projet SD-WAN pour F-SOCIETY

SERIGNE KHADIM FAYE

IT Network Systeme Security

Cyber Security Enthusiast

Fayekhadim96s@gmail.com

Projet SD-WAN

SERIGNE KHADIM FAYE, Sidy Mbaye

projet SD-WAN pour F-SOCIETY

II. SD-WAN

Introduction

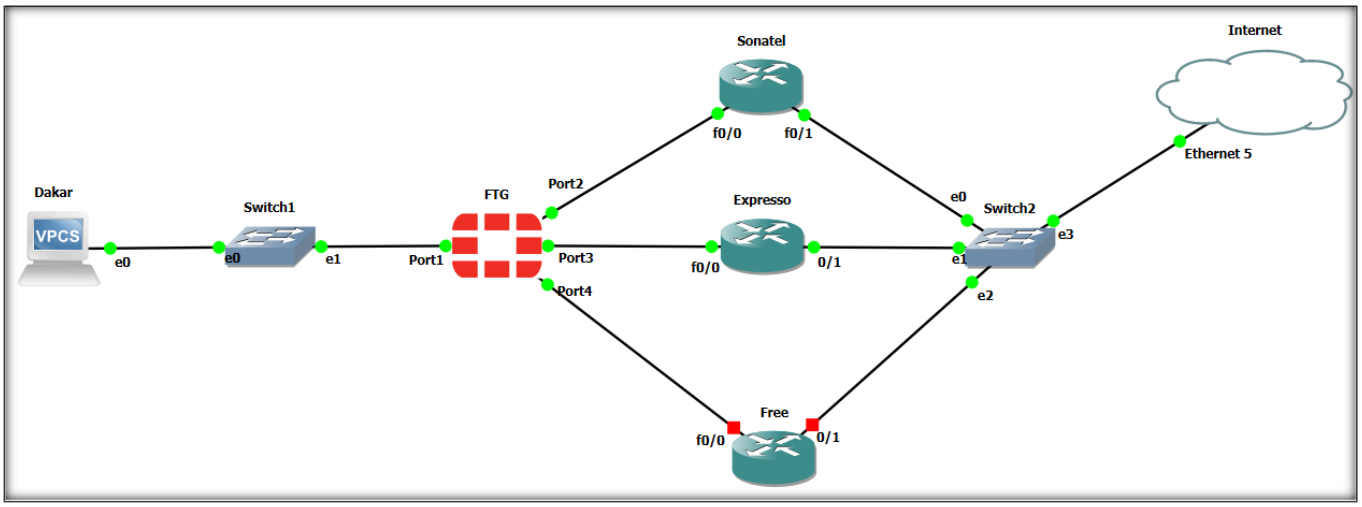
L'entreprise **F-SOCIETY** est située à **Dakar** et a besoin d'une solution robuste pour garantir la continuité de ses services, même en cas de panne sur plusieurs de ses liaisons internet. Elle a souscrit à trois connexions auprès de trois opérateurs différents : **Sonatel**, **Expresso**, et **Free**, afin d'assurer une redondance optimale. La technologie choisie pour répondre à cette exigence est le **SD-WAN** (Software-Defined Wide Area Network), intégrée à un **pare-feu Fortigate**.

Le **SD-WAN** permet de gérer efficacement les multiples connexions internet de l'entreprise en utilisant une approche logicielle pour l'acheminement du trafic réseau. Il est capable de sélectionner dynamiquement la meilleure route pour chaque flux de données en fonction de la performance des liens disponibles. Dans le cadre de ce projet, **F-SOCIETY** doit être capable d'accéder à l'internet même si deux des trois connexions deviennent indisponibles.

Objectifs du projet

1. **Disponibilité élevée** : Garantir que **F-SOCIETY** puisse accéder à l'internet en tout temps, même si deux des trois opérateurs subissent des interruptions.
2. **Optimisation des performances** : Acheminer le trafic internet par la meilleure connexion disponible selon les critères de latence, bande passante, et perte de paquets.
3. **Redondance intelligente** : Mettre en place une bascule automatique vers une autre connexion en cas de défaillance d'un ou plusieurs liens.
4. **Sécurisation** : Protéger l'accès à internet grâce au **pare-feu Fortigate**, en assurant une gestion centralisée des règles de sécurité.

Présentation de l'architecture de déploiement



L'architecture proposée pour **F-SOCIETY** repose sur un déploiement SD-WAN intégré au pare-feu **Fortigate**, permettant une gestion intelligente des connexions internet à travers trois opérateurs différents : **Sonatel**, **Expresso**, et **Free**. Chaque opérateur est connecté au **Fortigate** via une interface dédiée (Port2, Port3, Port4), assurant ainsi une séparation claire des liens pour une redondance optimale. Le SD-WAN surveille en permanence les performances de chaque connexion et redirige dynamiquement le trafic internet vers le lien le plus performant, en fonction de la latence, du débit, et de la disponibilité.

En cas de **dysfonctionnement** de deux des trois connexions, le système bascule **automatiquement** vers le lien restant, garantissant ainsi la continuité des services pour **F-SOCIETY**.

Plan d'adressage

Equipements	Interfaces	Connexion avec	Adresse IP	Masque
Sonatel	-	-	**41.208.100.0/30**	-
- Routeur Sonatel	f0/0	Fortigate (Port2)	41.208.100.1	255.255.255.252
- Fortigate	Port2	Routeur Sonatel (f0/0)	41.208.100.2	255.255.255.252
Expresso	-	-	**196.207.255.0/30**	-
- Routeur Expresso	f0/0	Fortigate (Port3)	196.207.255.1	255.255.255.252
- Fortigate	Port3	Routeur Expresso (f0/0)	196.207.255.2	255.255.255.252
Free	-	-	**102.64.120.0/30**	-
- Routeur Free	f0/0	Fortigate (Port4)	102.64.120.1	255.255.255.252
- Fortigate	Port4	Routeur Free (f0/0)	102.64.120.2	255.255.255.252
Accès Internet	-	-	**192.168.136.0/24**	-
- Switch2	e3	Internet	192.168.136.1	255.255.255.0
Réseau privé F-SOCIETY	-	-	**192.168.1.0/24**	-
- VPC (PC Dakar)	e0	Switch1 (e0)	DHCP	255.255.255.0
Forti Admin	e0	Switch1 (e0)	192.168.1.10	255.255.255.0

Configuration du Fortigate

Dans cette étape, nous allons configurer le FortiGate pour établir une architecture SD-WAN robuste et résiliente. Nous commencerons par définir les interfaces réseau pour chaque fournisseur de services Internet (ISP), à savoir Sonatel, Expresso et Free. Chaque interface sera configurée avec les adresses IP appropriées, permettant ainsi une connectivité directe avec les différentes liaisons.

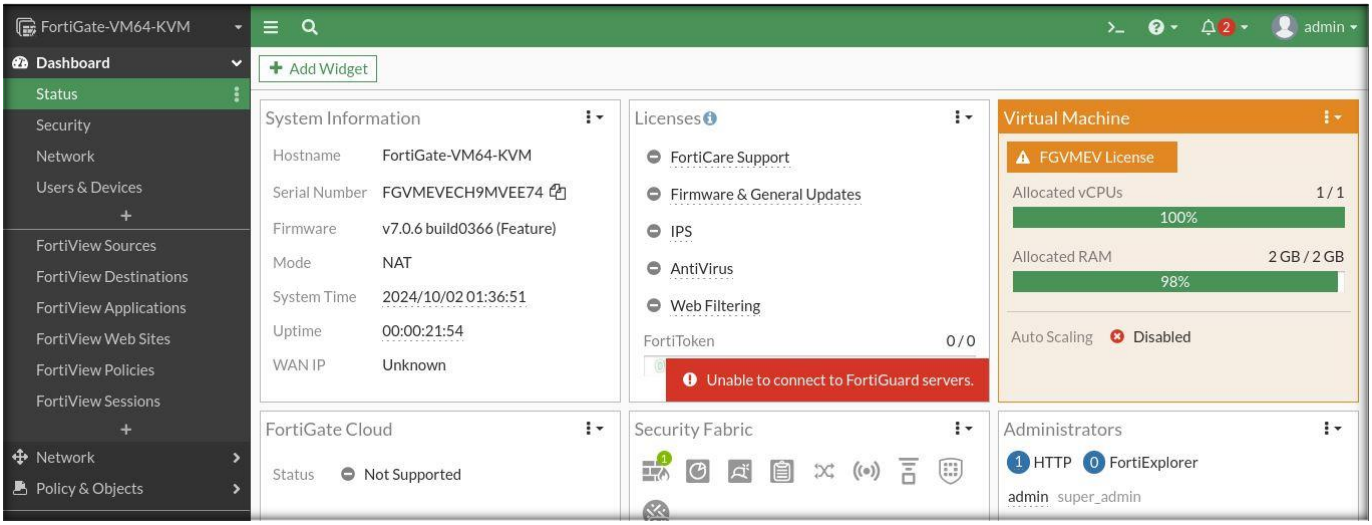
Ensuite, nous créerons une zone SD-WAN pour regrouper ces interfaces, ce qui facilitera la gestion et l'optimisation du trafic entre les différentes connexions.

Grâce à cette configuration, le FortiGate sera en mesure de rediriger le trafic de manière dynamique en fonction de l'état des liaisons, assurant ainsi la continuité des services même en cas de défaillance d'un des liens.

```
FortiGate-VM64-KVM login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port5

FortiGate-VM64-KVM (port5) # set mode static

FortiGate-VM64-KVM (port5) # set ip 192.168.1.10/24

FortiGate-VM64-KVM (port5) # set allowaccess ping http https

FortiGate-VM64-KVM (port5) #
```

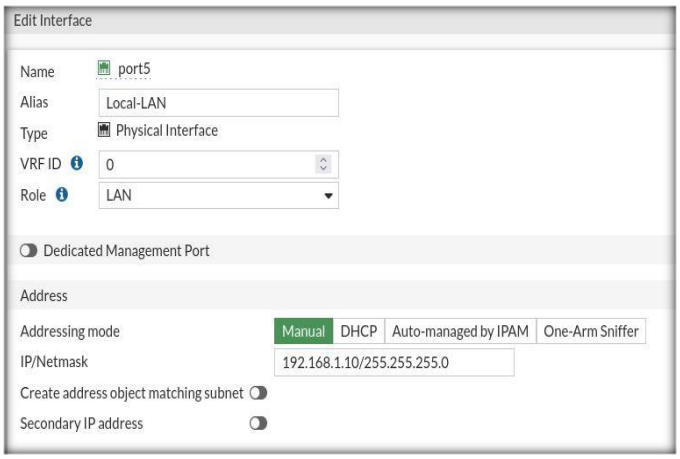
Se connecter sur le fortigate et fixer l'adresse ip de management ici 192.168.1.10

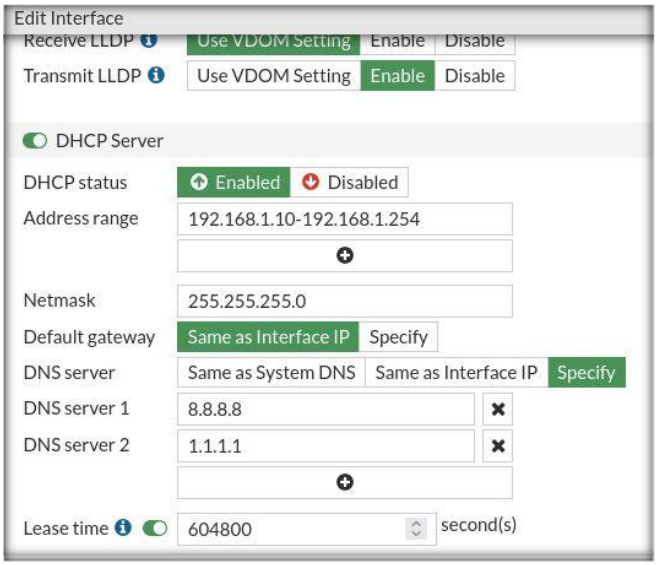
Connexion au GUI du fortigate

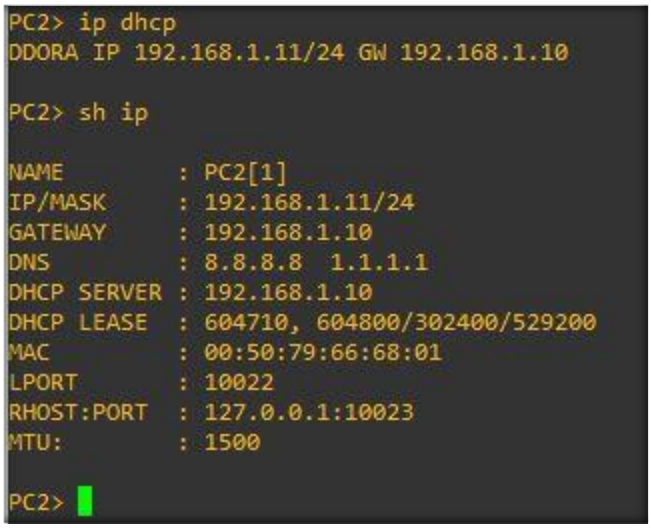


Configuration du service DHCP

Nous allons par la suite partir sur : Network ➔ Interfaces pour mettre en place le service dhcp sur le fortigate pour l'attribution automatique d'adresse ip aux hôtes.

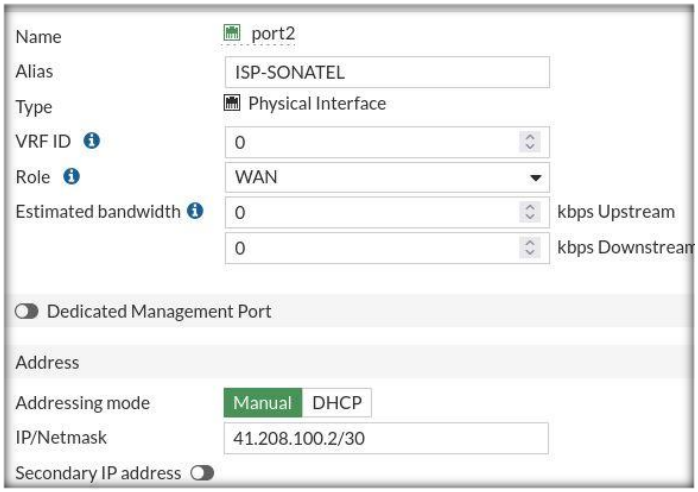


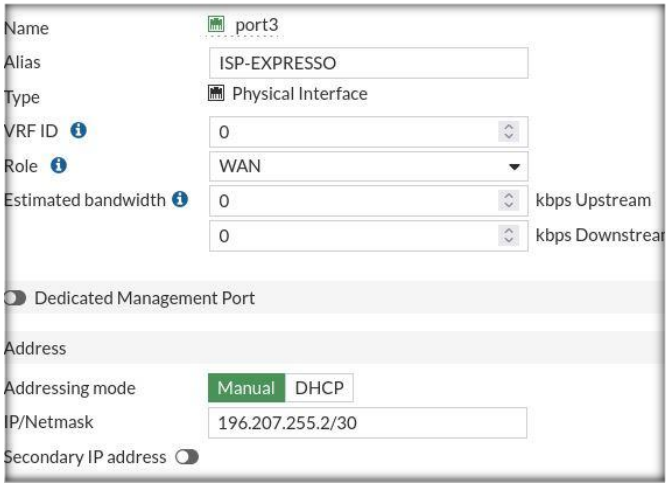




Configuration du service dhcp ok

- **Configuration des interfaces pour les trois IPS**
- **Network ➔ interfaces ➔ port 2 (ISP-SONATEL)**





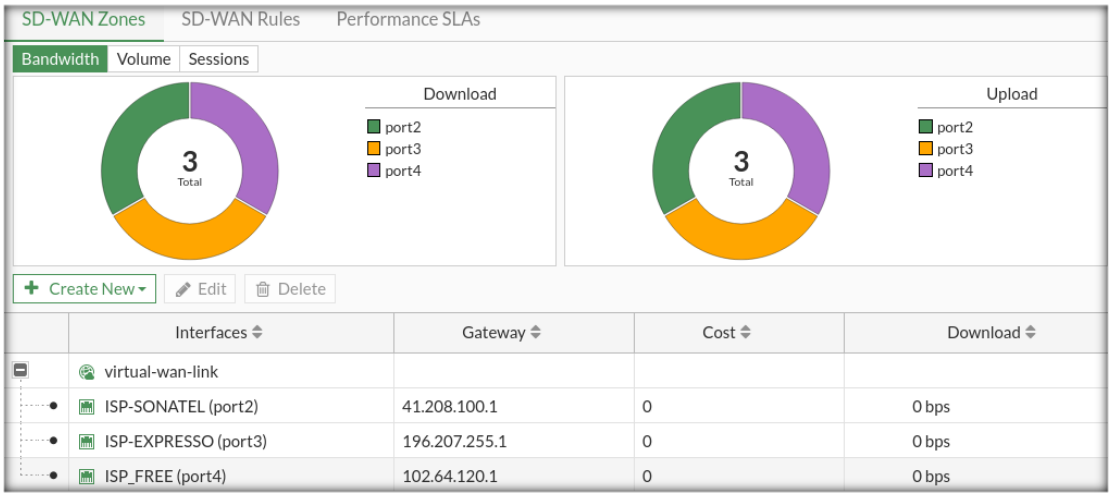
ISP-EXPRESSO (port3)	Physical Interface		196.207.255.2/255.255.255.252	PING HTTPS SSH FMG-Access
ISP-FREE (port4)	Physical Interface		102.64.120.2/255.255.255.252	PING HTTPS SSH FMG-Access
ISP-SONATEL (port2)	Physical Interface		41.208.100.2/255.255.255.252	PING HTTPS SSH

Ajout des différents ISP

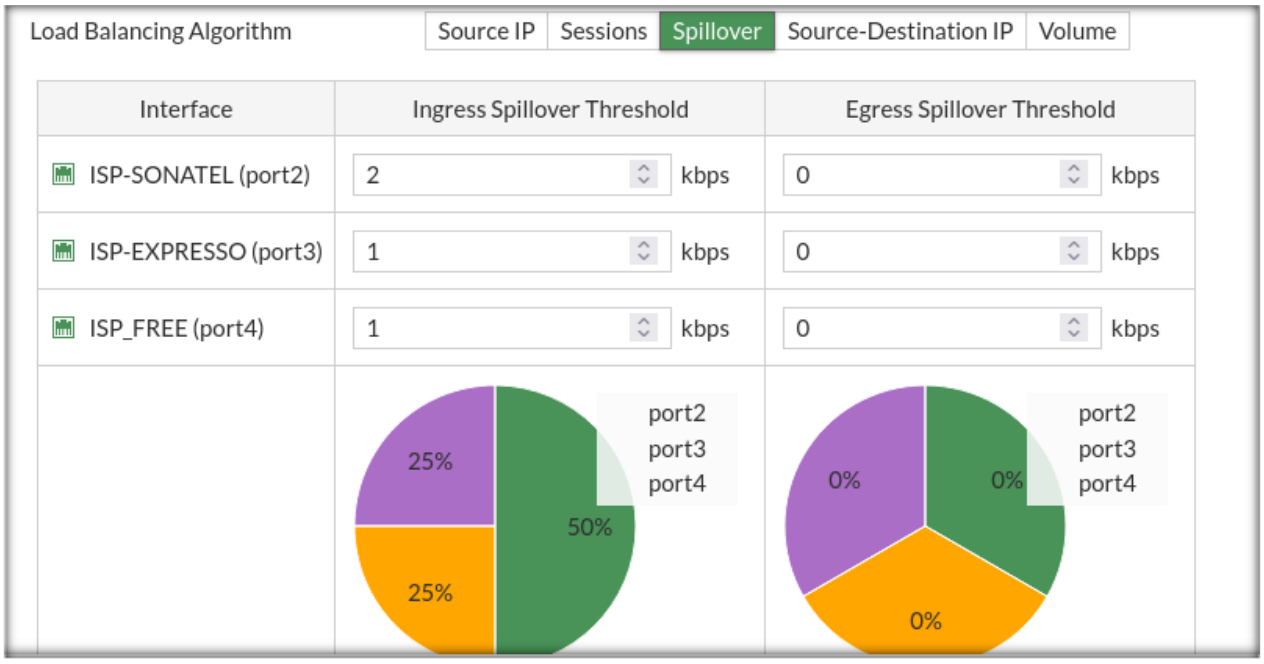
Apres avoir configurer les différents ports relies aux ISP, nous allons passer à la configuration de la technologie SD-WAN.

Network ➔ interfaces ➔ SD-WAN

Ici, nous allons créer une nouvelle zone SD-WAN (SD-WAN F-SOCIETY) et par la suite ajouter les différents ISP (SD-WAN Member).



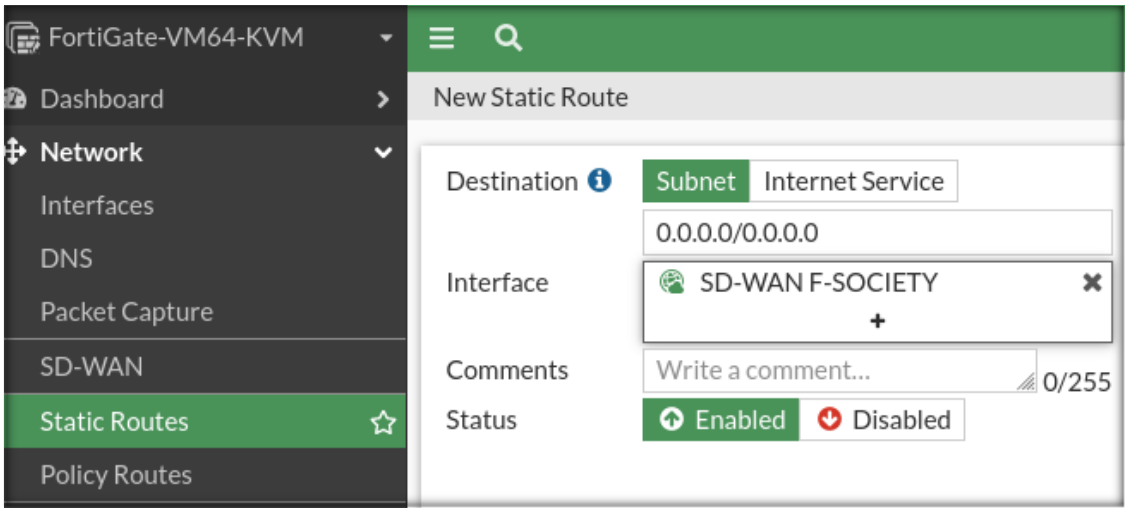
Il est aussi possible d'affiner les paramètres du Load Balancing, dans notre cas nous allons priorise ISP-SONATEL qui offre un meilleur débit.



Nous allons mettre en place une règle SD-WAN pour définir les paramètres de routage et optimiser la répartition du trafic entre les différents membres ISP du SD-WAN, garantissant ainsi une gestion efficace des flux réseau.

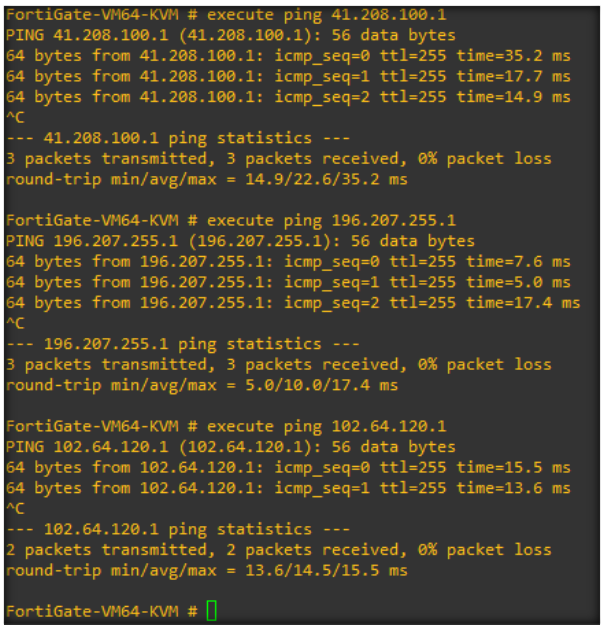
Nous allons également ajouter une route statique pour orienter le trafic vers la passerelle appropriée en fonction de la disponibilité des liens ISP.

Network ➔ Static Routes



Nous allons configurer une règle dans la section "Policy & Objects" du FortiGate pour définir une politique de pare-feu qui permettra de contrôler et sécuriser le trafic entre les différentes zones du réseau, tout en s'assurant que le trafic est correctement acheminé via les membres du SD-WAN.

Test de vérification : Nous allons faire un ping depuis le vers les différents ISP pour tester la connectivité. Ping ok



Passons maintenant à la configuration des différents ISP. Nous appliquerons les mêmes étapes pour chacun des trois fournisseurs, en veillant simplement à adapter les adresses IP et les interfaces spécifiques à chaque ISP.

ISP-SONATEL#sh running-config interface fastEthernet 0/0

interface FastEthernet0/0

ip address 41.208.100.1 255.255.255.252

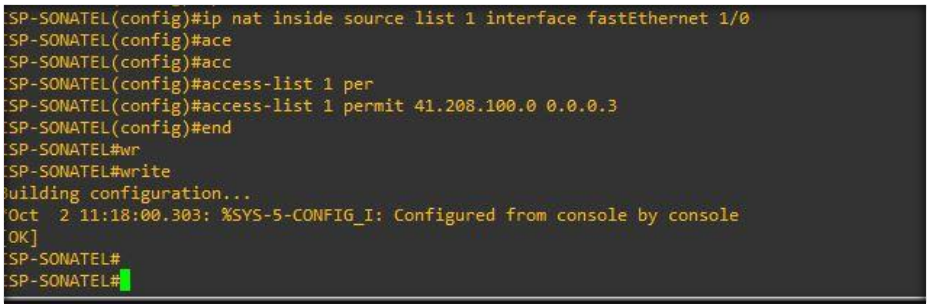
ip nat inside

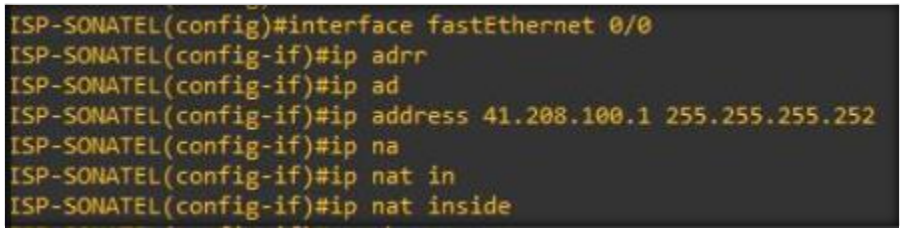
duplex full

exit

ip nat inside source list 1 interface FastEthernet1/0 overload

access-list 1 permit 41.208.100.0 0.0.0.3





Testons pour voir si les hôtes parviennent à communiquer avec Internet

Ping 192.168.136.1

```
PC1> ping 192.168.136.1
84 bytes from 192.168.136.1 icmp_seq=1 ttl=62 time=36.093 ms
84 bytes from 192.168.136.1 icmp_seq=2 ttl=62 time=32.274 ms
84 bytes from 192.168.136.1 icmp_seq=3 ttl=62 time=34.696 ms
84 bytes from 192.168.136.1 icmp_seq=4 ttl=62 time=33.574 ms
84 bytes from 192.168.136.1 icmp_seq=5 ttl=62 time=33.711 ms

PC1>
```

```
PC2> ping 192.168.136.1
84 bytes from 192.168.136.1 icmp_seq=1 ttl=62 time=33.176 ms
84 bytes from 192.168.136.1 icmp_seq=2 ttl=62 time=32.987 ms
84 bytes from 192.168.136.1 icmp_seq=3 ttl=62 time=33.175 ms
84 bytes from 192.168.136.1 icmp_seq=4 ttl=62 time=35.233 ms
84 bytes from 192.168.136.1 icmp_seq=5 ttl=62 time=34.972 ms

PC2>
```

Test OK, les hôtes de la F-SOCIETY peuvent accéder a internet

```
PC2> trace  192.168.136.1
trace to 192.168.136.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.10   4.211 ms  4.301 ms  2.905 ms
 2   102.64.120.1   17.755 ms  18.718 ms  17.564 ms
 3   *192.168.136.1   34.357 ms (ICMP type:3, code:3, De

PC2> trace  192.168.136.1
trace to 192.168.136.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.10   4.525 ms  7.469 ms  6.952 ms
 2   41.208.100.1   19.459 ms  18.009 ms  19.590 ms
 3   *192.168.136.1   32.235 ms (ICMP type:3, code:3, De

PC2> trace  192.168.136.1
trace to 192.168.136.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.10   5.727 ms  2.700 ms  3.496 ms
 2   196.207.255.1   19.319 ms  17.655 ms  18.638 ms
 3   *192.168.136.1   34.167 ms (ICMP type:3, code:3, De

PC2> trace  192.168.136.1
trace to 192.168.136.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.10   3.012 ms  4.090 ms  4.215 ms
 2   41.208.100.1   19.156 ms  18.234 ms  17.648 ms
 3   *192.168.136.1   32.735 ms (ICMP type:3, code:3, De

PC2>
```

Les tests de connectivité vers Internet se sont révélés concluants. En utilisant des commandes de traçage (traceroute), nous avons pu observer que le trafic emprunte différents chemins à travers les trois fournisseurs d'accès Internet (ISP). Cela démontre que le SD-WAN fonctionne comme prévu, en sélectionnant automatiquement le meilleur chemin en fonction des conditions du réseau, tout en assurant la redondance.

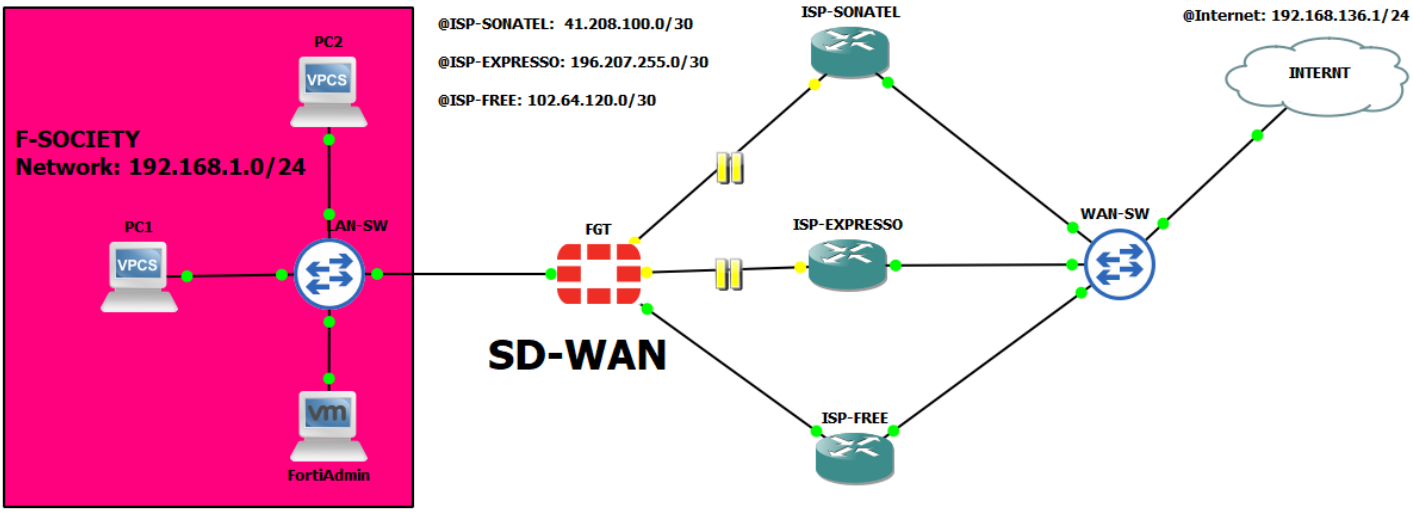
Les résultats du traceroute montrent que le trafic passe tantôt par l'ISP Sonatel, tantôt par les autres ISPs (Free et Expresso), ce qui valide la résilience et l'équilibrage des charges entre les différentes connexions configurées. Ces tests confirment que même en cas de défaillance d'un lien, les autres ISP prennent le relais sans interruption du service.

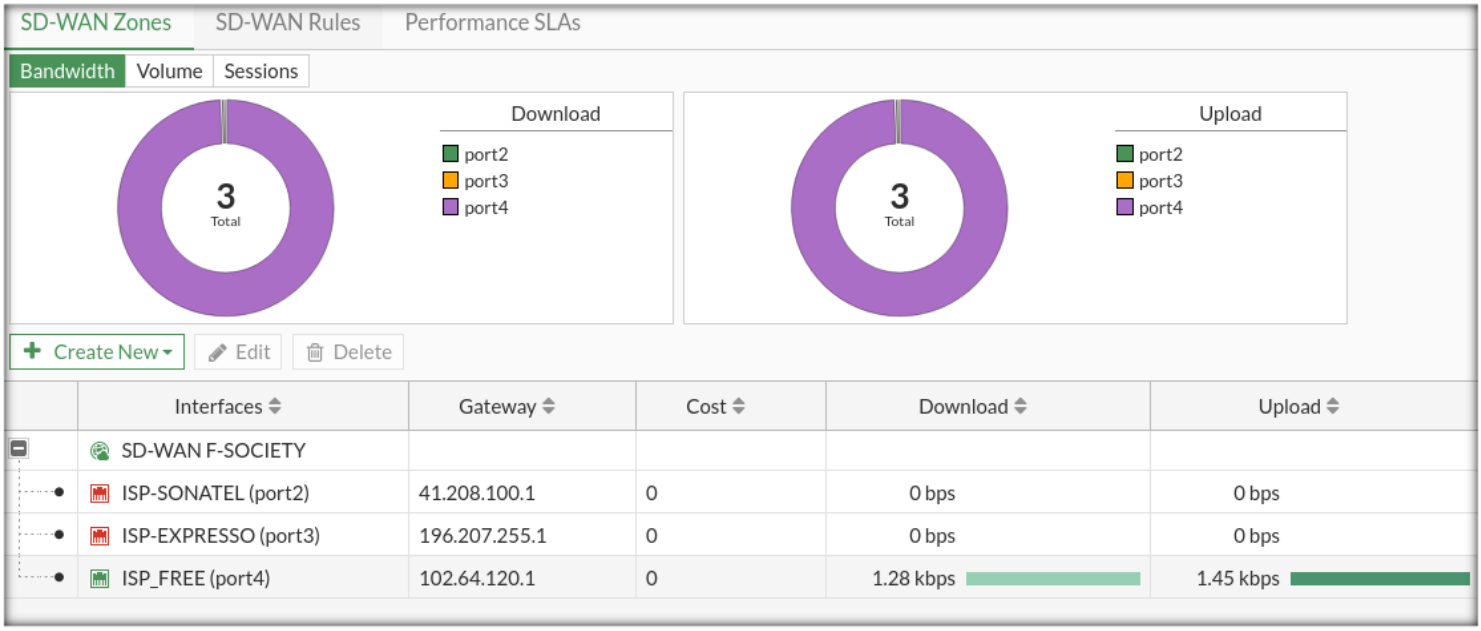
- **Test de Résilience**

Nous allons réaliser un test de résilience pour vérifier que, même en cas de perte simultanée des liens Sonatel et Expresso, le trafic sera redirigé automatiquement via le lien Free. Ce test permettra de s'assurer que le SD-WAN est configuré de manière à garantir la continuité du service, en exploitant pleinement les capacités de basculement (failover) entre les différents ISP.

```
PC1> trace 192.168.136.1
trace to 192.168.136.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.10   5.691 ms  3.018 ms  4.578 ms
 2   102.64.120.1   21.091 ms  17.884 ms  18.303 ms
 3   *192.168.136.1   35.411 ms (ICMP type:3, code:3, Destination port unreachable)

PC1> ping 192.168.136.1
84 bytes from 192.168.136.1 icmp_seq=1 ttl=62 time=34.417 ms
84 bytes from 192.168.136.1 icmp_seq=2 ttl=62 time=33.815 ms
84 bytes from 192.168.136.1 icmp_seq=3 ttl=62 time=33.635 ms
84 bytes from 192.168.136.1 icmp_seq=4 ttl=62 time=34.262 ms
84 bytes from 192.168.136.1 icmp_seq=5 ttl=62 time=33.731 ms

PC1> trace 192.168.136.1
trace to 192.168.136.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.10   4.117 ms  2.740 ms  3.533 ms
 2   102.64.120.1   18.366 ms  17.432 ms  18.250 ms
 3   *192.168.136.1   33.693 ms (ICMP type:3, code:3, Destination port unreachable)

PC1> trace 192.168.136.1
trace to 192.168.136.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.10   4.245 ms  2.645 ms  3.699 ms
 2   102.64.120.1   17.858 ms  18.348 ms  17.738 ms
 3   *192.168.136.1   32.260 ms (ICMP type:3, code:3, Destination port unreachable)
```

Ici, nous constatons que même en cas de coupure des liens Sonatel et Expresso, le trafic continue de passer par l'ISP Free. Les résultats des tests de ping et de tracert confirment que la redirection automatique est bien fonctionnelle, garantissant ainsi une continuité de service. Le système SD-WAN est capable de gérer les défaillances des liens tout en maintenant la connectivité via l'ISP restant, en l'occurrence Free.





Sur l'interface graphique on voit bien que le trafic passe par le ISP-FREE et les autres sont down.

Conclusion

En conclusion, la mise en œuvre du projet SD-WAN pour F-SOCIETY a permis d'assurer une connectivité internet résiliente et optimisée grâce à la gestion intelligente des liens avec les trois opérateurs (Sonatel, Expresso, et Free). Grâce aux fonctionnalités avancées du FortiGate, nous avons réussi à configurer des règles de routage dynamiques, assurant la redirection du trafic en cas de défaillance de l'un ou plusieurs des liens. Le système est ainsi prêt à garantir la continuité de service même en cas de perte simultanée de deux connexions, apportant une solution fiable et évolutive pour l'entreprise.