



**Configuration de Pare-feu par interface Web,  
Mise en place de règles de filtrages et présentations de services**





**Mots-clés : pare-feu, pare-feu externe, WAN, LAN, DMZ, sécurité**

**Philippe JUNDT  
BTS SIO option SISR**

## Table des matières

I.	Accès depuis un terminal au Fortinet et option pare-feu :.....	2
II.	Création des adresses : .....	5
III.	Configuration des services .....	6
IV.	Configuration des profils de sécurités .....	7
V.	Création de règles de filtrage des sites .....	8
VI.	Création de règles de pare-feu .....	10
VII.	Configurer l'accès en NAT du pare-feu .....	11
VIII.	Configurer l'accès par interface NAT au WAN .....	13
IX.	Mise en réseaux des postes de travail pour l'accès réseau local et l'accès à internet.....	16
X.	Evolution possible .....	18

## Fiche de présentation

	<b>BTS SIO</b> <b>Services Informatiques</b> <b>aux Organisations</b>		
	<b>Option</b>	<b>SISR</b>	
	<b>Session</b>	<b>2021</b>	

<b>Philippe JUNDT</b>	<b>Activité professionnelle N°</b>	<b>1</b>
-----------------------	------------------------------------	----------

<b>Nature de l'activité</b>	
<b>Contexte</b>	Une société cherche permettre au personnel de travailler dans des infrastructures sécurisées.
<b>Objectifs</b>	Mise en place d'un firewall hardware pour réduire les ports d'entrée à une installation réseau, Présenter des services complémentaires pour sécuriser les profils utilisateurs des employés.
<b>Lieu de réalisation</b>	Laboratoire

DESCRIPTION DE LA SOLUTION RETENUE	
<b>Conditions initiales</b>	Absence de firewall et risque de récupération d'information sur des sites non sécurisé
<b>Conditions finales</b>	Présenter une documentation technique pour mettre en place des équipements Hardware
<b>Outils utilisés</b>	Site Equipement CISCO pour comparative des équipements, Cisco Packet Tracer

CONDITIONS DE REALISATION	
<b>Matériels</b>	Fortigate 200B, Fortinet
<b>Logiciels</b>	Accès à la console, accès en Web Modélisation Edraw
<b>Contraintes</b>	Estimer l'aménagement en ayant peu l'occasion de se rendre dans les locaux.

COMPETENCES MISES EN OEUVRE POUR CETTE ACTIVITE PROFESSIONNELLE	
	A1.1.1 , Analyse du cahier des charges d'un service à produire A1.1.2 , Étude de l'impact de l'intégration d'un service sur le système informatique A1.2.1 , Élaboration et présentation d'un dossier de choix de solution technique A1.2.2 , Rédaction des spécifications techniques de la solution retenue A1.3.1 , Test d'intégration et d'acceptation d'un service A1.3.4 , Déploiement d'un service A2.3.2 , Proposition d'amélioration d'un service A3.1.1 , Proposition d'une solution d'infrastructure A3.1.2 , Maquettage et prototypage d'une solution d'infrastructure A3.1.3 , Prise en compte du niveau de sécurité nécessaire à une infrastructure A4.1.9 , Rédaction d'une documentation technique A5.1.3 , Suivi d'une configuration et de ses éléments A5.1.5 , Évaluation d'un élément de configuration ou d'une configuration

## Le cahier des charges

### Expression des besoins :

Une société cherche permettre au personnel de travailler dans des infrastructures sécurisées.

### Description de l'existant :

Actuellement la société dispose d'un pare-feu hardware Fortinet 200B. qu'elle n'a pas configurée.

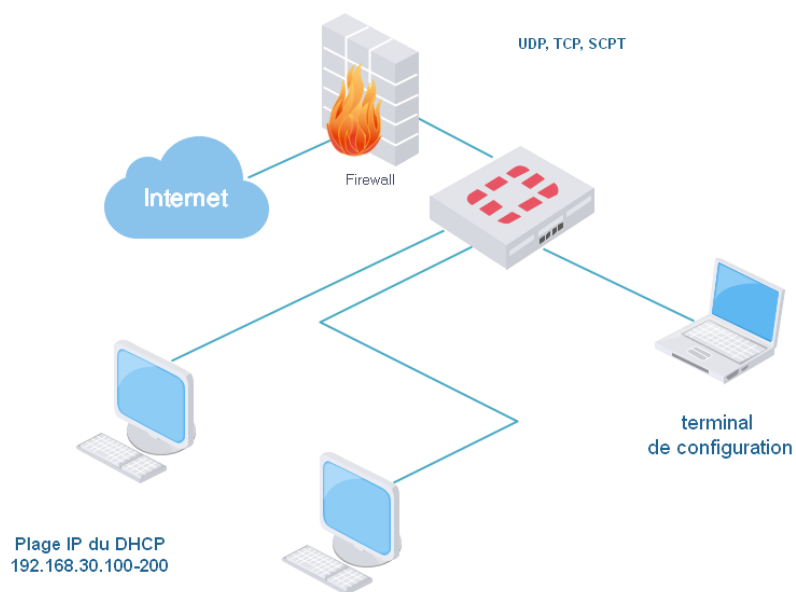
### Analyse du choix :

La société dispose déjà du matériel, il lui suffira de réaliser une mise à jour des licences anti-virus et pare-feu de l'équipement.

L'équipement est adapté aux TPME et PME offre des services tout en un avec notamment une prise en charge des services DMZ, une programmation de filtre de sites non souhaité.

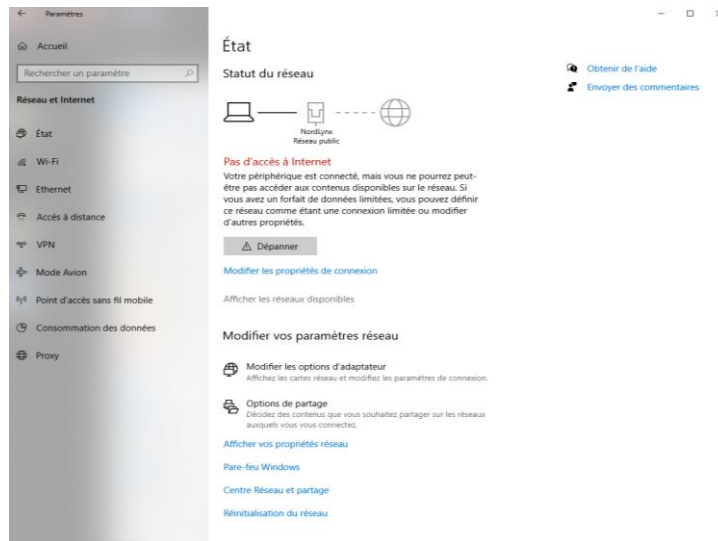
### Configuration du Fortinet

Pour limiter l'accès aux protocoles TCP, UDP et SCTP

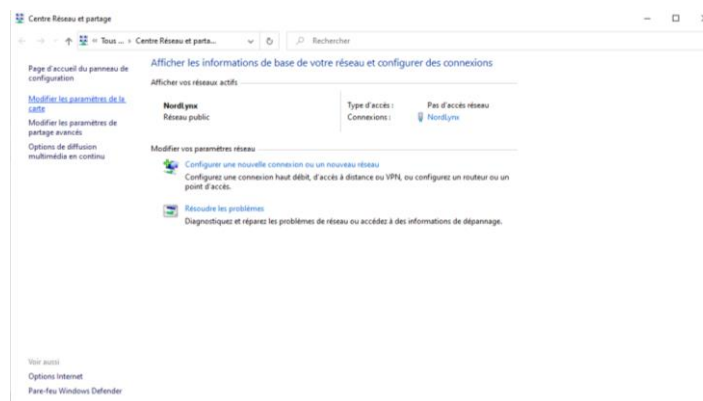


# Mise en œuvre

## I. Accès depuis un terminal au Fortinet et option pare-feu : Paramètre réseaux et internet :

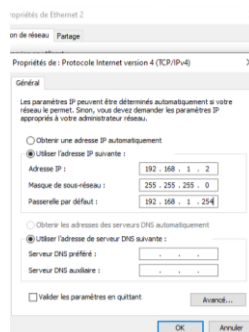


### Centre de réseau et de partage :



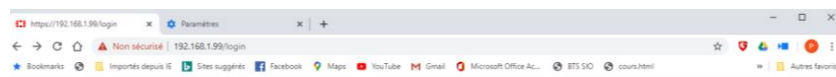
Configure le port qui permettra d'accéder à la console ou l'application Web du fortinet

Ip de terminal :192.168.1.2

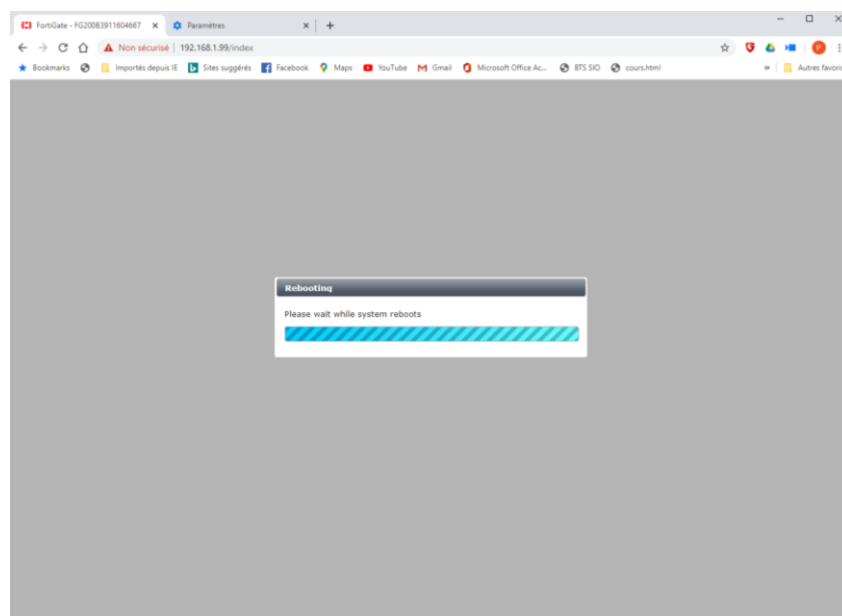


Une fois la carte réseau du terminal configurée, il reste à accéder à l'interface Web du fortinet :

Adresse constructeur : 192.168.1.99



Un rebooting est parfois nécessaire :



Il convient de s'assurer de la validité des certificats :

Name	Subject	Comments	Issuer	Expires	Status	Ref.
<b>Local CA Certificates (1)</b>						
Fortinet_CA_SSUProxy	C = US, CN = FortiGate CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority	This is the default CA certifi...	Fortinet	2030-03-06 11:43:20 GMT	OK	2
<b>Certificates (4)</b>						
Fortinet_Factory	C = US, CN = FG200B3911604667, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate	This certificate is embedded in...	Fortinet	2038-01-19 03:14:07 GMT	OK	1
Fortinet_Firmware	C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate	This certificate is embedded in...	Fortinet	2038-01-19 03:14:07 GMT	OK	1
Fortinet_SSUProxy	C = US, CN = FortiGate Server, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate		Fortinet	2030-03-06 11:43:22 GMT	OK	2
Fortinet_WiFi	C = US, CN = PositiveSSL, OU = auth-cert.fortinet.com	This certificate is embedded in...	Comodo CA Limited	2020-09-23 23:59:59 GMT	OK	1
<b>External CA Certificates (2)</b>						
Fortinet_CA	C = US, CN = support, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority		Fortinet	2038-01-19 22:34:39 GMT	OK	0
PositiveSSL_CA	CN = PositiveSSL CA, C = GB, L = Salford, O = Comodo CA Limited, ST = Greater Manchester		The USERTRUST Network	2020-05-30 10:48:38 GMT	OK	1

Il est possible de modifier la langue depuis les paramètres d'administration

**Paramètres des administrateurs**

Central Management  
☐ FortiManager ☒ FortiCloud ☐ Aucun

**Paramètres d'administration**

HTTP Port: 80 ☐ Redirect to HTTPS  
 HTTPS Port: 443 ☒ SSL-VPN Port Conflict  
 HTTPS Server Certificate: Fortinet\_Factory  
 Port Telnet: 23  
 Port SSH: 22  
 Administrateurs: 5 (1-480 mins)

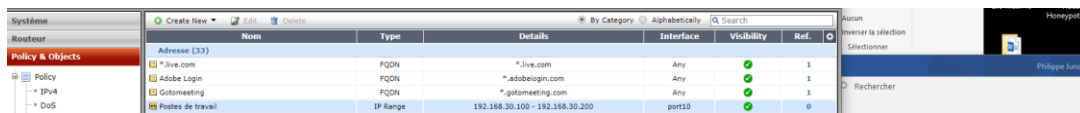
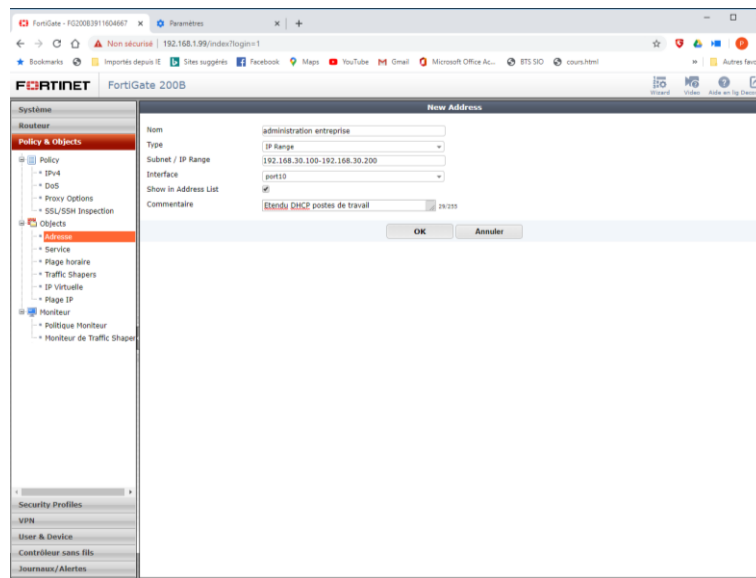
☐ Activer la politique des mots de passe

**View Settings**

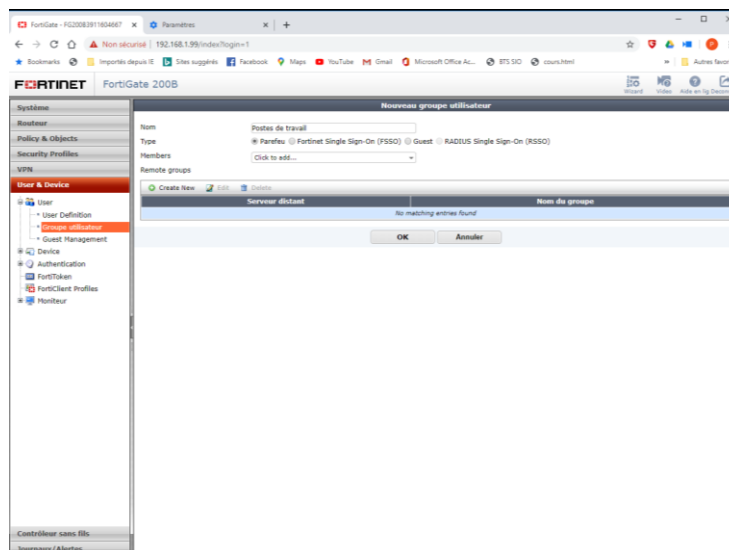
Language: Français  
 Lignes par page: 50 (20 - 1000)

Appliquer

## II. Création des adresses :



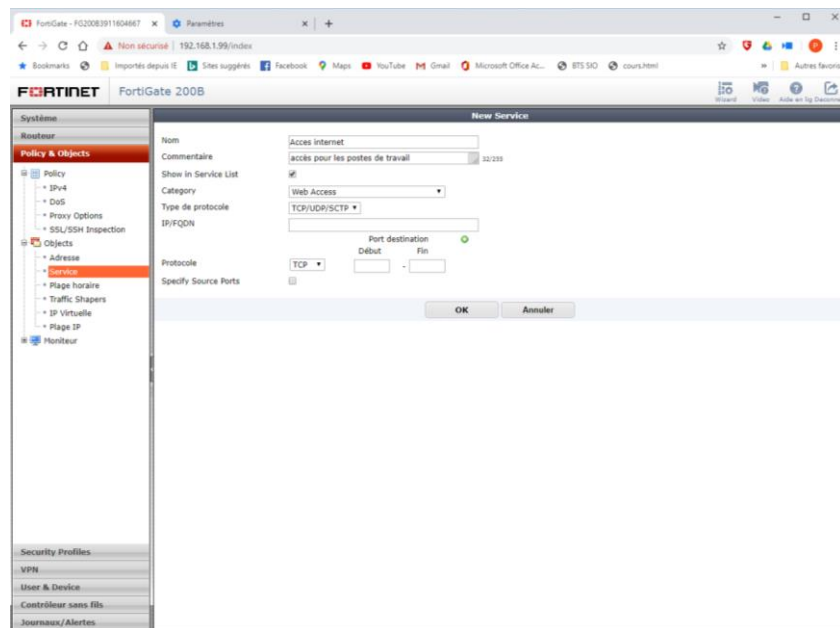
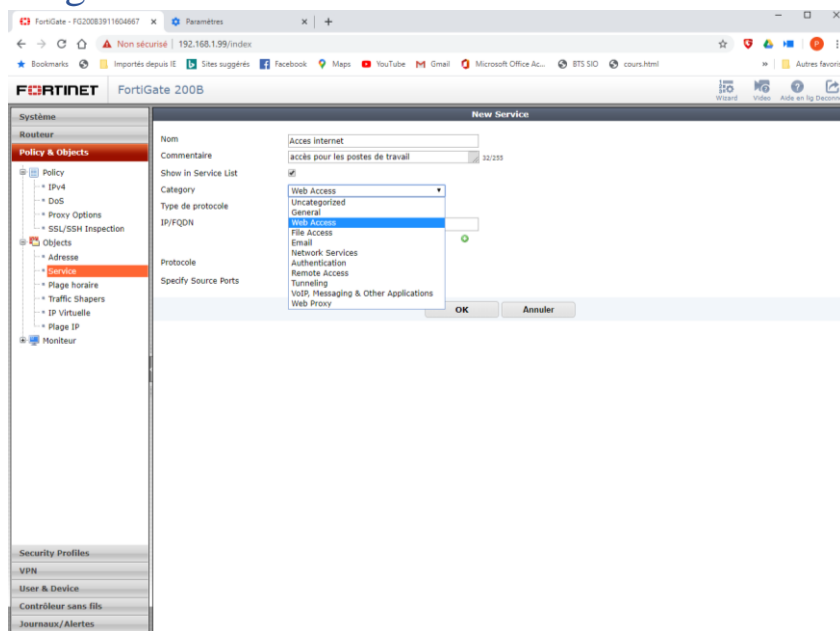
Ici nous mettons la même plage d'adresse IP que notre serveur DHCP qui est relié à une interface sur le Fortinet (Le port 10)



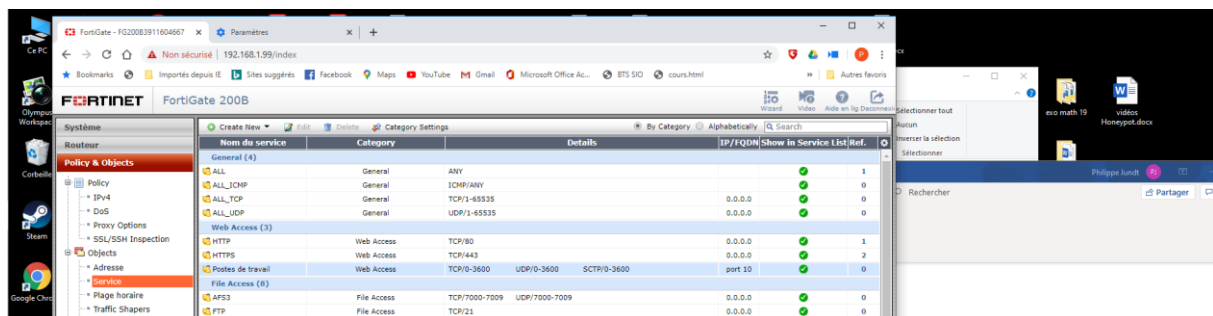
Il est possible si besoin de prévoir la création de LAN ou réseau interne via des mise en commandes dans les options de routage. Ici nous nous limiterons à un seul réseau de gestion et administration



### III. Configuration des services



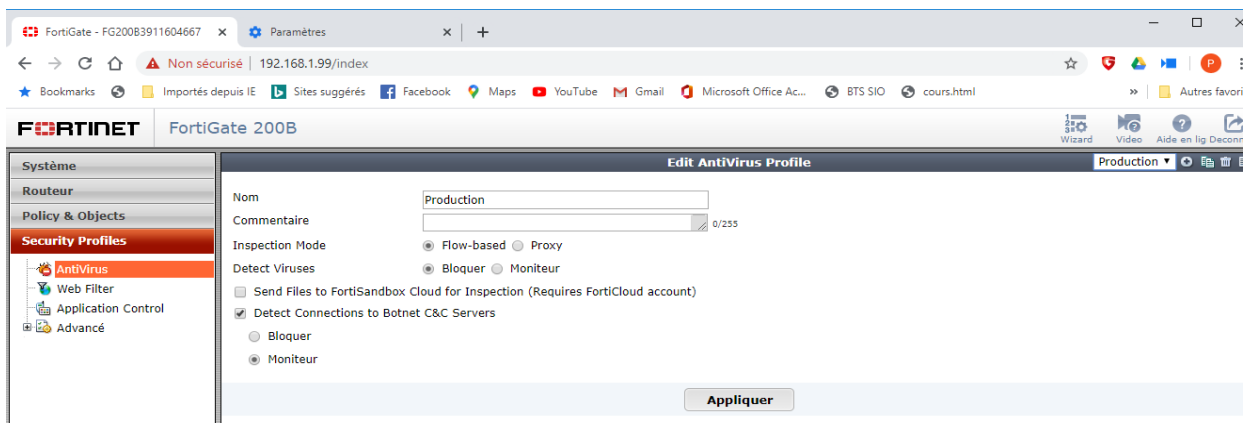
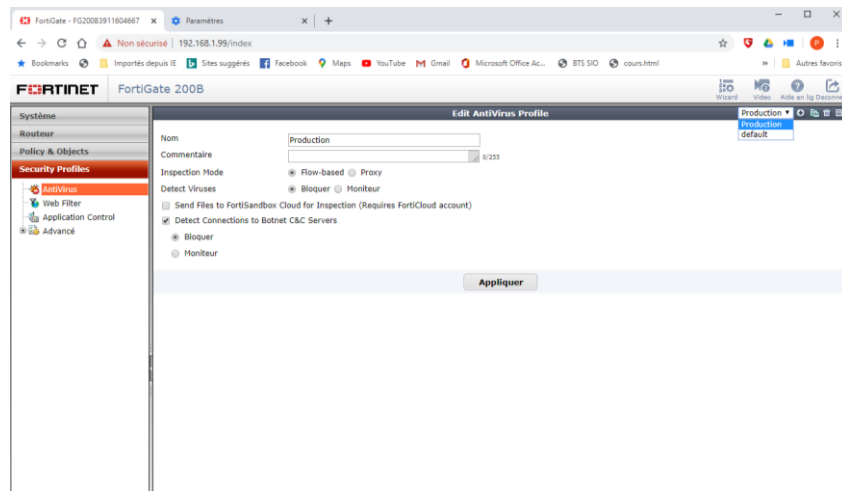
La création d'un groupe pour les services permettra une administration plus efficace par la suite.



A noter qu'il est parfois nécessaire de créer plusieurs demandes de service pour un même groupe en raison du paramétrage par filtre du pare-feu.

## IV. Configuration des profils de sécurité

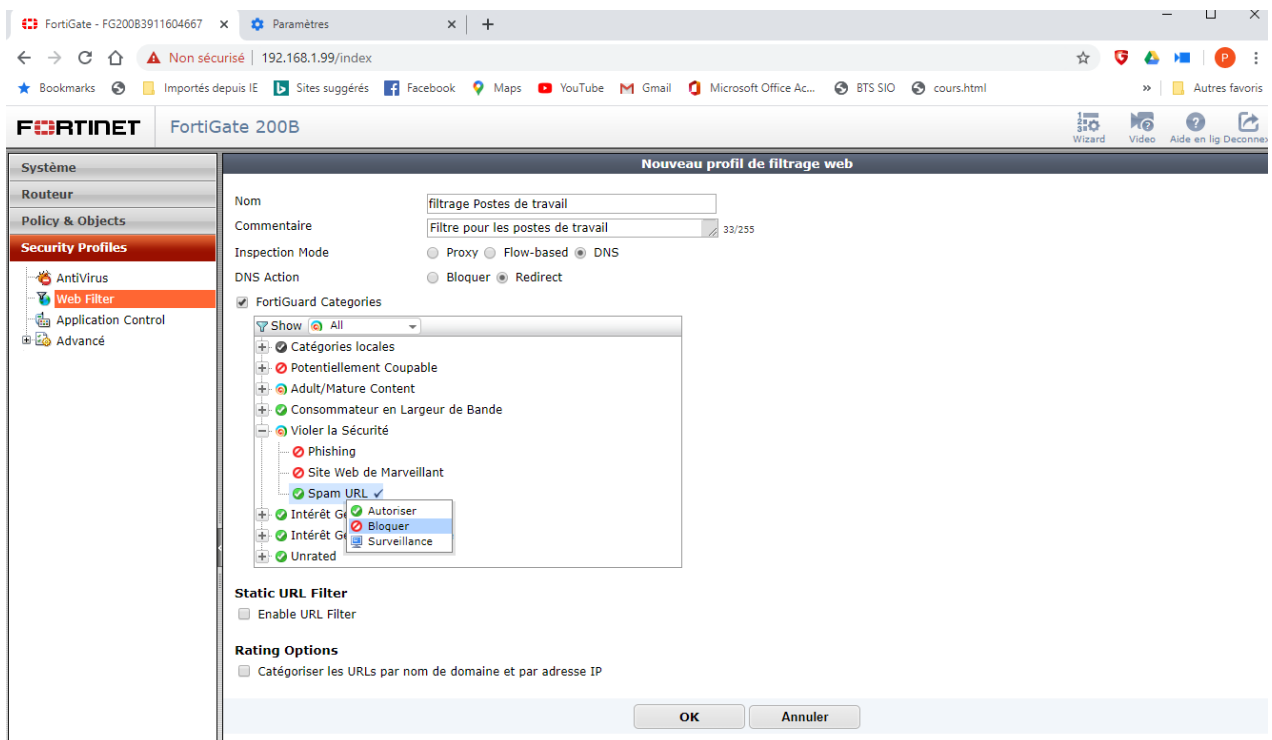
Il est important d'inclure l'analyse antivirus à l'interface de gestion, via l'onglet de profil de l'antivirus.



En fonction des configurations, un ensemble d'option apparait. Les protocoles sélectionnés implique des options par défaut.

## V. Création de règles de filtrage des sites

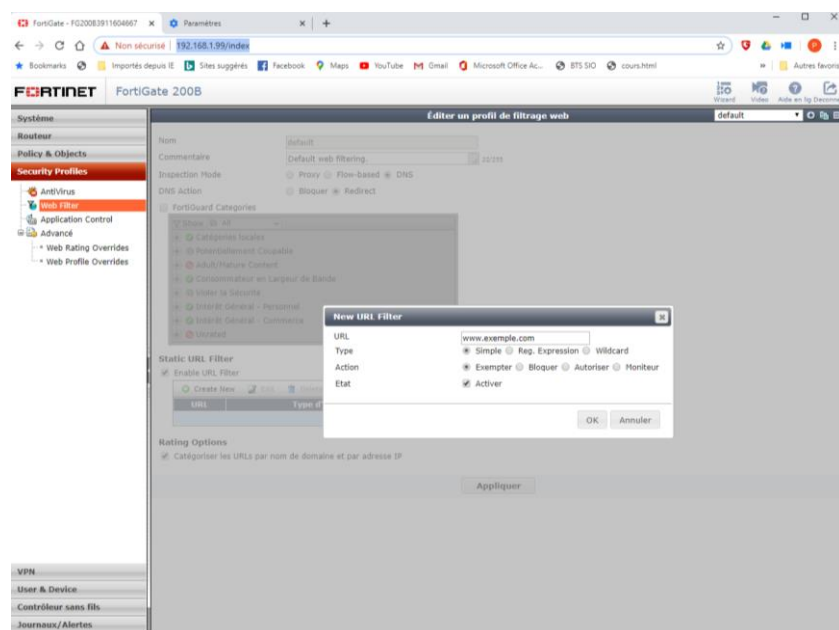
Pour que les catégories soient mises à jour la licence doit être valide.



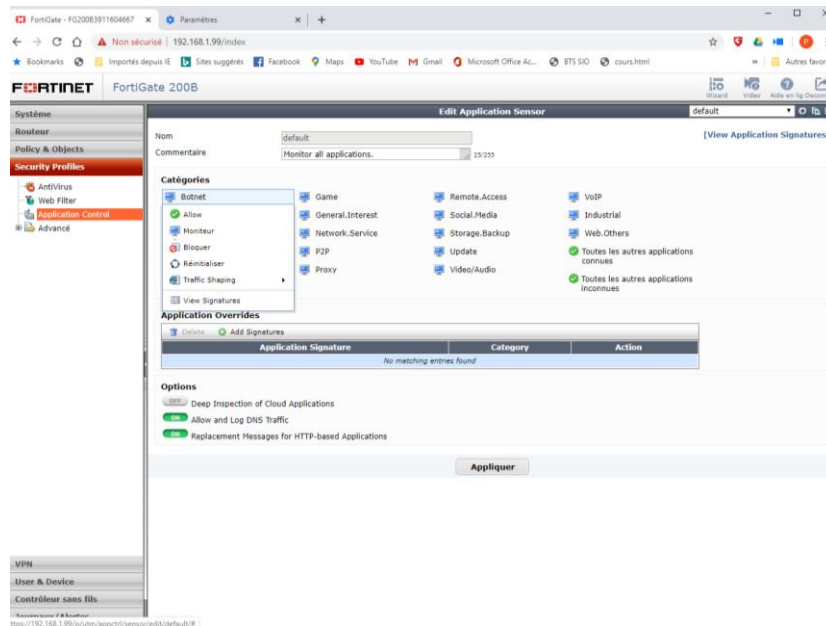
Il est possible d'ajouter de nouveaux utilisateurs ou de créer de nouvelles catégories.

La catégorie Adult/Mature Content contient la possibilité d'interdire ou autoriser les publicités d'alcool, de tabac...

En fonction des besoins de l'entreprise, il est également possible de filtrer des réseaux sociaux ou un site exemple :

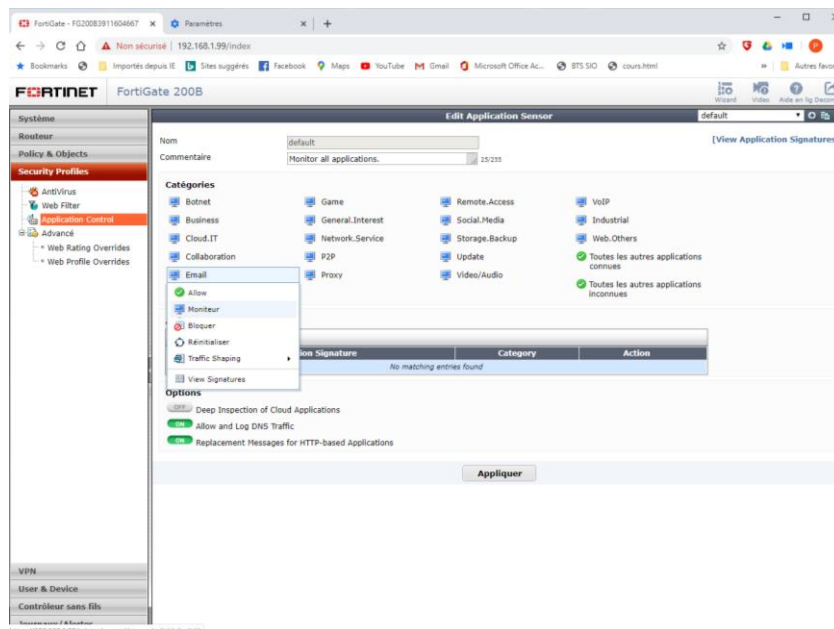


Dans l'onglet Security Profiles : il est notamment possible de filtrer ou monitorer les applications par type de protocole ou fonctionnement, notamment les botnet ou une inspection minutieuse des applications cloud.



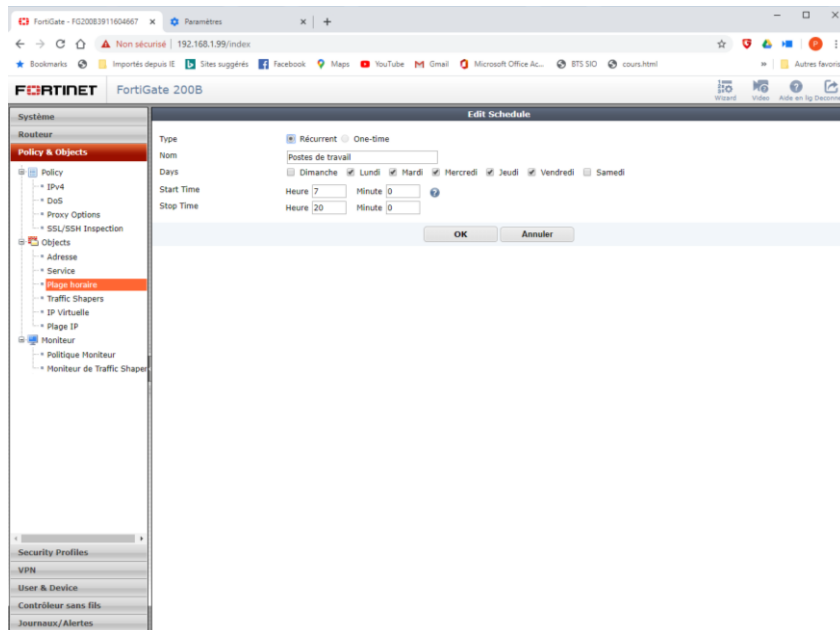
De plus il est possible d'étendre des règles ou fixer des priorités à certains services, comme la messagerie.

A noter qu'en entreprises les règles en matière d'intrusion des emails est stricte. Une entreprise peut avoir un besoin accru des protocoles IPOP et IMAP pour le bon fonctionnement de ses services. Ou limiter les accès vidéo ou audio à certains postes pour garantir une disponibilité des réseaux à d'autres applications.



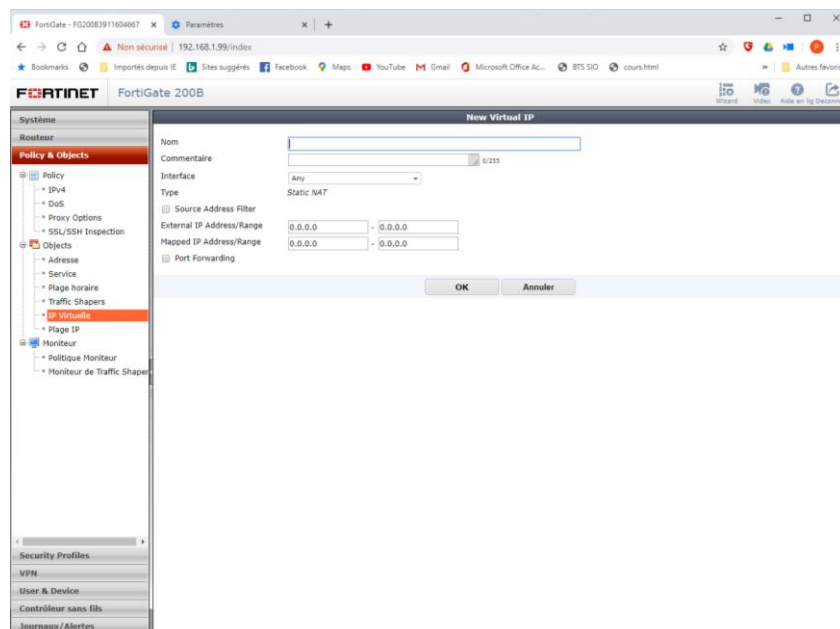
## VI. Création de règles de pare-feu

Prévoir de mettre en place des limites de temps dans l'utilisation de l'accès à l'internet.



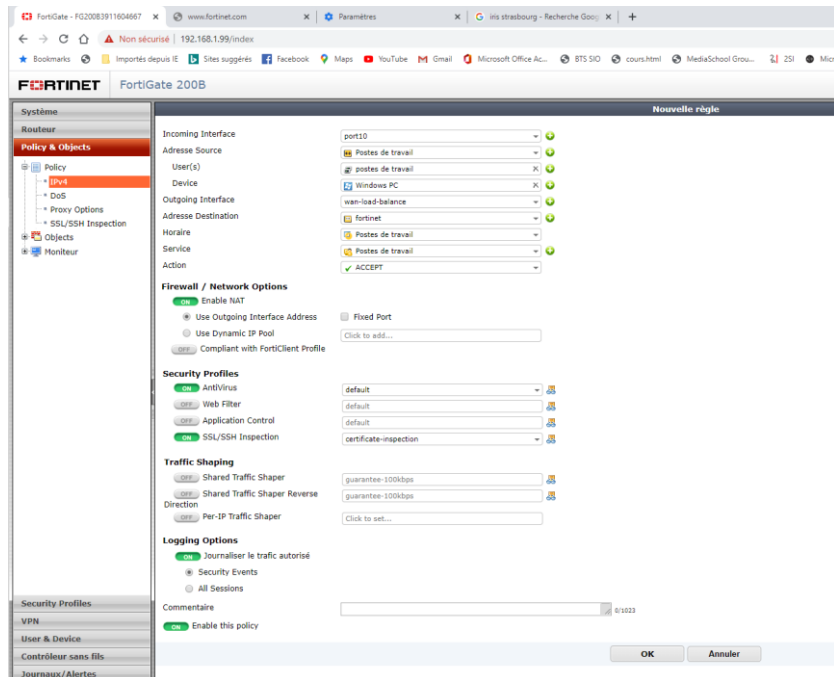
Notamment dans la perspective de réaliser des économies d'énergie, de permettre de sécuriser les installations informatiques.

A noter que le pare-feu inclut la possibilité de réaliser la virtualisation d'IP pour permettre de réaliser des VLAN, il est donc possible de moduler les horaires en fonction des besoins d'accès aux réseaux locaux ou WAN.



## VII. Configurer l'accès en NAT du pare-feu

La création des règles de pare-feu se réalise dans l'onglet policy & Objects IPv4

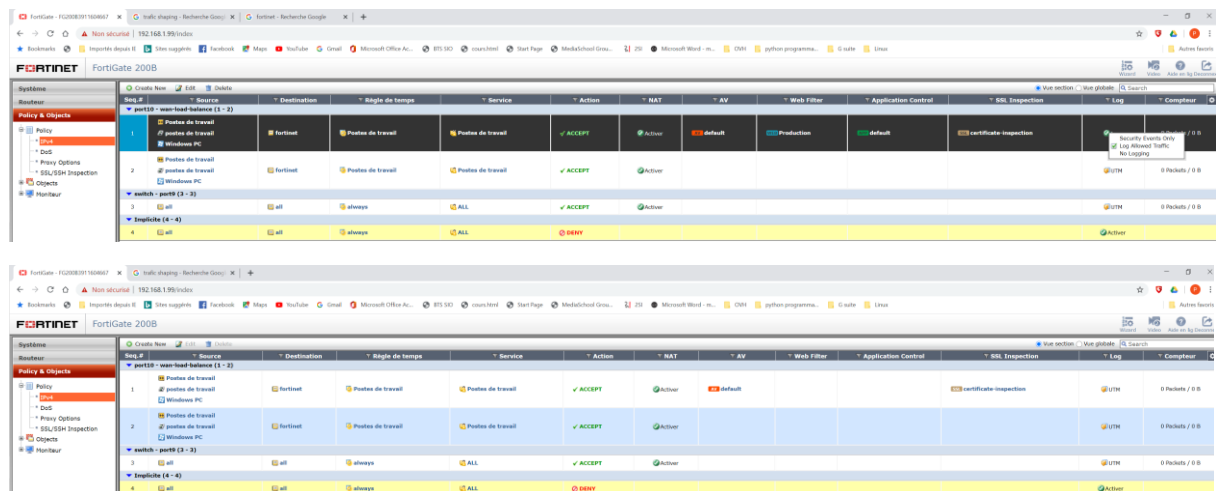


Etablir les règles :

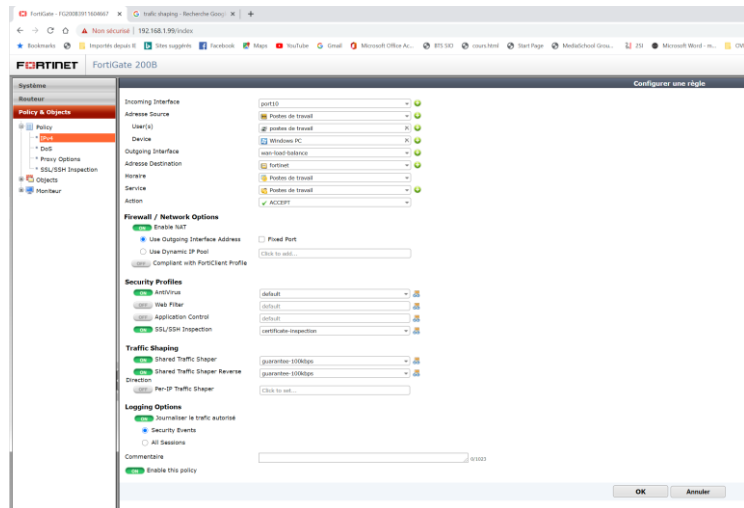
Dans cette interface Web l'hyperviseur ou interface d'activer ou non le filtre web (production) configuré en V.

S'assurer que le trafic est bien en NAT (Network Address Translation), ici le parefeu s'assure de l'authentification et inspection les certificats SSL.

Enfin il convient d'ouvrir les log qui par défaut sont en UTM (Security event only allowed) en log allowed traffic.



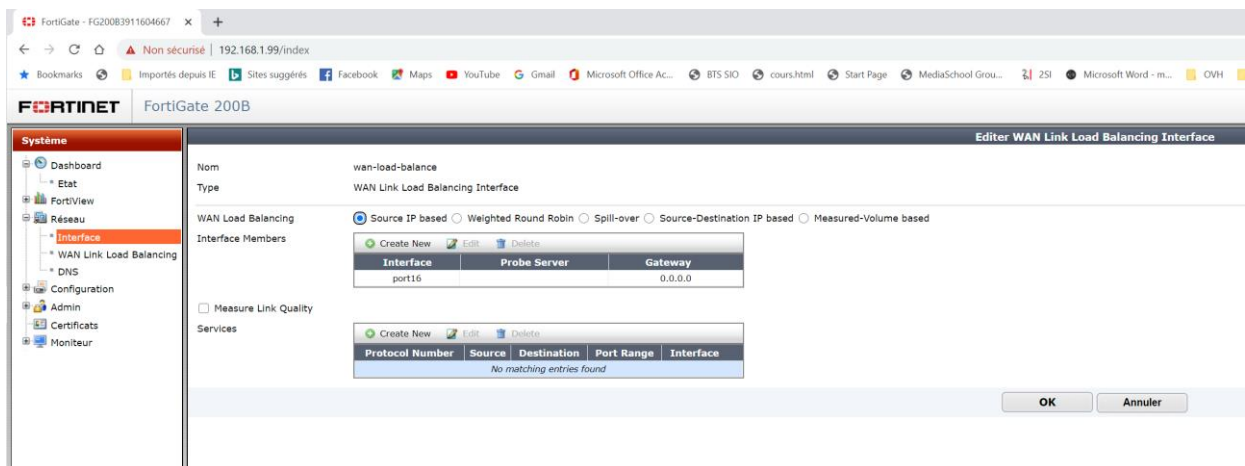
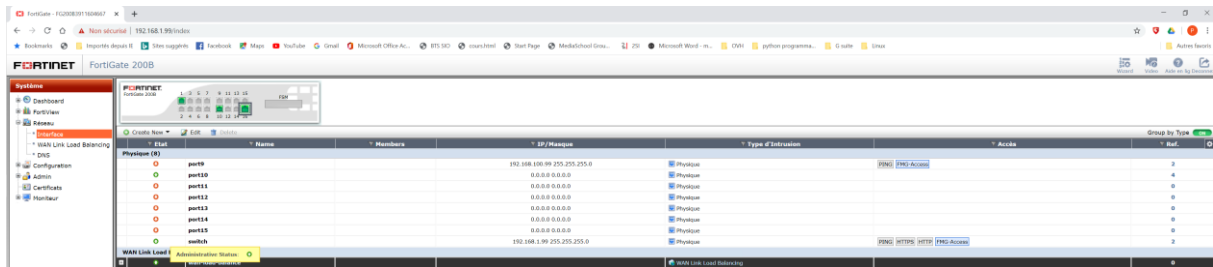
Shared Traffic Shaper/Share Traffic Shaper Reverse pour une gestion des flux et assurer un débit symétrique bridé à 100kbps.



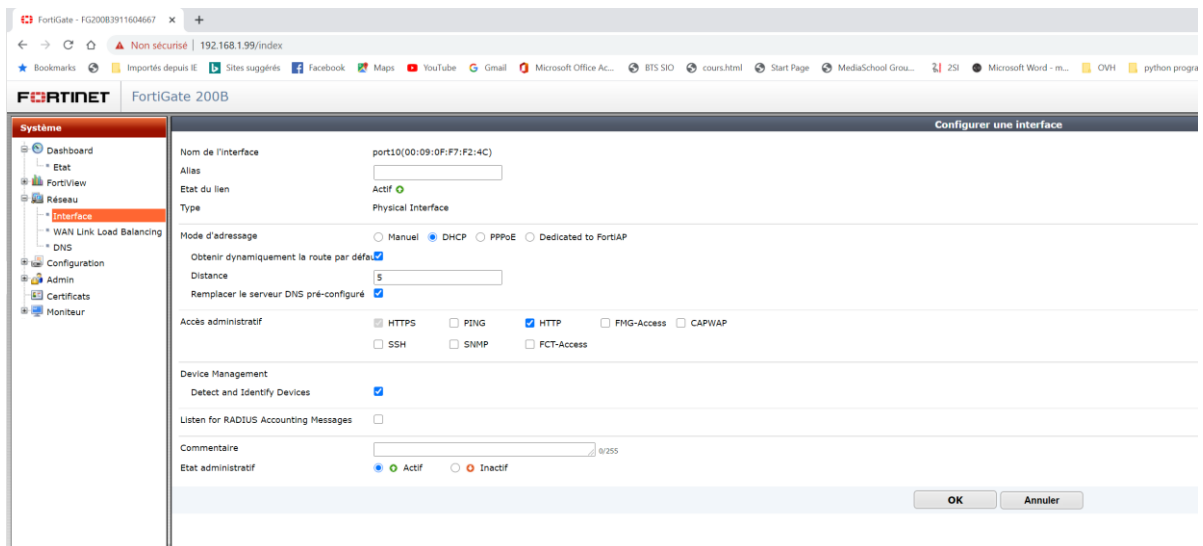
## VIII. Configurer l'accès par interface NAT au WAN

Pour s'assurer que le pare-feu remplit bien son rôle l'accès WAN n'est pas ouvert par défaut.

Mise en place du lien WAN et NAT sur le port 16 :



Modification des indications de gateway ou passerelle pour le port 16 destinée au NAT





**FortiGate 200B**

**Système**

- Dashboard
- Etat
- FortiView
- Reseau
  - Interface
  - WAN Link Load Balancing
- Configuration
- Admin
- Certificats
- Moniteur

**Configurer une interface**

Nom de l'interface: port10(00:09:0F:F7:F2:4C)

Alias:

Etat du lien: Actif

Type: Physical Interface

Mode d'adressage: ☒ Manuel ☐ DHCP ☐ PPPoE ☐ Dedicated to FortiAP

IP/Network Mask: 192.168.30.254/255.255.255.0

Accès administratif: ☐ HTTPS ☐ PING ☒ HTTP ☐ FMG-Access ☐ CAPWAP

☐ SSH ☐ SNMP ☐ FCT-Access

DHCP Server: ☐ Activer

Mode de sécurité: Aucun

Device Management: ☒ Detect and Identify Devices

Listen for RADIUS Accounting Messages: ☐

Adresse IP secondaire:

Commentaire:  0/255

Etat administratif: ☒ Actif ☐ Inactif

OK Annuler

Interface	Physique (Y)	IP/Masque	Type d'Interface	Accès	Group by Type
port9	<input checked="" type="radio"/>	192.168.100.0/255.255.255.0	Physique	<input checked="" type="checkbox"/> FMG-Access	2
port10	<input checked="" type="radio"/>	0.0.0.0/0.0.0.0	Physique	<input checked="" type="checkbox"/> FMG-Access	4
port11	<input checked="" type="radio"/>	0.0.0.0/0.0.0.0	Physique	<input checked="" type="checkbox"/> FMG-Access	0
port12	<input checked="" type="radio"/>	0.0.0.0/0.0.0.0	Physique	<input checked="" type="checkbox"/> FMG-Access	0
port13	<input checked="" type="radio"/>	0.0.0.0/0.0.0.0	Physique	<input checked="" type="checkbox"/> FMG-Access	0
port14	<input checked="" type="radio"/>	0.0.0.0/0.0.0.0	Physique	<input checked="" type="checkbox"/> FMG-Access	0
port15	<input checked="" type="radio"/>	0.0.0.0/0.0.0.0	Physique	<input checked="" type="checkbox"/> FMG-Access	0
switch	<input checked="" type="radio"/>	192.168.1.0/255.255.255.0	Physique	<input checked="" type="checkbox"/> FMG-Access	2
WAN Link Load	<input checked="" type="radio"/>				0

## Configuration du port 10

Précision sur le port 10 pour qu'il puisse capter les Poste de travail avec les adresses distribuées en DHCP 192.168.30.100 à 192.168.30.200

**FortiGate 200B**

**Système**

- Dashboard
- Etat
- FortiView
- Reseau
  - Interface
  - WAN Link Load Balancing
- Configuration
- Admin
- Certificats
- Moniteur

**WAN Link Load Balancing**

Nom: wan-link-load-balancing

Type: WAN Link Load Balancing Interface

WAN Link Load Balancing: ☒ Source IP based ☐ Weighted Round Robin ☐ Round Robin ☐ Source-Destination IP based

Interface Members:

**Editor Interface Member**

Interface: port10

Gateway IP: 192.168.30.254

☐ Health Check

Appliquer Fermer

FortiGate - FG200B3911604667
+

Non sécurisé | 192.168.1.99/index

Bookmarks
Importés depuis IE
Sites suggérés
Facebook
Maps
YouTube
Gmail
Microsoft Office Ac...
BTS SIO
cours.html
Start Page
MediaSchool Grou...
2SI
Microsoft Word - m...

**FORTINET** FortiGate 200B

Système

Dashboard
Etat
FortiView
Réseau
Interface
WAN Link Load Balancing
DNS
Configuration
Admin
Certificats
Moniteur

Configurer une interface

Nom de l'interface
port10(00:09:0F:F7:F2:4C)

Alias

Etat du lien
Actif

Type
Physical Interface

Mode d'adressage
Manuel
DHCP
PPPoE
Dedicated to FortiAP

IP/Network Mask
192.168.30.254/255.255.255.0

Accès administratif
HTTPS
PING
HTTP
FMG-Access
CAPWAP
SSH
SNMP
FCT-Access

DHCP Server
Activer

Mode de sécurité
Aucun

Device Management
Detect and Identify Devices

Listen for RADIUS Accounting Messages

Adresse IP secondaire

Commentaire
 0/255

Etat administratif
Actif
Inactif

OK
Annuler

## IX. Mise en réseaux des postes de travail pour l'accès réseau local et l'accès à internet.

Mise en place du poste qui aura une adresse IP dans le rang 192.168.30.100 à 192.168.30.200. Il est possible de réaliser l'adressage en statique ou dynamique.

A noter : ce matériel comprend un moniteur DHCP qui permet de connaître les adresses MAC des équipements connectés au port d'attribution.

L'équipe de production qui est désigné par le groupe poste de travail dans le pare-feu aura alors accès au réseau local et à internet.

### En conclusion :

- Notre intervention a permis de garantir une disponibilité du réseau équitable, notamment en paramétrant des disponibilités symétriques en up et down, plafonné à 100kbps.
- De respecter les réglementations de la loi EVIN et de réduire les risques pour l'entreprise de voir ses salariés exposés à des contenus illicites ou illégaux en ligne, cela réduit d'autant le phishing.
- Permettre de limiter l'utilisation du streaming ou musique en ligne sur lieu de travail, en limitant l'accès aux protocoles de transport.
- Limiter les menaces extérieures.
- Enfin la sécurité de l'entreprise se trouve renforcée face aux menaces extérieures.
- La mission aura pour objectif de finaliser la connexion des terminaux au réseau par le port NAT en connaissant notamment les adresse routeurs local.

**A noter : qu'il est intéressant de prévoir de configurer les ports en routeur pour faciliter la gestion des LAN ou VLAN de l'infrastructure.**

Présentation des réponses aux requêtes ICPM vers la passerelle de port 10.

**Après remise des ip en dynamique et mise branchement d'un port du parefeu sur le réseau en NAT (port 16), il semble qu'un problème de distribution des IP persiste malgré le branchement du PC de production sur le port 10.**

```
Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion. . . : 
Description. . . . . : Gigabit Network Connection
Adresse physique . . . . . : 
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse d'autoconfiguration IPv4 . . . : 169.254.153.146(préfére)
Masque de sous-réseau. . . . . : 255.255.0.0
Passerelle par défaut. . . . . : 
NetBIOS sur Tcpip. . . . . : Activé
```

Solution proposée : mettre en place une passerelle adaptée au réseau

Configuration d'un poste de travail en ip manuel



```

Invite de commandes
Microsoft Windows [version 10.0.18363.836]
(c) 2019 Microsoft Corporation. Tous droits réservés.

C:\Users\PC Philippe>ping 192.168.30.254

Envoi d'une requête 'Ping' 192.168.30.254 avec 32 octets de données :
Réponse de 192.168.30.101 : Impossible de joindre l'hôte de destination.
Délai d'attente de la demande dépassé.
Réponse de 192.168.30.101 : Impossible de joindre l'hôte de destination.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.30.254:
    Paquets : envoyés = 4, reçus = 2, perdus = 2 (perte 50%),

C:\Users\PC Philippe>

```

## Après désactivation des parefeu de l'OS et software

```

Invite de commandes

Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . :

C:\Users\PC Philippe>ping 192.168.30.é54
La requête Ping n'a pas pu trouver l'hôte 192.168.30.é54. Vérifiez le nom et essayez à nouveau.

C:\Users\PC Philippe>ping 192.168.30.254

Envoi d'une requête 'Ping' 192.168.30.254 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Réponse de 192.168.30.101 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.30.101 : Impossible de joindre l'hôte de destination.

Statistiques Ping pour 192.168.30.254:
    Paquets : envoyés = 4, reçus = 2, perdus = 2 (perte 50%),

C:\Users\PC Philippe>ping 192.168.30.254

Envoi d'une requête 'Ping' 192.168.30.254 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Réponse de 192.168.30.101 : Impossible de joindre l'hôte de destination.
Délai d'attente de la demande dépassé.
Réponse de 192.168.30.101 : Impossible de joindre l'hôte de destination.

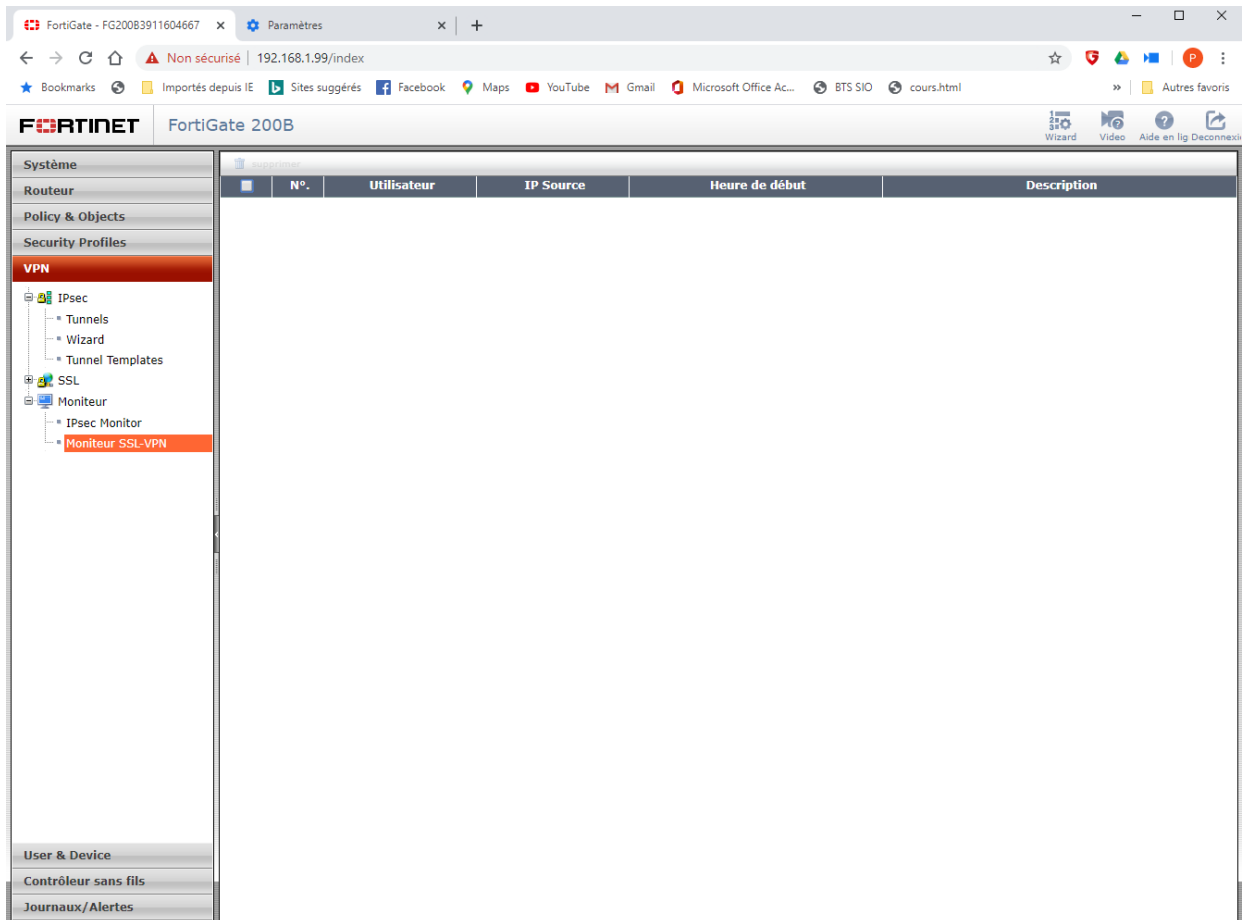
Statistiques Ping pour 192.168.30.254:
    Paquets : envoyés = 4, reçus = 2, perdus = 2 (perte 50%),

C:\Users\PC Philippe>

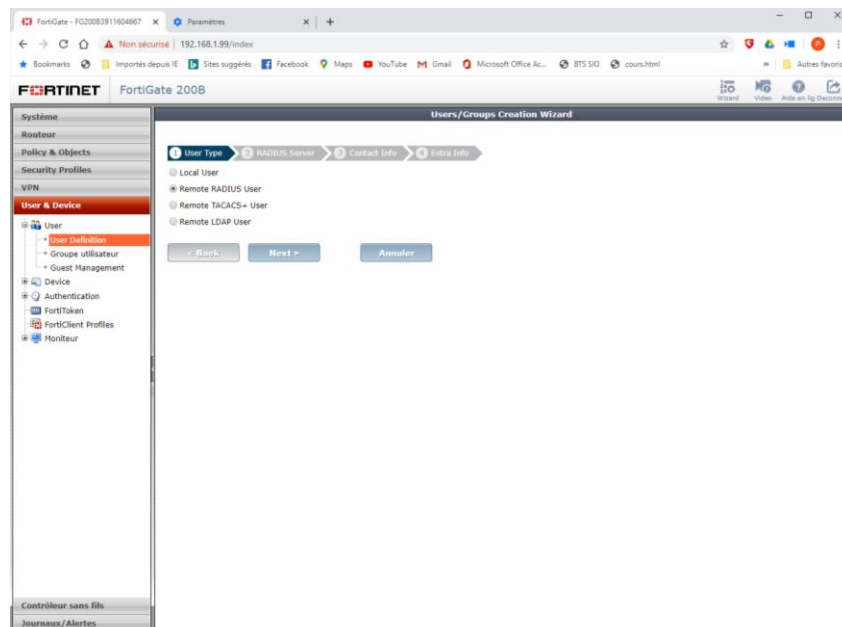
```

## X. Evolution possible

Il est enfin possible de créer un serveur Radius, des services VPN avec options implémentés :



Pour des accès à distances il est possible de configurer un serveur radius.



Possible mise en place d'option proxy : l'équipement comprend la possibilité d'intégrer des options de proxy et un protocole port mapping

**FortiGate 200B**

**Edit Proxy Options**

Nom: default

Commentaire: All default services. 21/255

Activer la journalisation des fichiers trop volumineux: ☐

**Protocol Port Mapping**

Activer	Protocol	Inspection Port(s)
<input checked="" type="checkbox"/>	HTTP	Any <input checked="" type="radio"/> Specifier 80
<input checked="" type="checkbox"/>	SMTP	Any <input checked="" type="radio"/> Specifier 25
<input checked="" type="checkbox"/>	POP3	Any <input checked="" type="radio"/> Specifier 110
<input checked="" type="checkbox"/>	IMAP	Any <input checked="" type="radio"/> Specifier 143
<input checked="" type="checkbox"/>	FTP	Any <input checked="" type="radio"/> Specifier 21
<input checked="" type="checkbox"/>	NNTP	Any <input checked="" type="radio"/> Specifier 119
<input checked="" type="checkbox"/>	MAPI	135
<input type="checkbox"/>	DNS	53

**Common Options**

Confort des Clients: ☐

Block Oversized File/Email: ☐

**Web Options**

Activer le Chunked Bypass: ☐

Add Fortinet Bar: ☐

**Email Options**

Laisser passer les messages fragmentés: ☒

Append Signature (SMTP): ☐