

Configuration d'un pare-feu Fortigate M2L

Dans le cadre de l'évolution et sécurisation du parc informatique de la M2L, la solution FORTINET a été choisie, C'est un routeur faisant également office de pare-feu équipé de multiples options de sécurisation , de filtrages web , configuration VPN et autres.

Cahier des charges

- Remplacement du commutateur SWM2L(lvl3) et du routeur RTRM2L du contexte.
- Le pare-feu FORTINET FORTIGATE 30e assure la sécurisation des zones LAN,DMZ,WAN mais également la translation d'adresse NAT/PAT entre LAN et WAN, le filtrage des accès web et la configuration VPN.

Contraintes

- Aucun changement sur le plan d'adressage

Initialisation

Tout d'abord pour réinitialiser le Fortinet il faudrait:

1. se rendre dans le mode console -
2. écrire admin
3. appuyer sur entrer 2 fois (vue qu'il n'y a pas encore de mot de passe (dans notre cas))
4. écrire execute factory et puis entrer

Configuration Initiale

Admin

config system interface #entre directement dans l'interface

edit port1 #pour edité l'interface n°1

set mode static #Port en statique donc pas de DHCP

set IP 172.1.2.254/24 (par exemple)

set allowaccess http ssh ping #accord des permission d'accès à distance avec l'adresse IP

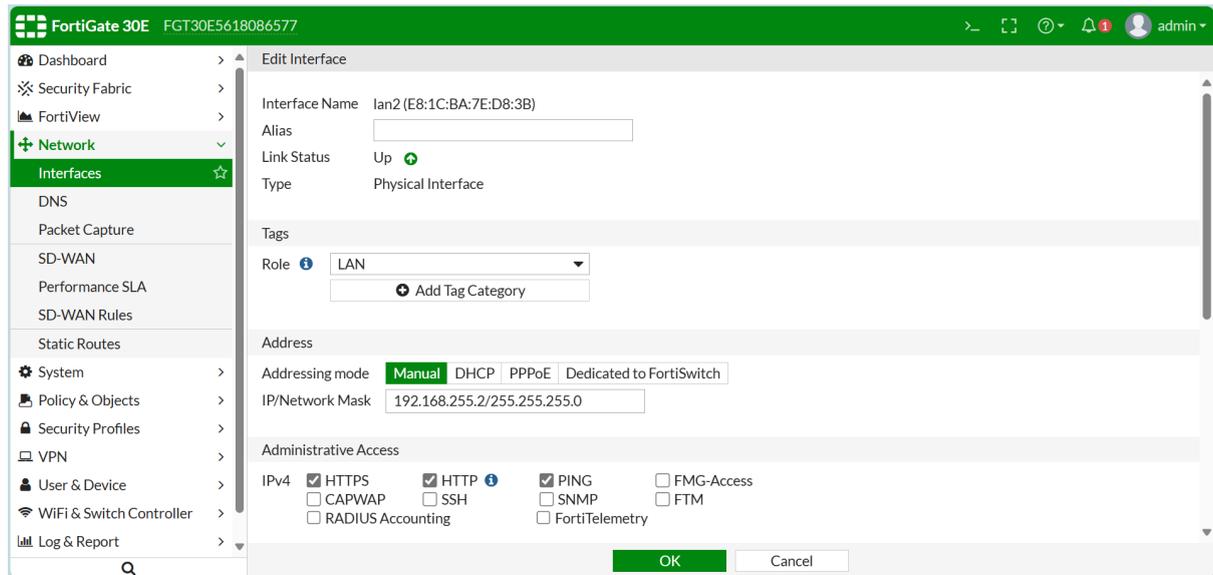
show #Vérification des paramètres

end #effectuer une sauvegarde

Configuration des interface LAN

Tout d'abord, après s'être log sur le routeur, on a créé une interface avec l'UI sur le LAN correspondant, ici le LAN 2 avec l'adresse 192.168.255.2 255.255.255.0 .

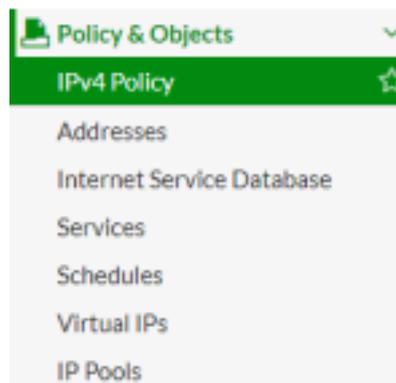
On'y active les accès HTTPS,HTTP pour les services web, PING pour les tests, SSH pour les connexions à distances CAPWAP et FMG-Access.



Filtrage firewall

Pour créer un filtrage firewall, il faut faire une **nouvelle Policy** mais avant de créer cette Policy il faudra créer des adresses (ce n'est pas obligatoire cela dépend de quel filtrage que tu veux faire), il y deux façons de le faire

La première méthode est d'aller directement dans adresse



Ensuite faire un create -> adresse, il faut lui donner un nom et une adresse range par exemple 10.49.0.0/16

Name	<input type="text" value="Data"/>
Type	IP/Netmask
Subnet / IP Range	<input type="text" value="10.49.0.0/255.255.0.0"/>
Interface	<input type="checkbox"/> any
Show in Address List	<input checked="" type="checkbox"/>
Static Route Configuration	<input type="checkbox"/>
Comments	<input type="text" value=""/> 0/255

La deuxième méthode est de créer directement dans l'IPv4 Policy

On fait créer une nouvelle Policy -> cliquer sur source

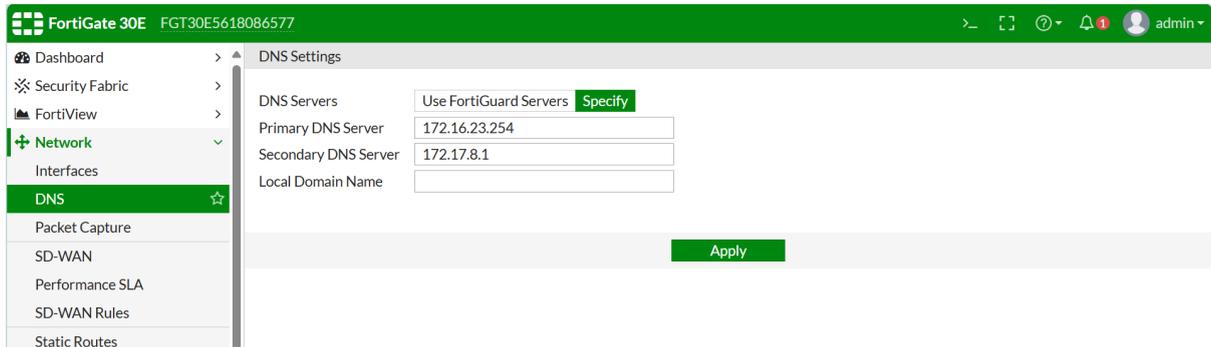
ensuite + puis **adresse** .

Par la suite nous allons dans IPv4 Policy, puis créer un filtre qui permet à la ranger de l'adresse 10.49.0.0 d'accéder à internet

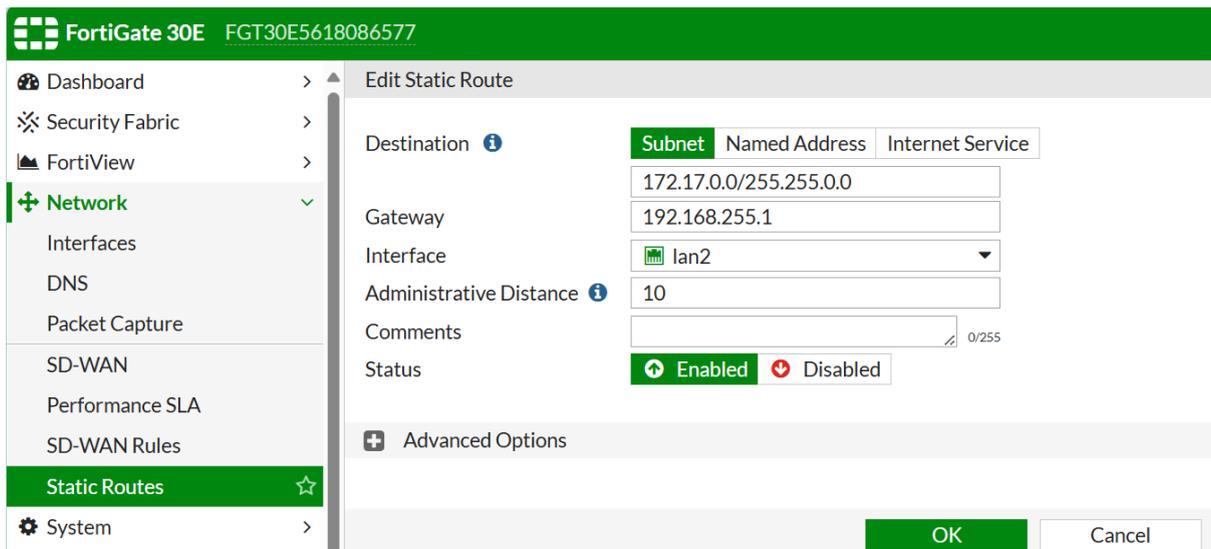
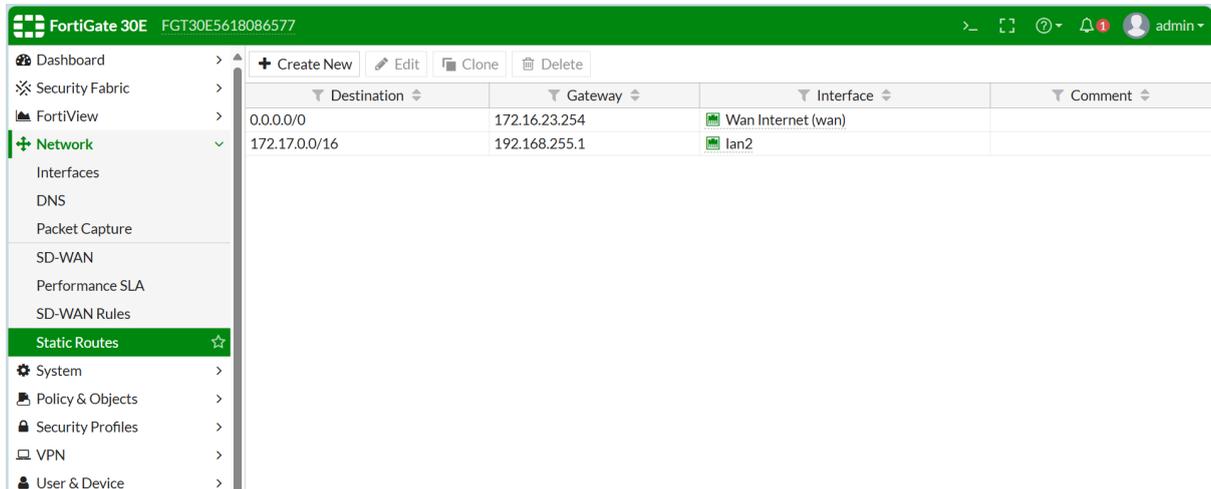
On fait créer une nouvelle Policy

Name	<input type="text" value="DATA => internet"/>
Incoming Interface	<input type="text" value="lan"/>
Outgoing Interface	<input type="text" value="wan2"/>
Source	<input type="text" value="Data"/>
Destination Address	<input type="text" value="all"/>
Schedule	<input type="text" value="always"/>
Service	<input type="text" value="ALL"/>
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN
Firewall / Network Options	
NAT	<input checked="" type="checkbox"/>
Fixed Port	<input type="checkbox"/>
IP Pool Configuration	<input checked="" type="checkbox"/> Use Outgoing Interface Address <input type="checkbox"/> Use Dynamic IP Pool
Security Profiles	
AntiVirus	<input type="checkbox"/>
Web Filter	<input type="checkbox"/>
DNS Filter	<input type="checkbox"/>
Application Control	<input type="checkbox"/>
CASI	<input type="checkbox"/>
SSL Inspection	<input type="checkbox"/>
Logging Options	
Log Allowed Traffic	<input checked="" type="checkbox"/> Security Events <input type="checkbox"/> All Sessions
Comments	<input type="text" value="Write a comment..."/> 0/1023
Enable this policy	<input checked="" type="checkbox"/>

Configuration du DNS

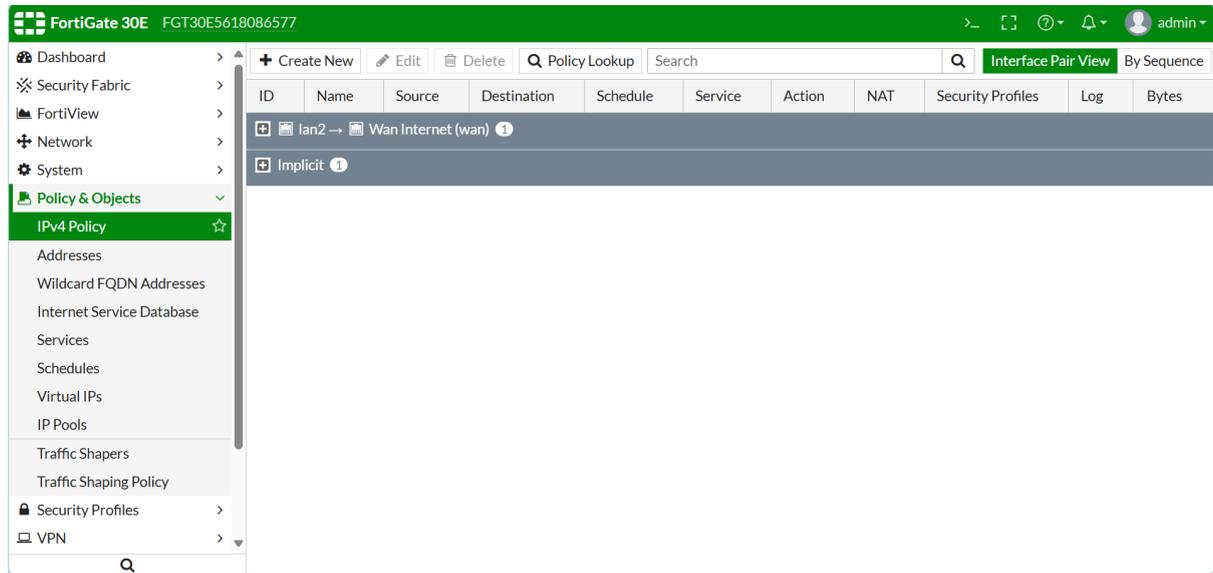


Configuration de la route statique



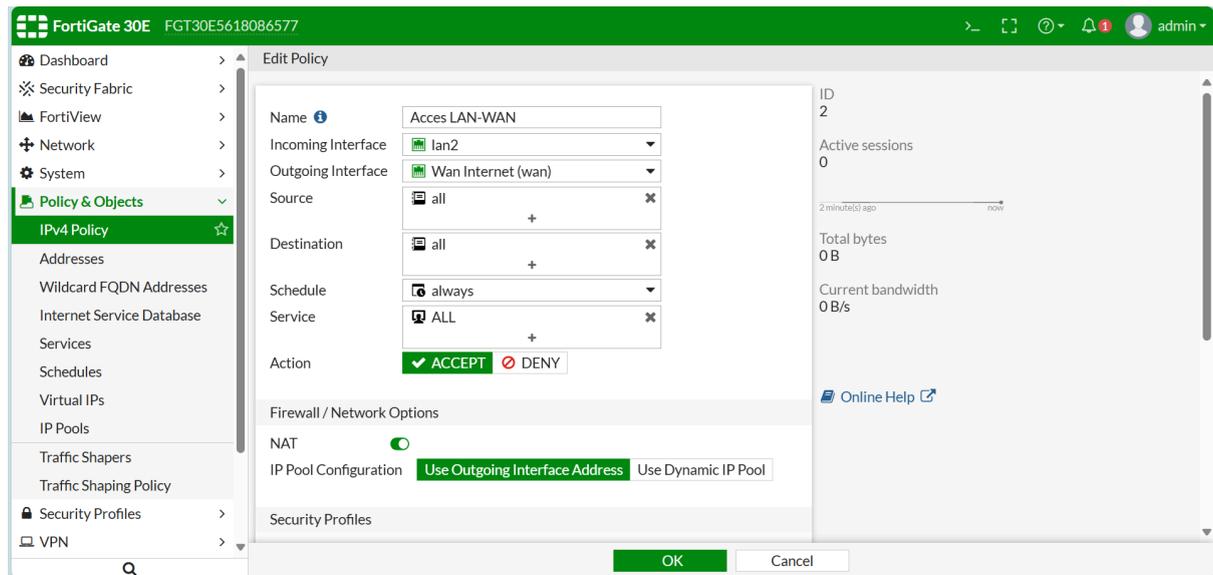
Liaison LAN-WAN

On va dans Policy & Objects > IPv4 Policy



The screenshot shows the FortiGate 30E management interface. The left sidebar is expanded to 'Policy & Objects' > 'IPv4 Policy'. The main area displays a table of IPv4 policies. The table has columns for ID, Name, Source, Destination, Schedule, Service, Action, NAT, Security Profiles, Log, and Bytes. Two policies are listed: 'lan2 -> Wan Internet (wan)' and 'Implicit'. The 'lan2 -> Wan Internet (wan)' policy is selected, and its details are visible in the 'Interface Pair View' tab at the top right.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
2	lan2 -> Wan Internet (wan)	lan2	Wan Internet (wan)							
1	Implicit									



The screenshot shows the 'Edit Policy' dialog box for the 'Access LAN-WAN' policy. The dialog is divided into several sections: 'Name', 'Incoming Interface', 'Outgoing Interface', 'Source', 'Destination', 'Schedule', 'Service', 'Action', 'Firewall / Network Options', and 'Security Profiles'. The 'Name' field is 'Access LAN-WAN'. The 'Incoming Interface' is 'lan2' and the 'Outgoing Interface' is 'Wan Internet (wan)'. The 'Source' and 'Destination' are both set to 'all'. The 'Schedule' is 'always' and the 'Service' is 'ALL'. The 'Action' is 'ACCEPT'. The 'Firewall / Network Options' section has 'NAT' checked and 'IP Pool Configuration' set to 'Use Outgoing Interface Address'. The 'Security Profiles' section is empty. On the right side, there are statistics: 'ID: 2', 'Active sessions: 0', 'Total bytes: 0 B', and 'Current bandwidth: 0 B/s'. At the bottom, there are 'OK' and 'Cancel' buttons.

Name: Access LAN-WAN

Incoming Interface: lan2

Outgoing Interface: Wan Internet (wan)

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT

Firewall / Network Options: NAT (checked)

IP Pool Configuration: Use Outgoing Interface Address

Security Profiles:

Statistics: ID: 2, Active sessions: 0, Total bytes: 0 B, Current bandwidth: 0 B/s

Configuration des Portail VPN SSL

Pour commencer, il faut cliquer sur VPN -> IPsec Wizard -> custom , vous appuyer sur Next

1 VPN Setup

Name

Template Type

< Back

Next >

Après il faut configurer le tunnel du VPN

FortiGate 60F FW_DPA_DEP_LAM

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN**
 - Overlay Controller VPN
 - IPsec Tunnels**
 - IPsec Wizard
 - IPsec Tunnel Templates
 - SSL-VPN Portals
 - SSL-VPN Settings
- User & Device
- WiFi & Switch Controller
- Log & Report

Edit VPN Tunnel

Name: DPA-SiegeSecour

Comments: DPA_ENTREPOT

Network

IP Version: IPv4

Remote Gateway: Static IP Address

IP Address: 185.91.234.39

Interface: SFR 4G (wan2)

Local Gateway:

Mode Config:

NAT Traversal: Enable Disable Forced

Keepalive Frequency: 10

Dead Peer Detection: Disable On Idle On Demand

Ensuite la création du tunnel du VPN

D'abord créer une clé pré-partagée

Network

Remote Gateway : Static IP Address (185.91.234.39) , Interface : wan2

Authentication

Method: Pre-shared Key

Pre-shared Key:

IKE

Version: 1 2

Phase 1 Proposal

Authentication

 Edit

Authentication Method : Pre-shared Key

IKE Version : 2

Phase 1 Proposal

 Add

Encryption

AES128

Authentication

SHA256

Diffie-Hellman Groups

- 31 30 29 28 27 21
 20 19 18 17 16 15
 14 5 2 1

Key Lifetime (seconds)

86400

Local ID

160

Phase 2 Selectors

Phase 1 Proposal

 Edit

Algorithms : AES128-SHA256

Diffie-Hellman Groups : 14, 5

Phase 2 Selectors

Name	Local Address	Remote Address
DPA-SiegeSecour	10.43.0.0/255.255.0.0	10.0.0.0/255.0.0.0 

Edit Phase 2

Name

DPA-SiegeSecour

Comments

Comments

Local Address

Subnet

10.43.0.0/255.255.0.0

Remote Address

Subnet

10.0.0.0/255.0.0.0

 Advanced...

Subnet

Advanced...

Phase 2 Proposal

Encryption Authentication

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group

<input type="checkbox"/>	31	<input type="checkbox"/>	30	<input type="checkbox"/>	29	<input type="checkbox"/>	28	<input type="checkbox"/>	27	<input type="checkbox"/>	21
<input type="checkbox"/>	20	<input type="checkbox"/>	19	<input type="checkbox"/>	18	<input type="checkbox"/>	17	<input type="checkbox"/>	16	<input type="checkbox"/>	15
<input checked="" type="checkbox"/>	14	<input checked="" type="checkbox"/>	5	<input type="checkbox"/>	2	<input type="checkbox"/>	1				

Local Port All

Remote Port All

Protocol All

Auto-negotiate

Autokey Keep Alive

Key Lifetime

Seconds

une fois que tout cela est fait , il faut créer une nouvelle route pour accéder au vpn

Destination

Device

Administrative Distance

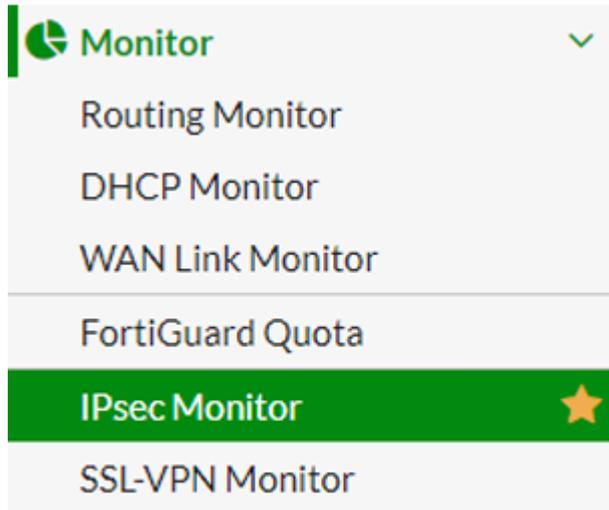
Comments 0/255

Status

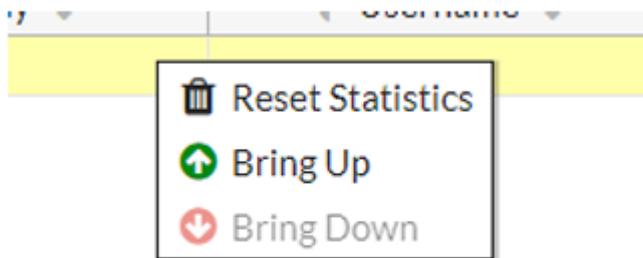
Advanced Options

Lorsque vous choisissez le vpn dans device, il retire automatiquement le Gateway

Une fois la route créer, il est nécessaire de d'aller dans monitor -> IPsec monitor

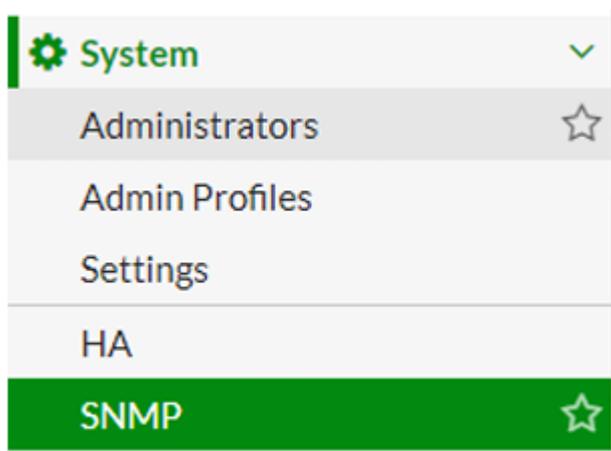


Puis vous faite une clique droite et vous cliquer sur Bring-up



Configuration SNMP

Donc dans l'onglet SNMP



On y ajoute le nom de la communauté et renseigner l'adresse du VPN, ensuite on active le SNMP Agent en haut de l'écran.

Community Name

Hosts:

IP Address/Netmask	Interface	Host Type	Delete
<input type="text"/>	ANY	Accept queries and send traps	

Queries:

Protocol	Port	Enable
v1	<input type="text" value="161"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="161"/>	<input checked="" type="checkbox"/>

Traps:

Protocol	Local	Remote	Enable
v1	<input type="text" value="162"/>	<input type="text" value="162"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="162"/>	<input type="text" value="162"/>	<input checked="" type="checkbox"/>

SNMP Events

- CPU usage is high
- Log disk space is low
- VPN tunnel up
- WiFi Controller AP up
- FortiSwitch Controller Session up
- HA cluster status is changed
- HA member up
- Virus detected
- Fragmented email detected
- Oversized file/email blocked
- AV bypass happens
- BGP Established
- IPS anomaly detected
- IPS package updated
- System enters conserve mode
- MultiAnalyzer disconnected
- Memory is low
- Interface IP is changed
- VPN tunnel down
- WiFi Controller AP down
- FortiSwitch Controller Session down
- HA heartbeat failure
- HA member down
- Matched file pattern detected
- Oversized file/email detected
- Oversized file/email passed
- BGP Backward Transition
- IPS attack detected
- IPS network queue overflow
- System configuration is changed
- Nacira detected