Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
Parcours cybersécurité

Migration d'un réseau MPLS vers un réseau hybride MPLS/SD-WAN

Quentin GARDA

NXO France

Responsable entreprise : Vincent MOGINOT

Responsable académique : Éric WÜRBEL

2023

Table des matières

1 Introduction 4
2 Présentation entreprise 5
2.1 Présentation NXO France 5
2.2 Présentation des activités de NXO France 6
2.3 Organigrammes 7
3 Mission principale 8
3.1 Contexte 8
3.2 Cahier des charges 8
3.3 Intitulé du projet 8
3.4 Environnement technique 9
3.5 Présentation du travail réalisé 10
3.5.1 Partie 0 : Intégration du projet 10
3.5.2 Partie 1 : Mise en place et mise à jour de la maquette 10
3.5.3 Partie 2 : Configuration Générale 12
3.5.4 Partie 3 : Configuration HUB 13
3.5.5 Partie 4 : Configuration sites distants 19
3.5.6 Partie 5 : Configuration des switchs 23
3.5.7 Partie 6 : Configuration des SRX 23
4 Missions secondaires et sujets abordés 25
4.1 Choses vues 25
5 Conclusion 27
6 Remerciements 29
7 Glossaire 31
8 Bibliographie 33

1 Introduction

Le BUT, Bachelor Universitaire de Technologie Réseaux et Télécommunications a pour objectif de nous apprendre les fondamentaux théoriques des réseaux et de toutes ses applications. En plus de la mise en pratique de ces fondamentaux au cours de TPs nous devons aussi les mettre en pratique lors d'un stage en entreprise de 10 semaines.

J'ai donc effectué mon stage en tant qu'Expert Projets dans l'entreprise d'intégration informatique NXO France sous la tutelle de Vincent MOGINOT, Service Manager pour le territoire Méditerranée Corse. J'ai été affecté avec toute une équipe sur un projet de migration d'un réseau MPLS, MultiProtocol Label Switching vers un réseau hybride SD-WAN, Software-Defined Wide Area Network/MPLS.

Je détaillerai en premier lieu l'historique, le panel d'activité et l'organisation de NXO France. Puis je vous présenterai le projet sur lequel j'ai travaillé ainsi que les missions secondaires auxquels j'ai participé.

2 Présentation entreprise

2.1 Présentation NXO France

NXO France (ex NextiraOne) est une entreprise indépendante spécialisée dans l'intégration de solutions informatiques et de services de communications, fondé en 2015 (1999 pour NextiraOne). Cette société est une SAS, société par actions simplifiée, dont le siège se situe à RUEIL-MALMAISON, possède 65 établissements pour 39 implémentations et compte 1250 employés. Depuis le 20 septembre 2021 NXO a rejoint le groupe Fayat, offrant de nouvelles opportunités à la société tel que dans le marché de la domotique.

L'entreprise fournit des solutions informatiques personnalisées à des entreprises. Elle accompagne ses clients du design jusqu'à la maintenance de la solution proposée. Pour pouvoir faire cela l'entreprise dispose de la filiale NXO Expert qui vient intervenir de manière indépendante en faisant du conseil, des études d'opportunités, des audits avant intégration et déploiement de la solution et en faisant de l'optimisation des coûts, de la gestion de vie du réseau, de l'assistance au pilotage de l'infogérance et du maintien post-déploiement.

NXO Télécom est une filiale régionale fondé en 2015 s'occupant des activités de l'entreprise dans le Haut Rhin et la franche Comté. C'est une société par actions simplifiée à associé unique dont le siège se situe au même endroit que NXO France.

NXO Océan-Indien est une filiale régionale fondé en 1992 s'occupant des activités de l'entreprise sur les territoires de la Réunion. Société par actions simplifiée dont le siège réside à SAINT-DENIS.

2.2 Présentation des activités de NXO France

Infrastructures Digitales :

NXO France propose de la mise en place d'infrastructures réseaux :

- LAN, Local Area Network – WLAN, Wireless Local Area Network
- WAN, Wide Area Network - SD-WAN
- Data Center
- Campus

Ainsi que de l'optimisation de réseaux déjà existants :

- Data Center - Virtualisation
- Performances réseaux (supervision, analyse, diagnostique, résolution et optimisation)

Communication et Collaboration :

NXO France propose des solutions téléphonie :

- Téléphonie sur IP, Téléphonie Cloud (UCaaS, Unified Communications as a Service)

Visio-Conférence :

- Installation de système de visio-conférence (Lifesize)
- Formation aux nouvelles technologies installées

D'Application Collaboratives :

- Outils de travail collaboratif

Solution pour centre de contact :

- Centre de contact omnicanaux

Cybersécurité :

Protection :

- Sécurisation des applications et des données dans les data centers et le cloud
- Infrastructure sécurisée

Connexion sécurisée :

- Passerelle web, email sécurisé
- Accès à distance
- Sécurité des terminaux

Traçabilité :

- Logs
- Traçabilité opérations IT

Cloud :

Offres cloud :

- Services cloud basé sur leurs propres infrastructures et celles de leurs partenaires

Offres Opérateur :

- Offre téléphone mobile basé sur leurs propres infrastructures et celles de leurs partenaires

Services :

- Audit et conseils
- Conception d'infrastructures réseaux, de la phase de projet jusqu'à la formation des équipes aux nouvelles technologies installées
- Formations aux outils informatique
- Maintenance informatique
- Infogérance informatique
- Supervision informatique
- Assistance technique

2.3 Organigrammes

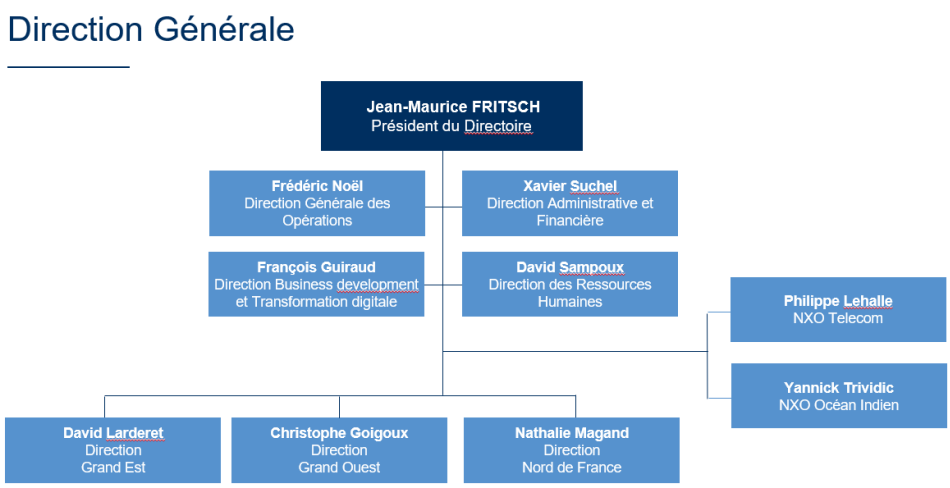


Figure 1 : Direction Générale

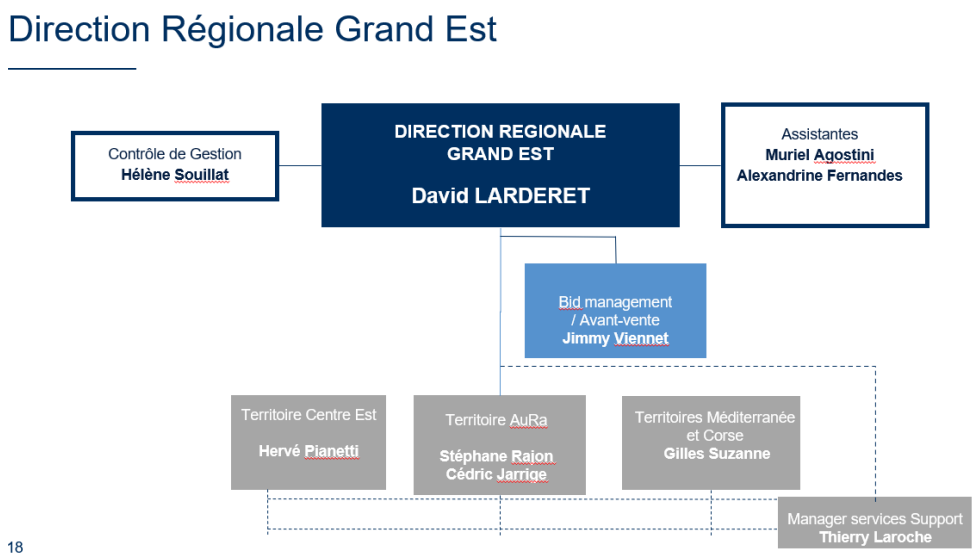


Figure 2 : Direction Régionale Grand Est

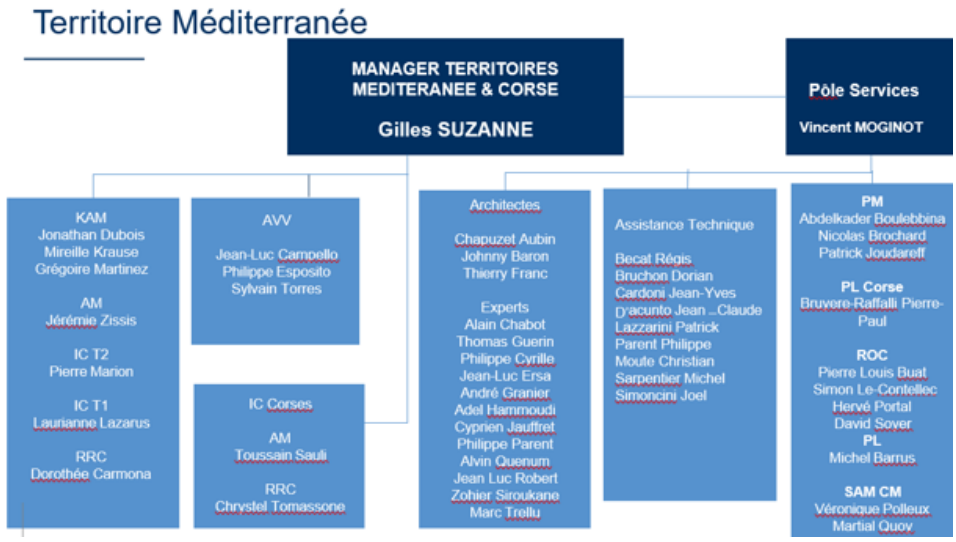


Figure 3 : Territoire Méditerranée

3 Mission principale

3.1 Contexte

NXO possède un client souhaitant migrer une partie de son réseau MPLS sur du SD-WAN, pour cela l'entreprise a donc lancé un projet commençant par la simplification du réseau du client, puis la collecte des configurations déjà présentes sur les équipements en place, la modification des règles présentes sur les équipements en place pour faciliter l'intégration des nouveaux équipements, la préparation des configurations pour les nouveaux équipements, l'intégration des nouveaux équipements et enfin la migration vers ceux-ci.

3.2 Cahier des charges

Le client ayant besoin d'un accès permanent les solutions de migration et de modification du réseau doit impacter au minimum le client

3.3 Intitulé du projet

Parmi toutes les missions qui m'ont été confié, la mission principale fut la migration d'un client de NXO d'un réseau MPLS vers un réseau hybride MPLS/SD-WAN. J'assistais donc l'équipe sur ce projet et ai participé aux multiples tâches tout au long du projet.

Ce projet vise à simplifier le réseau existant du client puis à y intégrer la solution MPLS/SD-WAN.

3.4 Environnement global

Ce projet n'englobe pas qu'une partie technique mais aussi une grande partie logistique, en effet ce projet la mobilisation de plusieurs équipes, je faisais principalement partie de l'équipe technique mais j'ai aussi participé à certaines tâches de l'équipe logistique.

Lors de ce rapport je vous présenterai principalement la partie technique, cependant j'ai aussi aidé lors de la mise à jour des documents techniques, lors de la préparation des envois des colis et lors du débogage des configurations.

Ce projet aura mobilisé une équipe technique réseau, une équipe technique sécurité, des agents sur terrains pour le déploiement et du travail à distance pour le support et la supervision des équipements.

3.4.1 Environnement technique

Les entreprises de tous types utilisent un réseau dit étendu (WAN) pour fournir à leurs employés des performances et une fiabilité suffisante afin de répondre aux besoins métiers de ces derniers. Comme la plupart des applications et des services utilisés par les employés sont généralement hébergés dans les centres de données de l'entreprise ou dans des centres de données hébergés dans le cloud, la conception du réseau étendu doit fournir à chaque utilisateur un accès fiable et réactif aux ressources de l'entreprise quel que soit son lieu de travail.
Il existe plusieurs offres de transport WAN qui peuvent être utilisées simultanément pour créer un réseau WAN robuste, sécurisé et rentable, notamment les réseaux privés virtuels (VPN) MPLS, Internet, les réseaux cellulaires (3G/LTE) et Carrier Ethernet. Les VPN, Virtual Private Network IP basés sur Internet offrent des prix attractifs pour la bande passante et peuvent augmenter les offres MPLS haut de gamme ou même remplacer l'offre MPLS dans certains scénarios. Une architecture réseau flexible doit pouvoir inclure toutes les offres de transport WAN possibles sans augmenter de manière significative la complexité de la conception globale.
Le SD-WAN est une application spécifique de la technologie SDN (Software-Defined Networking) appliquée aux réseaux étendus, qui sont utilisés pour connecter les réseaux d'entreprise - y compris les succursales et les centres de données - sur de grandes distances géographiques. Les cas d'utilisation courants du SD-WAN comprennent :

- **Contrôle du chemin d'accès au WAN** : Orientation du trafic des applications ou des préfixes sur des chemins déterministes du réseau étendu.
- **WAN hybride** : compléter le réseau de transport MPLS par le réseau de transport Internet pour augmenter la bande passante.
- **Routage applicatif** : Identification des applications par l'inspection approfondie des paquets afin de les orienter vers des chemins déterministes et de contourner les chemins défectueux qui violeraient les SLA.

Il y a de multiples sites distants sécurisé par des firewalls Fortinet (Fortigate 80F) raccordés au Firewall SaaS, Software as a Service (Fortigate 400F en cluster), ce Firewall SaaS est redondé grâce à un PRA, Plan de reprise d'activités (Fortigate 200F). Le tout est supervisé et contrôlé à distance grâce à un Fortimanager.
Le client possède 3 entités distinctes nécessitant des règles différentes pour chacune, cependant les 3 entités sont reliées au même firewall SaaS, donc pour pouvoir traitées chaque entité indépendamment malgré le boitier commun, nous avons créé des ADOMs, Administrative Domain et des VDOMs, Virtual Domain.

Les ADOMs permettent de regrouper et de superviser plusieurs VDOM dans la même "bulle". Les VDOMs quant à eux permettent de créer des règles de filtrage spécifique à certains appareils, cela revient à avoir plusieurs firewalls en un seul.

Une fois le matériel livré dans nos locaux nous avons pu maquetter la solution pour s'assurer de son bon fonctionnement et aussi faciliter l'intégration au réseau du client via le matériel ainsi configuré.

3.5 Présentation du travail réalisé

3.5.1 Partie 0 : Intégration du projet

Tout d'abord j'ai été intégré au projet via une réunion de présentation du projet où y était présenté la solution vendue au client, les différents objectifs et problématiques, et comment nous allions répondre à tout cela.

3.5.2 Partie 1 : Mise en place et mise à jour de la maquette

En premier lieu nous avons mis à jour l'ensemble du matériel vers la version souhaitée 6.4.6

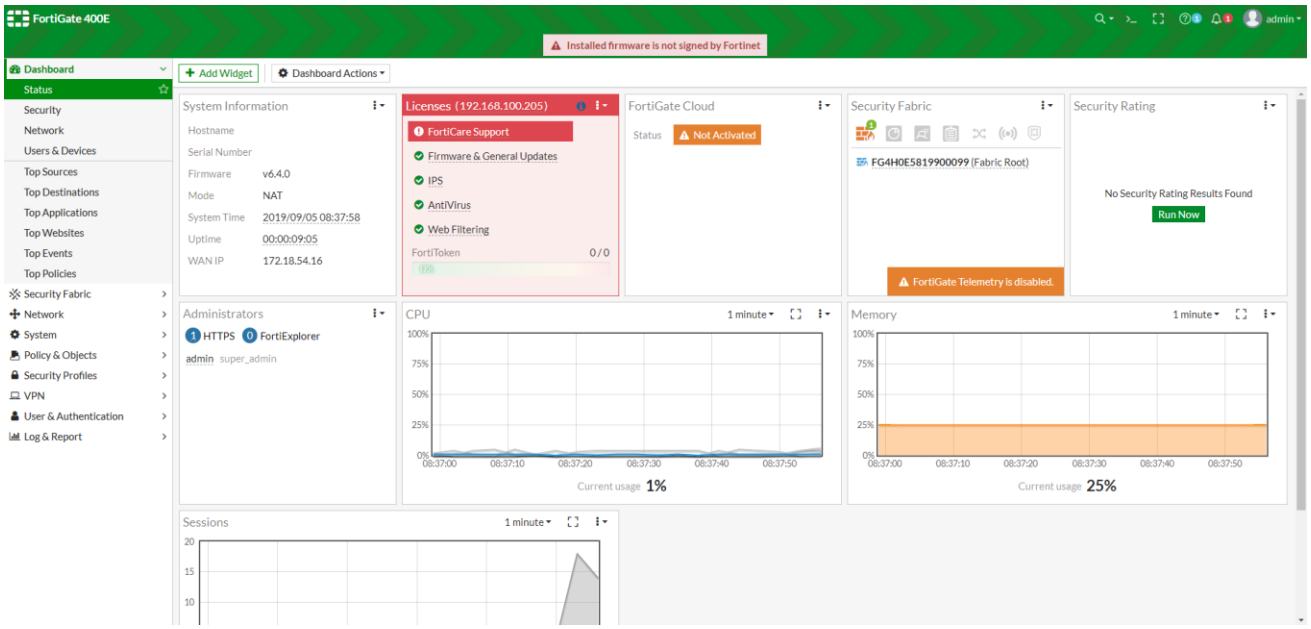


Figure 4 : Forti 6.4.6

Vers 7.0.11 (étant la dernière version stable à ce moment)

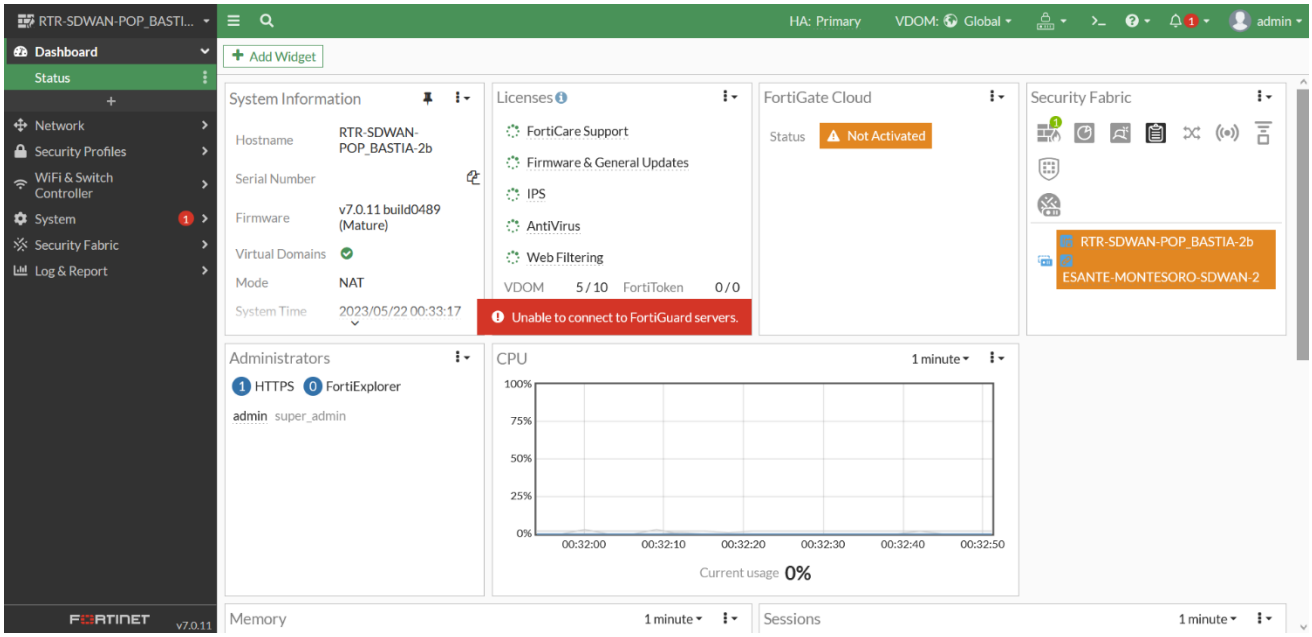


Figure 5 : Forti 7.0.11

Pour cela nous avons récupéré les images firmware correspondantes à la version désirée sur le site Fortinet et nous les avons ensuite installés sur les firewalls via leur interface web.

Une fois tout le matériel à jour, nous avons procédé aux configurations de base : hostname, alias, gateway, adresse internet et configuration des interface HA, high availability pour les clusters.

Ne pouvant malheureusement pas entièrement automatiser cette étape, nous avons copié une configuration vierge où nous avons variabiliser les valeurs que nous désirions changer

```
Hostname $_HOSTNAME_$
Hostname Alias $_LOCATION_$
IP WAN1 $_IPWAN1_$
GATEWAY $_GW_$
group-name "$_HA_GROUP_NAME"
group-id $_HA_GID_$
priority $_HA_PRIO_$
```

Figure 6 : Liste variable

Les nomenclatures suivent un standard étant celui-ci :
Dénomination-Lieu-BP-Num_membre_cluster

Les variables étaient donc remplacées ainsi :
Hostname = Dénomination-Lieu-BP-Num_membre_cluster
Alias = Lieu
IPwan = IPwan1
Gateway = IPgateway
Group_name = SITE_Lieu
Group_id = Groupid
Priority (seulement si cluster) = 128 ou 64 (128 si boitier principal du cluster sinon 64)

Pour pouvoir ensuite les remplacer via un Ctrl+F

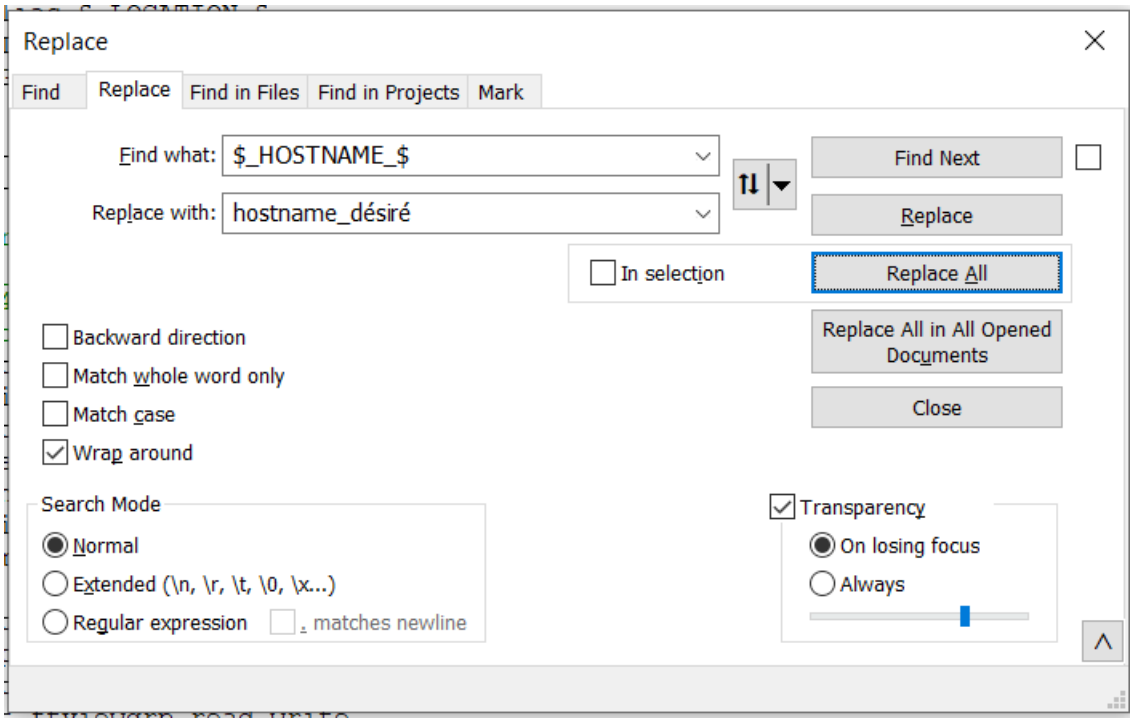


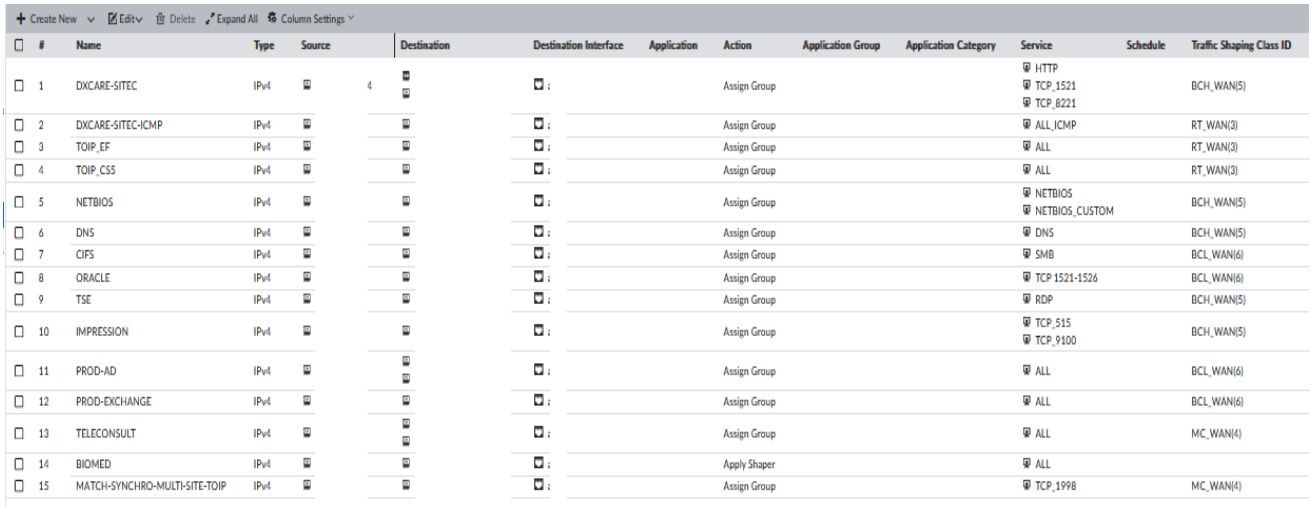
Figure 7 : Remplacement variable

Une fois toutes les variables modifiées nous supprimions le bloc de variable présenté plus haut puis nous sauvegardions une copie de la nouvelle configuration avec le nom du boitier de destination. Nous poussions ensuite la configuration voulu via CLI, Command-Line Interface sur les boitiers.

Une fois ceci fait nous avons pu ajouter les différents firewalls aux Fortimanager et créer un rôle admin avec mot de passe sécurisé pour ceux-ci.

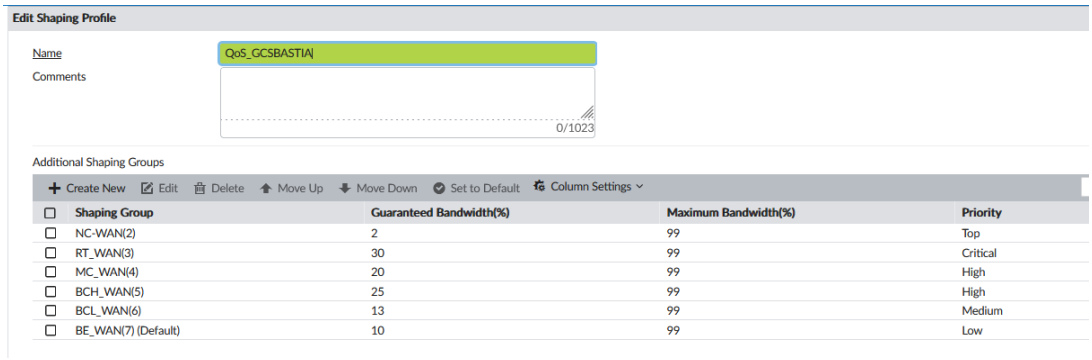
3.5.3 Partie 2 : Configuration Générale

Cette partie a été faite au fur et à mesure de l'avancement du projet, nous avons remarqué la nécessité de variabiliser certaines valeurs, ainsi que d'appliquer une QoS, Quality of Service aux différents VDOM.



#	Name	Type	Source	Destination	Destination Interface	Application	Action	Application Group	Application Category	Service	Schedule	Traffic Shaping Class ID
1	DXCARE-SITEC	IPv4					Assign Group			HTTP TCP_1521 TCP_8221		BCH_WAN(5)
2	DXCARE-SITEC-ICMP	IPv4					Assign Group			ALL_ICMP		RT_WAN(3)
3	TOIP_EF	IPv4					Assign Group			ALL		RT_WAN(3)
4	TOIP_CS5	IPv4					Assign Group			ALL		RT_WAN(3)
5	NETBIOS	IPv4					Assign Group			NETBIOS NETBIOS_CUSTOM		BCH_WAN(5)
6	DNS	IPv4					Assign Group			DNS		BCH_WAN(5)
7	CIFS	IPv4					Assign Group			SMB		BCL_WAN(6)
8	ORACLE	IPv4					Assign Group			TCP 1521-1526		BCL_WAN(6)
9	TSE	IPv4					Assign Group			RDP		BCH_WAN(5)
10	IMPRESSION	IPv4					Assign Group			TCP_515 TCP_9100		BCH_WAN(5)
11	PROD-AD	IPv4					Assign Group			ALL		BCL_WAN(6)
12	PROD-EXCHANGE	IPv4					Assign Group			ALL		BCL_WAN(6)
13	TELECONSULT	IPv4					Assign Group			ALL		MC_WAN(4)
14	BIOMED	IPv4					Apply Shaper			ALL		
15	MATCH-SYNCHRO-MULTI-SITE-TOIP	IPv4					Assign Group			TCP_1998		MC_WAN(4)

Figure 8 : Trafic Shaping Policy



Shaping Group	Guaranteed Bandwidth(%)	Maximum Bandwidth(%)	Priority
NC-WAN(2)	2	99	Top
RT_WAN(3)	30	99	Critical
MC_WAN(4)	20	99	High
BCH_WAN(5)	25	99	High
BCL_WAN(6)	13	99	Medium
BE_WAN(7) (Default)	10	99	Low

Figure 9 : Shaping Profile

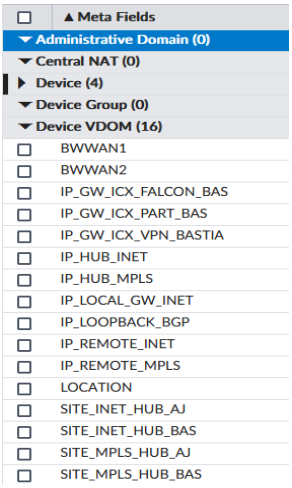


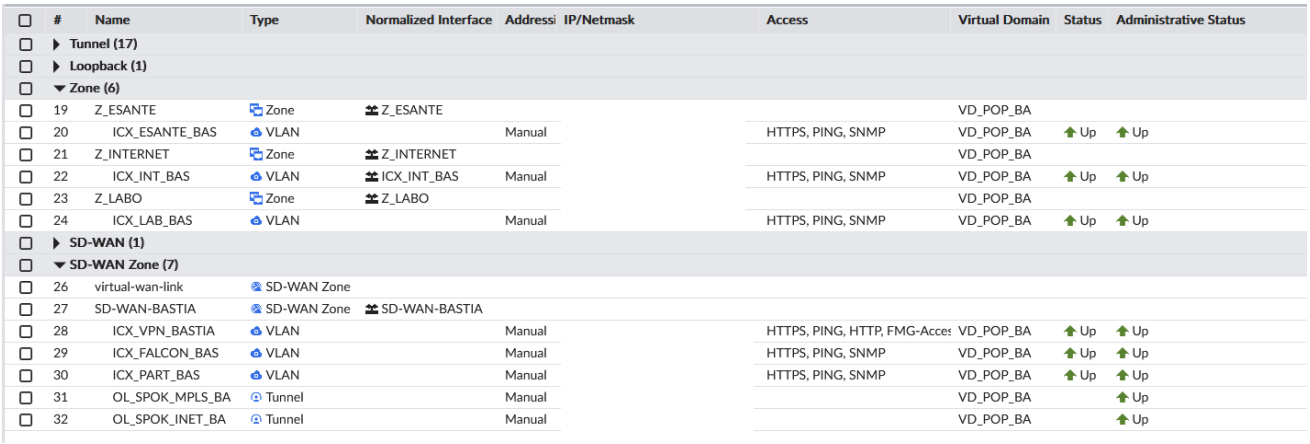
Figure 10 : Metafields Bastia

3.5.4 Partie 3 : Configuration HUB

Configuration Interfaces

Une fois tous les boitiers ajoutés nous avons alors commencé à configurer les HUB.

Nous avons alors commencé par ajouter les différentes interfaces aux VLANs, Virtual Local Area Network auxquelles elles avaient accès. Chaque VDOM avaient un VLAN pour Internet, un pour les serveurs Esante et un pour contacter les laboratoires partenaires.



#	Name	Type	Normalized Interface	Addressi	IP/Netmask	Access	Virtual Domain	Status	Administrative Status
	Tunnel (17)								
	Loopback (1)								
	Zone (6)								
19	Z_ESANTE	Zone	Z_ESANTE				VD_POP_BA		
20	ICX_ESANTE_BAS	VLAN		Manual		HTTPS, PING, SNMP	VD_POP_BA	Up	Up
21	Z_INTERNET	Zone	Z_INTERNET				VD_POP_BA		
22	ICX_INT_BAS	VLAN	ICX_INT_BAS	Manual		HTTPS, PING, SNMP	VD_POP_BA	Up	Up
23	Z_LABO	Zone	Z_LABO				VD_POP_BA		
24	ICX_LAB_BAS	VLAN		Manual		HTTPS, PING, SNMP	VD_POP_BA	Up	Up
	SD-WAN (1)								
	SD-WAN Zone (7)								
26	virtual-wan-link	SD-WAN Zone							
27	SD-WAN-BASTIA	SD-WAN Zone	SD-WAN-BASTIA						
28	ICX_VPN_BASTIA	VLAN		Manual		HTTPS, PING, HTTP, FMG-Acces	VD_POP_BA	Up	Up
29	ICX_FALCON_BAS	VLAN		Manual		HTTPS, PING, SNMP	VD_POP_BA	Up	Up
30	ICX_PART_BAS	VLAN		Manual		HTTPS, PING, SNMP	VD_POP_BA	Up	Up
31	OL_SPOK_MPLS_BA	Tunnel		Manual			VD_POP_BA		Up
32	OL_SPOK_INET_BA	Tunnel		Manual			VD_POP_BA		Up

Figure 11 : Interface du VLAN Bastia sur le VDOM Bastia

Les zones servent à regrouper plusieurs interfaces ensemble pour pouvoir leur apporter des changements en même temps, plutôt que de devoir modifier chaque interface une à une pour leur apporter les mêmes modifications.

Configuration templates

Une fois les interfaces des HUBs configurées, nous avons fait la configuration des templates. Les templates sont des configurations généralisées que nous créons nous-mêmes pour pouvoir ensuite l'appliquer à plusieurs boitiers ou un groupe de boitiers.

Les templates IPSec :

Nous configurons les tunnels VPN IPsec qui connecteront nos sites distants aux HUBs, ici nous sommes côté HUB, étant dans une topologie hybride il nous faut donc deux tunnels, un pour les flux passant par le réseau MPLS et un pour les flux passant par le réseau SD-WAN.

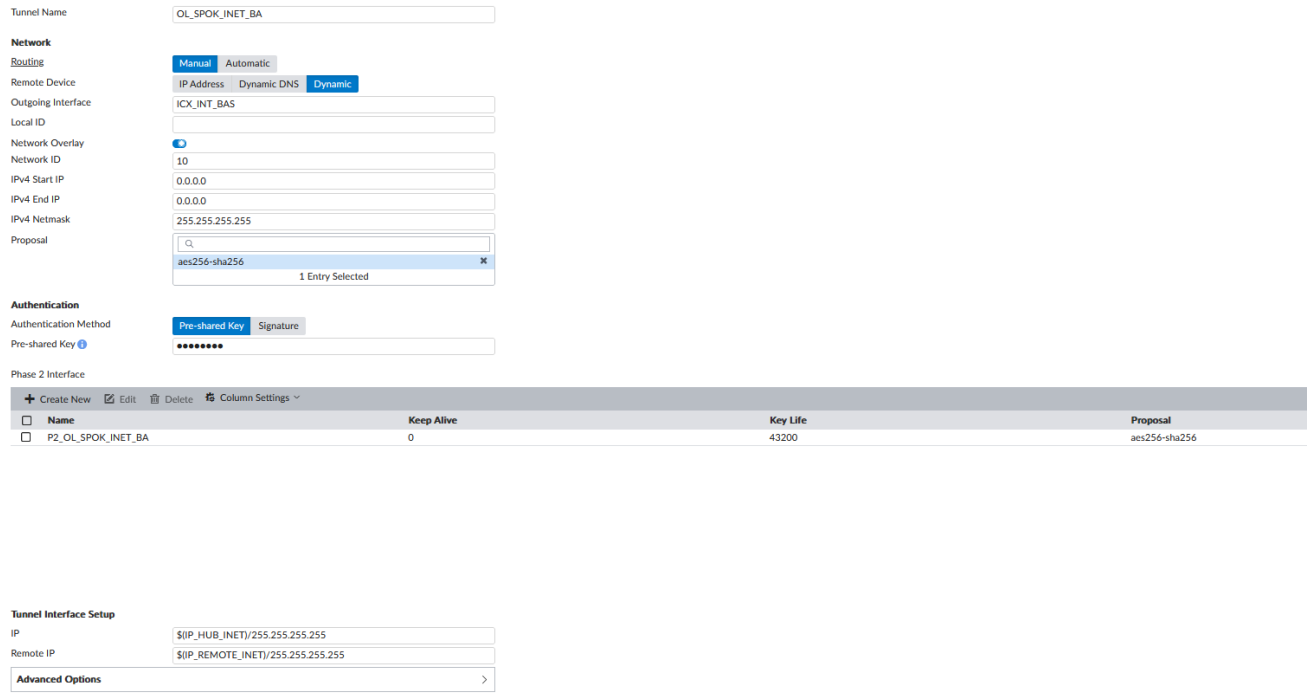


Figure 12 : Tunnel IPsec Internet vers les Spokes

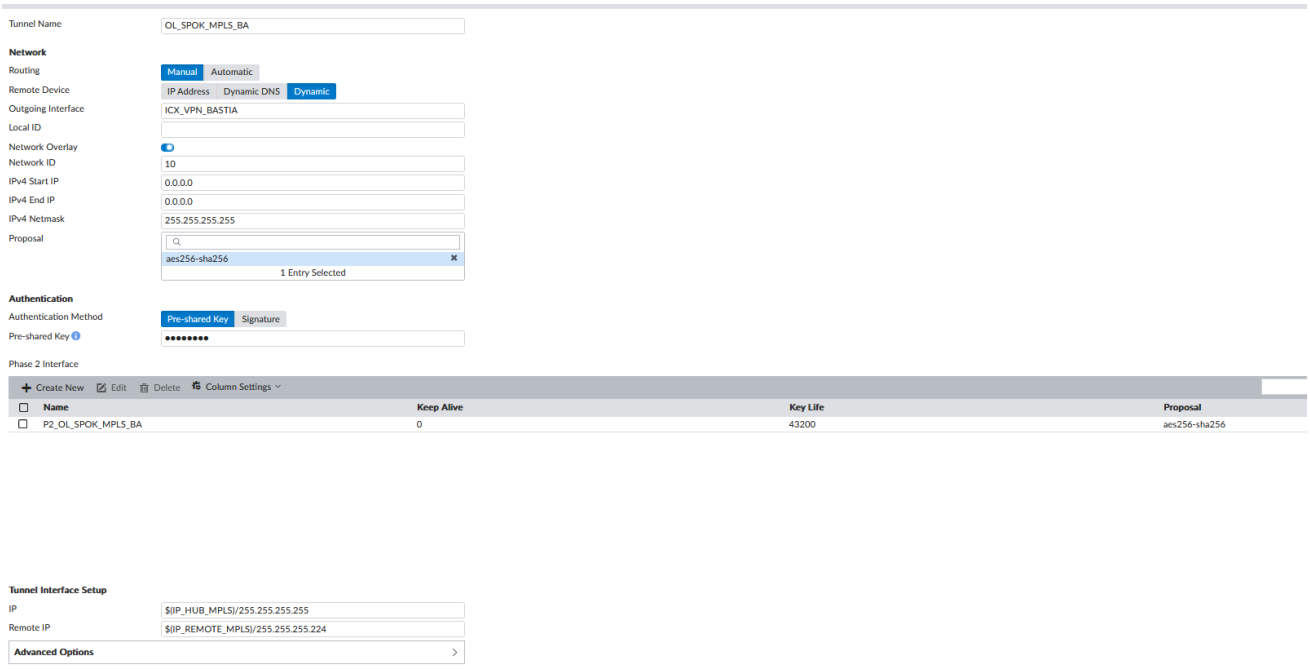


Figure 13 : Tunnel IPsec MPLS vers les Spokes

Les templates BGP :

Le protocole ayant été retenu pour ce projet est le protocole BGP, Border Gateway Protocol.

Des sessions iBGP sont maintenues dans la zone SD-WAN entre les Firewalls SaaS et les Firewalls des sites distants ainsi :

- Les sites distants apprennent les routes du Datacenter
- Le datacenter apprend les routes des sites distants
- Le datacenter renvoie les routes apprises par le biais du MPLS

Une session eBGP est active entre les Firewalls SaaS et les SRX550 jouant le rôle du CPE, Customer Premises Equipment ainsi :

- Les Firewalls SaaS distribuent les routes apprises du réseau SD-WAN au cœur du réseau Linker
- Le cœur du réseau Linker renvoie ses routes

Pour cela nous avons donc créé des templates spécifique aux hubs dans lesquels on retrouve :

- Le LOCAL AS, Autonomous System du HUB
- L'ID du HUB que nous avons variabilisés pour plus de simplicité
- Neighbors : Les voisins direct du HUB
- Neighbor Group : Les groupes de voisins passant par un même réseau
- Neighbor Ranges : Pour définir la taille du réseau correspondant aux différents Neighbor Group
- Les routes que nous redistribuons via les hubs sont les routes statiques.
- Nous avons également activé les routes reflectors, qui permet la redistribution des routes déjà apprises par un pair iBGP aux autres pairs de la même session iBGP.
- Nous avons aussi activé l'additional path sur le HUB de Bastia, car celui est un cluster composé de 2 FW, cette option nous permet donc de faire du load balancing et éviter de surcharger un lien et de laisser l'autre inutilisé.

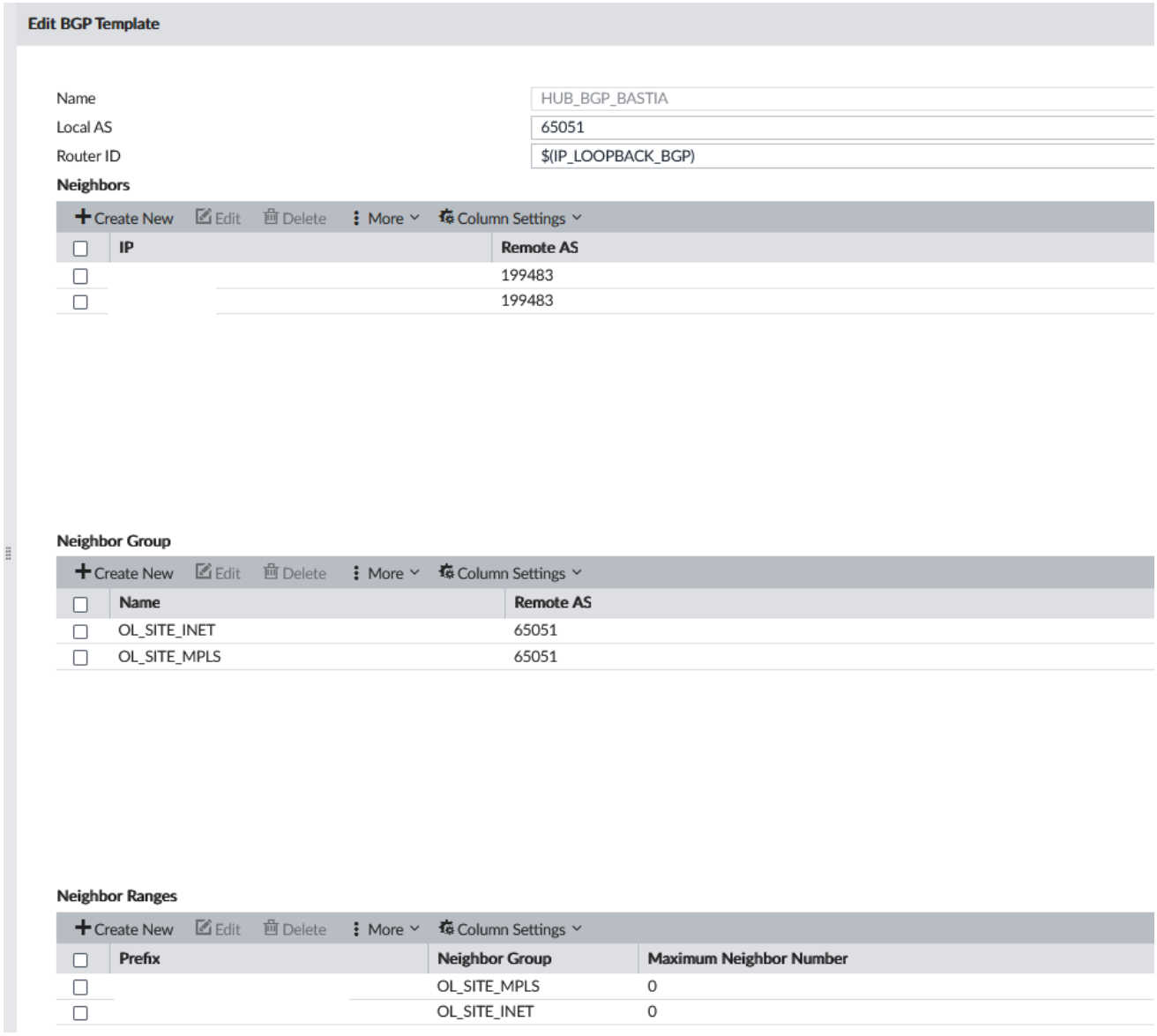


Figure 14 : Temple HUB BGP Bastia partie 1

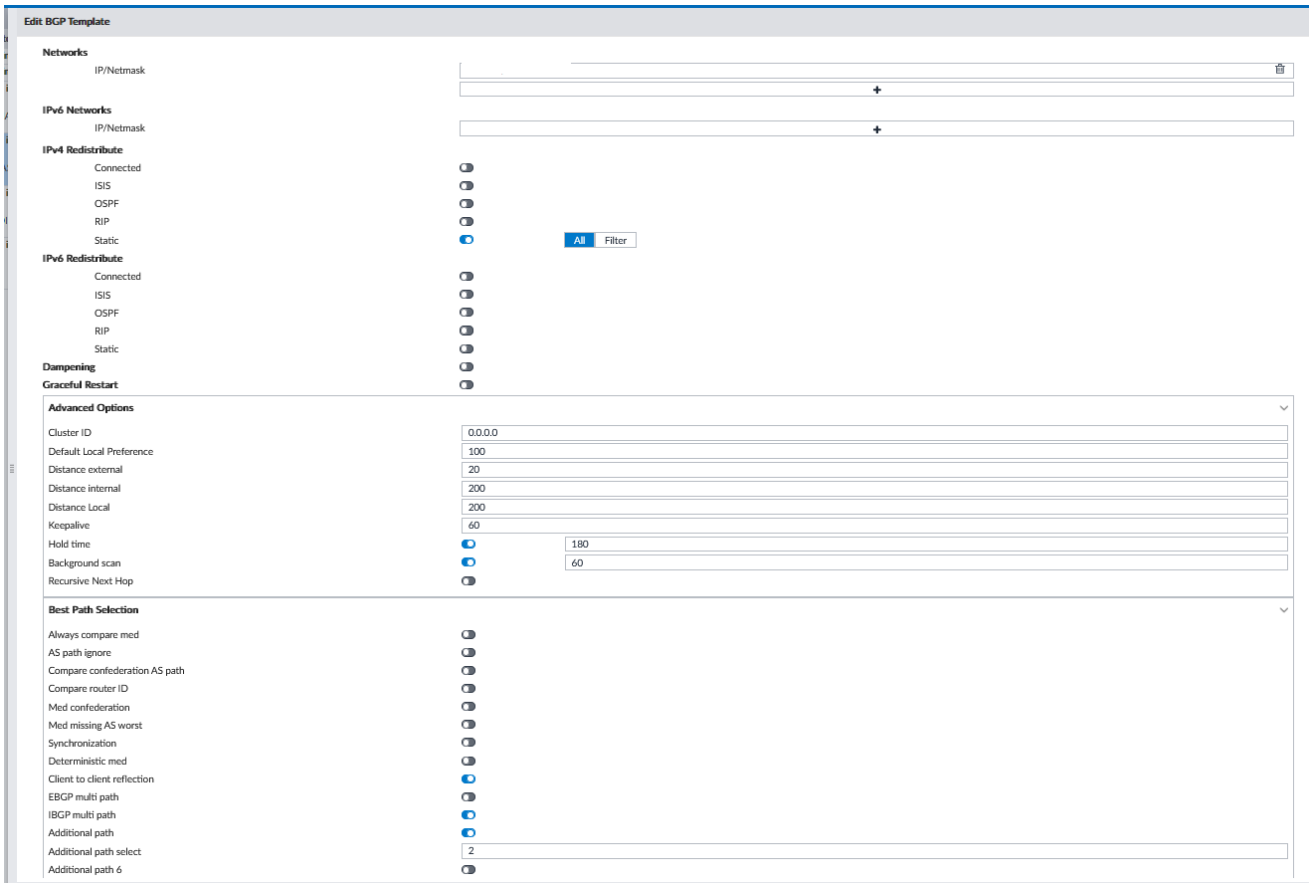


Figure 15 : Template HUB BGP Bastia partie 2

Les templates SD-WAN :

Pour que nous puissions définir quelles interfaces appartient à la zone SD-WAN nous avons dû crée un template qui nous a permis d'affecter les interfaces à une nouvelle zone SD-WAN que nous avons créé.

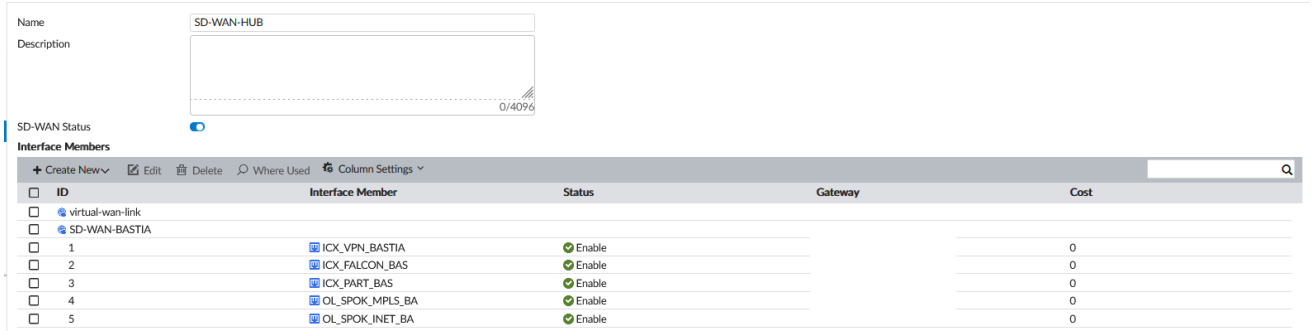


Figure 16 : Zone SD-WAN du HUB de Bastia

Les templates CLI :

Ce template que nous avons appliqué au HUB d'Ajaccio donc le PRA, est un template qui nous a permis de changer la métrique des routes BGP vers le HUB d'Ajaccio et ainsi lui appliquer une métrique plus élevée.

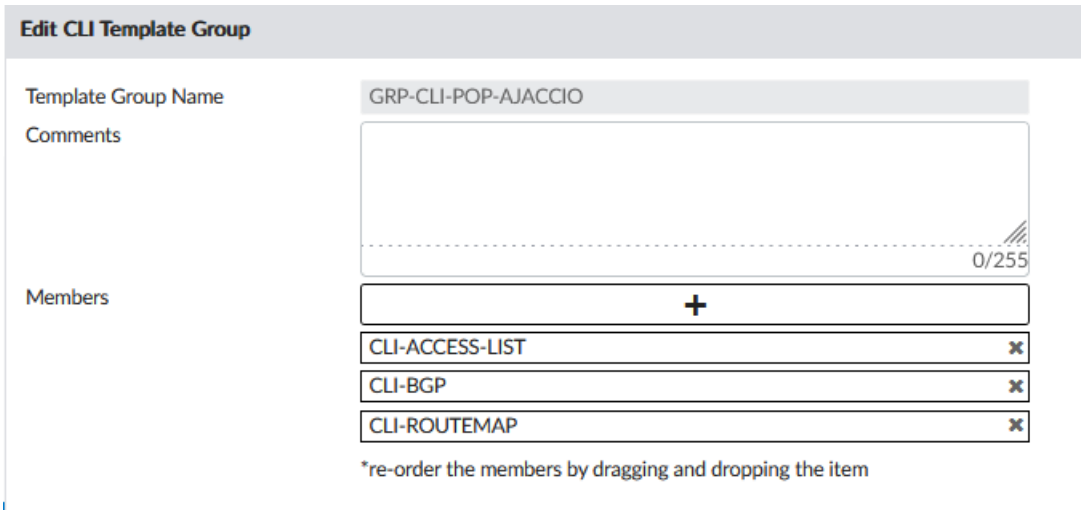


Figure 17 : Groupe template CLI métrique Ajaccio

Annexe 1.1

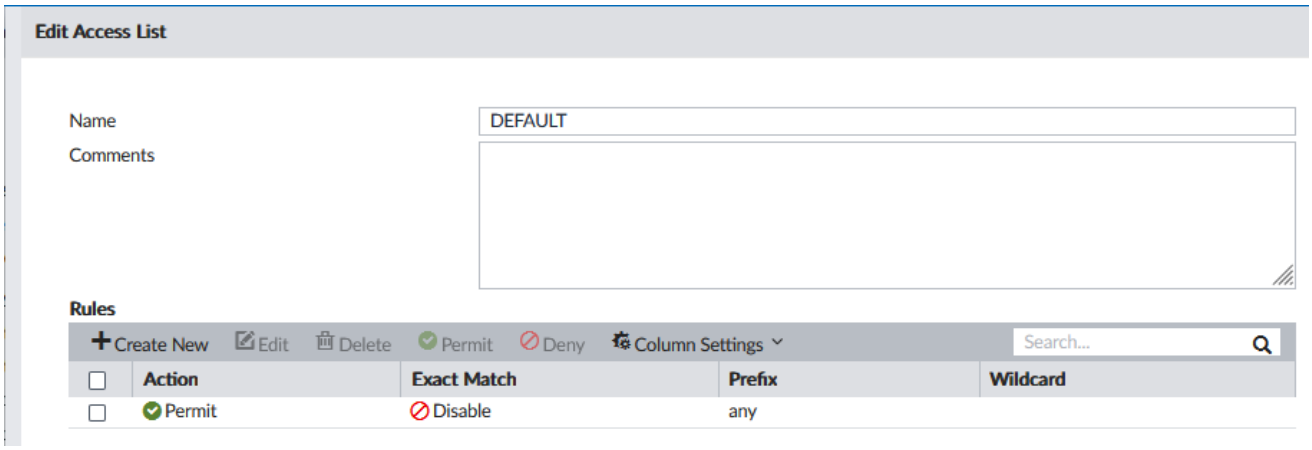


Figure 18 : ACL Default

Annexe 1.2

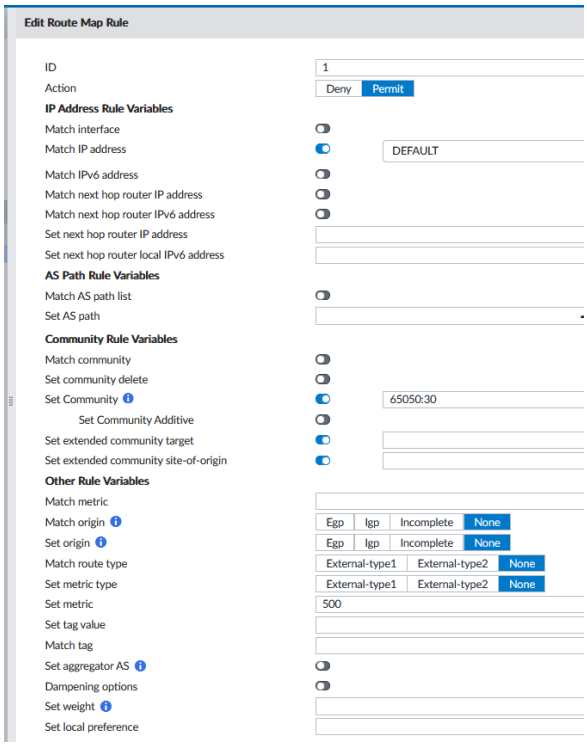


Figure 19 : Routemap

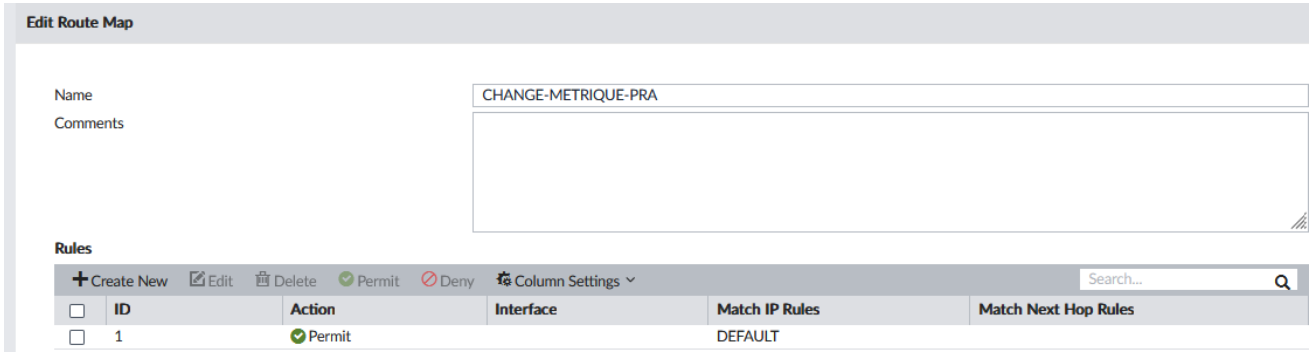


Figure 20 : Changement de la métrique pour le HUB de Ajaccio

Annexe 1.3

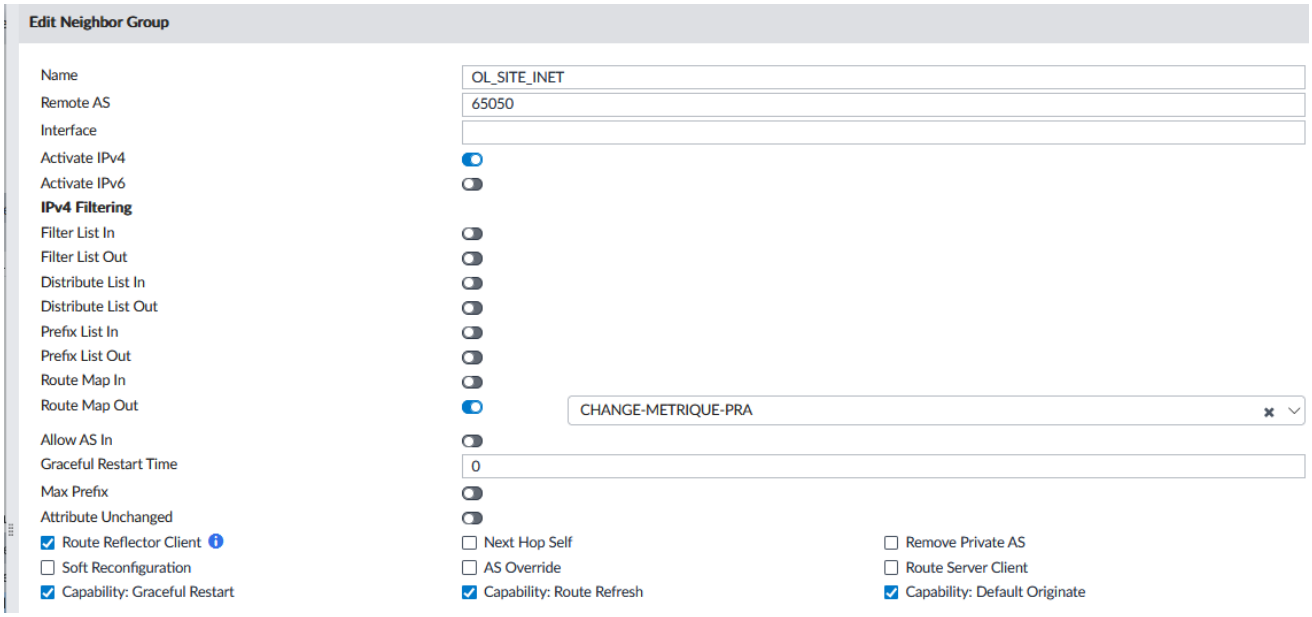


Figure 21 : BGP

Les templates systèmes :

Ce dernier template nous a permis de mettre le monitoring en place, en effet il sert à déclarer les agents SNMP, Simple Network Management Protocol et vers où les logs doivent être redirigés (ici le FAZ, FortiAnalyzer).

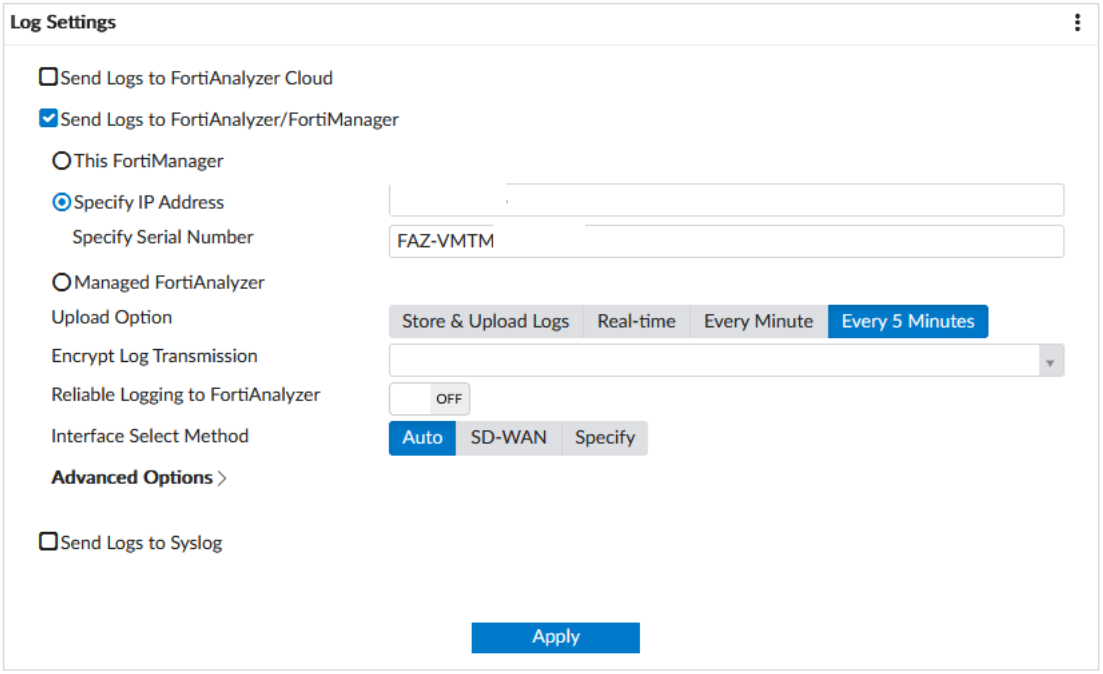


Figure 22 : FortiAnalyzer Des Hubs

3.5.5 Partie 4 : Configuration sites distants

La configuration des sites distants suit quasiment le même processus que les hubs.

Configuration interfaces

En effet pour les interfaces, les sites distants ne nécessitent pas la création du zone SD-WAN. Cependant il nous faut configurer les deux interfaces WAN pour les deux flux différents, SD-WAN et MPLS qui serviront à communiquer avec les autres sites distants et l'extérieur, ainsi que l'interface LAN qui servira à communiquer avec les réseaux internes du site.

#	Name	Type	Normalized Interface	Addressi	IP/Netmask	Access	Virtual Domain	Status	Adminis
Physical (9)									
1	wan1	Physical	wan1	Manual		HTTPS, PING, HTTP, FMG-Access	root	Up	Up
2	wan2	Physical	wan2	Manual		HTTPS, PING, HTTP, FMG-Access	root	Down	Up
3	internal2	Physical	internal2	Manual			root	Down	Up
4	internal3	Physical	internal3	Manual			root	Down	Up
5	internal4	Physical	internal4	Manual			root	Down	Up
6	internal5	Physical	internal5	Manual			root	Down	Up
7	internal6	Physical	internal6	Manual			root	Down	Up
8	a	Physical	a	Manual		HTTPS, PING, SSH, HTTP	root	Down	Up
9	b	Physical	b	Manual			root	Down	Up
Tunnel (7)									
10	naf.root	Tunnel	naf.root	Manual			root		Up
11	l2t.root	Tunnel	l2t.root	Manual			root		Up
12	ssl.root (SSL VPN interface	Tunnel	ssl.root	Manual			root		Up
13	OL_HUB_AJ_MPLS	Tunnel		Manual			root		Up
14	OL_HUB_BAS_MPLS	Tunnel		Manual			root		Up
15	OL_HUB_BAS_INET	Tunnel		Manual			root		Up
16	OL_HUB_AJ_INET	Tunnel		Manual			root		Up
Zone (2)									
17	Z_LAN	Zone					root		
18	internal1	Physical	internal1	Manual		PING	root	Up	Up
SD-WAN Zone (1)									
19	virtual-wan-link	SD-WAN Zone							

Figure 23 : Interfaces des sites distants

Configuration templates

<u>Les templates IPsec :</u>

Pour les tunnels IPsec des spokes vers le HUB nous avons par soucis de simplicité préféré crée 4 tunnels, 2 vers le hub de Bastia (MPLS et SD-WAN) et 2 vers le hub d'Ajaccio (MPLS et SD-WAN).
Les 4 tunnels ont la même configuration globale.

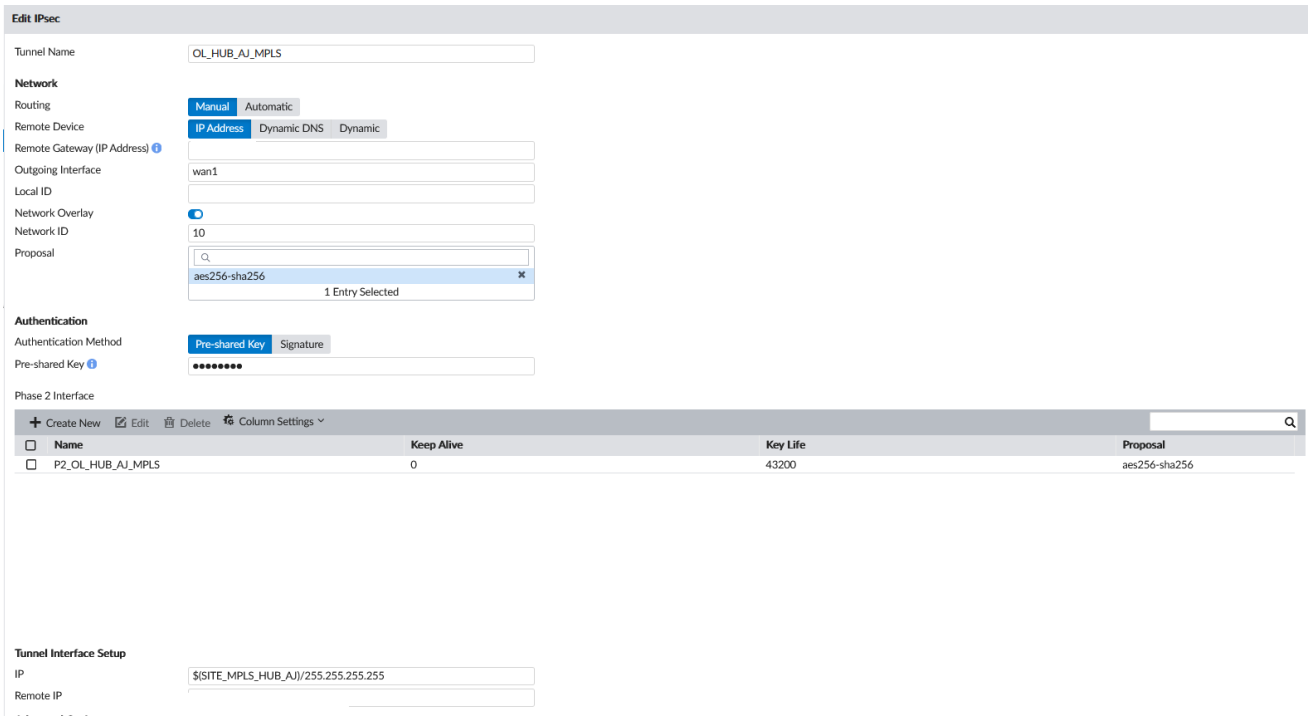


Figure 24 : Tunnel IPsec vers les HUBs

Les templates BGP :

Le template BGP des sites distants varie un peu de celui du HUB, en effet les sites distants n'ont que des voisins directs.

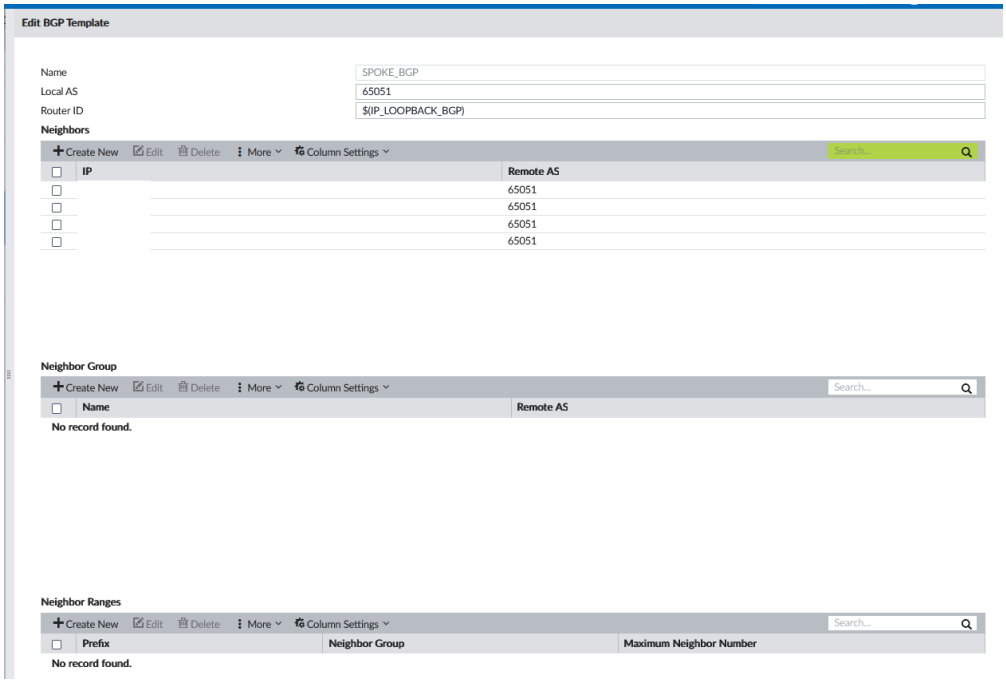


Figure 25 : Template BGP des Spokes partie 1

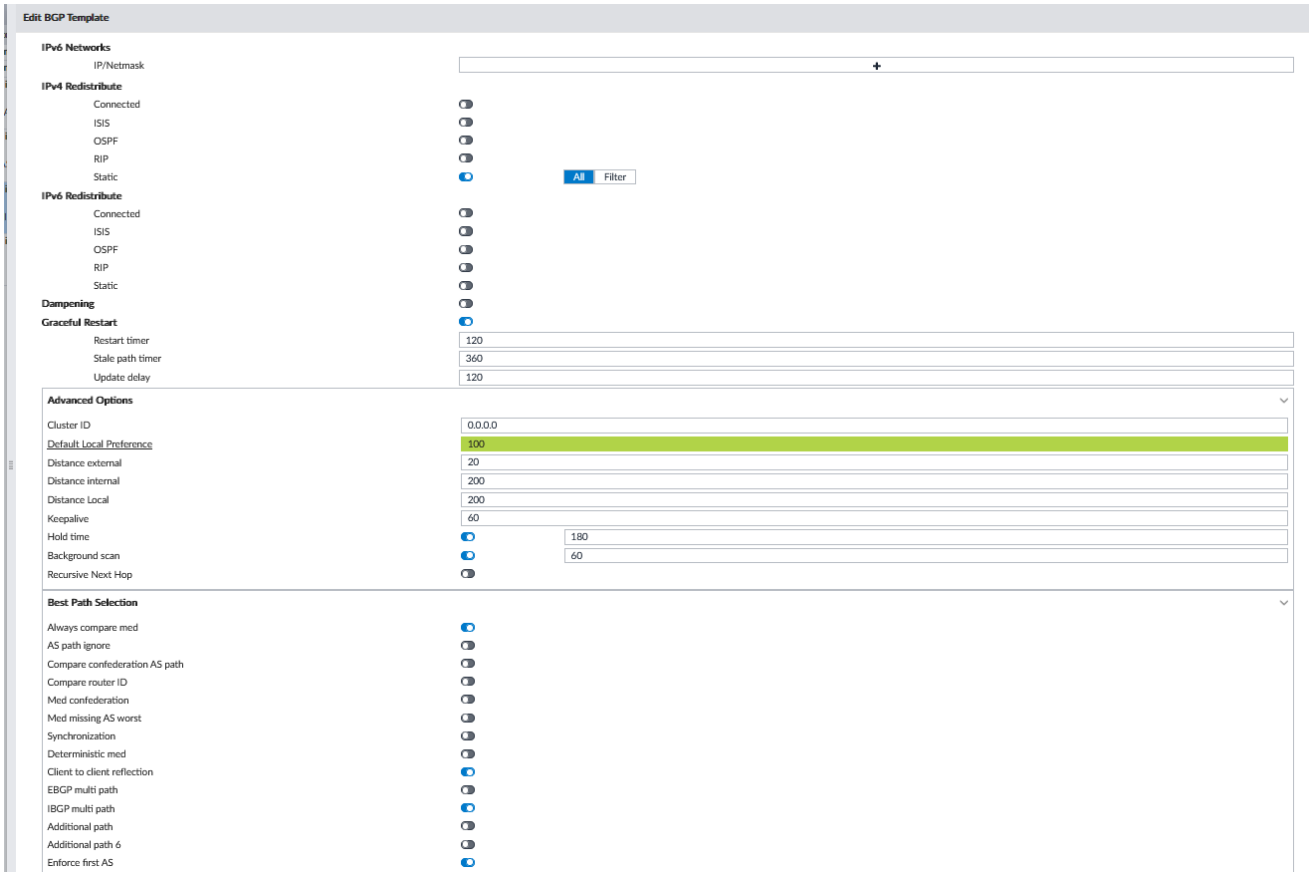


Figure 26 : Template BGP des Spokes partie 2

Les templates CLI :

Les templates CLI des sites distants ici sont totalement différents de ceux des HUBS, en effet les sites distants ne nécessitent pas de changement de métrique, cependant on doit leur appliquer les Shaping Profiles configuré précédemment et une bande passante, ainsi qu'ajouter quelques informations pour les agents SNMP.

Annexes 2 et 3

Les templates systèmes :

Ce dernier template nous a permis de mettre le monitoring en place, en effet il sert à déclarer les agents SNMP et vers où les logs doivent être redirigés (ici le FAZ).

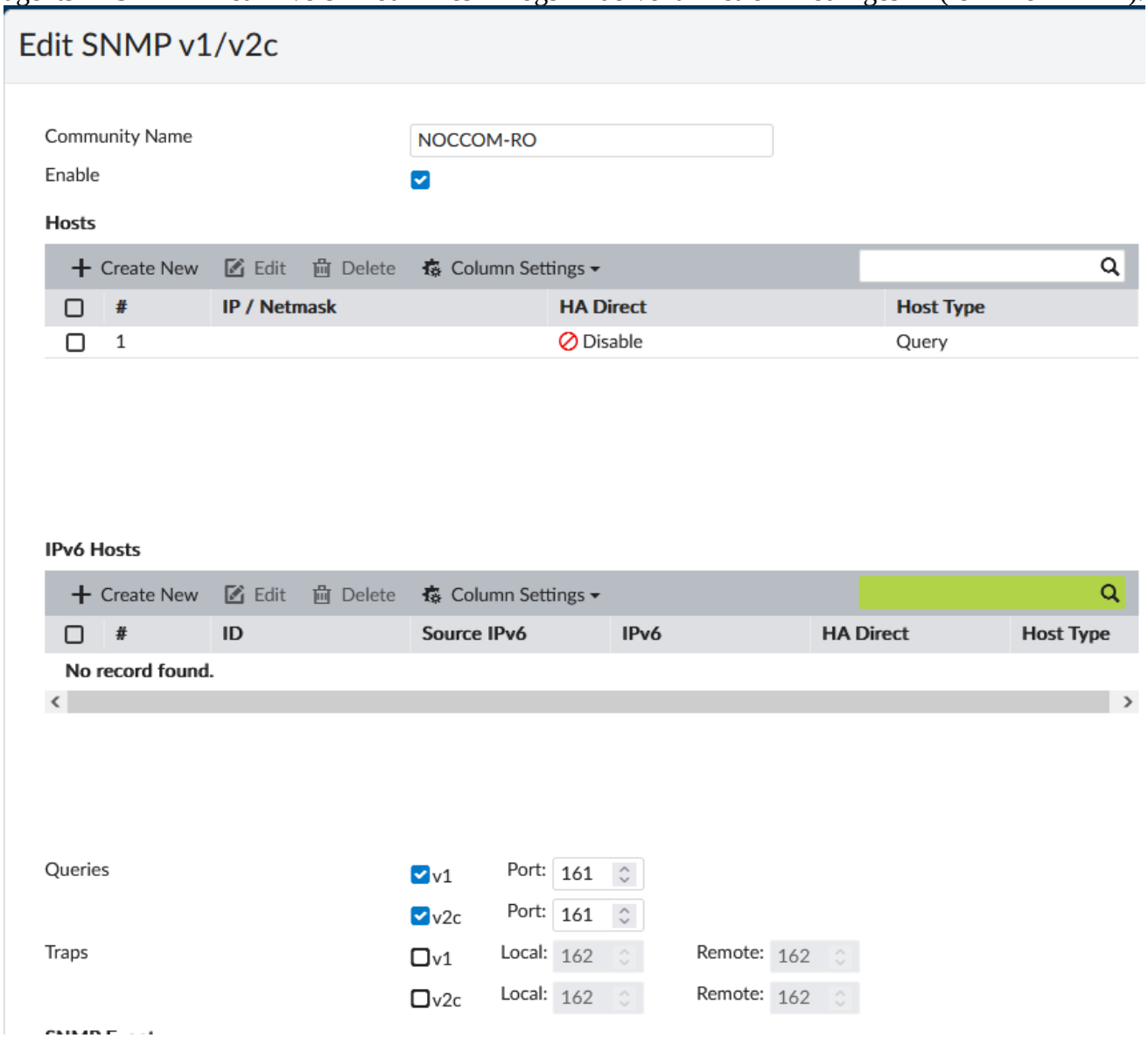


Figure 27 : Paramètres agents SNMP

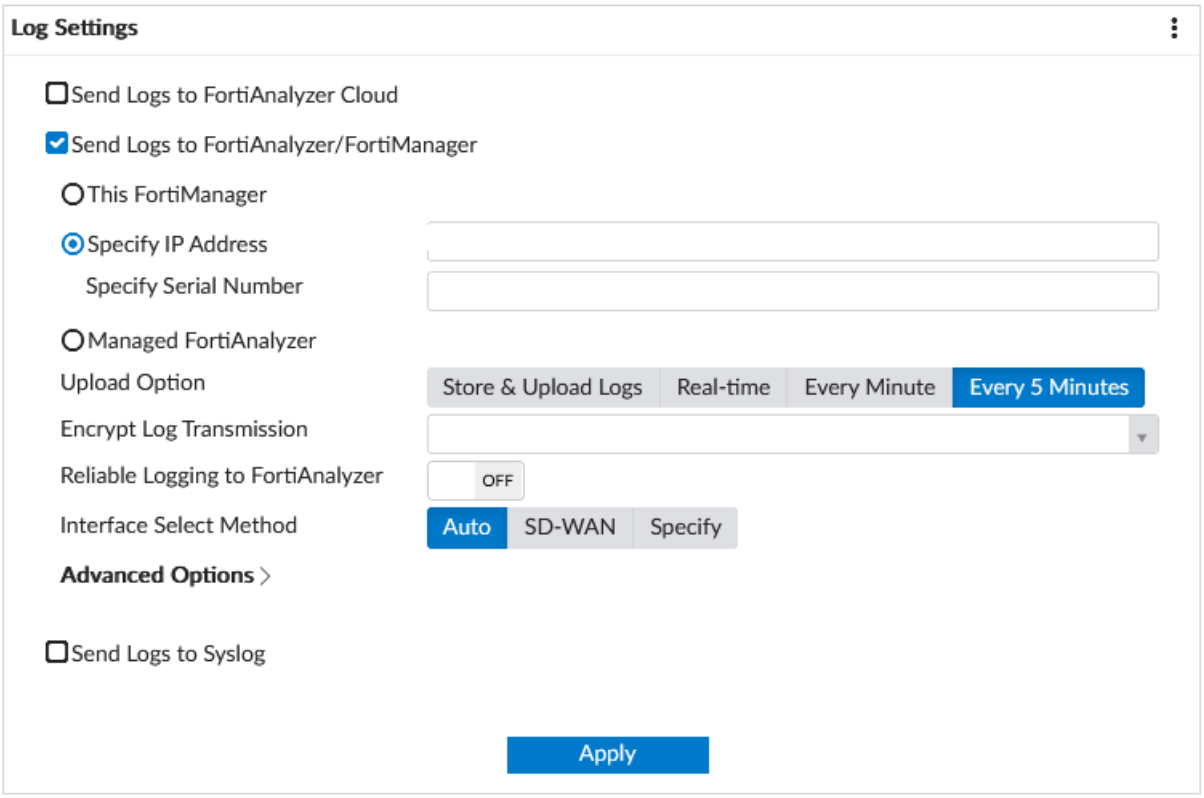


Figure 28 : Redirection FortiAnalyzer

3.5.6 Partie 5 : Configuration des switches

Je me suis aussi occupé d'une partie de la configuration des EX3400 qui font l'interconnexion entre les SRX550 et le Firewall SaaS. L'une des particularités du matériel Juniper est que le fichier de configuration est au format json, ce qui le rend donc plus simple de lecture et d'écriture qu'un hardware Cisco par exemple.

J'ai donc dû configurer les différents VLANs existant ainsi que les interfaces nécessaires.
Pour cela j'ai tout d'abord créé les VLANs désiré, puis j'ai configuré les interfaces en mode trunk et je leur ai ajouté les VLANs auxquelles elles étaient membres

3.5.7 Partie 6 : Configuration des SRX

La dernière chose dont j'ai pu m'occuper lors de ce projet est la configuration des SRX550. Ces équipements aussi sont des équipements Juniper et présente donc les mêmes particularités au niveau du fichier de configuration que les EX3400.

Les SRX sont des pares-feux mais peuvent aussi faire du routage et du commutage, dans ce projet nous nous en servons comme routeur.

La première action entrepris sur les SRX a donc été de supprimer toute la section security de la configuration et de ne laisser que ce bloc :

```
security {
    forwarding-options {
        family {
            mpls {
                mode packet-based;
            }
        }
    }
}
```

Figure 29 : Configuration sécurité SRX

Ce qui permet donc au SRX de ne plus se considérer comme un pare-feu mais un routeur, une fois ceci fait j'ai donc pu configurer les interfaces comme nous en avions besoin.

J'ai donc d'abord mis en place une description générale de l'interface physique sur laquelle j'ai pu ensuite configurer une ou plusieurs interfaces logiques selon les besoins. J'ai aussi activé le « flexible-vlan-tagging » pour pouvoir configurer de multiples vlans sur la même interface physique.

Annexe 4.1

Sur chaque interface logique j'ai configuré une description de l'interface logique, une bande passante, un vlan-id et une adresse IP.

Après avoir configuré les interfaces j'ai dû configurer des filtres d'export et d'import de routes pour pouvoir diffuser les réseaux voulus.
Pour cela je crée différents policy-statement dans lesquels je crée les multiples terms nécessaire où j'ajoute les route-filter désiré ainsi que comment les traiter.

Annexe 4.2

Enfin je crée des routing-instances, qui me servent à appliquer différents protocoles de routage ainsi que les différents filtre d'import/export sur les interfaces désirées.

Ici pour la routing instance VPN_GCSCORSE_BASTIA pour le protocole BGP je crée deux groupes que je nomme LINKER et SD-WAN, ces deux groupes sont configurés différemment, en effet le group Linker fera de l'iBGP et le groupe SD-WAN fera de l'eBGP, on y ajoute la configuration d'un import ou d'un export de filtre (si nécessaire), un peer-as (si nécessaire aussi) et les neighbors.

Annexe 4.3

Une fois ces deux groupes configurés on ajoute les interfaces auxquelles cette routing-instance s'appliquera et les options de la routing-instance qui sont le router-id et l'AS du matériel.

4 Missions secondaires et sujets abordés

4.1 Choses vues

Lors de ce stage j'ai aussi eu l'occasion de voir l'architecture d'un centre de contact, les différentes stratégies de routage mise en place pour ce genre d'architecture, les fiches d'exploitations mise en place pour rapidement identifier le problème et le résoudre. Ici j'ai pu voir le centre de contact du SAMU 06 avec l'architecte Johnny BARON.

J'ai aussi assisté à la configuration de système de visio-conférence pour le client ADNOV avec les Experts Projets André GRANIER et Thomas GUERIN.

Enfin j'ai pu configurer un tunnel VPN IPsec pour la commune de St-Tropez. En effet la commune de St-Tropez ayant un besoin de supervision de leur réseau j'ai eu l'occasion de monter un tunnel VPN IPsec entre la mairie de St-Tropez et le NOC, Network Operation Center de NXO, en collaboration avec Phone CHANTHAVONG.

5 Conclusion

Ce stage de dix semaines au sein de l'entreprise NXO France m'aura été grandement bénéfique principalement sur le côté technique, bien que aussi sur le plan humain.

J'ai ainsi pu découvrir le métier d'intégrateur réseau, ainsi que l'impact que peut avoir les différents aspects de ce métier sur les clients que ce soit lors d'intégration ou de migration de réseaux. Cela m'aura aussi permis de développer ma capacité à communiquer avec les équipes techniques et les clients.

Les nombreux partenariats de NXO m'auront permis de découvrir des constructeurs tel que Fortinet et Juniper. Le projet auquel j'ai participé m'a fait découvrir la technologie SD-WAN ainsi que toutes les notions de sécurité et de routage nécessaire au bon fonctionnement de ce type de réseau. J'ai aussi pu apprendre à faire et tenir une documentation à jour au fur et à mesure de l'avancement d'un projet.

En conclusion, ce stage m'a permis de renforcer mon intérêt pour le domaine de l'intégration réseau et d'enrichir mes connaissances.

6 Remerciements

Tout d'abord je souhaite remercier Vincent MOGINOT, mon tuteur, pour m'avoir accordé de son temps, pour l'intérêt qu'il a porté à mon travail et pour la chance qu'il m'a offerte au sein de l'entreprise NXO France.

Je remercie chaleureusement Aubin CHAPUZET qui m'aura guidé et appris énormément tout au long de ce projet SD-WAN.

Je remercie Sid-Ahmed BAININE et Remy BOISSEZON pour m'avoir assisté pendant l'entièreté du projet SD-WAN.

Je remercie Éric MICHEL pour la confiance qu'il m'a accordé en me laissant monter le tunnel VPN pour la commune de St-Tropez.

Plus globalement, je remercie la société NXO France pour m'avoir permis de découvrir leur entreprise, le domaine de l'intégration réseau.
Particulièrement, je remercie l'ensemble des membres de l'agence de Marseille qui m'ont accueilli, intégré et apporté leur aide tout au long de mon stage.

Pour finir, je remercie Éric WÜRBEL, mon responsable académique, pour le temps qu'il m'a accordé pour le bon déroulement de cette période.

7 Glossaire

BUT, Bachelor Universitaire de Technologie

SD-WAN, est une architecture WAN virtuelle qui permet aux entreprises de connecter les utilisateurs aux applications de façon sécurisée avec n'importe quelle combinaison de services de transport (notamment les services MPLS, LTE et Internet haut débit).

MPLS, est un protocole conçu pour optimiser et accélérer le trafic réseau.

VPN, est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux publics.

Template, un modèle généralisé pouvant être transposé sur plusieurs appareils.

Trafic Shaping, est le contrôle du volume des échanges dans un réseau informatique pour optimiser et garantir les performances.

Metafields, sont des champs où l'on peut stocker des informations à réutiliser plus tard, comme une variable.

PRA, permet à une entreprise de prévoir les démarches à entreprendre pour reconstruire et remettre en route un système informatique en cas de sinistre important.

8 Bibliographie

Sites Web:

JUNIPER: https://www.juniper.net/

FORTINET: https://www.fortinet.com/fr