

BTS SIO SISR

Situation professionnelle numéro 1

*Mise en place et configuration d'un pare-feu
Fortigate*

Le pare-feu est l'équipement réseau qui est souvent utilisé pour connecter un réseau LAN à Internet de façon sécurisé. En limitant ainsi le trafic on peut éviter les cyber-attaques .

Dans cette situation, nous verrons la création d'un port LAN, VPN et DMZ. Ainsi que l'activation des règles adéquates au bon fonctionnement du réseau, l'ajout des routes statiques, et enfin, les paramètres de sécurité du VPN.

Cette situation se terminera par un test ICMP afin de s'assurer de la bonne communication des machines du réseau

Plan de situation :

Le Cahier des charges.....	3
L'expression des besoins.....	3
La description de l'existant.....	3
Les offres du marché.....	4
L'analyse des choix.....	5
Le choix de fortinet.....	5
Les risques de ne pas posséder de fire-wall.....	6
Mise en Œuvre.....	7
Le plan.....	7
Câblage physique.....	7
Comment commencer la configuration.....	8
Configuration du pare-feu.....	10
Sécurité du VPN.....	15
Test de fonctionnement.....	18

Le cahier des charges

L'expression des besoins

Suite à la récente cyber-attaque de la KLLT Bank, la Direction des Systèmes d'information c'est questionnée face à l'utilité de leurs moyens de protection face aux Hackers. L'entreprise demande la mise en place d'une protection supplémentaire pour diminuer les risques d'une nouvelle attaque, ainsi qu'une solution spéciale pour protéger leur serveur WEB.

Ayant ouvert un site à Bastia, la société cherche également une solution pour relier ces deux sites entre eux, et veulent moderniser leurs équipements.

La description de l'existant

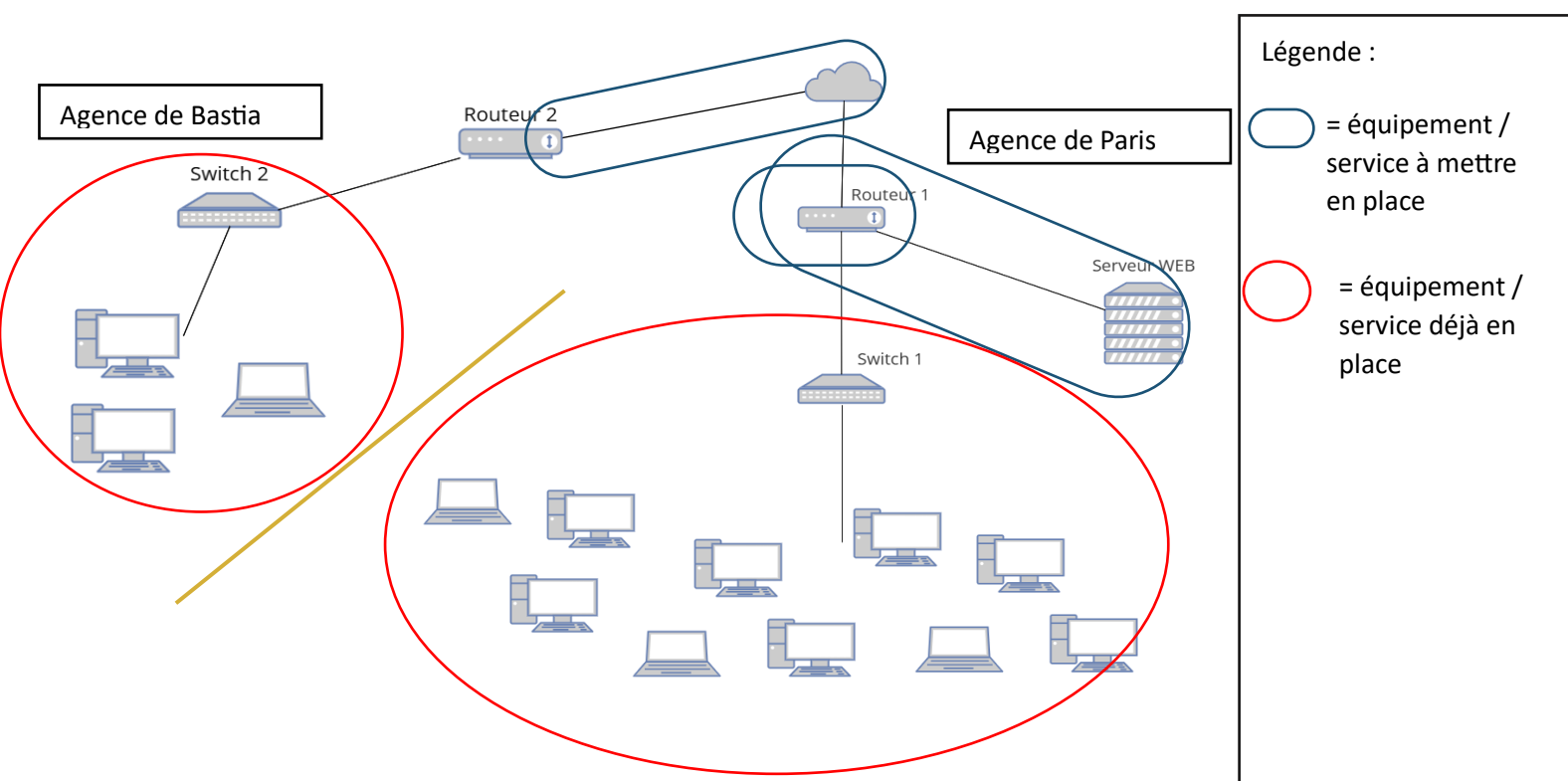
Sur le site de Paris, le commutateur est connecté directement à un routeur Cisco 881-k9, et le serveur WEB est également relié à ce dispositif. Le routeur permet la liaison entre le LAN et Internet.

Sur le site de Bastia, le commutateur est également à un autre routeur Cisco 881-k9.

Les caractéristiques techniques du Cisco 881-k9 :

Caractéristique	Description
Processeur	Intel Pentium M 1.1 GHz
RAM	256 MB (par défaut) / 768 MB (maximum)
Stockage Flash	128 MB
Nombre de ports LAN	4 ports 10/100 Ethernet (RJ-45)
Ports WAN	1 port 10/100 Ethernet (RJ-45)
Ports USB	1 port USB Type A
Ports PoE intégrés	2 ports PoE intégrés
Services intégrés	QoS, NAT transparence, IPSec, DMVPN, IPv4/IPv6 multicast, OSPF, BGP, EIGRP, NHRP, L2TPv3, VRF-lite, VRRP, HSRP, IGMPv3 snooping, 802.1x, SSL, DES, 3DES, AES 128, AES 192, AES 256

Voici un schéma de l'infrastructure actuelle :



Les offres du marché

Marque	Modèle	Processeur	RAM	Stockage Flash	Nombre de ports LAN	Ports WAN	Services intégrés
Fortinet	FortiGate 60E	FortiASIC SOC2	2 GB	4 GB	7 ports 10/100/1000	2 ports	Pare-feu, prévention des intrusions, filtrage de contenu, VPN, QoS, NAT transparence, IPSec, DMVPN, OSPF, BGP, EIGRP, NHRP, L2TPv3, VRF-lite, VRRP, HSRP, IGMPv3 snooping, 802.1x, SSL,
pfSense	SG-3100	Dual-core ARM Cortex A7	512 MB	8 GB	4 ports 10/100/1000	2 ports	Pare-feu, VPN, filtrage de contenu, QoS, NAT, IPSec, PPTP, L2TP, BGP, OSPF, SNMP, SSL, DES, 3DE
Stormshield	Stormshield S20	Intel Atom C3338	2 GB	16 GB	8 ports 10/100/1000	2 ports	Pare-feu, VPN, prévention des intrusions, filtrage de contenu, QoS, NAT, IPSec, OpenVPN, PPTP, L2TP, BGP, OSPF, SNMP, 802.1x, SSL,
Cisco	Cisco Firepower 1010	Intel Atom C3508	8 GB	32 GB	8 ports 10/100/1000	1 port	Pare-feu, prévention des intrusions, filtrage de contenu, VPN, QoS, NAT, IPSec, DMVPN, OSPF, BGP, EIGRP, NHRP, L2TPv3, VRF-lite, VRRP, HSRP, IGMPv3 snooping, 802.1x,

Analyse des choix

Fortinet FortiGate 60E :

- Point positif : Performance élevée, avec des options de sécurités avancées, une interface utilisateur très intuitive et facile à comprendre. Avec une connectivité fiable et une lecture des LOGS rapide.
- Point négatif : Le coût des licences peuvent être élevées.

PfSense SG-3100 :

- Point positif : Personnalisable avec excellent rapport qualité prix.
- Point négatif : Une interface utilisateur complexe et dispose de ressources matériels limitées.

Stormshield Stormshield S20 :

- Point positif : Sécurité avancée, avec option de haute disponibilité.
- Point négatif : Un coût plus élevé et une interface utilisateur plus complexe.

Cisco Cisco Firepower 1010 :

- Point positif : Performance excellente et possède de nombreuses options de sécurités.
- Point négatif : Un coût plus élevé et nécessite une formation pour utiliser toutes les fonctionnalités

Le choix de Fortinet

Pourquoi choisir le Fortinet FortiGate 60E :

Tout d'abord, Fortinet est l'un des leader du marché des pare-feu. Ils se distinguent par leurs équipements de haute performance, et d'une grande évolutivité. La technologie FortiGuard fournis des mises à jours en temps réels sur les menaces. Bonne intégration, les produits Fortinet s'intègrent bien entre eux et dans le réseau, offrant une sécurité réseau cohérente et complète ainsi qu'une vision des logs simple. Enfin, l'interface graphiques est très complète, et simplifié.

Tous ces avantages sont la raison pour laquelle j'ai choisis cette marque et ce modèle. Néanmoins, il existe tout de même un point négatif étant le coût des licences, augmentant le coût des dépenses globales.

Les risques de ne pas avoir de pare-feu / mauvaise sécurité

Il existe différentes lois obligent les sociétés à mettre en place certaines mesures de sécurité tels que :

Réglementation	Description	Obligations Clés
Loi pour la Confiance Numérique (LCN)	Vise à renforcer la sécurité des systèmes d'information et à protéger les données personnelles.	Mettre en place des mesures de sécurité adaptées aux risques Protéger les données personnelles.
Réglementation CIIP (Protection des Infrastructures Critiques de l'Information)	Établie par l'ANSSI, cette réglementation impose des règles de sécurité techniques et organisationnelles pour les opérateurs de systèmes d'information critiques.	Notifier les incidents de sécurité à l'ANSSI. Respecter des règles de sécurité techniques et organisationnelles.
Cybersecurity Act	Réglementation européenne mise en œuvre par l'ANSSI, établissant un cadre de certification de la sécurité des produits, services et processus numériques.	Se conformer aux normes de certification de sécurité.
Loi Informatique et Libertés (LIL)	Vise à protéger les données personnelles et à garantir la sécurité des systèmes d'information.	Mettre en place des mesures de sécurité appropriées. Assurer la protection des données personnelles.
CNIL	Commission Nationale de l'Informatique et des Libertés : Autorité française chargée de veiller à la protection des données personnelles.	Conserver les logs d'accès, de création, de modification et de suppression de données personnelles. Respecter les règles de traitement des données personnelles. Traitement conforme des données personnelles. Assurer la sécurité des systèmes d'information.

Ne pas posséder de pare-feu est une sécurité insuffisante. Qui équivaut à laisser les portes ouvertes aux hackers.

La mise en œuvre

Le plan

La demande initiale de l'entreprise KLLT Bank est de fournir une sécurité convenable, de lier les sites de Paris et de Bastia, et de sécuriser le serveur WEB. Pour ce faire, je vais mettre en place les équipements / technologies suivantes afin de répondre au mieux à la problématique.

Sécuriser : Mise en place d'un pare-feu Fortigate 60E sur le site de Paris, ainsi que sur le site de Bastia.

Relier les deux sites : Mise en place d'un VPN Site-to-site entre Paris et Bastia.

Sécuriser le serveur WEB de Paris : Mise en place d'une DMZ reliée au serveur WEB

Le câblage physique

Forti-Bastia : Internal 1 -> Switch 2 (Vers LAN)

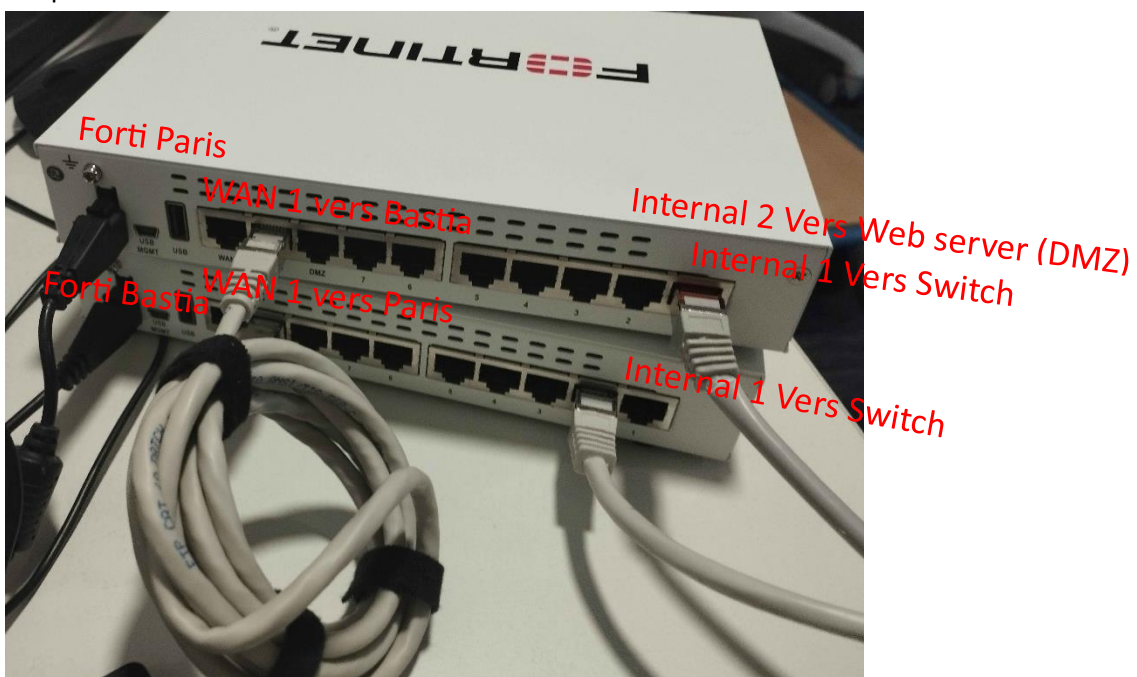
Forti-Bastia : WAN 1 -> Internet

Forti-Paris : Internal 1 -> Switch 1 (Vers LAN)

Forti-Paris : Internal 2 -> Serveur WEB (configuration DMZ)

Forti-Paris : WAN 1 -> Internet

Ce qui donne :

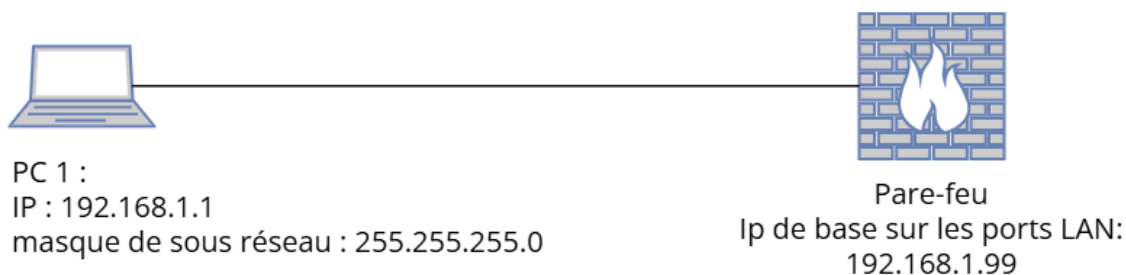


Comment commencer la configuration

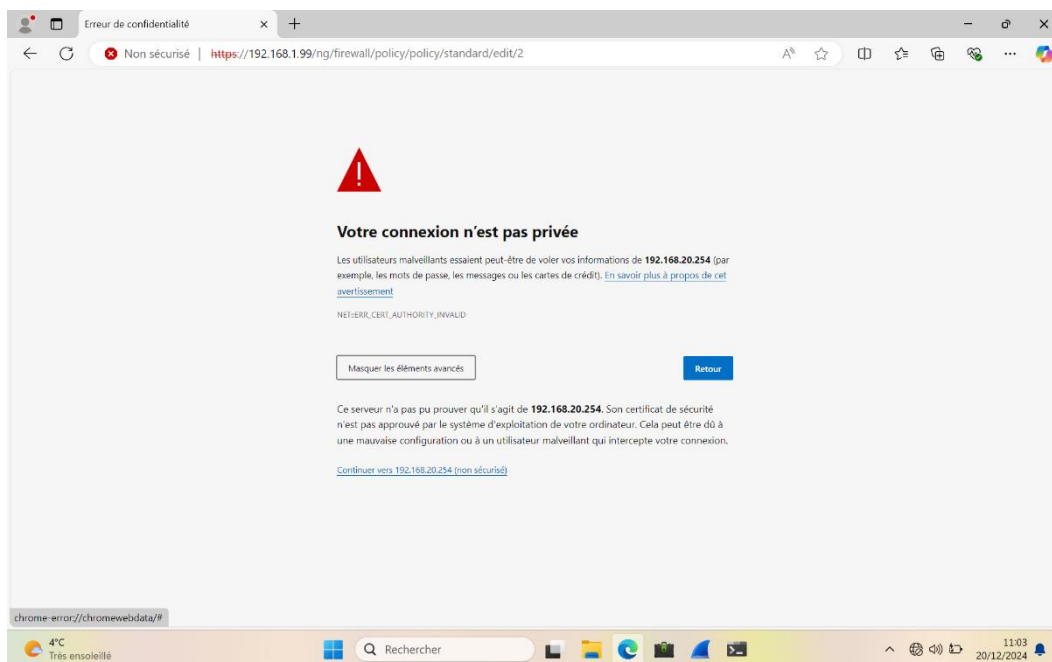
Au début, tant que les pare-feu ne communiquent pas entre eux, il faudra aller dessus manuellement en branchant un port (de internal 1 à 7) au pc, et en modifiant manuellement l'ip de son pc.

Commençons la configuration du premier pare-feu.

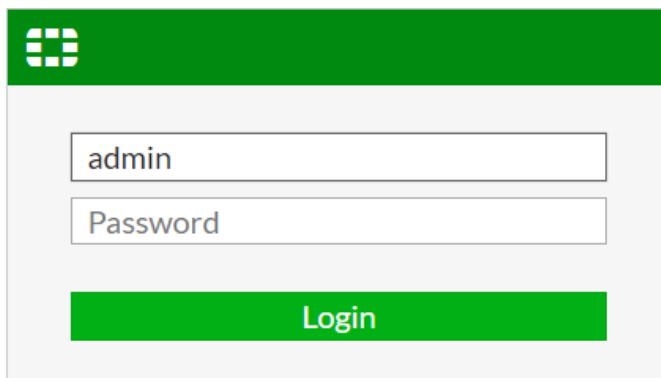
L'ip de base des ports Lan étant 192.168.1.99, il faut choisir et affecter au pc une ip différente, mais toujours dans le même réseau, tels que 192.168.1.1/24.



Une fois fait, nous pouvons communiquer avec le pare-feu. Un ping peut être effectué mais dans notre cas, cela ne servira à rien. Il suffit de rentrer dans le navigateur et de taper l'ip du port du pare-feu comme ceci.



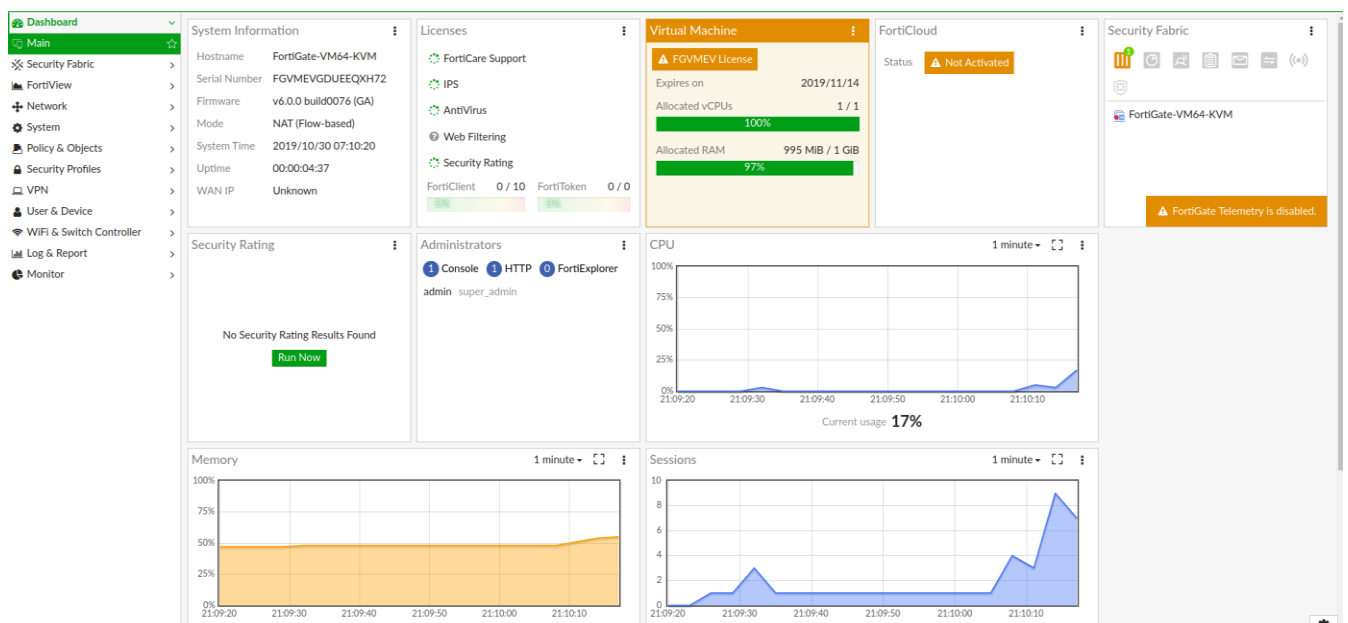
Puis cliquer sur avancer et sur 192.168.1. 1 .



The image shows the FortiGate login interface. It has a green header with the FortiGate logo. Below the header, there are two input fields: one for the username 'admin' and one for the password 'Password'. At the bottom, there is a green 'Login' button.

Cette page est la page de connexion au pare-feu. Par défaut, l'identifiant est « admin » et il n'y a pas de mot de passe.

Il est très recommandé de modifier l'identifiant et le mot de passe.



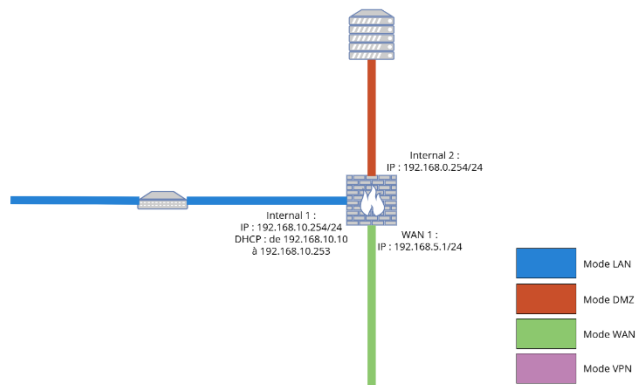
Voici la page d'administration de notre Fortigate. Voici les différentes page que l'on vas utiliser dans cette situation professionnelle.

- Le dashboard : c'est le centre de contrôle. On y trouve diverses informations tel que le pourcentage d'utilisation de CPU, RAM, et l'utilisation de la session.
- Network > Interface : c'est ce qui permet de modifier les interfaces du Fortigate. On peut y modifier l'ip, le type de port (LAN / WAN / DMZ), ainsi que faire un DHCP.
- Network > Static Routes : c'est ce qui permet de créer les routes pour dire au pare-feu quels sont les réseaux autour de lui.
- Policy & Objects > IPV4 : permet d'autoriser ou de refuser certains services d'une interface à une autre.
- VPN > IPsec Wizard : permet la création d'un VPN
- VPN > IPsec Tunnels : permet de voir les différents VPN, et voir le status (phase 1 ou 2 montées ?)

Configuration du pare-feu

Le but est de configurer un port LAN, WAN et DMZ. Dans notre cas, la DMZ (zone démilitarisée) vas permettre la séparation totale du serveur WEB sur le réseau. Cela permettra d'éviter que les attaques venant du WEB s'étendent sur le réseau.

Commençons par modifier les interfaces. Par défaut, toutes les interfaces sont regroupées en une pour faciliter la connexion.



Quand on clique sur ce groupe, on peut voir que tous les ports sont à l'intérieur. Il vas donc falloir cliquer sur la croix de tous les ports sauf le port 2, et configurer l'IP comme en dessous (192.168.0.254). Car si l'on retire tous les ports, aucune IP ne sera attribuée, et donc, il faudra le réinitialiser. Puis, il faut donner le rôle DMZ. (voir schéma du dessus).

Cette image est un screenshot de l'interface de configuration d'une interface réseau dans FortiGate. Les champs suivants sont visibles :

- Interface Name : lan
- Alias : (vide)
- Type : Software Switch
- Interface Members : Une grille de boutons pour sélectionner des ports (port3, port4, port5, port6, port7, port8, port9, port10). Les boutons port3, port4, port5, port6, port7, port8, port9 et port10 ont une croix rouge, indiquant qu'ils sont sélectionnés. Le bouton port2 n'est pas visible, ce qui correspond à la configuration DMZ décrite dans le texte.
- Tags : (vide)
- Role : DMZ (sélectionné dans un menu déroulant)
- Addressing mode : Manual (sélectionné), DHCP, Dedicated to FortiSwitch
- IP/Network Mask : 192.168.0.254/24

Ici, notre port 2 a été configuré en DMZ. Etant donné que c'est le seul à avoir une IP, il va falloir se brancher dessus avec l'ordinateur de configuration, et mettre l'IP 192.168.0.1/24. C'est une IP éphémère, le temps que l'on configure les autres ports. Quand on se reconnecte, on découvre que les autres ports sont maintenant assignables.

Configurons maintenant l'interface 1 comme ceci :

Cette image est un screenshot de l'interface de configuration d'une interface réseau dans FortiGate, montrant la configuration pour l'interface 1. Les champs suivants sont visibles :

- Interface Name : internal1 (08:5B:0E:A9:FF:EA)
- Alias : (vide)
- Link Status : Up
- Type : Physical Interface
- Tags : (vide)
- Role : LAN (sélectionné dans un menu déroulant)
- Addressing mode : Manual (sélectionné), DHCP, PPPoE, Dedicated to FortiSwitch
- IP/Network Mask : 192.168.10.254/255.255.255.0
- Administrative Access : Une grille de cases à cocher pour sélectionner des protocoles (IPv4, HTTPS, HTTP, PING, FMG-Access, CAPWAP, SSH, SNMP, FTM, RADIUS Accounting, FortiTelemetry). Toutes les cases sont cochées.
- DHCP Server : (coché)
- Address Range : Une grille de champs pour définir une plage d'adresses IP. Les champs Starting IP (192.168.10.1) et End IP (192.168.10.253) sont remplis. Le champ Netmask (255.255.255.0) est également rempli.

Cette configuration appliquera l'adresse IP 192.168.10.254/24 à l'interface 1 et créera un DHCP.

Pour ce qui est de l'interface WAN1, il suffit de rentrer cette configuration dans ce port :

L'interface se nommera VPN car elle permettra le passage du VPN, elle à le rôle WAN, et appliquera l'IP 192.168.5.2/24.

Enfin, nous pouvons voir que les interfaces ont correctement été créés :

Status	Name	Members	IP/Netmask	Type	Access	Ref.
Hardware Switch (1)						
	internal	1 2 3 4 5 6 7	192.168.1.99 255.255.255.0	Hardware Switch (1)	PING HTTPS SSH HTTP FMG-Access CAPWAP	0
Physical (9)						
+	dmz		10.10.10.1 255.255.255.0	Physical Interface	PING HTTPS SSH SNMP HTTP FMG-Access RADIUS-ACCT CAPWAP FTM FortiTelemetry	0
+	internal1		192.168.10.254 255.255.255.0	Physical Interface	PING HTTPS SSH SNMP HTTP FMG-Access RADIUS-ACCT CAPWAP FTM FortiTelemetry	3
+	DMZ		192.168.0.1 255.255.255.0	Physical Interface	PING HTTPS SSH SNMP HTTP FMG-Access RADIUS-ACCT CAPWAP FTM FortiTelemetry	3
+	internal4		0.0.0.0 0.0.0.0	Physical Interface		0
+	internal5		0.0.0.0 0.0.0.0	Physical Interface		0
+	internal6		0.0.0.0 0.0.0.0	Physical Interface		0
+	internal7		0.0.0.0 0.0.0.0	Physical Interface		0
+	wan1 (VPN)		192.168.5.1 255.255.255.0	Physical Interface	PING HTTPS SSH SNMP HTTP FMG-Access RADIUS-ACCT CAPWAP FTM FortiTelemetry	0
+	wan2		0.0.0.0 0.0.0.0	Physical Interface	PING FMG-Access	0

Nous pouvons maintenant connecter l'interface 1 au commutateur de paris, et quand on y branche un ordinateur avec une IP du réseau 192.168.10.x/24 avec une Gateway en 192.168.10.254. Elle sera capable de ping cette même Gateway. On fait les mêmes étapes pour le Pare-feu de Bastia mais avec l'internal 1 et 192.168.20.254 et le WAN 1 en 192.168.5.2

Passons à l'étape du routage. Cette étape est essentielle pour que les équipements puissent communiquer avec d'autres équipements du même réseau. Pour cela, je vais utiliser le routage statique.

Voici un plan des routes à faire :

Fortigate n°1		
Vers :	Via :	Via l'interface :
192.168.20.0	192.168.5.0	Wan 1
192.168.0.0	192.168.10.0	Internal 2

Fortigate n°2		
Vers :	Via :	Via l'interface :
192.168.10.0	192.168.20.0	Wan 1

Donc sur le Fortinet de PARIS (192.168.10.254) il faut aller dans Network > Static Routes et créer les routes comme dans le tableau.

FortiGate 60D FGT60D4614063251

Dashboard > Edit Static Route

Security Fabric >

FortiView >

Network >

Interfaces

DNS

Packet Capture

SD-WAN

Performance SLA

SD-WAN Rules

Static Routes ☆

System 1 >

Policy & Objects >

Dynamic Gateway ☒

Destination

192.168.20.0/255.255.255.0

Interface

Gateway Address 192.168.5.1

Administrative Distance 10

Comments Write a comment... 0/255

Status

Advanced Options

OK Cancel

FortiGate 60D FGT60D4614063251

Dashboard > Edit Static Route

Security Fabric >

FortiView >

Network >

Interfaces

DNS

Packet Capture

SD-WAN

Performance SLA

SD-WAN Rules

Static Routes ☆

System 1 >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

WiFi & Switch Controller >

Log & Report >

Monitor >

Dynamic Gateway ☒

Destination

192.168.0.0/255.255.255.0

Interface

Gateway Address 192.168.0.1

Administrative Distance 10

Comments Write a comment... 0/255

Status

Advanced Options

OK Cancel

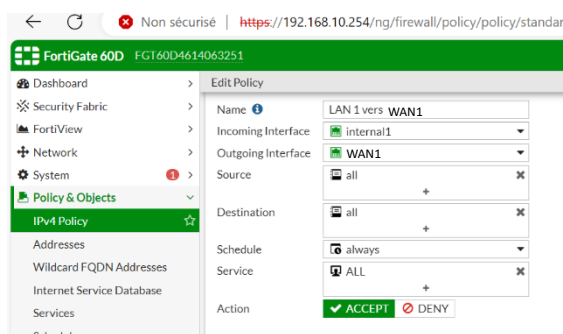
Et la route pour la DMZ.

Et faire les mêmes actions à l'envers sur le Forti 2 de Bastia.

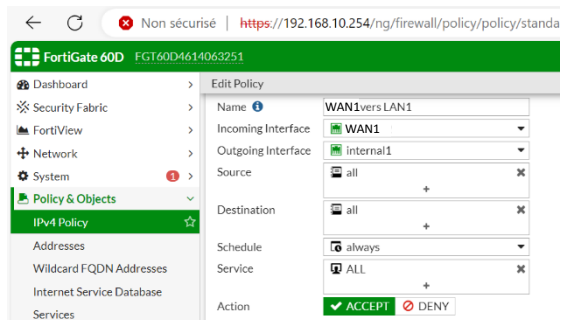
Les routes sont faites, mettons maintenant les règles en place.

Les règles permettent d'autoriser de restreindre ou de refuser le passage d'un flux d'une interface à une autre. Dans notre cas, nous allons commencer par mettre toutes les règles en ALL. Cela signifie que tout les flux peuvent passer d'un point A à un point B. Cela nous permettra de voir si le réseau fonctionne correctement. Pour bien mieux sécuriser le réseau, il faudrait filtrer les règles et les ports. Par exemple, il faudrait désactiver l'ICMP permettant de refuser les pings et donc, éviter que l'attaquant face un scan NMAP du réseau. Il est également essentiel de désactiver les ports inutilisées, en désactivant la totalité des ports, et en activant petit à petit les ports utiles aux logiciels.

Pour les règles du Fortigate 1 (Paris), voici comment procéder :



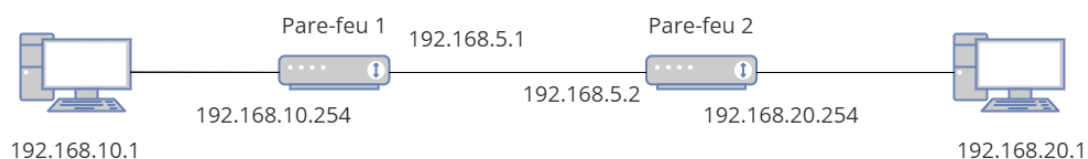
Ce paramétrage définit le trafic de l'interface 1 au wan1 (du lan au WAN) en all. Autrement dit, tout le trafic du Lan au Wan sera autorisé.



Ainsi que dans l'autre sens.

Et faire de même dans l'autre Fortinet.

Il est maintenant possible de ping l'autre pare-feu. Nous pouvons maintenant faire un test pour voir si les deux pare-feu communiquent. Pour cela, connectons deux machines de bout à bout comme ceci :



Et les ping entre eux :

```
C:\Users\adm-l.lecorre>ping 192.168.10.1

Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps=2 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=2 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

```
C:\Users\adm-l.lecorre>PING 192.168.20.254

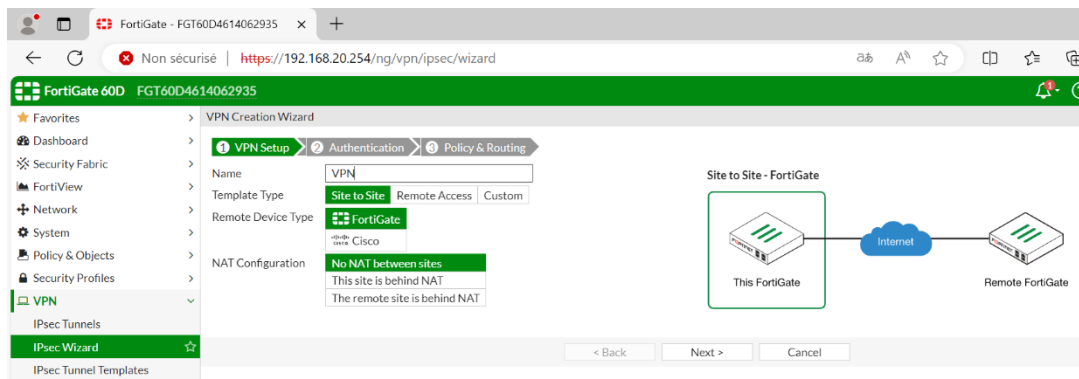
Envoi d'une requête 'Ping' 192.168.20.254 avec 32 octets de données :
Réponse de 192.168.20.254 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.20.254 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.20.254 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.20.254 : octets=32 temps=1 ms TTL=255

Statistiques Ping pour 192.168.20.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

Nous pouvons voir que les deux machines peuvent communiquer. Mais pour l'instant, elles ne peuvent communiquer uniquement quand elles sont physiquement reliées.

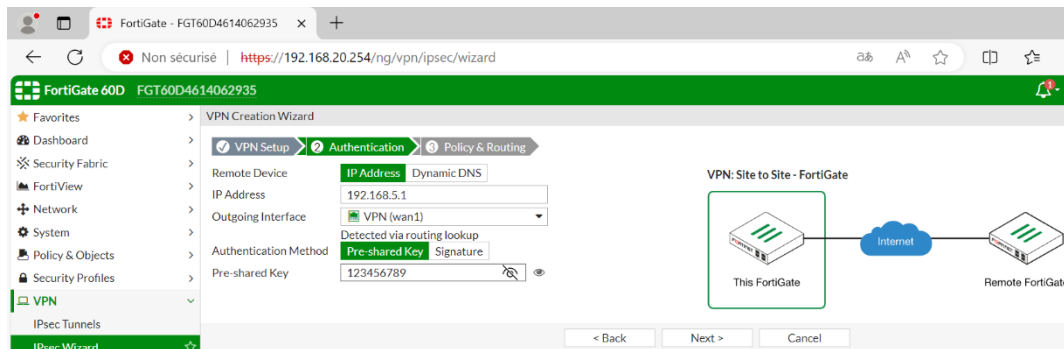
Pour qu'elles communiquent à distance, il faut mettre en place le VPN. En les reliant avec internet, ils communiqueront. Les deux pare-feu doivent avoir la même méthode de chiffrement pour communiquer. Le principe de ce chiffrement est d'éviter que des personnes mal intentionnées puissent écouter les informations qui transitent, ou bien de réussir à se connecter en réseau par le VPN.

Pour la mise en place de ce VPN, rendons nous dans VPN et Ipsec Wizard.

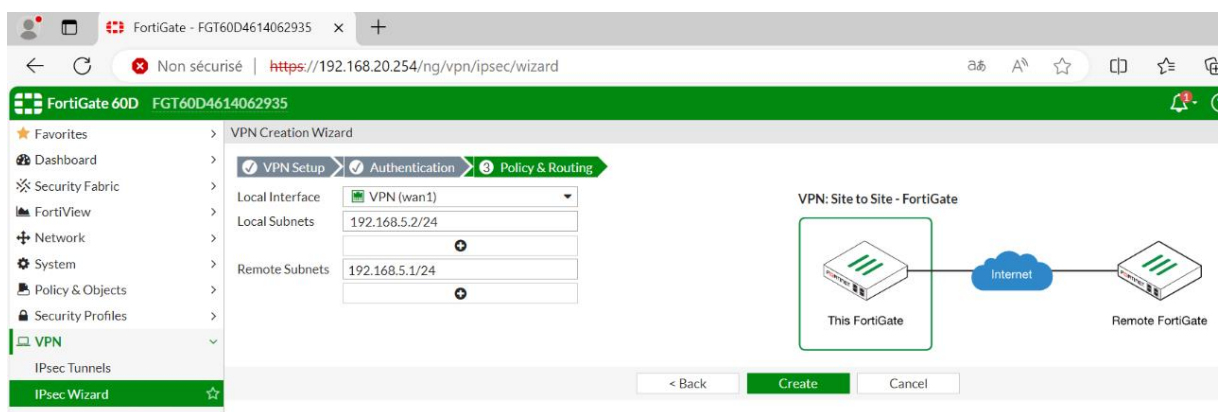


Nous devons donner un nom à ce VPN, et choisir une Template. Dans ce cas, je choisis le site to site. Étant donné que le second pare-feu est de la marque Fortinet, le Remote Device Type sera Fortinet. Et choisir This site is behind NAT.

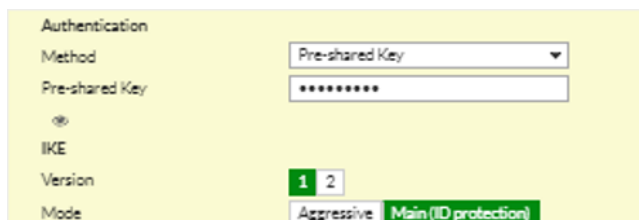
Sécurité du VPN



Puis en authentification, il suffit de mettre l'ip du Wan du Fortinet cible. Qui est dans ce cas 192.168.5.1. Il est également nécessaire d'indiquer vers quel port le flux VPN sortiras. Enfin, il faut définir une Pre-shared Key. Cette suite de caractère se doit d'être complexe (ce qui n'est pas le cas de cette exemple) car elle est utile pour que les deux pare-feu puissent vérifier leurs identités avant même d'établir une connexion. Une fois cette étape passée, cette même PSK est utilisée pour chiffrer et déchiffrer les données.



Suite à la création de ce VPN, nous pouvons modifier les différentes étapes de ce même VPN.



La première étape étant l'authentification. Comme dit précédemment, la PSK est vitale au bon déroulement du VPN. Nous pouvons voir qu'une option supplémentaire est apparue. C'est le mode. Le mode Aggressive diminue le nombre d'échanges lors de

l'authentification, ce qui le rend plus rapide mais également plus vulnérable aux attaques. Je n'active pas cette option.

Phase 1 Proposal ➕ Add

Encryption	AES128	Authentication	SHA256	✕
Encryption	AES256	Authentication	SHA256	✕
Encryption	AES128	Authentication	SHA1	✕
Encryption	AES256	Authentication	SHA1	✕

Diffie-Hellman Groups

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

Key Lifetime (seconds)

Local ID

Ces options permettent de sécuriser l'échange des clés. Nous pouvons voir que je chiffre l'encryption à partir des méthodes de chiffrement AES128 et AES256. Pour l'authentification, c'est le SHA256 et SHA1 qui sont utilisées. Diffie-Hellman Groups permet de sélectionner la force de complexité de l'échange de clés. La durée de vie de cette clé est de 24h comme spécifiée dans la section Key Lifetime.

Phase 2 Selectors

Name	Local Address	Remote Address
vpn_demonstration		

New Phase 2 ⊕ ⊖

Name

Comments

Local Address

Remote Address

⚙ Advanced...

Phase 2 Proposal ➕ Add

Encryption	AES128	Authentication	SHA1	✕
Encryption	AES256	Authentication	SHA1	✕
Encryption	AES128	Authentication	SHA256	✕
Encryption	AES256	Authentication	SHA256	✕
Encryption				✕
Encryption				✕
Encryption				✕

Enable Replay Detection ☒

Enable Perfect Forward Secrecy (PFS) ☒

Diffie-Hellman Group

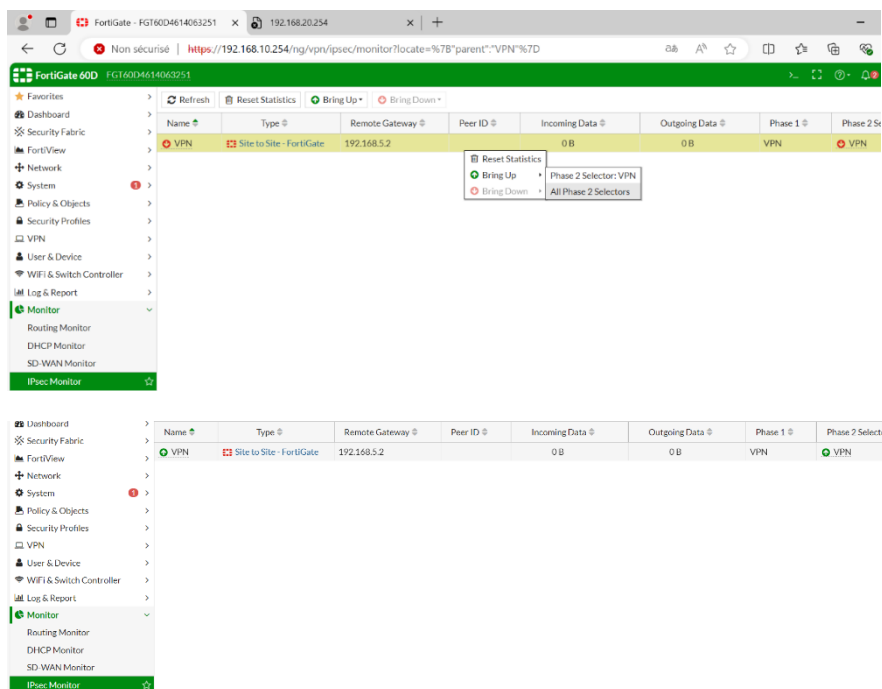
☒ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27 ☐ 21
☐ 20 ☐ 19 ☒ 18 ☒ 17 ☐ 16 ☐ 15
☐ 14 ☐ 5 ☐ 2 ☐ 1

La phase 2 quant à elle, est la suite de la phase 1. Elle établit les tunnels sécurisé par lequel les données seront échangées. Elle permet également la négociation des paramètres de sécurités spécifiques pour protéger les données échangées via le tunnel VPN. Sa façon de le paramétrer est semblable à celle de la phase 1.

Pour la configuration VPN du second pare-feu, il suffit d'inverser les IP. Cependant, il faut que la sécurité soit la même. Sinon, le VPN ne se montra pas.

Maintenant crée, le VPN vas pouvoir être montée. Mais d'abord, il vas falloir monter le VPN manuellement pour que les deux phases s'activent.

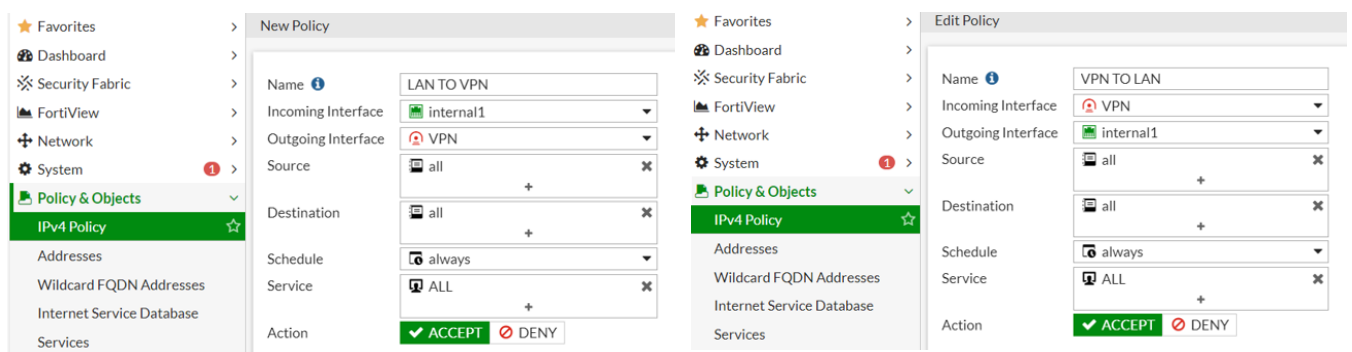
Pour ce faire, il faut aller dans Monitor, puis, IPsec Monitor. Nous pouvons voir que notre VPN est apparu.



Clique droit, Bring Up, all Phase 2 Selectors pour faire monter le VPN.

L'indicateur apparait en vert.

Maintenant, il ne manque plus qu'à créer deux nouvelles règles pour autoriser le trafic entre le LAN et le VPN.



Ces deux règles autorisent le trafic dans les deux sens. Il faut les mettre dans les deux pare-feu.

Test de fonctionnement

Nous allons tout d'abord voir si les deux phases du VPN sont montées. Pour cela, il faut écrire dans l'invite de commande du pare-feu la commande `diagnose vpn tunnel list`.

```
Connected

FGT60D4614062935 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=VPN _FIN ver=1 serial=3 192.168.2.2:0->192.168.2.1:0
bound_if=6 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/8 options[0008]=np
proxyid_num=1 child_num=0 refcnt=5 ilast=3 olast=783 ad=/0 itn-status=64
stat: rxp=258 txp=1537 rxb=240 txb=458831
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN _FIN proto=0 sa=1 ref=2 serial=1
  src: 0:192.168.20.0/255.255.255.0:0
  dst: 0:192.168.10.0/255.255.255.0:0
  SA: ref=5 options=10226 type=00 soft=0 mtu=1438 expire=41758/0B replaywin=
    seqno=64a esn=0 replaywin_lastseq=00000100 itn=0
  life: type=01 bytes=0/0 timeout=42930/43200
  dec: spi=0560e8c1 esp=aes key=16 fa25335b61cdd6382e4c77b82a975722
    ah=sha1 key=20 93f7fe8648278f4cb869907b194a41cb5b99f1ca
  enc: spi=9cbf4b8d esp=aes key=16 8b0931057bed42645f15a3455731bd33
    ah=sha1 key=20 2e30a228f47e284eb324ca1a37ce3fd8e73ec3da
  dec:pkts/bytes=258/120, enc:pkts/bytes=1937/972059
  npu_flag=03 npu_rgwy=192.168.2.1 npu_lgwy=192.168.2.2 npu_selid=4
-----
name=Tunnel ver=1 serial=2 192.168.5.2:0->192.168.5.2:0
bound_if=5 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/8 options[0008]=np
proxyid_num=1 child_num=0 refcnt=4 ilast=1 olast=1 ad=/0 itn-status=64
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=Tunnel proto=0 sa=0 ref=1 serial=1
  src: 0:192.168.20.0/255.255.255.0:0
  dst: 0:192.168.10.0/255.255.255.0:0
-----
name=VPN ver=1 serial=1 10.10.10.1:0->192.168.5.1:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/8 options[0008]=np
proxyid_num=1 child_num=0 refcnt=4 ilast=4 olast=4 ad=/0 itn-status=64
stat: rxp=0 txp=0 rxb=0 txb=0
```

On peut voir que les phases fonctionnent car :

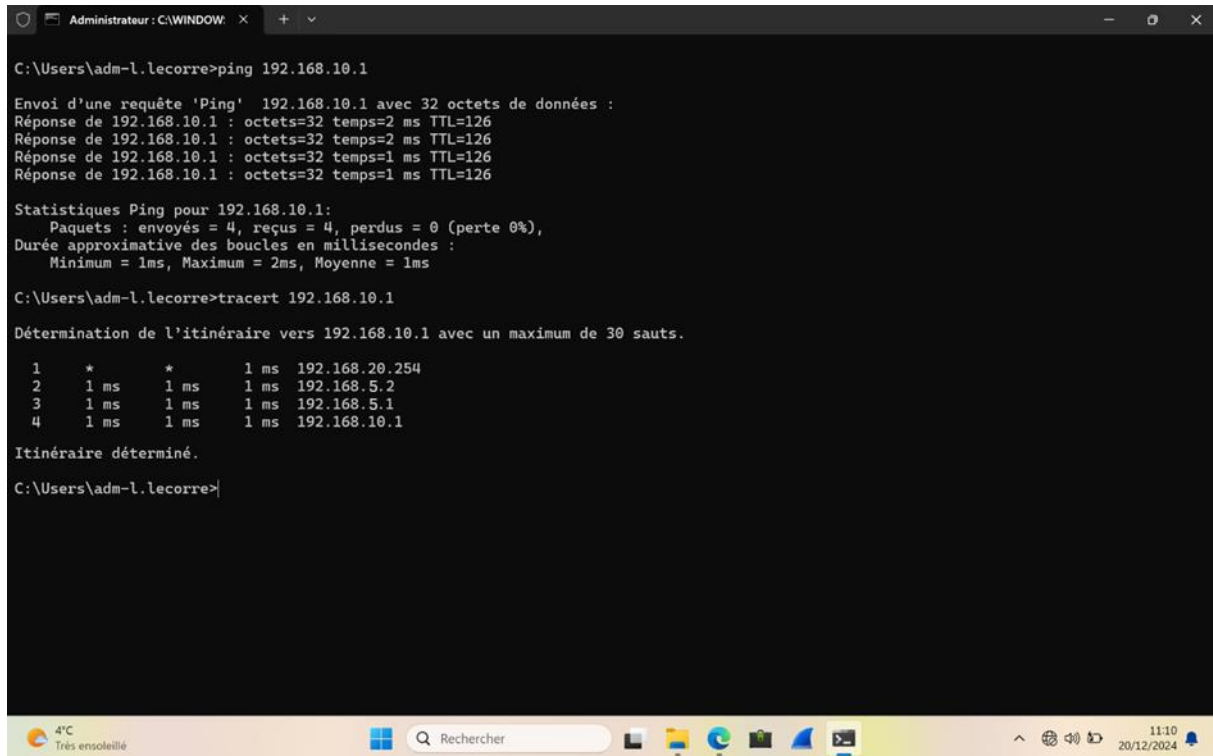
Phase 1 (IKE) est indiquée par la présence de `enc: spi=...` et `dec: spi=...`.

Phase 2 (IPsec) est confirmée par la présence de `proxyid=...` `proto=0` `sa=1` `ref=2` `serial=1`.

Enfin, finissons le test par un ping.

La commande est la suivante : ping 192.168.10.1 venant du pc en 192.168.20.1 .

Pour vérifier que les données passent par les bonnes « portes », on peut utiliser la commande
tracert 192.168.10.1



```
C:\Users\adm-l.lecorre>ping 192.168.10.1

Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps=2 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=2 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms

C:\Users\adm-l.lecorre>tracert 192.168.10.1

Détermination de l'itinéraire vers 192.168.10.1 avec un maximum de 30 sauts.

  1  *          *           1 ms  192.168.20.254
  2  1 ms      1 ms        1 ms  192.168.5.2
  3  1 ms      1 ms        1 ms  192.168.5.1
  4  1 ms      1 ms        1 ms  192.168.10.1

Itinéraire déterminé.
C:\Users\adm-l.lecorre>
```

On peut voir que le ping est concluant. Et que la réponse au tracert indique que les données venant du pc 192.168.20.1 passe tout d'abord par sa passerelle par défaut étant 192.168.20.254 puis par le côté WAN 192.168.5.2. Il rejoint ensuite le second routeur par le WAN en 192.168.5.1 et le LAN de Bastia pour aller jusqu'au pc en 192.168.10.1.