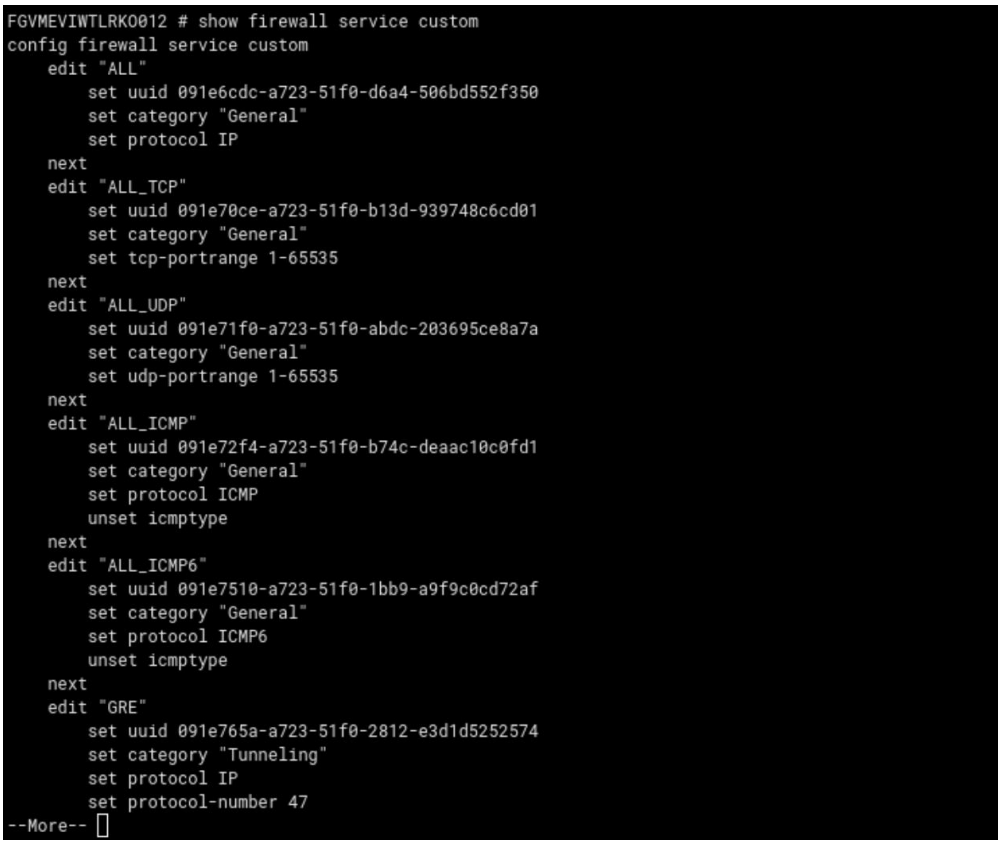
A mon avis pour les operations lourdes vaut mieu passer en CLI et les operations légères vaut mieu passer par la WEBUI

Voir les groupes de services

Show firewall service group

```
FGVMEVIWTLRKO012 # 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



On peut aussi pour les groupe effectur

Config firewall service grou

Show

End

```
FGVMEVIWTLRKO012 # config firewall service group

FGVMEVIWTLRKO012 (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

FGVMEVIWTLRKO012 (group) # end
```

Création d'un service group WEB_ONLY

```
FGVMEVIWTLRKO012 # config firewall service group

FGVMEVIWTLRKO012 (group) # edit WEB_ONLY
new entry 'WEB_ONLY' added

FGVMEVIWTLRKO012 (WEB_ONLY) # set member HTTP HTTPS

FGVMEVIWTLRKO012 (WEB_ONLY) # next

FGVMEVIWTLRKO012 (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

```
FGVMEVIWTLRKO012 # config firewall service custom

FGVMEVIWTLRKO012 (custom) # edit TCP_8080
new entry 'TCP_8080' added

FGVMEVIWTLRKO012 (TCP_8080) # set tcp-portrange 8080

FGVMEVIWTLRKO012 (TCP_8080) # next

FGVMEVIWTLRKO012 (custom) # end
```

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

```
FGVMEVIWTLRKO012 # config firewall service group

FGVMEVIWTLRKO012 (group) # edit WEB_ONLY

FGVMEVIWTLRKO012 (WEB_ONLY) # append member TCP_8080

FGVMEVIWTLRKO012 (WEB_ONLY) # next

FGVMEVIWTLRKO012 (group) # end
```

Créer une règle

```
FGVMEVIWTLRKO012 # config firewall policy

FGVMEVIWTLRKO012 (policy) # edit 10
new entry '10' added

FGVMEVIWTLRKO012 (10) # set name "LAN_TO_WAN_WEB"

FGVMEVIWTLRKO012 (10) # set srcintf "port2"

FGVMEVIWTLRKO012 (10) # set dstintf "port1"

FGVMEVIWTLRKO012 (10) # set srcaddr "all"

FGVMEVIWTLRKO012 (10) # set dstaddr "all"

FGVMEVIWTLRKO012 (10) # set action accept

FGVMEVIWTLRKO012 (10) # set schedule "always"

FGVMEVIWTLRKO012 (10) # set service "WEB_ONLY"

FGVMEVIWTLRKO012 (10) # set nat enable

FGVMEVIWTLRKO012 (10) # next

FGVMEVIWTLRKO012 (policy) # end

FGVMEVIWTLRKO012 #
```

Voila la base pour créer une regle dans le firewall

Afficher contenue d'une règle

Show firewall policy <numero regle>

```
FGVMEVIWTLRKO012 # 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 configué

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 reconfigré le DHCP qui englobe l’interface LAN

```
FGVMEVIWTLRKO012 # config system dhcp server

FGVMEVIWTLRKO012 (server) # edit 2

FGVMEVIWTLRKO012 (2) # set interface "port2"

FGVMEVIWTLRKO012 (2) # set netmask 255.255.255.0

FGVMEVIWTLRKO012 (2) # set default-gateway 10.0.0.254

FGVMEVIWTLRKO012 (2) # set dns-service default

FGVMEVIWTLRKO012 (2) # config ip-range

FGVMEVIWTLRKO012 (ip-range) # delete 1

FGVMEVIWTLRKO012 (ip-range) # edit 1
new entry '1' added

FGVMEVIWTLRKO012 (1) # set start-ip 10.0.0.1

FGVMEVIWTLRKO012 (1) # set end-ip 10.0.0.253

FGVMEVIWTLRKO012 (1) # next

FGVMEVIWTLRKO012 (ip-range) # end

FGVMEVIWTLRKO012 (2) # next

FGVMEVIWTLRKO012 (server) # end

FGVMEVIWTLRKO012 #
```

Activer le serveur

```
FGVMEVIWTLRKO012 # config system dhcp server

FGVMEVIWTLRKO012 (server) # edit 2

FGVMEVIWTLRKO012 (2) # set status enable

FGVMEVIWTLRKO012 (2) # next

FGVMEVIWTLRKO012 (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

```
FGVMEVIWTLRKO012 # diagnose debug application  dhcps -1
Debug messages will be on for 30 minutes.

FGVMEVIWTLRKO012 # [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

```
FGVMEVIWTLRKO012 # config firewall vip

FGVMEVIWTLRKO012 (vip) # edit "webserver"
new entry 'webserver' added

FGVMEVIWTLRKO012 (webserver) # set extinf "port1"

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

FGVMEVIWTLRKO012 (webserver) # set extintf "port1"

FGVMEVIWTLRKO012 (webserver) # set extip 192.168.0.29

FGVMEVIWTLRKO012 (webserver) # set mappedip 10.0.0.3

FGVMEVIWTLRKO012 (webserver) # set portforward enable

FGVMEVIWTLRKO012 (webserver) # set extport 8080

FGVMEVIWTLRKO012 (webserver) # set mappedport 80

FGVMEVIWTLRKO012 (webserver) # next

FGVMEVIWTLRKO012 (vip) # end

FGVMEVIWTLRKO012 #
```

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

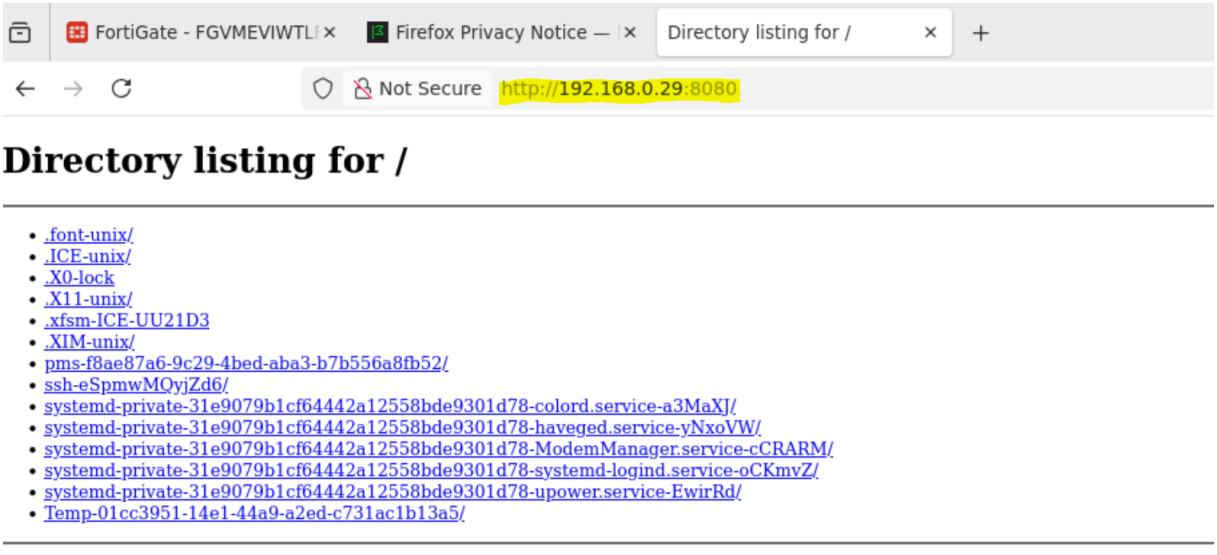
```
FGVMEVIWTLRKO012 # config firewall policy

FGVMEVIWTLRKO012 (policy) # edit 11
new entry '11' added

FGVMEVIWTLRKO012 (11) # set name "WAN_TO_WEBSERVER"

FGVMEVIWTLRKO012 (11) # set srcintf "port1"

FGVMEVIWTLRKO012 (11) # set dstintf "port2"

FGVMEVIWTLRKO012 (11) # set srcaddr "all"

FGVMEVIWTLRKO012 (11) # set dstaddr "webserver"

FGVMEVIWTLRKO012 (11) # set action accept

FGVMEVIWTLRKO012 (11) # set schedule "always"

FGVMEVIWTLRKO012 (11) # set service "WEB_ONLY"

FGVMEVIWTLRKO012 (11) # set nat enable

FGVMEVIWTLRKO012 (11) # next

FGVMEVIWTLRKO012 (policy) # end

FGVMEVIWTLRKO012 #
```

Pour voir nos adresse virtuelles sois nos DNAT

Il faut faire show firewall vip

```
FGVMEVIWTLRKO012 # 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



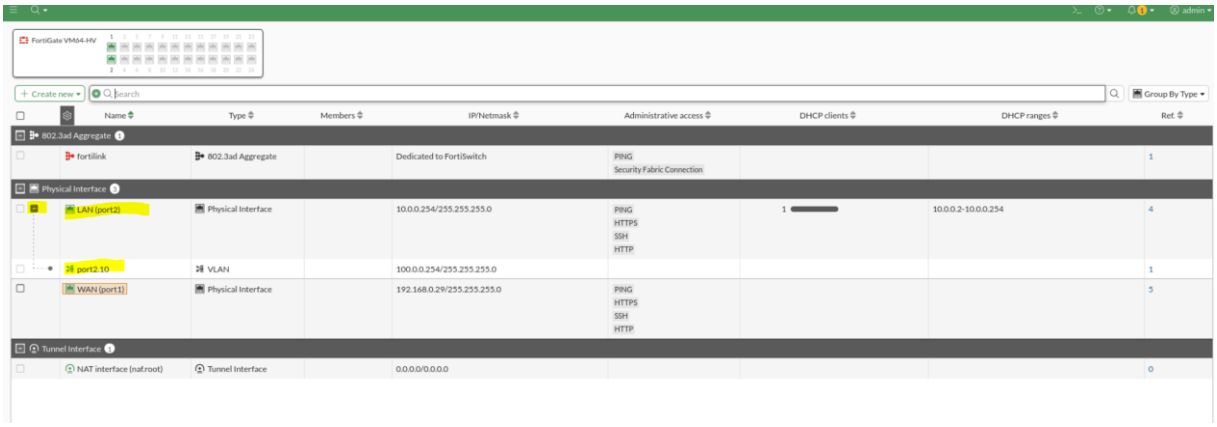
Interface virtuelle pour routage intervlan

La premiere interface virtuelle

config system interface

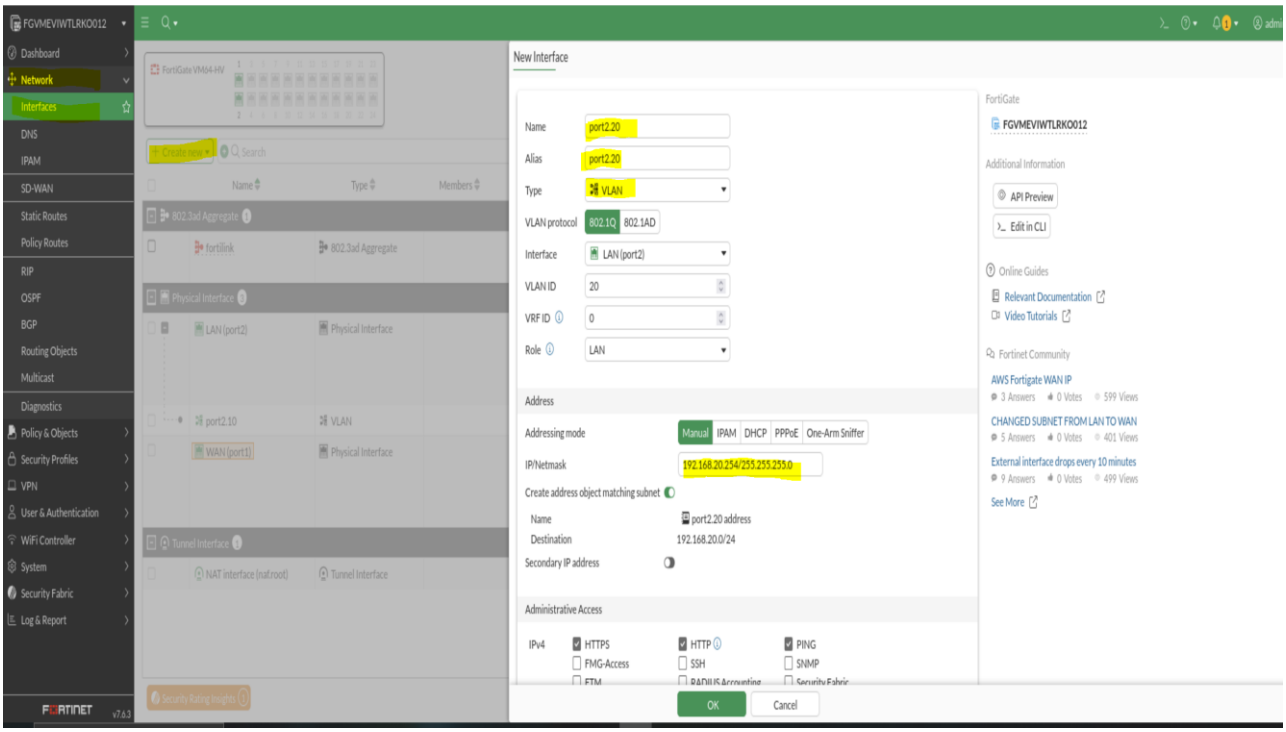
```
FGVMEVIWTLRKO012 (interface) # edit port2.10
new entry 'port2.10' added

FGVMEVIWTLRKO012 (port2.10) # set vdom root

FGVMEVIWTLRKO012 (port2.10) # set vlanid 10

FGVMEVIWTLRKO012 (port2.10) # set ip 100.0.0.254/24

FGVMEVIWTLRKO012 (port2.10) # set interface port2

FGVMEVIWTLRKO012 (port2.10) # next

FGVMEVIWTLRKO012 (interface) # end

FGVMEVIWTLRKO012 #
```

Dans l'interface graphique je vois l'interface virtuelle

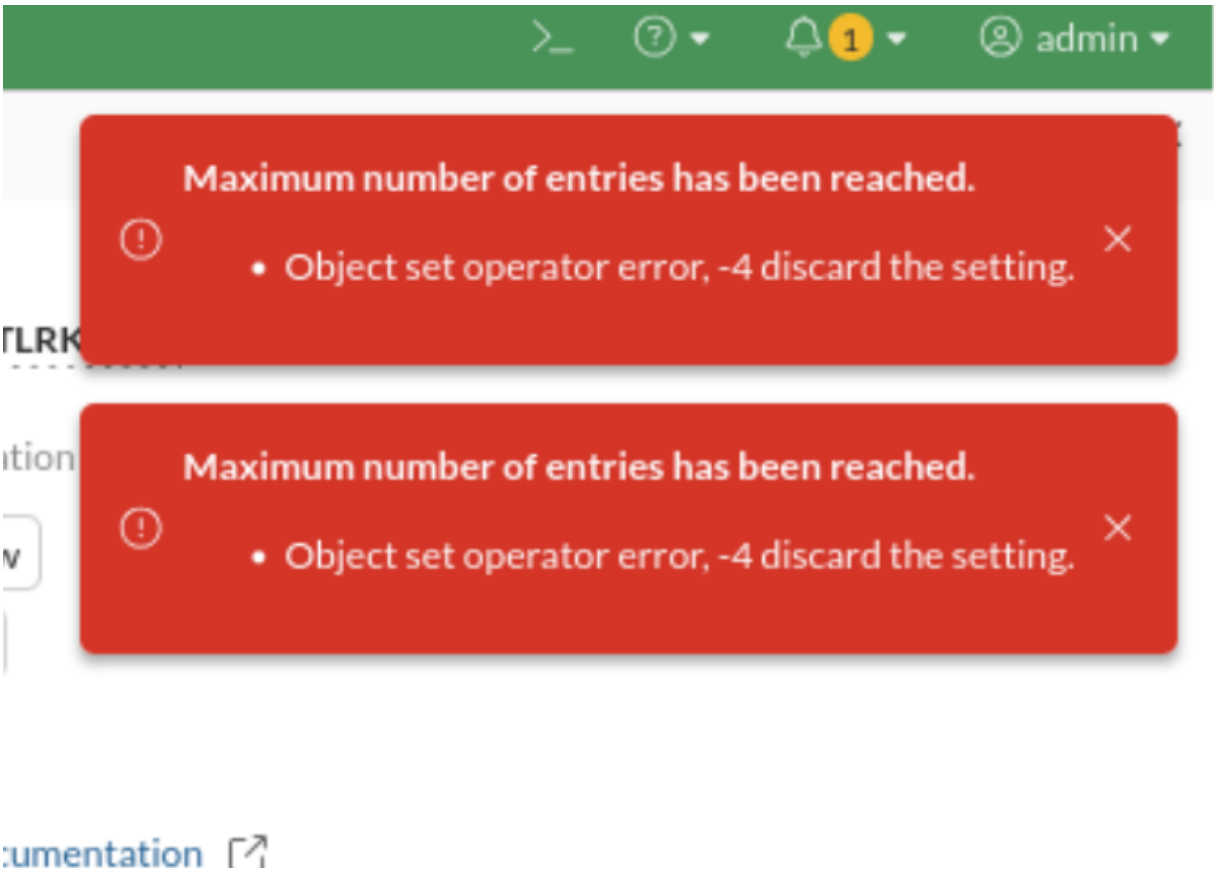


Pour la seconde interface je passe en interface graphique mais erreur licence gratuite donc impossible

Car je fais face à une erreur bizarre



Erreur nombre maximum d’interface



cumentation

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

```
FGVMEVIWTLRKO012 # config system dhcp server

FGVMEVIWTLRKO012 (server) # edit 3
new entry '3' added

FGVMEVIWTLRKO012 (3) # set interface "port2.10"

FGVMEVIWTLRKO012 (3) # set netmask 255.255.255.0

FGVMEVIWTLRKO012 (3) # set default-gateway 100.0.0.254

FGVMEVIWTLRKO012 (3) # set dns-service default

FGVMEVIWTLRKO012 (3) # config ip-range

FGVMEVIWTLRKO012 (ip-range) # edit 1
new entry '1' added

FGVMEVIWTLRKO012 (1) # set start-ip 100.0.0.1

FGVMEVIWTLRKO012 (1) # set end-ip 100.0.0.250

FGVMEVIWTLRKO012 (1) # next

FGVMEVIWTLRKO012 (ip-range) # end

FGVMEVIWTLRKO012 (3) # next

FGVMEVIWTLRKO012 (server) # end

FGVMEVIWTLRKO012 #
```

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