

Mise en place de firewalls virtuels sur une Appliance

FORTINET®
adapté au module 146

Mai 2023

Damien Mayor
SI-CA2a
Route de Forchy 3
1146 Mollens
damien.mayor@pm.me

1 Table des matières

1.1	Introduction.....	5
1.2	Objectifs.....	5
1.3	Cahier des charges.....	5
1.4	Module 146	5
1.5	Planification initiale	6
2	Analyse / Conception	7
2.1	Méthode de travail.....	7
2.2	Organisation du travail.....	8
2.3	Informations générales	9
2.3.1	Définitions	9
2.3.2	Fortinet	9
2.3.3	Réseau CPNV	10
2.4	Concept	11
2.4.1	Déroulement du projet.....	11
2.5	Dossier de conception	11
2.5.1	Liste du matériel utilisé :	11
2.5.2	Schéma :	12
2.5.3	Internet.....	12
2.5.4	Adressage IP	12
2.5.5	Table de routage.....	13
2.6	Stratégie de test	13
2.7	Liste des tests	14
2.8	Risques techniques.....	15
2.8.1	Connaissances limitées en VPN	15
2.8.2	Connaissances limitées en pare-feu.....	15
2.8.3	Complexités liées au réseau de l'école et à ses contraintes	15
2.8.4	Connaissances non-acquises pendant le pré-TPI	15
2.9	Planification finale	16
3	Réalisation	18
3.1	Dossier de réalisation	18
3.1.1	1 ^{ère} phase.....	18
3.1.2	2 ^{ème} phase.....	32
3.2	Preuves des tests effectués.....	33
3.3	Erreurs restantes	33
3.4	Nombre maximal d'implémentations	33

3.4.1	VDOM	33
3.4.2	VPN	34
3.4.3	Limitation physique	34
3.5	Liste des documents fournis.....	35
4	Conclusions.....	35
4.1	Objectifs atteints / non-atteints	35
4.2	Points positifs / négatifs	35
4.2.1	Négatif	35
4.2.2	Positif	35
4.3	Difficultés particulières.....	35
4.4	Améliorations	36
4.5	Retour personnel.....	36
5	Remerciements	37
6	Table des illustrations.....	38
7	Annexes	39
7.1	Résumé du rapport de TPI.....	39
7.2	Cahier des charges.....	40
7.3	Identification du module 146	44
7.4	Preuves des tests	46
7.5	Sources	55
7.6	Glossaire	56
7.7	Journal de travail	57
7.8	Archives du projet	59

Analyse préliminaire

1.1 Introduction

Ce TPI est un dérivé de la fiche signalétique qui avait été soumise en décembre 2022 au doyen en fonction à cette date, Mr. Claude Egger, qui avait pour titre : *"Assurer la sécurité d'un réseau informatique"* et pour description générale : *"Assurer la cybersécurité d'une entreprise à l'aide d'une approche sous 3 angles ; matériel (Firewall, IDS, UTM), outils (proxy, vpn) et politique (droits de partage, ntfs, politique mot de passe, subnetting)."*

Page | 5

À la suite d'une discussion avec Mr. Varela, mon chef de projet, il s'est avéré que ce projet aurait été trop théorique et par conséquent pas adapté à un travail de TPI. Cependant il m'a été proposé par Mr. Varela d'effectuer un travail dans la lignée de ma fiche signalétique, me permettant de faire mes premières expériences avec un pare-feu physique tout en mettant en pratique une partie des connaissances acquises pendant ma formation FPA, notamment concernant la partie réseau informatique. Mon travail de pré-TPI avait pour titre : *"Mise en service d'un pare-feu Fortinet"*.

1.2 Objectifs

Tiré du cahier des charges :

"Le module 146 abordant les grands réseaux d'entreprise avec des VPN site à site et clients, et du NAT, ce projet cherche à évaluer les possibilités d'implémenter le schéma ci-dessous à l'aide d'un seul firewall Fortinet, en exploitant les capacités de virtualisation de FortiGate."

Pour résumer, ce TPI va consister en la mise en place de :

- Réseau "Siège principal"
- Réseau "Succursale secondaire"
- Stations "Télétravailleur"
- Pare-feu, VDOMs, règles de pare-feu et table de routage
- Mise en place d'une partie "internet"
- Tunnels site à site
- FortiClient VPN

1.3 Cahier des charges

Le cahier des charges est disponible à l'annexe 7.2

1.4 Module 146

Le module 146 cité au point 1.2 de ce document se réfère au module IC-T 146 intitulé : *"Relier une entreprise à Internet"*. La fiche d'identification du module est disponible à l'annexe 7.3

1.5 Planification initiale

Projet

Mise en place de firewalls virtuels sur une Appliance Fortinet, adaptée au module 146

Planification

Mise en place de firewalls virtuels sur une Appliance Fortinet, adaptée au module 146			Planning											
Total			02.05.23	08.05.23	15.05.23	22.05.23	29.05.23	05.06.23	12.06.23					
Prévu		90 h 05	18 h 20	23 h 55	16 h 45	23 h 55	7 h 10							
Mayor														
			SEM	18	19	20	21	22	23	24				
1 Analyse											18 h 00			
	1.1 Planification	Prévu	4 h 00								4 h 00			
		Mayor												
	1.2 Recherches	Prévu	4 h 00	2 h 00	1 h 00	1 h 00					8 h 00			
		Mayor												
	1.3 Elaboration des stratégies de test	Prévu	2 h 00								2 h 00			
		Mayor												
	1.4 Adressage IP	Prévu	2 h 00								2 h 00			
		Mayor												
	1.5 Règles de pare-feu	Prévu	2 h 00								2 h 00			
		Mayor												
2 Implémentation 1er temps											15 h 00			
	2.1 Création réseau siège principal	Prévu		2 h 00							2 h 00			
		Mayor												
	2.2 Création VMs siège principal (serveur, client * 2)	Prévu		1 h 00							1 h 00			
		Mayor												
	2.3 Création serveur VPN siège principal	Prévu		2 h 00							2 h 00			
		Mayor												
	2.4 Implémentation pare-feu siège principal	Prévu		2 h 00							2 h 00			
		Mayor												
	2.5 Création réseau succursalee 2	Prévu		1 h 00							1 h 00			
		Mayor												
	2.6 Création VMs succursalee 2	Prévu		1 h 00							1 h 00			
	Mayor													
	2.7 Création client VPN succursalee 2	Prévu		2 h 00							2 h 00			
		Mayor												
	2.8 Implémentation pare-feu succursalee 2	Prévu		1 h 00							1 h 00			
		Mayor												
	2.9 Création réseau télétravailleur	Prévu		1 h 00							1 h 00			
		Mayor												
	2.10 Création VM télétravailleur	Prévu		1 h 00							1 h 00			
		Mayor												
	2.11 Création client VPN télétravailleur	Prévu		1 h 00							1 h 00			
		Mayor												
	3 Implémentation 2ème temps											22 h 00		
	3.1 Implémentation/adaptation serveur VPN siège	Prévu			4 h 00						4 h 00			
		Mayor												
	3.2 Implémentation/adaptation client VPN succursale 2	Prévu			2 h 00						2 h 00			
		Mayor												
	3.3 Implémentation/adaptation client VPN télétravailleur	Prévu			2 h 00						2 h 00			
		Mayor												
	3.4 Implémentation physique du pare-feu	Prévu			2 h 00						2 h 00			
		Mayor												
	3.5 Implémentation/adaptation règles pare-feu siège	Prévu			2 h 00	2 h 00					4 h 00			
		Mayor												
	3.6 Implémentation/adaptation règles pare-feu	Prévu				4 h 00					4 h 00			
		Mayor												
	3.7 Implémentation/adaptation règles pare-feu	Prévu				4 h 00					4 h 00			
	Mayor													
4 Tests											18 h 50			
	4.1 Tests réseau siège principal	Prévu		0 h 30							0 h 30			
		Mayor												
	4.2 Tests système siège principal	Prévu		0 h 30							0 h 30			
		Mayor												
	4.3 Tests réseau succursale 2	Prévu		0 h 30							0 h 30			
		Mayor												
	4.4 Tests système succursale 2	Prévu		0 h 30							0 h 30			
		Mayor												
	4.5 Tests VPN site-to-site	Prévu		0 h 30							0 h 30			
		Mayor												
	4.6 Tests pare-feu site-to-site	Prévu		0 h 30							0 h 30			
		Mayor												
	4.7 Tests système télétravailleur	Prévu		0 h 30							0 h 30			
		Mayor												
	4.8 Tests VPN client-to-site	Prévu		0 h 30							0 h 30			
		Mayor												
	4.9 Tests pare-feu client-to-site	Prévu			0 h 30						0 h 30			
		Mayor												
	4.10 Tests VPN site-to-site 2ème temps	Prévu				2 h 00					2 h 00			
		Mayor												
	4.11 Tests VPN client-to-site 2ème temps	Prévu				2 h 00					2 h 00			
		Mayor												
	4.12 Tests pare-feu site-to-site	Prévu				2 h 00					2 h 00			
		Mayor												
	4.13 Tests pare-feu client-to-site	Prévu				2 h 00					2 h 00			
		Mayor												
	4.14 Tests généraux	Prévu	1 h 35	0 h 10	0 h 30	2 h 10	1 h 55				6 h 20			
		Mayor												
5 Documentation											13 h 30			
	5.1 Documentation	Prévu	2 h 00	2 h 00	2 h 00	2 h 00	4 h 30				10 h 30			
		Mayor												
	5.2 Journal de travail	Prévu	0 h 45	0 h 45	0 h 45	0 h 45	0 h 45				3 h 00			
		Mayor												
	5.3 Préparation présentation	Prévu												
		Mayor												
	5.4 Maladie	Prévu												
		Mayor												
	5.5 Absence	Prévu												
		Mayor												
	5.6 Temps flexible	Prévu												

Figure 1 planification initiale

Cette planification initiale a été effectuée le 2 mai 2023, jour du début de ce TPI, avec un délai de rendu au 2 mai 2023 ; 16 :55. Je me suis basé sur mon vécu du déroulement du module 146, qui s'est déroulé du 14 novembre 2022 au 27 janvier 2023.

Ce module s'est déroulé en salle de classe de manière virtuelle, à l'aide de VMware Workstation Pro et de GNS3 à l'exception de l'examen qui s'est lui déroulé en salle C111 sur du matériel physique.

Page | 7

Mon premier réflexe, lors de l'élaboration de ma planification initiale, a été de recopier la méthodologie employée lors du cours, à savoir la virtualisation. Après réflexion dans les heures qui ont suivi le rendu, j'ai pris la décision de changer mon approche et d'utiliser une approche physique plutôt que virtuelle. Le sujet a été abordé avec Mr. Varela, le 3 mai 2023.

Comme vous pouvez vous en douter, ce changement à un impact significatif à ma planification initiale notamment sur la partie : "2 Implémentation 1^{er} temps". Pour des raisons de temps et de respect d'esprit d'une planification initiale, j'ai pris la décision de ne pas la modifier. (ladite planification).

2 Analyse / Conception

2.1 Méthode de travail

Pendant la formation nous avons pu découvrir à travers le module I-CT 431 intitulé "Exécuter des mandats de manière autonome dans un environnement informatique" le framework Scrum, méthode dite agile.

Selon moi cette méthodologie est excellente pour les développeurs qui travaillent en équipe et qui ont un besoin de partage accru par l'interdépendance inhérent au développement informatique mais se prête moins à un projet mené par une unique personne, d'autant plus dans le domaine du réseau informatique, plus linéaire.

C'est pour cette raison que j'ai choisi la méthodologie "Waterfall" (ou cascade) qui me semble plus appropriée. D'ailleurs, le document de base utilisé pour cette documentation, téléchargée du site www.tpivd.ch, est bâtie sur ce modèle en cascade.

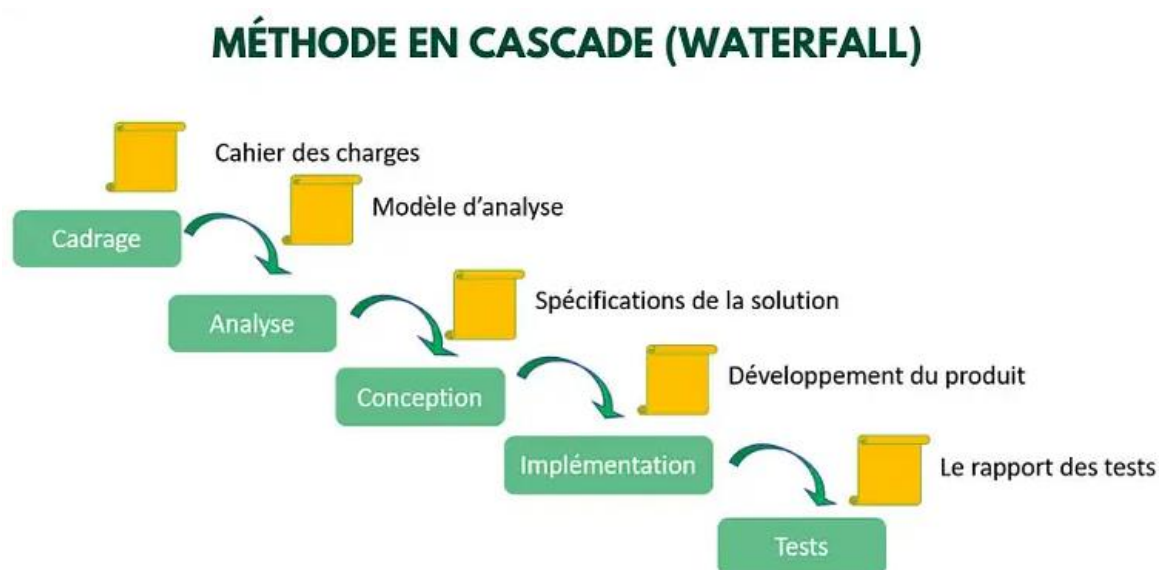


Figure 2 méthode en cascade.

Les avantages de cette méthode sont qu'elle est simple, facile à mettre en place, logique et structurée. Son inconvénient principal et son manque de flexibilité dû à son déroulement séquentiel.

2.2 Organisation du travail

Afin de respecter le point "2 PROCÉDURE" du cahier des charges : *"Le candidat est entièrement responsable de la sécurité de ses données."*, j'ai choisi l'approche de sauvegarde 3-2-1 à savoir : **3** copies d'un même fichier sur **2** supports différents dont au moins **1** sauvegarde hors-site.

Page | 8

J'ai donc 1 copie de mes données TPI sur mon PC05 du CPNV, une copie sur un SSD externe amovible ainsi qu'une copie sur mon NAS personnel localisé à mon domicile accessible à l'adresse :

<http://damienmayorpmme.quickconnect.to>

En ce qui concerne l'organisation de mes données, voici la nomenclature choisie :

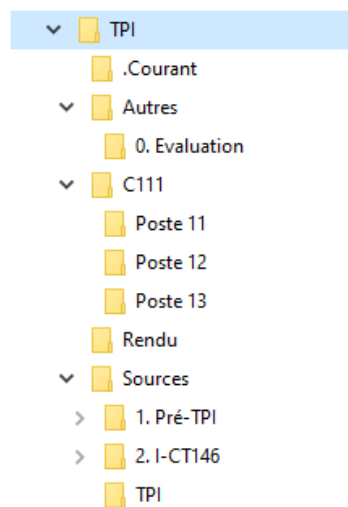


Figure 3 organisation des fichiers

2.3 Informations générales

2.3.1 Définitions

pare-feu

nom masculin invariable

1. Synonyme de [pare-étincelles](#).

SYNONYME :

[pare-étincelles](#)

2. Écran ajouré, adaptable au casque de sapeur-pompier, pour protéger le visage contre la chaleur et les flammes de l'incendie.

SYNONYME :

[garde-feu](#)

3. Zone aménagée le long d'une voie ferrée traversant une forêt pour éviter les risques d'incendie.

4. Synonyme de [coupe-feu](#).

SYNONYME :

[coupe-feu](#)

Informatique

5. Équipement situé entre le réseau Internet et le réseau privé d'une entreprise pour accroître la sécurité de ce dernier en filtrant le trafic en provenance ou à destination d'Internet (calque de l'anglais *fire-wall*).

Figure 4 définition pare-feu

VPN

nom masculin

(sigle de l'anglais *virtual private network*, réseau privé virtuel)

Informatique

Réseau privé qui assure l'anonymat, la confidentialité et la sécurité des informations échangées en ligne, par leur circulation chiffrée à l'intérieur d'un réseau public (Internet, notamment). (Le VPN est utilisé en particulier pour le télétravail.)

Figure 5 définition VPN

2.3.2 Fortinet

Fortinet, Inc. est une entreprise américaine fondée en 2000, basée à Sunnyvale en Californie et qui compte 13'000 employés. Cette société développe des appareils et des logiciels pour la sécurité de l'information tels que : pare-feu, programmes antivirus ou encore des systèmes de détection d'intrusion.

Disaggregation of Revenue

The following table presents our revenue disaggregated by major product and service lines (in millions):

	Year Ended December 31,		
	2022	2021	2020
Product	\$ 1,780.5	\$ 1,255.0	\$ 916.4
Service:			
Security subscription	1,427.0	1,125.0	918.7
Technical support and other	1,209.9	962.2	759.3
Total service revenue	2,636.9	2,087.2	1,678.0
Total revenue	\$ 4,417.4	\$ 3,342.2	\$ 2,594.4

Figure 6 évolution revenus Fortinet 2020-2022

Avec des revenus supérieurs à 4 milliards de dollars, environ 60% viennent de la vente de services et les 40% restant proviennent de la vente de matériel.

Fortinet tire donc ses revenus majoritairement de la vente de services liés à leurs appareils. Ceci a conduit l'entreprise à réduire fortement les fonctionnalités disponibles sur leurs appareils ne nécessitant pas d'abonnement.

2.3.3 Réseau CPNV

Les plans du réseau du CPNV, fournis par le SIp, seront nécessaires pour la seconde phase du projet :

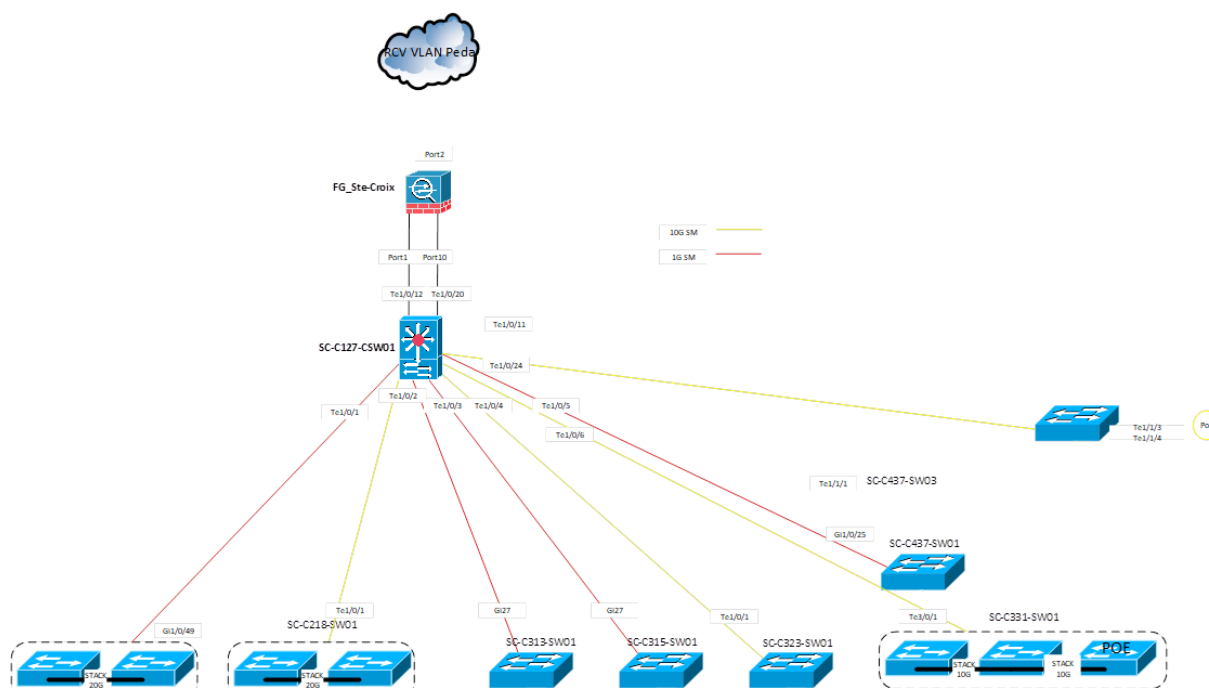


Figure 7 schéma physique CPNV-SC

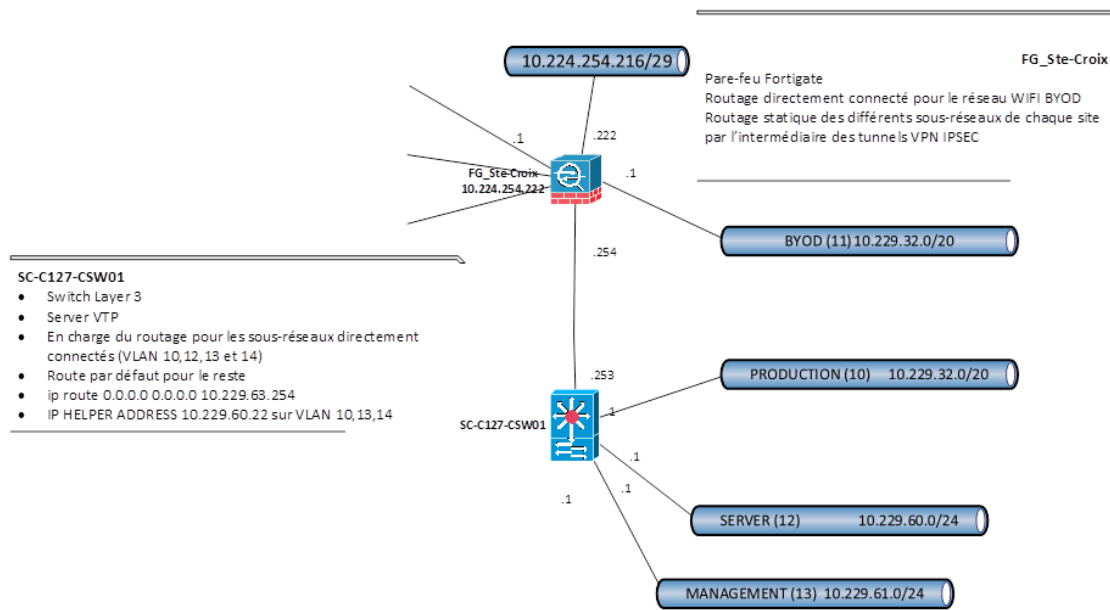


Figure 8 schéma physique CPNV-SC

2.4 Concept

2.4.1 Déroulement du projet

Je prévois une implémentation du projet en 4 parties :

Mise en place de l'infrastructure réseau (0) : ceci implique la création d'un réseau physique incluant un pc principal, une imprimante, un serveur Windows 2019 virtualisé en mode bridge via VMWare Workstation Pro 2016. Configuration du pare-feu physique, des VDOMs pour pare-feu logique et d'un routeur pour simulation du réseau internet.

Mise en place du VPN site à site (1.1) : configuration du routage, des règles de pare-feu nécessaire ainsi que du tunnel site à site

Mise en place du VPN client à site (1.2) : installation et configuration de FortiClient VPN sur poste de travail en salle C111 et connexion au siège principal.

Transfert sur réseau de l'école (2) : branchement du FortiGate sur le réseau de l'école en place du routeur de la salle C111, observation de ce changement et modification nécessaires selon besoin.
Accès à distance sur un pc situé en salle de classe C236

2.5 Dossier de conception

2.5.1 Liste du matériel utilisé :

	Matériel	OS/Logiciel
PC C111	Dell Optiplex 9010	Windows 10 Edu
PC C236	Dell Optiplex 7070	Windows 10 Edu
Pare-feu	Fortinet FortiGate 80F	FortiOS 6.4.12
Routeur p1	Cisco Catalyst 1900 Series	-
Routeur p2	Cisco Catalyst 3560 Series*	-
Commutateur	Netgear 300 switch Series	-

Imprimante	Xerox Phase 6600	-
Client VPN	-	FortiClient VPN 7.0.8.0427
Terminal	-	PuTTY 0.78

* le Cisco Catalyst 3560 est un commutateur capable de router.

2.5.2 Schéma :

Page | 12

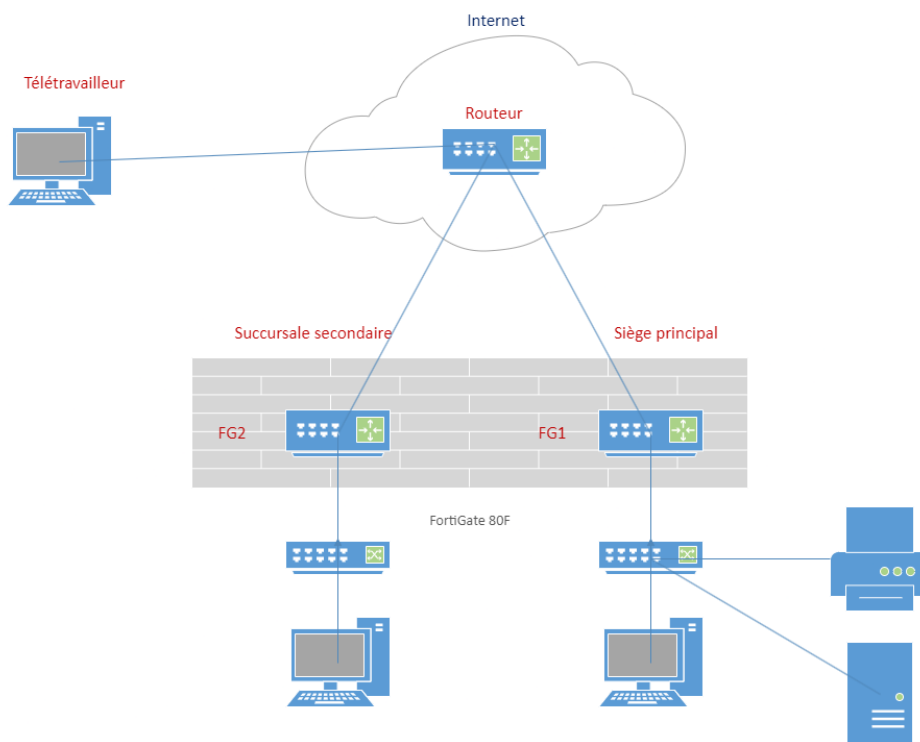


Figure 9 schéma du projet TPI

Le schéma est le même pour la phase 1 comme pour la phase 2 : la différence venant dans la partie « internet » qui sera recrée à l'aide d'un routeur alors que pour la deuxième phase, le réseau du CPNV servira d'internet.

Seconde différence, l'emplacement du télétravailleur : en salle C111 dans la première phase, dans une autre salle en deuxième phase.

A noter : selon le schéma du cahier des charges, la succursale secondaire devrait avoir une imprimante. Après discussion avec le chef de projet (25.5.2023), il s'avère que ceci n'est pas nécessaire. Il n'y aura donc pas d'imprimante dans le réseau de la succursale secondaire.

2.5.3 Internet

Comme indiqué par le schéma trouvé au point 2.8.2, internet sera simulé par un routeur Cisco Catalyst 1900 series dans un premier temps, par un switch Cisco Catalyst 3560 series dans un deuxième temps et finalement par le routeur du CPNV pour la dernière partie.

2.5.4 Adressage IP

Basé sur le cahier des charges, 120 hôtes maximum pour le site principal et 24 hôtes maximum pour la succursale secondaire.

Réseau	Passerelle	Plage d'adresse	Diffusion
<i>Site principal</i>			
192.168.128.0/25	192.168.128.1/25	192.168.128.2-126/25	192.168.128.127/25
<i>Succursale secondaire</i>			
192.168.128.128/27	192.168.128.129/27	192.168.128.130-158/27	192.168.128.159/27
<i>Télétravailleurs</i>			
192.168.228.0/24	192.168.228.1/24	192.168.228.2-254/24	192.168.228.255/24
<i>Tunnel pour télétravailleurs</i>			
-	-	10.0.128.1-10/8	-

2.5.5 Table de routage

Réseau destination	Masque de sous-réseau	Via	Interface FortiGate
<i>Router Cisco 1900 (1.1)</i>			
192.168.128.0	255.255.255.128	10.0.0.3	-
192.168.128.128	255.255.255.224	172.16.0.4	-
<i>Switch-Routeur Cisco 3560 (1.2)</i>			
192.168.128.0	255.255.255.128	10.0.0.3	-
192.168.128.128	255.255.255.224	172.16.0.4	-
<i>VDOM Siège principal</i>			
172.16.0.0	255.255.255.0	10.0.0.1	WANPrincipal
192.168.128.128	255.255.255.224	-	IPSEC_TO_Sec
192.168.228.0	255.255.255.0	10.0.0.1	WANPrincipal
<i>VDOM Succursale secondaire</i>			
10.0.0.0	255.0.0.0	172.16.0.1	WANSecondaire
192.168.128.0	255.255.255.128	-	IPSEC_TO_Princ

2.6 Stratégie de test

Basé sur mon expérience des tests dans le domaine des réseaux informatique : mes tests vont être très linéaire, chacun étant la suite logique de l'autre. J'ai une liste d'une vingtaine de tests qui va pouvoir, tout au long de l'implémentation du projet, tester le bon déroulement de ladite implémentation. Ceux-ci seront de niveau unitaire et de type fonctionnel.

Chaque phase va être testée dans l'ordre de réalisation au travers des commandes "ping" et "tracert" soit depuis le pc, le FortiGate ou l'appareil faisant office d'internet (routeur ou switch).

Je prévois des tests assez simples : "obtient-on le résultat attendu ?" Si la réponse est oui : on passe à la prochaine implémentation, si la réponse est non : on revient en arrière sur les choses mises en place depuis le dernier test réussi.

Je prévois de les expérimenter moi-même dans un premier temps et par la suite de les faire faire par un de mes camarades avec l'aide des notes prises pendant le déroulement de l'implémentation.

Les preuves sont disponibles dans les annexes au point 7.4

Edit : Au final, je me suis trouvé à court de temps. Je les ai donc réalisés seul.

2.7 Liste des tests

N°	Nom du test	But du test	Résultat attendu	Status
<i>Réseau général</i>				
1	Configuration PC siège principal	Vérifier le fonctionnement DHCP du FortiGate	IP 192.168.128.xx	☑
2	Configuration PC succursale 2	Vérifier le fonctionnement DHCP du FortiGate	IP 192.168.128.yy	☑
3	Configuration Serveur	Vérifier l'adressage du serveur	IP 192.168.128.126	☑
4	Configuration Imprimante	Vérifier l'adressage de l'imprimante	IP 192.168.128.125	☑
5	Configuration Routeur IP 0/0 & 0/1	Vérifier que les bonnes adresses soient attribuées	10.0.0.1 & 172.16.0.1	☑
6	Table de routage Routeur	Vérifier que la table de routage corresponde aux besoins	Voir table de routage dans rapport	☑
7	Configuration Switch IP & no switchport 0/1, 0/2 & 0/13	Vérifier que les bonnes adresses soient attribuées & que les ports puissent router	10.0.0.1 / 172.16.0.1 / 192.168.128.1 & no switchport	☑
8	Table de routage Switch	Vérifier que la table de routage corresponde aux besoins	Voir table de routage dans rapport	☑
<i>Phase 1</i>				
9	Tracert PC succursale 2 depuis PC siège principal	Vérifier qu'on arrive à joindre un ordinateur de la succursale 2	Un itinéraire déterminé	☑
10	Tracert gateway depuis siège principal	Vérifier que le trajet n'emprunte pas le VPN site à site mais passe par le routeur	Un itinéraire différent qui ne passe pas par le VPN	☑
11	Tracert PC siège principal depuis succursale 2	Vérifier qu'on arrive à joindre un ordinateur de la succursale 2	Un itinéraire déterminé	☑
12	Tracert gateway depuis succursale 2	Vérifier que le trajet n'emprunte pas le VPN site à site mais passe par le routeur	Un itinéraire différent qui ne passe pas par le VPN	☑
13	Ping server depuis siège principal	Vérifier qu'on arrive à joindre le serveur depuis le siège principal	Ping réussi	☑
14	Ping server depuis succursale succursale 2	Vérifier qu'on arrive à joindre le serveur depuis la succursale 2	Ping réussi	☑
15	Ping printer depuis succursale succursale 2	Vérifier qu'on arrive à joindre l'imprimante depuis la succursale 2	Ping réussi	☑
16	Ping server depuis télétravailleur	Vérifier qu'on arrive à joindre le serveur depuis le télétravailleur	Ping réussi	☑
17	Ping printer depuis télétravailleur	Vérifier qu'on arrive à joindre l'imprimante depuis le télétravailleur	Ping réussi	☑
18	Connexion via clien vpn	Vérifier que le télétravailleur arrive à établir une connexion VPN au siège principal	Connexion arrive à s'établir	☑
<i>Phase 2</i>				
19	Accès à l'interface Site principal depuis PC05	Prouver que l'on est connecté au réseau de l'école	Adresse IP de l'école	☑
20	Connexion VPN site à site	Prouver que le VPN site à site fonctionne	Un tunnel site à site utilisant le réseau du CPNV	☑
21	Connexion VPN client à site depuis PC05	Prouver que le VPN cliet à site fonctionne	Une connexion depuis un PC de la salle C236	☑

2.8 Risques techniques

2.8.1 Connaissances limitées en VPN

Mes connaissances apprises en dehors du CPNV sur le VPN s'arrêtent à l'installation de Proton VPN sur un ordinateur privé. Celles apprises au CPNV l'ont été pendant le module 146, et cela consistait en une simple configuration à travers un réseau virtuel constitué sur GNS3.

Page | 15

Afin de combler mon manque de connaissances, j'ai fait des recherches sur internet et suis arrivé sur un site de l'université de British Columbia, site spécialisé sur FortiGate et incluant les VPNs : <https://pressbooks.bccampus.ca/fortigatefirewall/>

2.8.2 Connaissances limitées en pare-feu

Mes connaissances en pare-feu se limitent à celles découvertes pendant mon pré-TPI à savoir les règles permettant l'accès à internet. Le site cité au point 2.7.2 a été utilisé pour combler ces lacunes.

2.8.3 Complexités liées au réseau de l'école et à ses contraintes

La plus grande inconnue de ce projet, le SIp (Service Informatique pédagogique) ne sait pas comment le réseau du CPNV va réagir à l'arrivée d'un deuxième FortiGate sur le réseau de l'école. Il pourrait y avoir un problème de boucle dans le réseau.

Pour combler ce risque potentiel, je me renseigne sur le protocole "Spanning Tree".

2.8.4 Connaissances non-acquises pendant le pré-TPI

Ce point m'était inconnu au début du projet est c'est révélé être très important. En effet, ma planification initiale ainsi que la première semaine et demie de mon TPI s'est déroulée avec une solution ne permettant l'implémentation de firewalls virtuels.

En effet, bien que ma solution se soit montrée efficace pour le pré-TPI, elle était totalement inefficace pour répondre au cahier des charges du TPI.

En plus de ceci, l'option VDOM n'apparaît pas dans le GUI du FortiGate, ni de FortiOS 6.4.12. Il a fallu l'activer via la CLI.

Une simple discussion avec mon chef de projet a suffi à résoudre ce problème. Il aurait été nécessaire de faire un débriefing complet entre le pré-TPI et le TPI pour s'assurer que cette connaissance fondamentale ait bien été apprise.

2.9 Planification finale

Projet		Planification							
Mise en place de firewalls virtuels sur une Appliance Fortinet, adaptée au module 146									
	Total								
Prévu	90 h 05	02/05/23	09/05/23	15/05/23	22/05/23	29/05/23	05/06/23	12/06/23	
Mayor	87 h 55	18 h 20	23 h 55	16 h 45	23 h 55	7 h 10			
		16 h 25	23 h 50	16 h 45	23 h 45	7 h 10			
1 Analyse		SEM	18	19	20	21	22	23	24
									18 h 00
									21 h 15
1.1 Planification	Prévu	4 h 00							4 h 00
	Mayor	4 h 10	0 h 35						4 h 45
1.2 Recherches	Prévu	4 h 00	2 h 00	1 h 00	1 h 00				8 h 00
	Mayor	5 h 30	2 h 00	2 h 00	2 h 00				11 h 30
1.3 Elaboration des stratégies de test	Prévu	2 h 00		1 h 00					2 h 00
	Mayor								1 h 00
1.4 Adressage IP	Prévu	2 h 00							2 h 00
	Mayor	1 h 30	0 h 30						2 h 00
1.5 Règles de pare-feu	Prévu	2 h 00							2 h 00
	Mayor		2 h 00						2 h 00
2 Implémentation 1er temps									15 h 00
									15 h 00
2.1 Création réseau siège principal	Prévu		2 h 00						2 h 00
	Mayor		2 h 00						2 h 00
2.2 Création VMs siège principal (serveur, client * 2)	Prévu		1 h 00						1 h 00
	Mayor		1 h 00						1 h 00
2.3 Création serveur VPN siège principal	Prévu		2 h 00						2 h 00
	Mayor		2 h 00						2 h 00
2.4 Implémentation pare-feu siège principal	Prévu		2 h 00						2 h 00
	Mayor		2 h 00						2 h 00
2.5 Création réseau succursale 2	Prévu		1 h 00						1 h 00
	Mayor		1 h 00						1 h 00
2.6 Création VMs succursale 2	Prévu		1 h 00						1 h 00
	Mayor		1 h 00						1 h 00
2.7 Création client VPN succursale 2	Prévu		2 h 00						2 h 00
	Mayor		2 h 00						2 h 00
2.8 Implémentation pare-feu succursale 2	Prévu		1 h 00						1 h 00
	Mayor		1 h 00						1 h 00
2.9 Création réseau télétravailleur	Prévu		1 h 00						1 h 00
	Mayor			1 h 00					1 h 00
2.10 Création VM télétravailleur	Prévu		1 h 00						1 h 00
	Mayor				1 h 00				1 h 00
2.11 Création client VPN télétravailleur	Prévu		1 h 00						1 h 00
	Mayor				1 h 00				1 h 00
3 Implémentation 2ème temps									22 h 00
									4 h 00
3.1 Implémentation/adaptation serveur VPN siège	Prévu			4 h 00					4 h 00
	Mayor				1 h 00				1 h 00
3.2 Implémentation/adaptation client VPN succursale 2	Prévu			2 h 00					2 h 00
	Mayor				1 h 00				1 h 00
3.3 Implémentation/adaptation client VPN	Prévu			2 h 00					2 h 00
	Mayor				1 h 00				1 h 00
3.4 Implémentation physique du pare-feu	Prévu			2 h 00					2 h 00
	Mayor				1 h 00				1 h 00
3.5 Implémentation/adaptation règles pare-feu siège	Prévu			2 h 00	2 h 00				4 h 00
	Mayor								
3.6 Implémentation/adaptation règles pare-feu	Prévu				4 h 00				4 h 00
	Mayor								
3.7 Implémentation/adaptation règles pare-feu	Prévu				4 h 00				4 h 00
	Mayor								
4 Tests									16 h 50
									14 h 30
4.1 Tests réseau siège principal	Prévu		0 h 30						0 h 30
	Mayor		0 h 30						0 h 30
4.2 Tests système siège principal	Prévu		0 h 30						0 h 30
	Mayor		0 h 30						0 h 30
4.3 Tests réseau succursale 2	Prévu		0 h 30						0 h 30
	Mayor		0 h 30						0 h 30
4.4 Tests système succursale 2	Prévu		0 h 30						0 h 30
	Mayor		0 h 30						0 h 30
4.5 Tests VPN site-to-site	Prévu		0 h 30						0 h 30
	Mayor			1 h 30					1 h 30
4.6 Tests pare-feu site-to-site	Prévu		0 h 30						0 h 30
	Mayor			1 h 30					1 h 30
4.7 Tests système télétravailleur	Prévu		0 h 30						0 h 30
	Mayor				0 h 30				0 h 30
4.8 Tests VPN client-to-site	Prévu		0 h 30						0 h 30
	Mayor				1 h 00				1 h 00
4.9 Tests pare-feu client-to-site	Prévu			0 h 30					0 h 30
	Mayor								
4.10 Tests VPN site-to-site 2ème temps	Prévu				2 h 00				2 h 00
	Mayor				1 h 00				1 h 00
4.11 Tests VPN client-to-site 2ème temps	Prévu				2 h 00				2 h 00
	Mayor				1 h 00				1 h 00
4.12 Tests pare-feu site-to-site	Prévu				2 h 00				2 h 00
	Mayor								
4.13 Tests pare-feu client-to-site	Prévu				2 h 00				A
	Mayor								
4.14 Tests généraux	Prévu	1 h 35	0 h 10	0 h 30	2 h 10	1 h 55			6 h 20
	Mayor			4 h 00	2 h 00				6 h 00
5 Documentation									13 h 30
									33 h 10
5.1 Documentation	Prévu	2 h 00	2 h 00	2 h 00	2 h 00	4 h 30			10 h 30
	Mayor	2 h 30	1 h 00	1 h 00	10 h 15	7 h 10			21 h 55
5.2 Journal de travail	Prévu	0 h 45	0 h 45	0 h 45	0 h 45	0 h 45			3 h 00
	Mayor	0 h 45	0 h 45	0 h 45					2 h 15
5.3 Préparation présentation	Prévu								
	Mayor								
5.4 Maladie	Prévu								
	Mayor								
5.5 Administratif	Prévu								
	Mayor	2 h 00	1 h 00						3 h 00
5.6 Temps flexible	Prévu								
	Mayor		2 h 00	4 h 00					6 h 00

Figure 10 planification finale

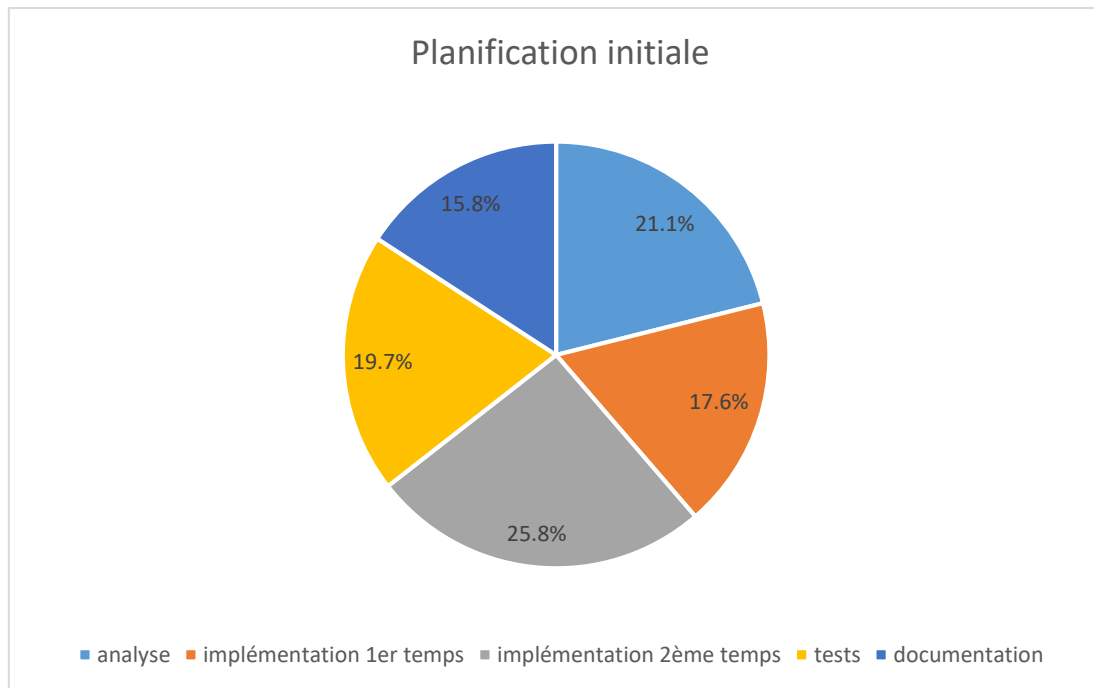


Figure 11 planification initiale %

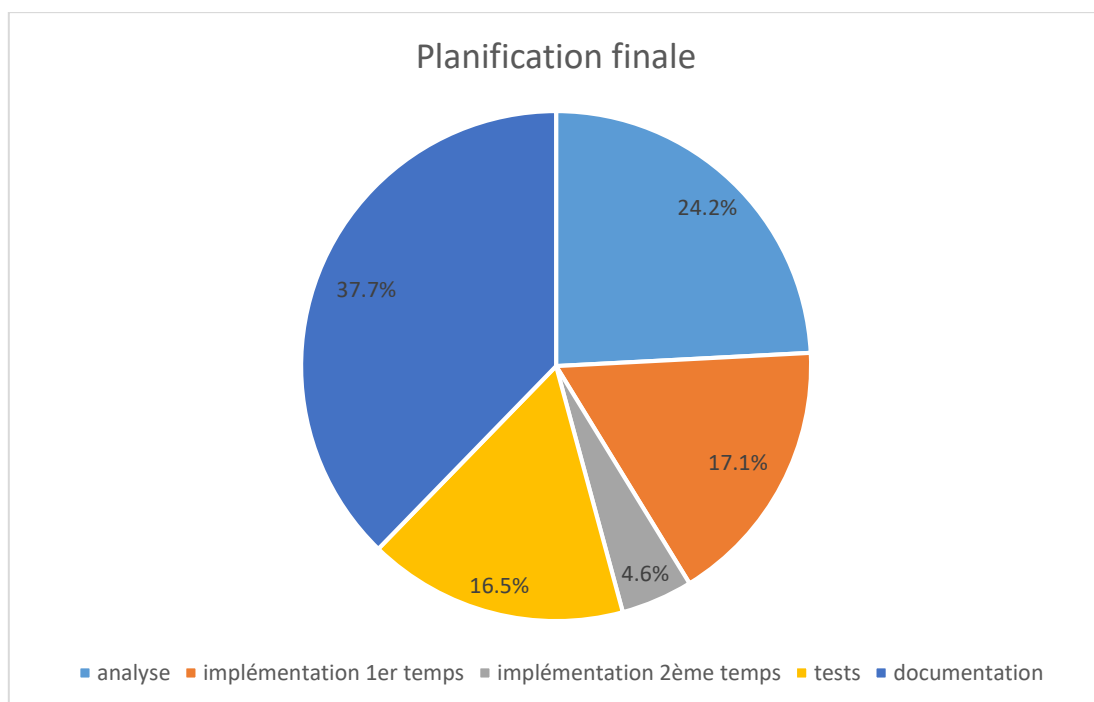


Figure 12 planification finale %

On se rend compte au premier coup d'œil de deux grosses différences entre la planification initiale et la planification finale : "implémentation 2^{ème} temps" et "documentation".

Ces différences s'expliquent très facilement : l'implémentation du 2^{ème} temps s'est faite en 4 heures seulement alors que plus de 20 heures étaient prévues. En effet, il a suffi de brancher le FortiGate et de changer les adresses IP du tunnel original par les adresses IP distribuées par le serveur DHCP.

Une fois cette deuxième implémentation faite, tout le temps restant est passé dans la documentation.

3 Réalisation

3.1 Dossier de réalisation

3.1.1 1^{ère} phase

Note : après discussion avec le chef de projet : il s'avère qu'une imprimante dans la succursale secondaire n'est pas nécessaire, elle n'a donc pas été implémentée.

Page | 18

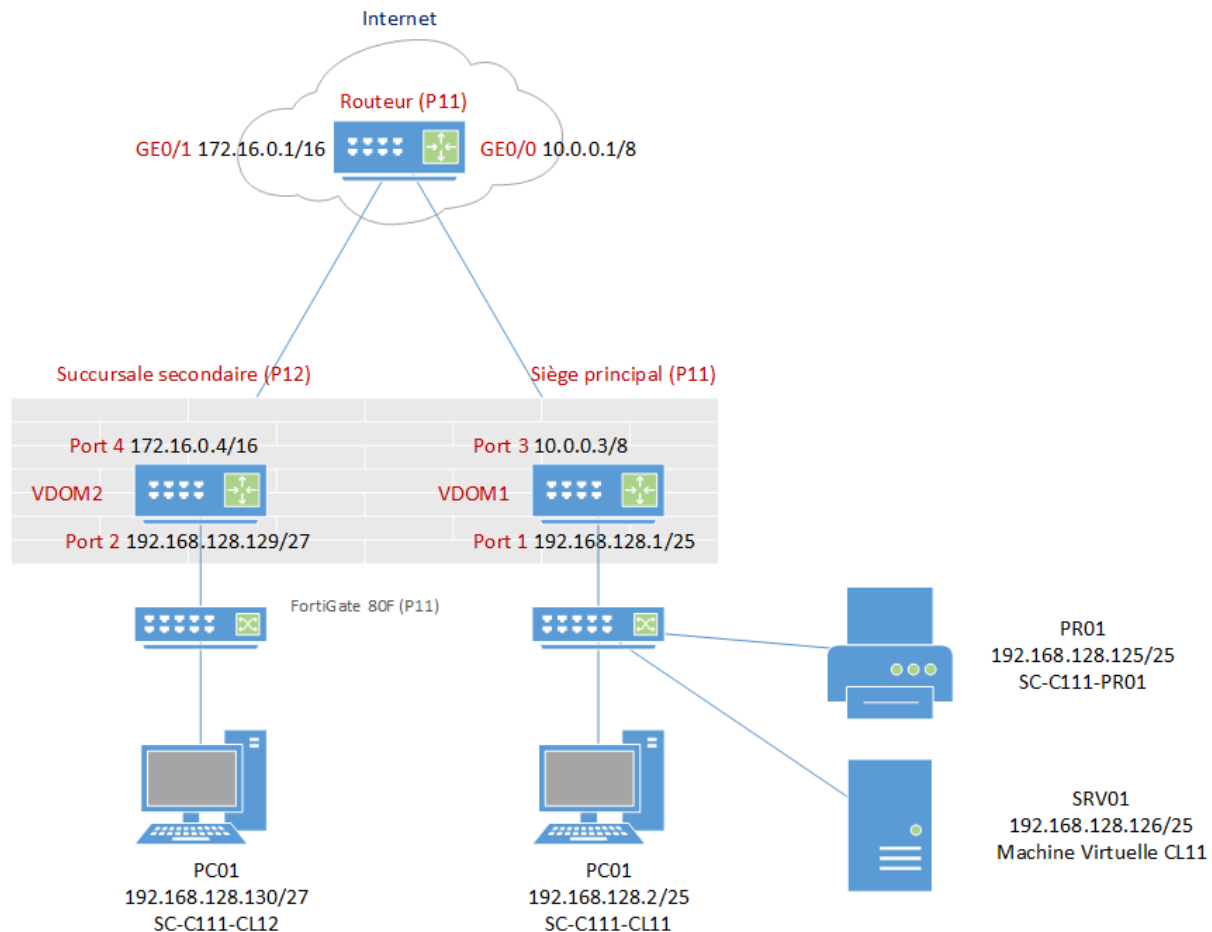


Figure 13 schéma implémentation phase 1 site à site

3.1.1.1 Configuration réseau Siège principal

Vérifier le système d'exploitation : Windows 10 Edu

Vérifier que l'ordinateur n'a pas d'adresse IP fixe mais qu'il est bien en mode DHCP

Panneau de control : réseaux et internet : centre de partage : Ethernet : Propriétés : IPv4 : Obtenir une adresse IP automatiquement

A l'aide de VMWare, créer un machine virtuelle Windows server 2019, en mode bridge et lui attribuer l'adresse fixe 192.168.128.126/25

Relier le port Ethernet du PC au port 1 du switch Netgear

Relier le port Ethernet de l'imprimante au port 2 du switch Netgear

Relier le port 8 du switch Netgear au port 1 du FortiGate

3.1.1.2 Configuration FortiGate 80F

Ouvrir browser 192.168.1.99

Username : admin

Password : (vide)

Choisir un nouveau mot de passe (Pa\$\$w0rd)

Se connecter

Page | 19

System : Settings

Time zone : GMT+1:00

Sync interval : 1

Apply

3.1.1.3 Activation VDOM :

Qu'est-ce qu'un VDOM ? Un firewall virtuel. Tel un ordinateur physique qui peut accueillir plusieurs ordinateurs logiques, un FortiGate peut accueillir plusieurs VDOMs.

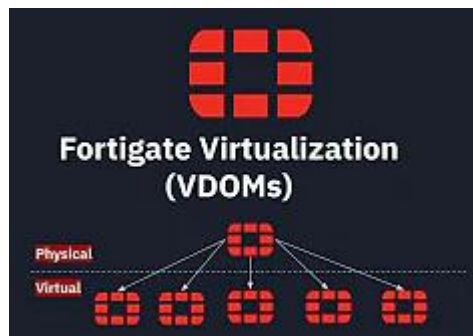


Figure 14 FortiGate VDOMs

Sur le FortiGate 80F l'option VDOM n'apparaît pas sous "System" dans le GUI. Il faut l'activer à l'aide du CLI.

Dans le coin supérieur droite du GUI, cliquer sur le symbol `>_` pour ouvrir le CLI et taper:

```
#config sys global
```

```
(global) #set vdom-mode multi-vdom
```

Ceci va nous déconnecter, se reconnecter.

Dans le coin supérieur gauche du GUI, au-dessus de Dashboard, un menu déroulant est apparu avec deux options ; **Global** et **root**.

Global se réfère aux réglages généraux non-spécifiques aux VDOMs donc toutes les options telles que les règles de pare-feu, adresses, tables de routage ou encore VPNs vont disparaître.

Root accueille toutes les options citées plus haut qui n'apparaissent pas sous Global

Se rendre dans **root** : Network : interfaces : Hardware Switch : internal : cliquer sur internal

Dans Interface members: cliquer sur les croix des interfaces 1, 2, 3 et 4 : cliquer sur OK

3.1.1.4 Création du domaine Principal

Se rendre dans **Global** : System : VDOM : Create New

Virtual Domain : nommer notre VDOM : Principal : cliquer sur OK

Se rendre dans Network : Interfaces : double cliquer sur internal1 :

Alias : Siège principal

Virtual domain : Principal

Role : LAN

IP/Netmask 192.168.128.1/255.255.255.128

Administrative Access :

IPv4 : tout ticker

DHCP Server : On

Address range : 192.168.128.2-192.168.128.126

Netmask : 255.255.255.128

OK

Double cliquer sur internal3 :

Alias : WANPrincipal

Virtual domain : Principal

Role : WAN

IP/Netmask 10.0.0.3/255.0.0.0

Administrative Access :

IPv4 : tout ticker

OK

3.1.1.5 Création du domaine Secondaire

Se rendre dans **Global** : System : VDOM : Create New

Virtual Domain : nommer notre VDOM : Secondaire : cliquer sur OK

Se rendre dans Network : Interfaces : double cliquer sur internal2 :

Alias : Succursale 2

Virtual domain : Secondaire

Role : LAN

IP/Netmask 192.168.128.129/255.255.255.224

Administrative Access :

IPv4 : tout ticker

DHCP Server : On

Address range : 192.168.128.130-192.168.128.158

Netmask : 255.255.255.224

OK

Double cliquer sur internal4 :

Alias : WANSecondaire

Virtual domain : Secondaire

Role : WAN

IP/Netmask 172.16.0.4/255.255.0.0

Administrative Access :

IPv4 : tout ticker

OK

3.1.1.6 Création des administrateurs

Toujours dans Global

Se rendre dans System : Administrators : Create New : Administrator

Username : adminPrincipal

Type : Local User

Password : Pa\$\$w0rd

Confirm Password : Pa\$\$W0rd

Administrator Profile : prof_admin

Virtual Domains : enlever root, ajouter Principal

OK

System : Administrators : Create New : Administrator

Username : adminSecondaire

Type : Local User

Password : Pa\$\$w0rd

Confirm Password : Pa\$\$W0rd

Administrator Profile : prof_admin

Virtual Domains : enlever root, ajouter Secondaire

OK

3.1.1.7 Mise en place VDOM Principal

Dans le browser rentrer l'adresse de l'interface Siège principal : 192.168.128.1

Username : adminPrincipal

Password : Pa\$\$w0rd

Policy & Objects : Addresses

Create New : Address

Name : LANSiegePrincipal

Color : Violet

Type : Subnet

IP/Netmask 192.168.128.0 255.255.255.128

Interface : any

Static route configuration : Off

OK

Create New : Address

Name : LANSecondaire

Color : Vert

Type : Subnet

IP/Netmask 192.168.128.128 255.255.255.224

Interface : any

Static route configuration : Off

OK

3.1.1.8 Attribuer une adresse fixe à l'imprimante :

Se rendre dans Network : Interfaces : Siège principal : double clic

Sous DHCP Server : Advanced :

IP Address Assignment Rules : Add from DHCP Client List

Ajouter l'imprimante avec sa MAC Address : 9c:93:4e:2d:93:45

Page | 22

3.1.1.9 Création règle "open bar" pour le pare-feu

Policy & Objects : Firewall Policy

Create New

Name : OpenBarLocalPrinc

Incoming Interface : Siège principal

Outgoing Interface : WANPrincipal

Source : all

Destination : all

Schedule : always

Service : ALL

...

Enable this policy : on

OK

Policy & Objects : Firewall Policy

Create New

Name : OpenBarPrincLocal

Incoming Interface : WANPrincipal

Outgoing Interface : Siège principal

Source : all

Destination : all

Schedule : always

Service : ALL

...

Enable this policy : on

OK

Network : Static Routes : Create New

Destination : Subnet

172.16.0.0/255.255.0.0

Gateway Address : 10.0.0.1

Interface : WANPrincipal

OK

3.1.1.10 Mise en place VDOM Secondaire

Dans le browser rentrer l'adresse de l'interface Siège principal : 192.168.128.129

Username : adminSecondaire

Password : Pa\$\$w0rd

Policy & Objects : Addresses

Create New : Address

Name : LANSiegePrincipal

Color : Violet

Type : Subnet

IP/Netmask 192.168.128.0 255.255.255.128

Interface : any

Static route configuration : On

OK

Create New : Address

Name : LANSecondaire

Color : Vert

Type : Subnet

IP/Netmask 192.168.128.128 255.255.255.224

Interface : any

Static route configuration : Off

OK

Policy & Objects : Firewall Policy

Create New

Name : OpenBarLocalSec

Incoming Interface : Succursale 2

Outgoing Interface : WANSecondaire

Source : all

Destination : all

Schedule : always

Service : ALL

...

Enable this policy : on

OK

Policy & Objects : Firewall Policy

Create New

Name : OpenBarSecLocal

Incoming Interface : WANSecondaire

Outgoing Interface : Succursale 2

Source : all

Destination : all

Schedule : always

Service : ALL

...

Enable this policy : on

OK

Network : Static Routes : Create New

Destination : Subnet

10.0.0.0/255.0.0.0

Gateway Address : 172.16.0.1

Interface : WANSecondeaire

OK

Page | 24

3.1.1.11 Configuration routeur

Se connecter au router via un câble Serial RS-232 depuis le PC01

Ouvrir PuTTY et sélectionner : Serial

Attribution d'adresses IP au deux ports GigabitEthernet du routeur

```
enable
```

```
conf t
```

```
interface GigabitEthernet0/0
```

```
ip address 10.0.0.1 255.0.0.0
```

```
no shutdown
```

```
exit
```

```
enable
```

```
conf t
```

```
interface GigabitEthernet1/0
```

```
ip address 172.16.0.1 255.255.0.0
```

```
no shutdown
```

```
exit
```

Tables de routage

```
enable
```

```
conf t
```

```
ip route 192.168.128.0 255.255.255.128 10.0.0.3
```

```
no shutdown
```

```
exit
```

```
enable
```

```
conf t
```

```
ip route 192.168.128.128 255.255.255.224 172.16.0.4
```

```
no shutdown
```

```
exit
```


3.1.1.12 Configuration réseau Succursale secondaire

Vérifier le système d'exploitation : Windows 10 Edu

Vérifier que l'ordinateur n'a pas d'adresse IP fixe mais qu'il est bien en mode DHCP

Panneau de control : réseaux et internet : centre de partage : Ethernet : Propriétés : IPv4 : Obtenir une adresse IP automatiquement

Page | 25

Relier le port Ethernet du PC au port 1 du switch Netgear

Relier le port 8 du switch Netgear au port 2 du FortiGate

3.1.1.13 Configuration tunnels site-à-site

Création du tunnel

Se rendre dans Principal

VPN : IPsec Wizard :

Name : IPSEC_TO_Sec

Template type : Custom

Next

Remote Gateway : Statip IP Adress

IP Address 172.16.0.4

Interface WANPrincipal

Method Pre-shared Key

Pre-Shared Key : Pa\$\$w0rd

Dans Phase 1 Proposal :

Garder Encryption AES256 et Authentication SHA256, enlever le reste

Diffie-Hellman Groups : 5

Type : Disabled

Dans New Phase 2 Selector :

Local Address : Subnet : 192.168.128.0 / 255.255.255.128

Remote Address : Subnet : 192.168.128.128 / 255.255.255.224

Advanced :

Garder Encryption AES256 et Authentication SHA256, enlever le reste

Diffie-Hellman Groups : 5

OK

3.1.1.14 Création règle pare-feu pour tunnel

Policy & Objects : Firewall Policy Create New

Name : LAN-IPSEC Access

Incoming Interface : Siège principal

Outgoing Interface : IPSEC_TO_Sec

Source : LANSiegePrincipal

Destination : LANSecondaire

Schedule : always

Service : ALL

Enable this policy :

OK

Cette règle va permettre le trafic de Principal à Secondaire. Il faut créer sa règle inverse pour que le trafic puisse aller dans le sens inverse.

Faire un clic droit sur la règle LAN-IPSEC Access et sélectionner : Clone Reverse

Nommer cette règle : IPSEC_LAN Access

OK

3.1.1.15 Création route pour tunnel

Network : Static Routes : Create New

Destination Subnet

192.168.128.128/255.255.255.224

Interface : IPSEC_TO_Sec

OK

Maintenant, il faut créer le tunnel depuis le site Secondaire, en suivant les mêmes étapes :

3.1.1.16 Création du tunnel

Se rendre dans Principal

VPN : IPsec Wizard :

Name : IPSEC_TO_Princ

Template type : Custom

Next

Remote Gateway : Statip IP Adress

IP Address 10.0.0.3

Interface WANSecondaire

Method Pre-shared Key

Pre-Shared Key : Pa\$\$w0rd

Dans Phase 1 Proposal :

Garder Encryption AES256 et Authentication SHA256, enlever le reste

Diffie-Hellman Groups : 5

Type : Disabled

Dans New Phase 2 Selector :

Local Address : Subnet : 192.168.128.128 / 255.255.255.224

Remote Address : Subnet : 192.168.128.0 / 255.255.255.128

Advanced :

Garder Encryption AES256 et Authentication SHA256, enlever le reste

Diffie-Hellman Groups : 5

OK

3.1.1.17 Création de la policy

Policy & Objects : Firewall Policy Create New

Name : LAN-IPSEC Access

Incoming Interface : Succursale 2

Outgoing Interface : IPSEC_TO_Princ

Source : LANSecondaire

Destination : LANSiegePrincipal

Schedule : always

Service : ALL

Enable this policy :

OK

Page | 27

Faire un clic droit sur la règle LAN-IPSEC Access et sélectionner : Clone Reverse

Nommer cette règle : IPSEC_LAN Access

OK

3.1.1.18 Création de la route

Network : Static Routes : Create New

Destination Subnet

192.168.128.0/255.255.255.128

Interface : IPSEC_TO_Princ

OK

Note : le routeur Cisco 1900 series ne possède que deux ports LAN, pour l'implémentation d'un télétravailleur, il a donc été décidé avec le chef de projet d'utiliser un switch Cisco 3560 qui a la possibilité de travailler en couche 3 du modèle OSI à la place de sa couche 2 habituelle, ceci grâce à la commande `no switchport`

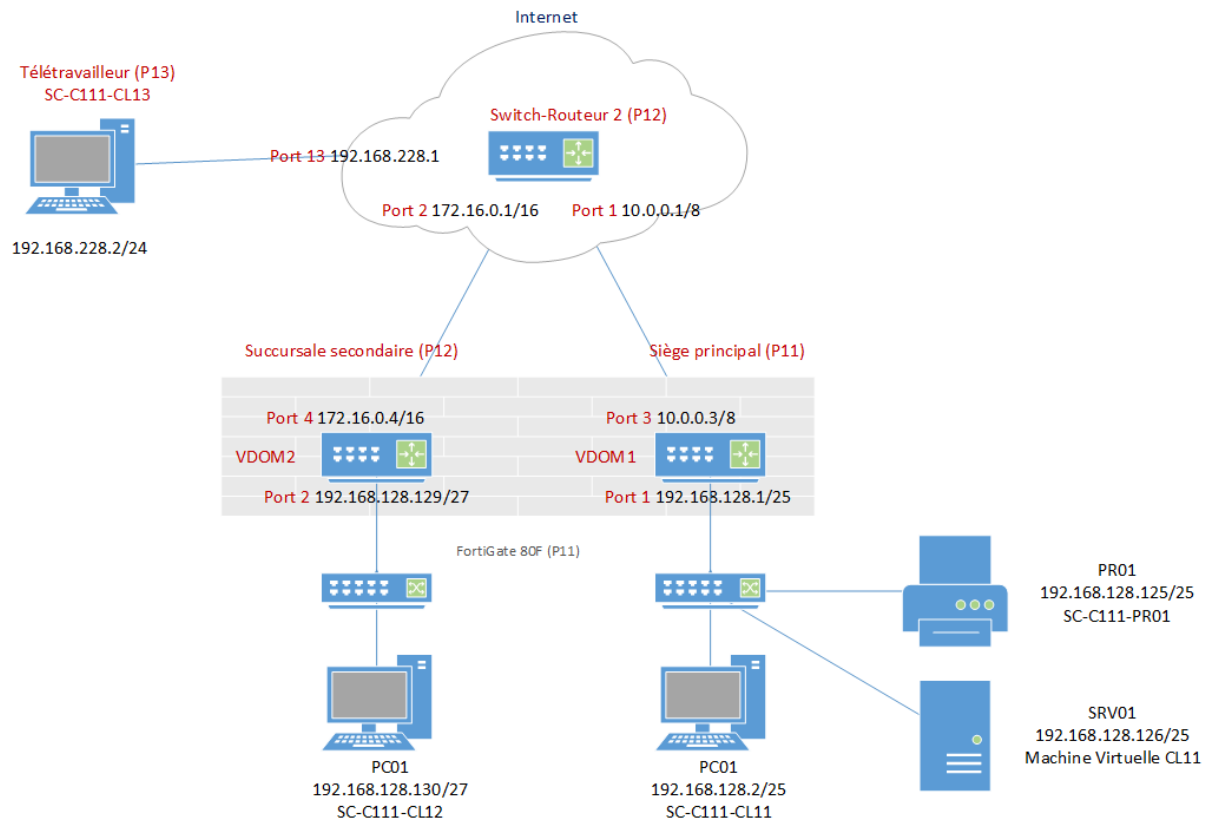


Figure 15 schéma implémentation phase 1.2 client à site

3.1.1.19 Configuration switch

Relier le port 3 du FortiGate au port 1 du switch avec un câble ethernet.
Relier le port 4 du FortiGate au port 2 du switch avec un câble ethernet.

Se connecter au router via un câble Serial RS-232 depuis le PC01
Ouvrir PuTTY et sélectionner : Serial

Configuration des ports nécessaires en ports routable et attribution des adresses IP:

```
enable
conf t
interface FastEthernet0/1
no switchport
ip address 10.0.0.1 255.0.0.0
no shutdown
exit
```

```
enable
conf t
interface FastEthernet0/1
no switchport
```

```
ip address 172.16.0.1 255.255.0.0
no shutdown
exit

enable
conf t
interface FastEthernet0/1
no switchport
ip address 192.168.228.1 255.255.255.0
no shutdown
exit
```

Tables de routage

```
enable
conf t
ip route 192.168.128.0 255.255.255.128 10.0.0.3

no shutdown
exit

enable
conf t
ip route 192.168.128.128 255.255.255.224 172.16.0.4
no shutdown
exit
```

3.1.1.20 Configuration PC13 Télétravailleur

Vérifier le système d'exploitation : Windows 10 Edu

Vérifier que l'ordinateur n'a pas d'adresse IP fixe mais qu'il est bien en mode DHCP

Panneau de control : réseaux et internet : centre de partage : Ethernet : Propriétés : IPv4 : Obtenir une adresse IP automatiquement

Relier le port Ethernet du PC au 13 du switch Cisco

3.1.1.21 Configuration tunnel client-à-site

Dans VDOM Principal

Création d'un utilisateur de VPN

User & Authentification : User Definition : Create New

Local User

Username : teletravailleur

Password : Pa\$\$w0rd

Contact Info : Next

Extra Info : Submit

Configuration du tunnel

Création d'un groupe:

User & Authentication : User Groups : Create New

Name : Télétravailleurs

Type : Firewall

Members : teletravailleur

Page | 30

Création du tunnel client-à-site

VPN : IPsec Wizard :

Name : VPNtt

Template type : Remote Access

Remote device type : Client-based

FortiClient

Next

Incoming Interface : WANPrincipal

Authentication method : Pre-shared Key

Pre-shared key : Pa\$\$W0rd

User Group : Télétravailleurs

Next

Local interface : Siège principal

Local Address : LANSiegePrincipal

Client Address Range : 10.0.128.1-10.0.128.10

Subnet Mask : 255.0.0.0

Next

Save Password : off

Next

Se rendre dans VPN : IPsec Tunnels

Modifier Phase 1 Proposal afin d'avoir:

Encryption : AES256

Authentication : SHA256

Diffie-Hellman Group : 5

OK

Modifier Phase 2 : Advanced

Encryption : AES256

Authentication : SHA256

Diffie-Hellman Group 5

OK

Rajouter une route pour le réseau du télétravailleur :

Network : Static Routes : Create New

Destination : Subnet

192.168.228.0/255.255.255.0

Gateway Address 10.0.0.1

Interface : WANPrincipal

OK

3.1.1.22 Configuration FortiClient VPN

Sur le poste de travail du télétravailleur

Télécharger FortiClient VPN à l'adresse : <https://www.fortinet.com/support/product-downloads>

Installer FortiClient VPN

Configuration du VPN

New VPN Connection

VPN : VPN IPsec

Nom de la connexion : VPNtt

Passerelle distante : 10.0.0.3

Méthode d'authentification : Clé partagée (Pa\$\$wOrd)

Advanced Settings

Phase 1

IKE Proposal : Encryption : AES256 Authentication : SHA256

DH Group 5

Phase 2

IKE Proposal : Encryption : AES256 Authentication : SHA256

DH Group 5

SAVE

Nom du VPN : VPNtt

Nom d'utilisateur : teletravailleur

Mot de passe : Pa\$\$wOrd

Connecter

VPN Connected!

3.1.2 2^{ème} phase

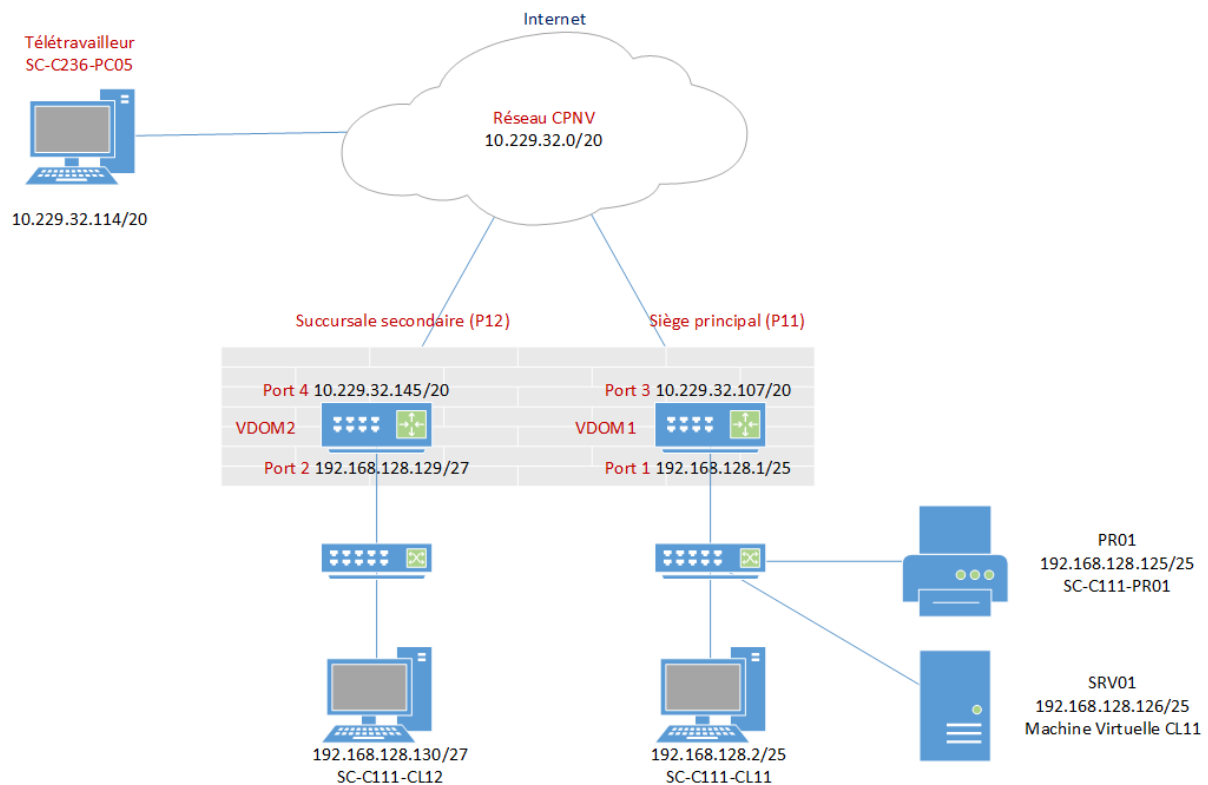


Figure 16 schéma implémentation phase 2 branchement sur réseau CPNV

3.1.2.1 Connexion du pare-feu au réseau du CPNV :

En salle C111, connecter le port 3 et le port 4 au switch disponible dans l'armoire réseau de la salle.

Modifier le tunnel site à site pour phase 2 :

Se connecter au FortiGate

Se rendre dans Principal : Network : Interfaces : WANPrincipal et double cliquer.

Address : Addressing mode : DHCP

OK

Se connecter au FortiGate

Se rendre dans Secondaire : Network : Interfaces : WANSecondaire et double cliquer.

Address : Addressing mode : DHCP

OK

Les firewalls reçoivent maintenant une adresse du CPNV, en 10.229.32.x/20.

Il faut maintenant adapter les tunnels à ces nouvelles adresses WAN

Se rendre dans Principal : VPN : IPsec Tunnels : IPSEC_TO_Sec et mettre à jour IP Address. Dans mon cas avec la nouvelle adresse reçue du CPNV : 10.229.32.145 (ou adresse IP distribuée par le DHCP)

Se rendre dans Secondaire : VPN : IPsec Tunnels : IPSEC_TO_Princ et mettre à jour IP Address avec la nouvelle adresse : 10.229.32.107

ATTENTION ces adresses IP ne sont pas fixes ! Donc elles vont changer en cas de perte de baille DHCP.

3.1.2.2 Installer et configurer FortiClient VPN

Sur le poste de travail du télétravailleur en salle C236

Configuration du VPN

New VPN Connection

VPN : VPN IPsec

Nom de la connexion : VPNtt

Passerelle distante : 10.229.32.107 (ou adresse IP distribuée par le DHCP)

Méthode d'authentification : Clé partagée (Pa\$\$w0rd)

Advanced Settings

Phase 1

IKE Proposal : Encryption : AES256 Authentication : SHA256

DH Group 5

Phase 2

IKE Proposal : Encryption : AES256 Authentication : SHA256

DH Group 5

SAVE

Nom du VPN : VPNtt

Nom d'utilisateur : teletravailleur

Mot de passe : Pa\$\$w0rd

Connecter

VPN Connected !

Page | 33

3.2 Preuves des tests effectués

Voir annexe 7.4

3.3 Erreurs restantes

Toutes les demandes du cahier des charges ont été satisfaites. Néanmoins des améliorations sont possibles et ont été formulées au point 4.4

3.4 Nombre maximal d'implémentations

Sans tenir compte des performances, il existe 3 facteurs qui pourraient impacter le nombre d'implémentations maximal :

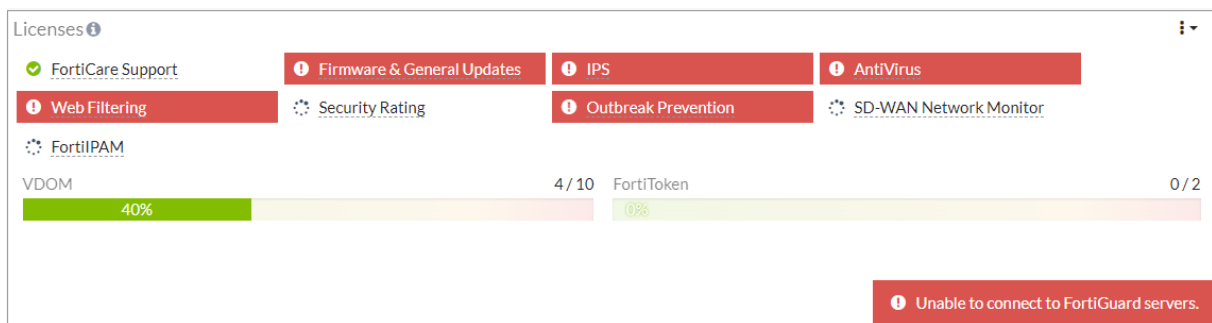
3.4.1 VDOM

Selon la documentation de Fortinet, le FortiGate 80F permet la création de 10 VDOMs (<https://docs.fortinet.com/max-value-table>).

By default, most FortiGate models support a maximum of 10 VDOMs in any combination of NAT/Route and Transparent operating modes. For FortiGate models 1000D and higher, a license key can be purchased to increase the maximum number.

Figure 17 nombre VDOMs maximum selon documentation Fortinet

L'interface du FortiGate confirme cette limitation :



Page | 34

Figure 18 nombre VDOMs maximum selon notre FortiGate 80F

A noter : dès la création du premier VDOM, une des VDOM va être automatiquement réservée pour le VDOM root qui permet la gestion centralisée des VDOMs. Il y a donc en réalité 9 VDOMs disponible pour la création de combinaisons siège principal/succursale secondaire.









3.4.2 VPN

Pas de limite au niveau logiciel quant au nombre de connexions via FortiClient VPN, cependant il y a probablement des limitations liées à l'appareil utilisé. Le lien partagé au point 3.6.1 indique certaines valeurs mais je n'ai pas la compétence nécessaire pour déterminer quelle catégorie détermine cette limitation.

3.4.3 Limitation physique

A l'exception du VDOM root, chaque VDOM a besoin d'un port physique WAN et d'un port LAN. Le FortiGate 80F possède 6 ports physique disponible et 2 ports dédiés à d'autres appliances Fortinet. On est donc limité à 3 VDOMs à moins d'utiliser un FortiSwitch.

3.5 Liste des documents fournis

-  Rapport de TPI DMA.pdf
-  Résumé du rapport de TPI (à l'annexe 7.1)
-  Cahier des charges (à l'annexe 7.2)
-  Identification du module (à l'annexe 7.3)
-  Preuves des tests (à l'annexe 7.4)
-  Sources (à l'annexe 7.5)
-  Glossaire (à l'annexe 7.6)
-  Journal de travail (à l'annexe 7.7)

4 Conclusions

4.1 Objectifs atteints / non-atteints

En se basant sur le point 8 du cahier des charges : « Points techniques évalués spécifiques au projet »
Les points mesurables : 3, 4, 6 et 7 sont atteints.

Les points faisant appel à la notion de "pertinence" ont été abordés en gardant à l'esprit le contexte de ce TPI à savoir l'intégration au module 146 et donc en visant la simplicité et l'efficacité sans néanmoins atteindre l'efficacité.

4.2 Points positifs / négatifs

4.2.1 Négatif

J'ai trouvé pesant que 2 ans de formations soient jugés par un seul projet. Il est vrai que mon cas est différent par rapport à la grande majorité de mes camarades de classe, sans même prendre en compte l'ensemble des apprentis du CPNV.

Le dénouement positif de mon projet ne s'est confirmé qu'en dernière semaine et cela à ajouter une dose de stress non-négligeable.

Bien qu'en sachant qu'on peut réussir son TPI tout en échouant à mettre le projet en place, cela devient vite une expérience difficile.

4.2.2 Positif

Le sujet était très intéressant ; travailler sur des VPNs avec un pare-feu pour quelqu'un, comme moi, qui se destine pour la cybersécurité était vraiment motivant. Le plaisir et l'expérience acquise pendant ce TPI, ainsi que pendant mon pré-TPI, me conforte par rapport à la direction que je souhaite donner à ma carrière.

4.3 Difficultés particulières

-Mauvaise planification initiale basée sur la façon dont s'est déroulé notre module 146, à savoir de manière entièrement virtuelle. J'ai fait le bon choix de passer à une réalisation physique mais j'aurais dû prendre le temps de refaire ma planification.

-Ne pas avoir découvert les VDOMs pendant mon pré-TPI m'ont fait partir du mauvais pied et prendre un retard non négligeable.

-J'étais tellement concentré sur les tables de routage du routeur qu'il m'a fallu les lumières de Mr. Varela pour me faire remarquer que j'avais oublié celles du pare-feu

-Une erreur dans mes plages d'adresses IP m'ont fait perdre du temps. Cette erreur a été vite corrigé, mais une table de routage à échapper à cette correction pendant quelques heures, causant bien des soucis.

4.4 Améliorations

-Pour le moment les adresses IP reçues du CPNV ne sont pas fixes, donc soumises aux baux du serveur DHCP. L'imprimante du siège principal à une adresse fixe venant du FortiGate mais le serveur lui reçoit son adresse de son système d'exploitation. Il sera bien d'homogénéiser ceci selon les besoins du module.

-Les règles de pare-feu mises en place l'ont été dans le but d'assurer l'ouverture du réseau, sans aucune optimisation ou autre approche sécuritaire. C'est un point qui pourrait clairement être amélioré, surtout dans l'optique d'implémentation au module 146, qui est sensé traiter de ce sujet.

-Montage du FortiGate sur un FortiRack et implémentation dans l'armoire de la salle C111 pour résidence permanente.

-J'ai fait le projet au mieux de mes capacités dans le temps imparti, j'aimerais beaucoup que quelqu'un de plus expérimenté relise et partage ses idées d'améliorations ainsi que les éventuelles corrections.

4.5 Retour personnel

Ces mots sont écrits le 31.05.2023. Mon TPI est presque sous presse, ou pour être plus en adéquation avec notre époque : presque exporté en .pdf avant envoyer par email à 16h50 à mon chef de projet ainsi qu'à mes experts.

Ce travail restera gravé dans ma mémoire pour plusieurs raisons : à commencer malheureusement par le décès tragique de mon cousin Esteban.

Le projet n'a pas été de tout repos : un cahier des charges un peu difficile à aborder, une planification initiale complètement chamboulée moins de 24 heures après avoir été planifiée. Une semaine et demi plus tard, c'est la découverte qu'un élément fondamental à la réussite du projet m'est resté inconnu. Rajouter à ceci une erreur d'adresse IP par-ci, une table de routage oubliée par-là, sans oublier de saupoudrer le tout de stress induit par la challenge d'une reconversion professionnelle a passé 40 ans...et...

Mais on m'a appris au CPNV à découper un gros "bout" en petit "bouts", on m'a appris à documenter mes tentatives ainsi que mes échecs afin que lorsque le moment arrive d'aller demander de l'aide ; je peux être précis et concis dans ma demande. On m'a appris que tout en informatique laisse des traces, et qu'un simple fichier de logs contient plus d'information et de réponses que 10'000 vidéos youtube.

Au final je rends un projet fini, avec des solutions efficaces. J'aurai aimé utiliser l'adjectif efficaces mais un CFC c'est un peu comme le permis de conduire : c'est lorsque l'on est lâché sur la route que l'on apprend vraiment à conduire.

Quelle belle aventure...

5 Remerciements

A Madame **Nicole Mayor** pour les corrections de l'orthographe et la grammaire de ce document.

A Madame **Beatriz Martin** pour sa relecture et son support tout au long de ce TPI.

A Messieurs **Sylvain Fasola & Laurent Jaggi** pour avoir pris le temps de répondre à mes questions.

6 Table des illustrations

Figure 1 planification initiale.....	6
Figure 2 méthode en cascade.....	7
Figure 3 organisation des fichiers	8
Figure 4 définition pare-feu.....	9
Figure 5 définition VPN	9
Figure 6 évolution revenus Fortinet 2020-2022	10
Figure 7 schéma physique CPNV-SC	10
Figure 8 schéma physique CPNV-SC	11
Figure 9 schéma du projet TPI.....	12
Figure 10 planification finale.....	16
Figure 11 planification initiale %.....	17
Figure 12 planification finale %.....	17
Figure 13 schéma implémentation phase 1 site à site	18
Figure 14 FortiGate VDOMs	19
Figure 15 schéma implémentation phase 1.2 client à site	28
Figure 16 schéma implémentation phase 2 branchement sur réseau CPNV.....	32
Figure 17 nombre VDOMs maximum selon documentation Fortinet	33
Figure 18 nombre VDOMs maximum selon notre FortiGate 80F	34

7 Annexes

7.1 Résumé du rapport de TPI

Ce TPI intitulé : *"Mise en place de firewalls virtuels sur une Appliance Fortinet, adapté au module 146"* est la suite logique de mon travail de pré-TPI : *"Mise en service d'un pare-feu Fortinet"* lui-même dérivé d'une fiche signalétique : *"Assurer la sécurité d'un réseau informatique"*. Le module 146 mentionné dans le titre fait référence au module I-CT 146 : *"Relier une entreprise à Internet"* auquel j'ai assisté lors du 6^{ème} trimestre de ma formation.









Page | 39

Les challenges sont multiples au début de ce TPI, l'expérience relative aux VPNs ainsi qu'aux pare-feux étant limitée aux connaissances acquises durant mon pré-TPI. C'est un projet très varié qui englobe la création de réseau, la configuration de switch et router ainsi qu'une "simulation" d'internet. Tout ceci, pendant la première phase du projet dans un "bac à sable" à savoir la salle C111, complètement isolée du reste de l'école d'un point de vue de son réseau informatique. Dans la 2^{ème} du projet, le FortiGate 80F, utilisé pour le routage et la virtualisation de pare-feu, est raccordé au réseau de l'école en lieu et place d'internet et c'est ici que l'inconnu commence : comment le réseau du CPNV accepte-il cet appareil ? Est-il possible de se connecter depuis une salle de classe aux pare-feux virtuels créés sur le FortiGate comme le demande le module 146 ?

Au final, la configuration du pare-feu et de ses machines virtuelles s'est montrée longue et pleine de découvertes. Le transfert du bac à sable de la salle C111 au réseau du CPNV s'est révélé sans aucune embûche, un simple réglage de configuration à suffit à faire fonctionner tant le VPN site à site que le VPN client à site. Je suis donc capable de fournir une solution efficace à ce travail de TPI et de remplir tous les points techniques spécifiques au projet qui seront évalués.

7.2 Cahier des charges

1 INFORMATIONS GENERALES

Candidat :	Nom : MAYOR	Prénom : Damien																				
	 : damien.mayor@cpnv.ch	 : +41 78 918 43 75																				
Lieu de travail :	<input type="checkbox"/> CPNV, Rue de la Gare 14, 1450 Sainte-Croix																					
Orientation :	<input type="checkbox"/> 88601 Développement d'application <input checked="" type="checkbox"/> 88602 Informatique d'entreprise <input type="checkbox"/> 88603 Technique des systèmes																					
Chef de projet :	Nom : VARELA	Prénom : Francis																				
	 : francis.varela@cpnv.ch	 : +41 78 775 20 07																				
Expert 1 :	Nom : WOLF	Prénom : Benjamin																				
	 : bw-tpi@hotmail.com	 : +41 79 793 34 65																				
Expert 2 :	Nom : MBUYI	Prénom : Junior																				
	 : junior.mbuyi@epfl.ch	 : +41 79 519 02 58																				
Période de réalisation :	Du mardi 2 mai 2023 à 8h00 au mardi 30 mai 2023 à 16h50																					
Horaire de travail :	<table border="0"> <tr> <td>Lundi</td> <td>09h50-12h15</td> <td>13h30-16h55</td> <td><i>Pentecôte 29 mai</i></td> </tr> <tr> <td>Mardi</td> <td>08h00-12h15</td> <td>13h30-16h55</td> <td></td> </tr> <tr> <td>Mercredi</td> <td>08h00-12h15</td> <td>-</td> <td></td> </tr> <tr> <td>Jeudi</td> <td>08h00-12h15</td> <td>13h30-16h55</td> <td><i>Ascension 18 mai</i></td> </tr> <tr> <td>Vendredi</td> <td>-</td> <td>-</td> <td><i>Pont de l'Ascension 19 mai</i></td> </tr> </table> <p><i>Toutes les demi-journées ont une pause obligatoire de 15 minutes, sauf si elles se commencent à 09h50.</i></p>		Lundi	09h50-12h15	13h30-16h55	<i>Pentecôte 29 mai</i>	Mardi	08h00-12h15	13h30-16h55		Mercredi	08h00-12h15	-		Jeudi	08h00-12h15	13h30-16h55	<i>Ascension 18 mai</i>	Vendredi	-	-	<i>Pont de l'Ascension 19 mai</i>
Lundi	09h50-12h15	13h30-16h55	<i>Pentecôte 29 mai</i>																			
Mardi	08h00-12h15	13h30-16h55																				
Mercredi	08h00-12h15	-																				
Jeudi	08h00-12h15	13h30-16h55	<i>Ascension 18 mai</i>																			
Vendredi	-	-	<i>Pont de l'Ascension 19 mai</i>																			
Nombre d'heures :	90 heures																					
Planning (en H ou %)	Analyse 20%, Implémentation 40%, Tests 25%, Documentation 15%																					
Présentation :	Dates retenues : 12 ou 13 juin 2023																					

2

Le candidat réalise un travail personnel sur la base d'un cahier des charges reçu le 1er jour.

Le cahier des charges est approuvé par les deux experts. Il est en outre présenté, commenté et discuté avec le candidat. Par sa signature, le candidat accepte le travail proposé.

Le candidat a connaissance de la feuille d'appréciation avant de débiter le travail.

Le candidat est entièrement responsable de la sécurité de ses données.

En cas de problèmes graves, le candidat avertit au plus vite les deux experts et son CdP.

Le candidat a la possibilité d'obtenir de l'aide, mais doit le mentionner dans son dossier.

A la fin du délai imparti pour la réalisation du TPI, le candidat doit transmettre par courrier électronique le dossier de projet aux deux experts et au chef de projet. En parallèle, une copie papier du rapport doit être fournie sans délai en trois exemplaires (L'un des deux experts peut demander à ne recevoir que la version électronique du dossier). Cette dernière doit être en tout point identique à la version électronique.

Page | 41

3

Mise en place de firewalls virtuels sur une Appliance Fortinet, adapté au module 146

4

1 ordinateur type CPNV avec accès Internet

1 Environnement (Windows10, Office, VMware)

Matériel en salle C111 (Serveurs, postes clients, Switch Cisco, routeurs)

1 pare-feu Fortinet entrée de gamme FG-80F

Toutes les licences nécessaires pour Windows Server 2019 et Windows 10 1 imprimante réseau

(Liste non exhaustive pouvant dépendre des choix techniques effectués)

5

Le candidat possède les bases pour installer et configurer :

Un poste client sous Windows 10

VMware Workstation

Un pare-feu Fortinet, notamment les protocoles réseau nécessaires au projet, les règles de pare-feux et les pare-feux virtuels

6

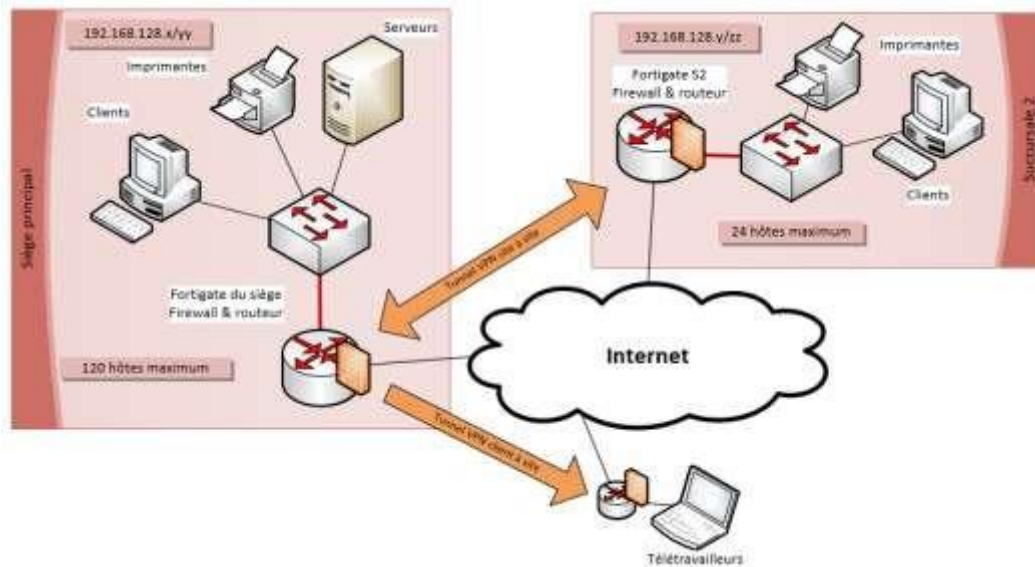
Le module 146 abordant les grands réseaux d'entreprise avec des VPN site à site et clients, et du NAT, ce projet cherche à évaluer les possibilités d'implémenter le schéma ci-dessous à l'aide d'un seul firewall Fortinet en exploitant les capacités de virtualisation de FortiGate.

Dans un 1^{er} temps la mise en place se fera en salle C111, afin de réaliser l'implémentation du schéma physique indépendamment du réseau de l'école.

Dans un 2^{ème} temps le FortiGate sera connecté au réseau physique de l'école en conservant sa configuration tel quel, afin de d'évaluer les possibilités et les limites d'une telle implémentation. L'idée étant que le module soit réalisé à distance en exploitant des PC et des VM dans les salles de classes.

Les éléments nécessaires pour constituer la partie « Internet » et représenter les hôtes et les switches, sont laissés au choix du candidat, en tenant compte que lors du 2^{ème} temps se sera le réseau réel du CPNV qui sera utilisé.

Page | 42



7

Le candidat est responsable de livrer à son chef de projet et aux deux experts :

- Une planification initiale le mardi 2 mai 2023 à 16h55
- Le rapport de projet et le journal de travail 2 fois par semaine (Le mardi à 16h55 et le jeudi à 16h55)
- Un rapport de projet final le mardi 30 mai 2023 à 16h50
- Un journal de travail final le mardi 30 mai 2023 à 16h50
- Toutes les sources finales utilisées le mardi 30 mai 2023 à 16h50

8

La grille d'évaluation définit les critères généraux selon lesquels le travail du candidat sera évalué (documentation, journal de travail, respect des normes, qualité, ...).

En plus de cela, le travail sera évalué sur les 7 points spécifiques suivants (Point A14 à A20) :

1. Pertinence de l'implémentation du 1^{er} temps
2. Pertinence de la partie « Internet » proposée dans le 1^{er} temps
3. A la fin du 1^{er} temps tous les clients et le télétravailleur peuvent atteindre le serveur et les imprimantes par leur adresse IP
4. Adressage IP proposé pour le siège, la succursale et le télétravailleur conforme au schéma du CDC

5. Pertinence de l'implémentation du 2^{ème} temps
6. A la fin du 2^{ème} temps tous les clients et le télétravailleur peuvent atteindre le serveur et les imprimantes par leur adresse IP
7. En fonction des caractéristiques de l'Appliance Fortinet, déterminer le nombre maximal d'implémentations du schéma proposé qu'il est théoriquement possible de réaliser sans tenir compte des performances

9

	Lu et approuvé le :	Signature :
Candidat :		
Expert n°1 :		
Expert n° 2 :		
Chef de projet :		

7.3 Identification du module 146



Identification du module

Page | 44

Numéro de module	146
Titre	Relier une entreprise à Internet
Compétence	Développer, projeter et réaliser un raccordement d'une entreprise à Internet en prenant en considération les aspects de sécurité, de disponibilité et de performance.
Objectifs opérationnels	<ol style="list-style-type: none"> 1 Déterminer la liaison Internet selon les directives du client (sécurité, performance, disponibilité et maintenance). 2 Classer les exigences selon priorité et signification pour l'entreprise, créer un cahier des charges pour l'évaluation d'un fournisseur de services (Provider). 3 Représenter les résultats de l'évaluation sur la base du cahier des charges et des aspects économiques. 4 Réaliser ou adapter le schéma et le plan du réseau. 5 Déterminer les composants matériels et logiciels nécessaires, élaborer une demande d'acquisition. 6 Planifier et réaliser la mise en exploitation avec les composants de la connexion Internet. Organiser et exécuter la remise de l'installation.
Domaine de compétence	Network Management
Objet	Réseau clients/serveur existant et nouvelle connexion Internet.
Version du module	3.0
Créé le	11.02.2021

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	146
------------------	-----

Titre Relier une entreprise à Internet

Compétence Développer, projeter et réaliser un raccordement d'une entreprise à Internet en prenant en considération les aspects de sécurité, de disponibilité et de performance.

Page | 45

Objectifs opérationnels et connaissances opérationnelles nécessaires

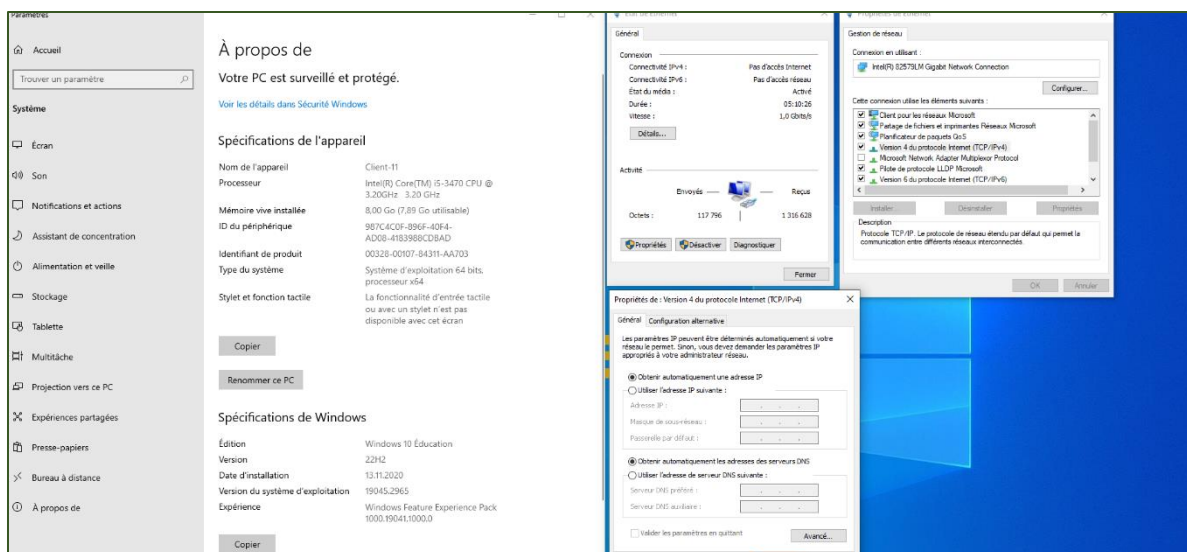
1	1.1	Connaître les exigences (largeur de bande, disponibilité, ampleur du support, sécurité etc.) en matière de lien Internet
	1.2	Connaître les mesures de surveillance et de sécurité lors de l'exploitation d'un réseau Internet.
2	2.1	Connaître les possibilités technologiques d'accès Internet ainsi que leur fournisseur (Provider).
	2.2	Connaître des méthodes de classification des directives des clients.
	2.3	Connaître l'organisation et le contenu d'un cahier des charges.
	2.4	Connaître le déroulement d'un processus d'évaluation.
3	3.1	Connaître les critères principaux pour l'évaluation d'une offre.
	3.2	Connaître les types de représentation pour l'évaluation d'une offre.
4	4.1	Connaître les règles pour l'élaboration d'un concept de dénomination et de numérotation.
	4.2	Connaître la fonctionnalité d'un Firewall, DMZ, Proxy et DNS.
	4.3	Connaître les types courants de représentation et symboles pour des schémas et plan de réseau.
5	5.1	Connaître l'organisation et le contenu d'une demande d'acquisition issue de l'évaluation.
	6.1	Connaître le déroulement pour la planification et la mise en service de l'accès Internet.
6	6.2	Connaître le déroulement pour la remise du système dans l'exploitation opérationnelle.
	6.3	Connaître l'organisation et le contenu d'un procès-verbal de remise.

Version du
module 3.0
Créé
le 11.02.2021

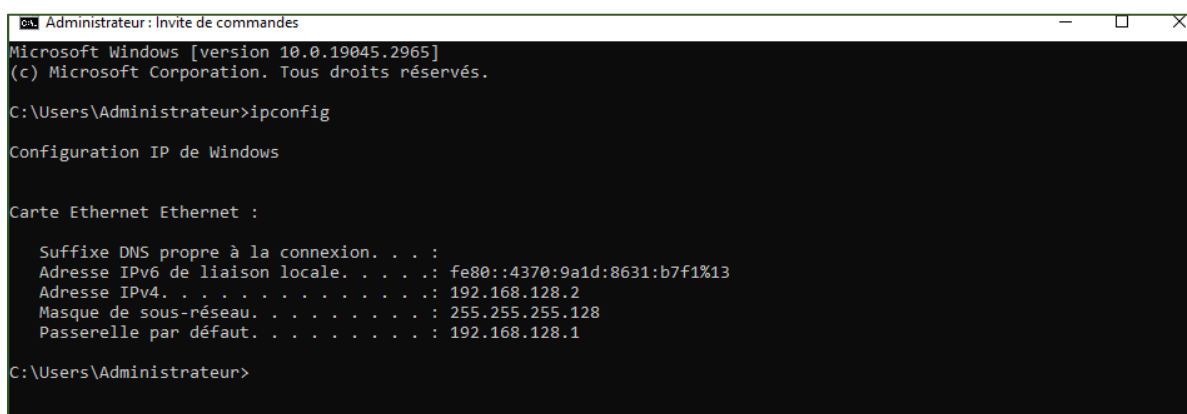
7.4 Preuves des tests

En plus de ces tests, l'ensemble des captures d'écrans sont disponible sur demande.

1. Configuration PC Siège principal



Page | 46



2. Configuration PC Succursale secondaire

Mode tablette	Spécifications de l'appareil	
Multitâche	Nom de l'appareil	SC-C111-CL12
Projection sur ce PC	Processeur	Intel(R) Core(TM) i5-3470 CPU @ 3.20GHz 3.20 GHz
Expériences partagées	Mémoire RAM installée	8,00 Go (7,89 Go usable)
Bureau à distance	ID de l'appareil	9550DFD2-A069-40C1-9E84-B7A4EA3B545D
Informations système	ID de produit	00328-10000-00001-AA489
	Type du système	64-bit operating system, x64-based processor
	Stylet et fonction tactile	La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran
	Renommer ce PC	

```

Administrateur : Invite de commandes

C:\Users\Administrateur>ipconfig

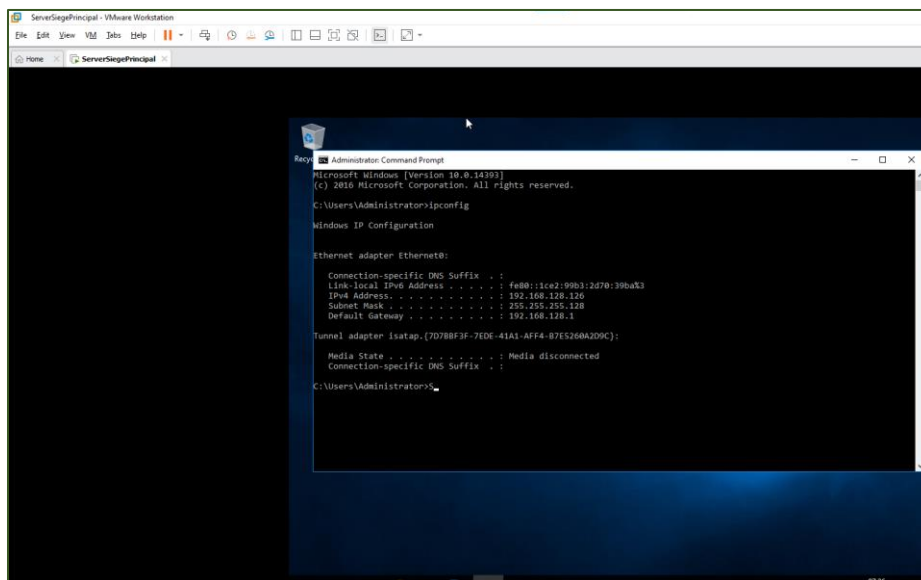
Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::cd1f:5c3d:ee40:cfa6%11
    Adresse IPv4. . . . . : 192.168.128.130
    Masque de sous-réseau. . . . . : 255.255.255.224
    Passerelle par défaut. . . . . : 192.168.128.129

C:\Users\Administrateur>
  
```

3. Configuration serveur



```

ServerSagePrincipal - VMware Workstation
File Edit View VM Help
Home ServerSagePrincipal

Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrateur>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

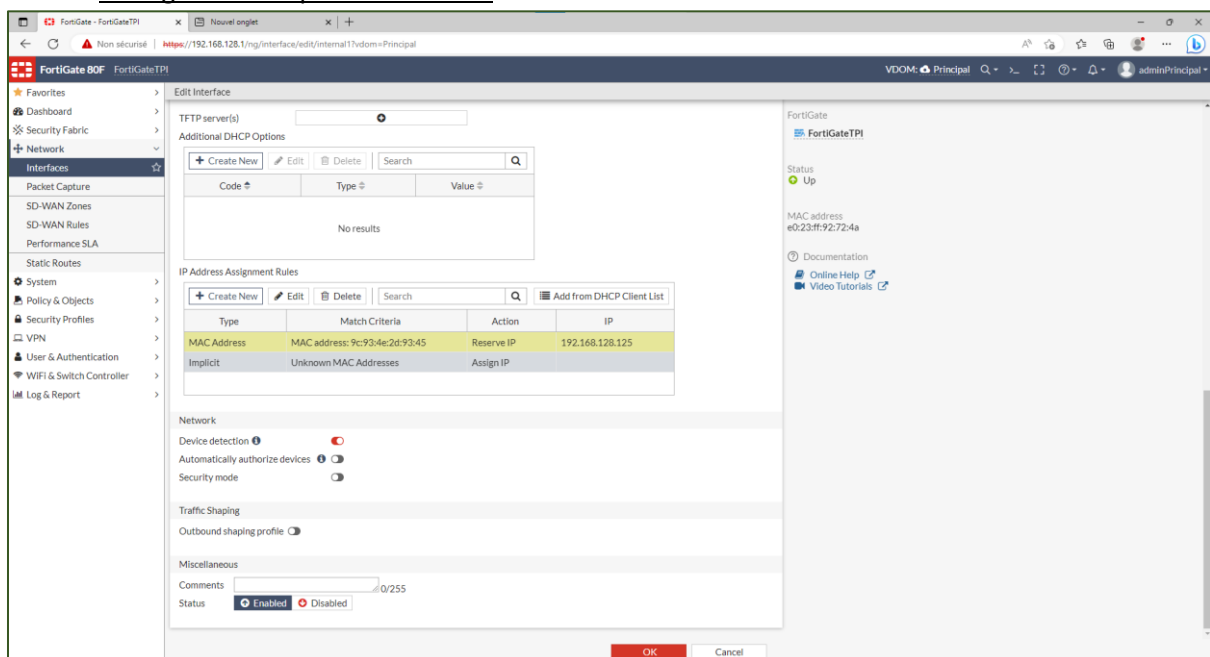
    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::1ce2:99b3:2d70:39ba%3
    IPv4 Address. . . . . : 192.168.128.126
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 192.168.128.1

Tunnel adapter Isatap.{7D78BF3F-7ED6-41A1-AF74-87E5260A2D9C}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\Administrateur>
  
```

4. Configuration imprimante IP Fixe



The screenshot shows the FortiGate GUI with the 'Edit Interface' configuration page. The 'IP Address Assignment Rules' section is expanded, showing a table with two rules:

Type	Match Criteria	Action	IP
MAC Address	MAC address: 9c:93:4e:2d:93:45	Reserve IP	192.168.128.125
Implicit	Unknown MAC Addresses	Assign IP	

Below the table, the 'Network' section shows 'Device detection' and 'Automatically authorize devices' both enabled. The 'Traffic Shaping' section shows 'Outbound shaping profile' set to 'None'. The 'Miscellaneous' section shows 'Comments' as '0/255' and 'Status' as 'Enabled'.

5. Configuration routeur IP 0/0 & 0/1

```
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
ip address 10.0.0.1 255.0.0.0
duplex auto
speed auto
no mop enabled
!
interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
duplex auto
speed auto
!
interface ATM0/0/0
no ip address
shutdown
no atm ilmi-keepalive
!
interface Ethernet0/0/0
no ip address
shutdown
!
```

Page | 48

6. Table de routage du routeur

```
!
no ip http server
no ip http secure-server
!
ip route 192.168.128.0 255.255.255.128 10.0.0.3
ip route 192.168.128.128 255.255.255.224 172.16.0.4
!
```

7. Configuration du switch IP & "no switchport" 0/1, 0/2 & 0/13

```
!
interface FastEthernet0/1
no switchport
ip address 10.0.0.1 255.0.0.0
!
interface FastEthernet0/2
no switchport
ip address 172.16.0.1 255.255.0.0
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
no switchport
ip address 192.168.228.1 255.255.255.0
!
--More--
```


8. Table de routage du switch

```
COM1 - Tera Term VT
File Edit Setup Control Window Help
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 192.168.128.0 255.255.255.128 10.0.0.3
ip route 192.168.128.128 255.255.255.224 172.16.0.4
ip http server
ip http secure-server
!
```

Page | 49

9. Tracert PC succursale 2 depuis PC siège principal

```
Administrateur : Invite de commandes
C:\Users\Administrateur>tracert 192.168.128.130

Détermination de l'itinéraire vers 192.168.128.130 avec un maximum de 30 sauts.

 1  <1 ms    <1 ms    <1 ms    192.168.128.1
 2  <1 ms    <1 ms    <1 ms    192.168.128.129
 3  <1 ms    <1 ms    <1 ms    192.168.128.130

Itinéraire déterminé.
C:\Users\Administrateur>
```

10. Tracert gateway depuis Siège principal

```
Administrateur : Invite de commandes
C:\Users\Administrateur>tracert 192.168.128.130

Détermination de l'itinéraire vers 192.168.128.130 avec un maximum de 30 sauts.

 1  <1 ms    <1 ms    <1 ms    192.168.128.1
 2  <1 ms    <1 ms    <1 ms    192.168.128.129
 3  <1 ms    <1 ms    <1 ms    192.168.128.130

Itinéraire déterminé.
C:\Users\Administrateur>tracert 172.16.0.4

Détermination de l'itinéraire vers 172.16.0.4 avec un maximum de 30 sauts.

 1  <1 ms    <1 ms    <1 ms    192.168.128.1
 2  <1 ms    <1 ms    <1 ms    10.0.0.1
 3  <1 ms    <1 ms    <1 ms    172.16.0.4

Itinéraire déterminé.
C:\Users\Administrateur>
```

11. Tracert PC Siège principale depuis Succursale secondaire

```
Administrateur : Invite de commandes

C:\Users\Administrateur>tracert 192.168.128.2

Détermination de l'itinéraire vers 192.168.128.2 avec un maximum de 30 sauts.

  1  <1 ms    <1 ms    <1 ms  192.168.128.129
  2  <1 ms    <1 ms    <1 ms  192.168.128.1
  3  4 ms     <1 ms    <1 ms  192.168.128.2

Itinéraire déterminé.

C:\Users\Administrateur>
```

Page | 50

12. Tracert gateway depuis Succursale secondaire

```
Administrateur : Invite de commandes

C:\Users\Administrateur>tracert 10.0.0.1

Détermination de l'itinéraire vers 10.0.0.1 avec un maximum de 30 sauts.

  1  <1 ms    <1 ms    <1 ms  192.168.128.129
  2  1 ms     <1 ms    <1 ms  10.0.0.1

Itinéraire déterminé.

C:\Users\Administrateur>
```

13. Ping serveur depuis Siège principal

```
Administrateur : Invite de commandes

Microsoft Windows [version 10.0.19045.2965]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::4370:9a1d:8631:b7f1%13
    Adresse IPv4. . . . . : 192.168.128.2
    Masque de sous-réseau. . . . . : 255.255.255.128
    Passerelle par défaut. . . . . : 192.168.128.1

Carte Ethernet VMware Network Adapter VMnet1 :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::e77d:9cea:468a:7b34%24
    Adresse IPv4. . . . . : 192.168.245.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

Carte Ethernet VMware Network Adapter VMnet8 :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::5142:3809:c21b:a94a%25
    Adresse IPv4. . . . . : 192.168.101.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

C:\Users\Administrateur>ping 192.168.128.126

Envoi d'une requête 'Ping' 192.168.128.126 avec 32 octets de données :
Réponse de 192.168.128.126 : octets=32 temps<1ms TTL=128
Réponse de 192.168.128.126 : octets=32 temps<1ms TTL=128
Réponse de 192.168.128.126 : octets=32 temps<1ms TTL=128
Réponse de 192.168.128.126 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.128.126:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>
```

14. Ping serveur depuis Succursale secondaire

```
Administrateur : Invite de commandes

C:\Users\Administrateur>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::cd1f:5c3d:ee40:cfa6%11
    Adresse IPv4. . . . . : 192.168.128.130
    Masque de sous-réseau. . . . . : 255.255.255.224
    Passerelle par défaut. . . . . : 192.168.128.129

C:\Users\Administrateur>ping 192.168.128.126

Envoi d'une requête 'Ping' 192.168.128.126 avec 32 octets de données :
Réponse de 192.168.128.126 : octets=32 temps<1ms TTL=126
Réponse de 192.168.128.126 : octets=32 temps<1ms TTL=126
Réponse de 192.168.128.126 : octets=32 temps<1ms TTL=126
Réponse de 192.168.128.126 : octets=32 temps<1ms TTL=126

Statistiques Ping pour 192.168.128.126:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>
```

Page | 51

15. Ping imprimante depuis succursale secondaire

```
Administrateur : Invite de commandes

C:\Users\Administrateur>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::cd1f:5c3d:ee40:cfa6%11
    Adresse IPv4. . . . . : 192.168.128.130
    Masque de sous-réseau. . . . . : 255.255.255.224
    Passerelle par défaut. . . . . : 192.168.128.129

C:\Users\Administrateur>ping 192.168.128.125

Envoi d'une requête 'Ping' 192.168.128.125 avec 32 octets de données :
Réponse de 192.168.128.125 : octets=32 temps<1ms TTL=62
Réponse de 192.168.128.125 : octets=32 temps<1ms TTL=62
Réponse de 192.168.128.125 : octets=32 temps<1ms TTL=62
Réponse de 192.168.128.125 : octets=32 temps<1ms TTL=62

Statistiques Ping pour 192.168.128.125:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>
```

16. Ping serveur depuis télétravailleur

```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.16299.15]
(c) 2017 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::38b3:7d04:c903:8fc1%14
    Adresse IPv4. . . . . : 10.0.128.1
    Masque de sous-réseau. . . . . : 255.0.0.0
    Passerelle par défaut. . . . . :

Carte Ethernet Ethernet 3 :

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

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::c059:62ea:b511:cf69%7
    Adresse IPv4. . . . . : 192.168.228.2
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.228.1

C:\Users\Administrateur>ping 192.168.128.126

Envoi d'une requête 'Ping' 192.168.128.126 avec 32 octets de données :
Réponse de 192.168.128.126 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.128.126 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.128.126 : octets=32 temps<1ms TTL=127
Réponse de 192.168.128.126 : octets=32 temps<1ms TTL=127

Statistiques Ping pour 192.168.128.126:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\Administrateur>
```

Page | 52

17. Ping imprimante depuis télétravailleur

```
Administrateur : Invite de commandes

C:\Users\Administrateur>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::38b3:7d04:c903:8fc1%14
    Adresse IPv4. . . . . : 10.0.128.1
    Masque de sous-réseau. . . . . : 255.0.0.0
    Passerelle par défaut. . . . . :

Carte Ethernet Ethernet 3 :

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

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::c059:62ea:b511:cf69%7
    Adresse IPv4. . . . . : 192.168.228.2
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.228.1

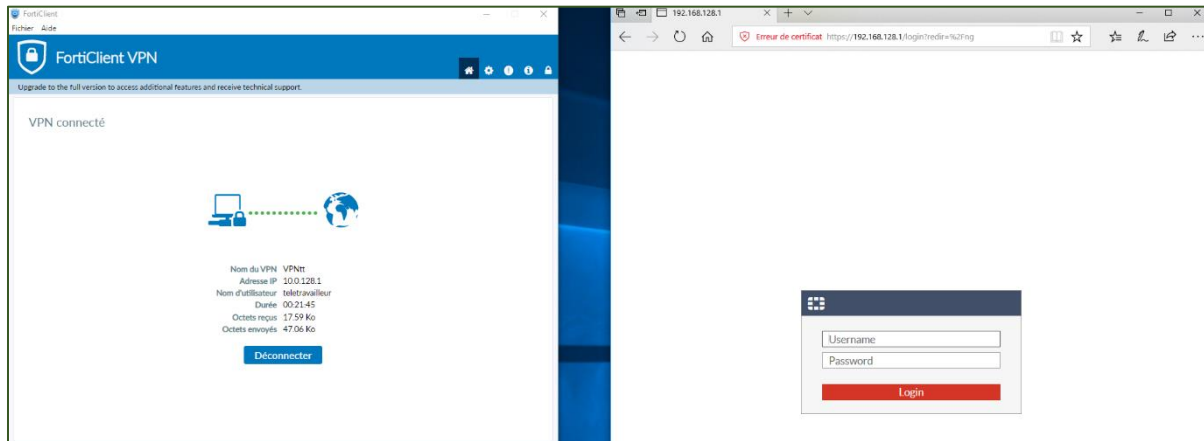
C:\Users\Administrateur>ping 192.168.128.125

Envoi d'une requête 'Ping' 192.168.128.125 avec 32 octets de données :
Réponse de 192.168.128.125 : octets=32 temps<1ms TTL=63
Réponse de 192.168.128.125 : octets=32 temps<1ms TTL=63
Réponse de 192.168.128.125 : octets=32 temps<1ms TTL=63
Réponse de 192.168.128.125 : octets=32 temps<1ms TTL=63

Statistiques Ping pour 192.168.128.125:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

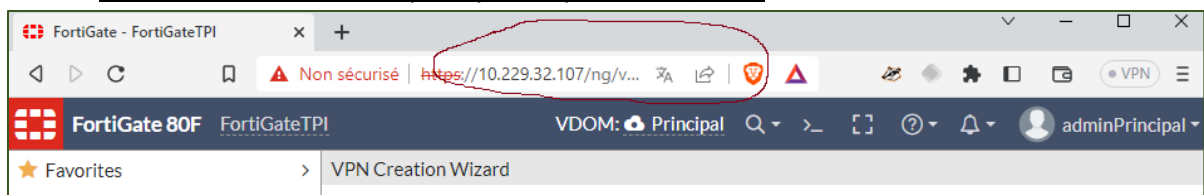
C:\Users\Administrateur>
```

18. Connexion via client VPN

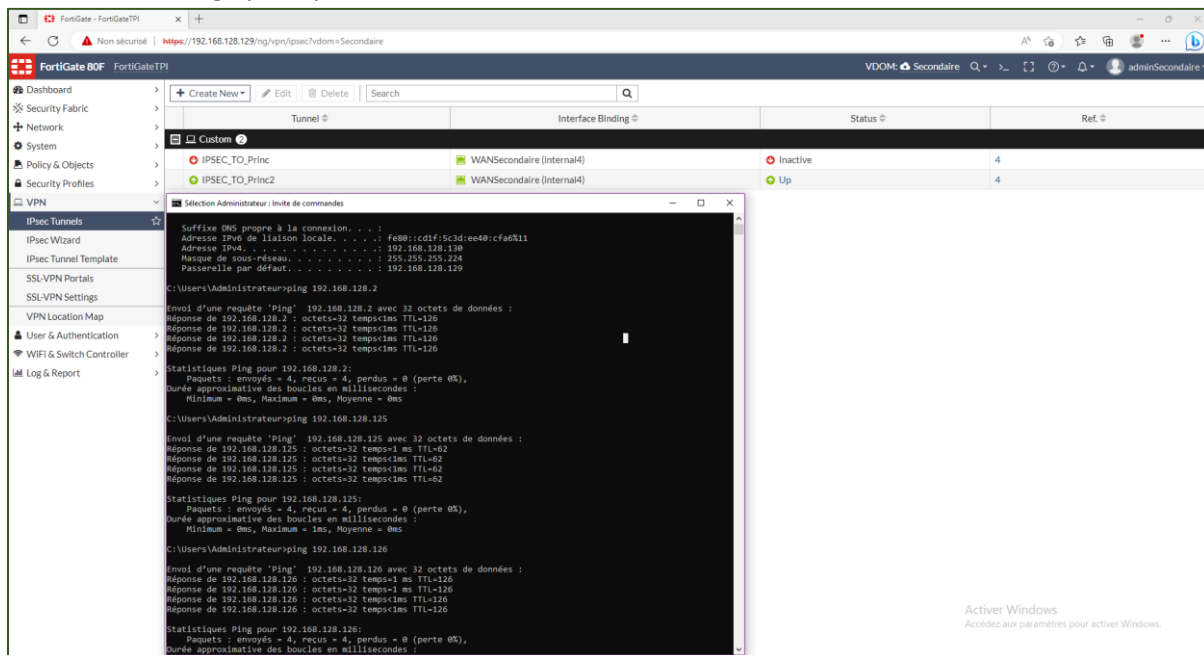


Page | 53

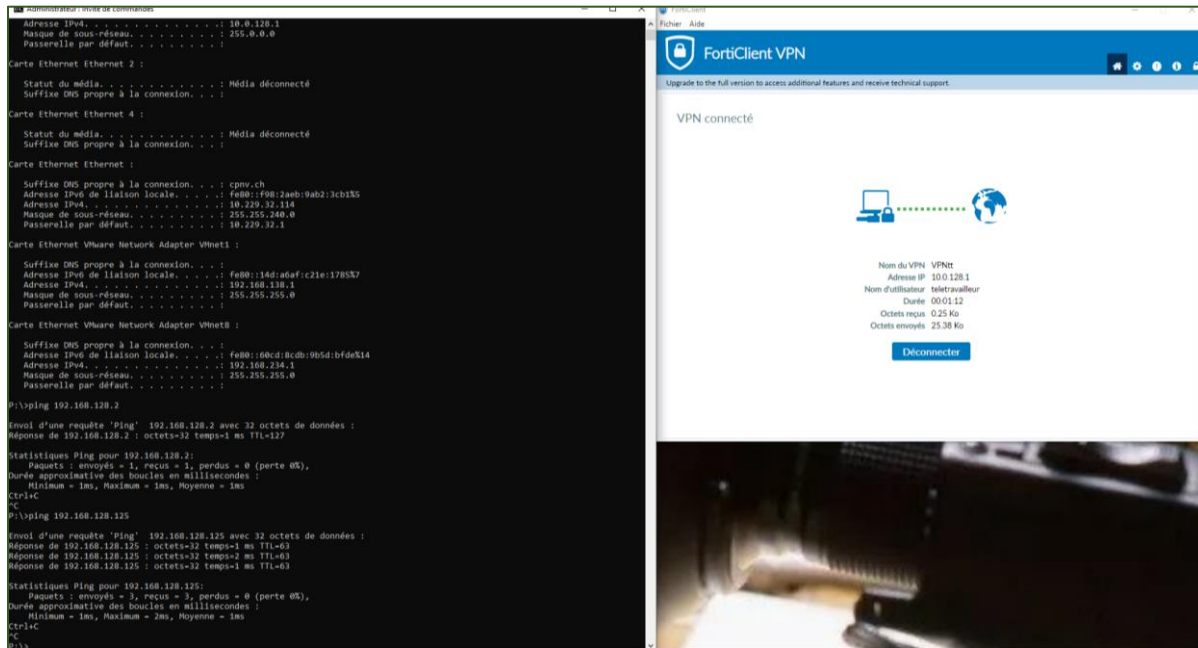
19. P2 Accès à l'interface Site principale depuis PC05 (C236)



20. P2 Connexion VPN site à site avec ping PC, ping serveur et ping imprimante de la succursale secondaire au siège principale



21. P2 Connexion VPN client à site depuis PC05



7.5 Sources

Titre	Source	Consultation
Définitions	https://www.larousse.fr/	02.05.2023
FortiOS-6.4.12-Administration_Guide.pdf	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/FortiOS-6.4.12-Administration_Guide.pdf	03.05.2023
Relier une entreprise à internet	I-CT146	03.05.2023
Pratique réseau	MA-23	03.05.2023
Mettre en service des composants réseaux	I-CT129	03.05.2023
IPSec vs SSLVPN Fortigate	https://www.onlc.com/blog/comparing-ipsec-vs-ssl-vpns/	03.05.2023
FortiOS-6.4.12-CLI-References.pdf	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/FortiOS-6.4.12-CLI_Reference.pdf	03.05.2023
Mise en service d'un pare-feu Fortinet	Travail de pré-TPI, disponible sur demande	04.05.2023
Site officiel ICT Formation professionnelle	https://www.modulbaukasten.ch/module/146/3/fr-FR?title=Relier-une-entreprise-%C3%A0-Internet	04.05.2023
Application matérielle	https://fr.wikipedia.org/wiki/Application_mat%C3%A9rielle	04.05.2023
Question Mr. Varela	Question à Mr. Varela par rapport au FortiGate/routeur: le fortigate sert de routeur! (comme pour la structure du CPNV)	04.05.2023
FortiGate : Practical Guidance and Hands-On Labs	https://pressbooks.bccampus.ca/fortigatefirewall/	09.05.2023
Virtual domains	https://www.fortinetguru.com/2016/12/virtual-domains/	09.05.2023
Fonctionnement VPN	Laurent Yaggi	10.05.2023
VPN Site à site	https://www.youtube.com/watch?v=meH6ADWJas8	15.05.2023
Cisco Catalyst 3500 series	https://community.cisco.com/t5/switching/switch-to-behave-as-a-router/td-p/2678676	17.05.2023
Plan de réseau CPNV	Sylvain Fasola	23.05.2023
VTP	https://www.cisco.com/c/fr_ca/support/docs/lan-switching/vtp/10558-21.pdf	23.05.2023
Client VPN pour téléchargement	https://www.fortinet.com/support/product-downloads	23.05.2023
Limitations system	https://docs.fortinet.com/max-value-table	26.05.2023
Définitions	https://www.wikipedia.org/	31.05.2023

7.6 Glossaire

Terme	Définition
Adresse IP	Internet Protocol: numéro d'identification attribué à chaque périphérique relié à un réseau informatique.
AES256	Advanced Encryption Standard 256 : algorithme de chiffrement.
Appliance	Application matérielle, appareil informatique spécifiquement conçu pour exécuter un logiciel destiné à fournir une ressource informatique distincte.
CLI	Commande Ligne Interface : interface en ligne de commande / en opposition à l'interface graphique.
DH	Diffie-Hellman Groups: détermine la force de la clé utilisée dans un processus d'échange de clé cryptographique.
DHCP	Dynamic Host Configuration Protocol : protocole de configuration dynamique des hôtes. Sert à distribuer automatiquement des adresses IP.
GUI	Graphical User Interface : interface graphique / en opposition à la ligne de commande.
IPSec	Internet Protocol Security: ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP.
LAN	Local Area Network: réseau local.
Modèle OSI	Open Systems Interconnection: norme de communication en réseau.
Ping	Commande servant à vérifier les connexions établies.
SHA256	Secure Hash Algorithm 256 : fonction de hachage.
Slp	Service Informatique pédagogique : service informatique du CPNV.
SSL	Secure Sockets Layer : protocole de sécurisation des échanges par réseau informatique, notamment par internet.
STP	Spanning Tree Protocol : protocole réseau de niveau 2 permettant de déterminer une topologie sans boucle.
Tracert	Commande servant à suivre les chemins des paquet IP.
VDOM	Virtual Domain: Pare-feu virtuel.
WAN	Wide Area Network: réseau étendu.

7.7 Journal de travail

Date	Sem	Activité	Heures	Remarques
02.05.2023	18	5.5 Administratif	1:00	Prise de connaissance du cahier des charges
02.05.2023	18	5.1 Documentation	1:00	Préparation de la documentation
02.05.2023	18	5.5 Administratif	1:00	Séance avec Mr. Wolf
02.05.2023	18	1.1 Planification	4:10	Préparation de la planification initiale
03.05.2023	18	5.2 Journal de travail	0:30	Mise à jour journal de travail et correction document planification (problème avec des formules)
03.05.2023	18	1.4 Adressage IP	1:30	Recherches adressage IP
03.05.2023	18	1.2 Recherches	1:00	Recherches VPN
03.05.2023	18	5.5 Administratif	0:30	Set-up stations salle C111 (réservation pc, installation HDD, vérification fonctionnement des ordinateurs, et périphériques).
03.05.2023	18	1.2 Recherches	0:45	Recherches VPN suite
04.05.2023	18	5.5 Administratif	0:30	Administratif divers
04.05.2023	18	5.1 Documentation	1:30	Mise à jour
04.05.2023	18	1.2 Recherches	0:45	Recherches FortiGate
04.05.2023	18	1.2 Recherches	1:30	Recherches cisco catalyste 3560 + cisco 1900 series
04.05.2023	18	1.2 Recherches	1:30	Rafraîchissement mémoire du module 146
04.05.2023	18	5.2 Journal de travail	0:15	Mise à jour journal de travail
08.05.2023	19	1.4 Adressage IP	0:30	Création de réseaux tests sur packet-tracer pour valider les plages IP créées
08.05.2023	19	2.1 Création réseau siège principal	2:00	Configuration PC et FortiGate 80F
08.05.2023	19	4.1 Tests réseau siège principal	0:30	IP attribuées selon plan, et pings
08.05.2023	19	2.2 Création VMs siège principal (serveur, client * 2)	1:00	Installé sur machines physique, pas sur VM, selon changement du 03.05.2023
08.05.2023	19	4.2 Tests système siège principal	0:30	Les OS fonctionnent selon les attentes
08.05.2023	19	2.4 Implémentation pare-feu siège principal	1:00	Implémentation du pare-feu
09.05.2023	19	2.5 Création réseau succursale 2	1:00	
09.05.2023	19	2.6 Création VMs succursale 2	1:00	Installé sur machines physique, pas sur VM, selon changement du 03.05.2023
09.05.2023	19	4.3 Tests réseau succursale 2	0:30	IP attribuées selon plan, et pings
09.05.2023	19	4.4 Tests système succursale 2	0:30	IP attribuées selon plan, et pings
09.05.2023	19	5.5 Administratif	0:30	Visite avec M. Varela du pare-feu FortiGate de l'école.
09.05.2023	19	5.5 Administratif	0:30	J'ai réalisé que mon approche de création de sous-réseaux employée pendant mon pré-tpi, ne permet pas une implémentation de vpn site à site, par contre, une voie non explorée car inconnue: les Virtual Domains, eux permettent le site à site.
09.05.2023	19	1.2 Recherches	2:00	VDOM et Fortigate
09.05.2023	19	5.1 Documentation	1:00	Mise à jour: ajouts divers
09.05.2023	19	5.2 Journal de travail	0:10	Mise à jour
10.05.2023	19	2.3 Création serveur VPN siège principal	2:00	Création d'adresse, du tunnel et de la table de routage
10.05.2023	19	1.5 Règles de pare-feu	1:00	Approfondissement des connaissances
10.05.2023	19	2.4 Implémentation pare-feu siège principal	1:00	Création des règles nécessaires
11.05.2023	19	2.7 Création client VPN succursale 2	2:00	Création d'adresse, du tunnel et de la table de routage
11.05.2023	19	1.5 Règles de pare-feu	1:00	Approfondissement des connaissances
11.05.2023	19	2.8 Implémentation pare-feu succursale 2	1:00	Création des règles nécessaires

11.05.2023	19	5.6 Temps flexible	1:00	Problème n°1: la perte de l'accès au GUI du fortinet, sans raison connue. Se loguer sur d'autre port, et même le reset complet de l'appareil n'a pas résolu le problème. Je l'ai résolu en me loguant grace à la prise serial et en utilisant la CLI pour rétablir le gui.
11.05.2023	19	5.6 Temps flexible	1:00	Problème n°2: Les accès administrateurs des VDOM 1 et ont simplement cessés de fonctionner, pendant une heure. C'est un problème quasi-similaire à ce que j'avais rencontré pendant mon pré-tpi. Pas de réponse connue, il faut attendre que cela passe ou effectuer un reset physique de l'appareil.
11.05.2023	19	5.2 Journal de travail	0:35	Mise à jour
11.05.2023	19	1.1 Planification	0:35	Planification pour semaine 3
15.05.2023	20	4.5 Tests VPN site-to-site	1:30	
15.05.2023	20	4.6 Tests pare-feu site-to-site	1:30	
15.05.2023	20	1.2 Recherches	1:00	
15.05.2023	20	4.14 Tests généraux	1:30	
16.05.2023	20	1.3 Elaboration des stratégies de test	1:00	
16.05.2023	20	1.2 Recherches	1:00	
16.05.2023	20	4.14 Tests généraux	2:30	
16.05.2023	20	2.9 Création réseau télétravailleur	1:00	Nos routeurs n'ayant que deux port, il est décidé d'utilisé un switch routable afin d'avoir les 3 ports nécessaire à l'ajout de la partie client
16.05.2023	20	5.1 Documentation	1:00	Travail sur schéma physique et logique + divers
16.05.2023	20	5.2 Journal de travail	0:45	Mise à jour
17.05.2023	20	5.6 Temps flexible	4:00	Journal de travail présente un blanc pour cette journée.
22.05.2023	21	5.5 Administratif		Absence décès, compensation le 26.05.2023
23.05.2023	21	2.10 Création VM télétravailleur	1:00	Amenagement du poste de travail du télétravailleur
23.05.2023	21	2.11 Création client VPN télétravailleur	1:00	Téléchargement et installation FortiClientVPN
23.05.2023	21	4.7 Tests système télétravailleur	0:30	Succès
23.05.2023	21	4.8 Tests VPN client-to-site	1:00	Ne fonctionnait pas, ai essayé plusieurs correction et au final c'est la consultation des log vpn du fortigate qui indique un problème de phase 2. Donc mes protocoles d'authentification et d'encryption ne correspondent pas entre la configuration du client et celle du pare-feu. Après correction, le client se connecte.
23.05.2023	21	1.2 Recherches	1:00	Recherches Spanning Tree Protocol
23.05.2023	21	1.2 Recherches	1:00	Recherches réseau du CPNV
23.05.2023	21	5.1 Documentation	1:40	Mise au propres de différents éléments qui rejoindront la présentation: table de routage, plan réseau, tests. Arrivant au bout du projet, je vais commencer à mettre les différentes pièces dans le document final.
24.05.2023	21	4.14 Tests généraux	1:00	Test de fonctionnement du site2site, client2site, divers pings et tracerts
24.05.2023	21	5.1 Documentation	3:00	Screenshots et logs de toute la partie phase 1 et retranscription au format numérique des notes manuelles.
25.05.2023	21	3.4 Implémentation physique du pare-feu	1:00	Branchement du pare-feu sur réseau de l'école, cablage du site principal et succursale secondaire
25.05.2023	21	3.1 Implémentation/adaptation serveur VPN siège principal	1:00	Installation VMWare + windows server 2016. Attribution ip fixe selon cahier des charges. Création d'un tunnel adapté au réseau du cpnv
25.05.2023	21	3.2 Implémentation/adaptation client VPN succursale 2	1:00	Création du tunnel adapté au réseau du cpnv

25.05.2023	21	3.3 Implémentation/adaptation client VPN télétravailleur	1:00	Installation FortiClient sur PC05 en salle C236, configuration.
25.05.2023	21	4.10 Tests VPN site-to-site 2ème temps	1:00	Pings divers entre succursale principale et site secondaire
25.05.2023	21	4.11 Tests VPN client-to-site 2ème temps	1:00	Pings depuis salle de classe à destination du site principal (serveur, imprimante, PC)
25.05.2023	21	4.14 Tests généraux	1:00	Tests divers
26.05.2023	21	5.1 Documentation	5:35	Remplacement du 22.05
30.05.2023	22	5.1 Documentation		Absence enterrement, compensation le 31.05.2023
31.05.2023	22	5.1 Documentation	7:10	Remplacement du 30.05 et rendu TPI

7.8 Archives du projet

-Version digital envoyée le 31.05.2023 à 16:50

bw-tpi@hotmail.com

junior.mbuyi@epfl.ch

francis.varela@cpnv.ch

-Version imprimée pour chef de projet remise au chef de projet le 01.06.2023

-Version imprimée pour expert n°1 Mr. Wolf remise au secrétariat pour envoi le 01.06.2023