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

Table des matières

[1 Analyse préliminaire 4](#_Toc136293068)

[1.1 Introduction 4](#_Toc136293069)

[1.2 Objectifs 4](#_Toc136293070)

[1.3 Cahier des charges 4](#_Toc136293071)

[1.4 Module 146 4](#_Toc136293072)

[1.5 Planification initiale 5](#_Toc136293073)

[2 Analyse / Conception 6](#_Toc136293074)

[2.1 Méthode de travail 6](#_Toc136293075)

[2.2 Organisation du travail 7](#_Toc136293076)

[2.3 Informations générales 7](#_Toc136293077)

[2.3.1 Définitions 7](#_Toc136293078)

[2.3.2 Fortinet 8](#_Toc136293079)

[2.3.3 Réseau CPNV 9](#_Toc136293080)

[2.4 Concept 10](#_Toc136293081)

[2.4.1 Déroulement du projet 10](#_Toc136293082)

[2.5 Dossier de conception 10](#_Toc136293083)

[2.5.1 Liste du matériel utilisé : 10](#_Toc136293084)

[2.5.2 Schéma : 11](#_Toc136293085)

[2.5.3 Internet 11](#_Toc136293086)

[2.5.4 Adressage IP 11](#_Toc136293087)

[2.5.5 Table de routage 12](#_Toc136293088)

[2.6 Stratégie de test 12](#_Toc136293089)

[2.7 Risques techniques 12](#_Toc136293090)

[2.7.1 Connaissances limitées en VPN 12](#_Toc136293091)

[2.7.2 Connaissances limitées en pare-feu 13](#_Toc136293092)

[2.7.3 Complexités liées au réseau de l'école et à ses contraintes 13](#_Toc136293093)

[2.7.4 Connaissances non-acquises pendant le pré-TPI 13](#_Toc136293094)

[2.8 Planification finale 14](#_Toc136293095)

[3 Réalisation 16](#_Toc136293096)

[3.1 Dossier de réalisation 16](#_Toc136293097)

[3.1.1 1er temps 16](#_Toc136293098)

[3.1.2 2ème temps 24](#_Toc136293099)

[3.2 Description des tests effectués 24](#_Toc136293100)

[3.2.1 1er temps 24](#_Toc136293101)

[3.2.2 2ème temps 24](#_Toc136293102)

[3.3 Erreurs restantes 25](#_Toc136293103)

[3.4 Nombre maximal d’implémentations 25](#_Toc136293104)

[3.4.1 VDOM 25](#_Toc136293105)

[3.4.2 VPN 25](#_Toc136293106)

[3.5 Liste des documents fournis 26](#_Toc136293107)

[4 Conclusions 26](#_Toc136293108)

[4.1 Objectifs atteints / non-atteints 26](#_Toc136293109)

[4.2 Points positifs / négatifs 26](#_Toc136293110)

[4.2.1 Négatif 26](#_Toc136293111)

[4.2.2 Positif 26](#_Toc136293112)

[4.3 Difficultés particulières 26](#_Toc136293113)

[4.4 Améliorations 27](#_Toc136293114)

[4.5 Retour personnel 27](#_Toc136293115)

[5 Remerciements 27](#_Toc136293116)

[6 Table des illustrations 27](#_Toc136293117)

[7 Annexes 27](#_Toc136293118)

[7.1 Résumé du rapport du TPI 27](#_Toc136293119)

[7.2 Cahier des charges 28](#_Toc136293120)

[7.3 Identification du module 32](#_Toc136293129)

[7.4 Manuel de tests 34](#_Toc136293130)

[7.5 Sources – Bibliographie 34](#_Toc136293131)

[7.6 Glossaire 34](#_Toc136293132)

[7.7 Journal de travail 34](#_Toc136293133)

[7.8 Archives du projet 34](#_Toc136293134)

# Analyse préliminaire

## 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).*"

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".

## 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"

-station "Télétravailleur"

-pare-feu, VDOMs, règles de pare-feu et table de routage

-mise en place d'une partie "internet"

-tunnel site à site

-FortiClient VPN

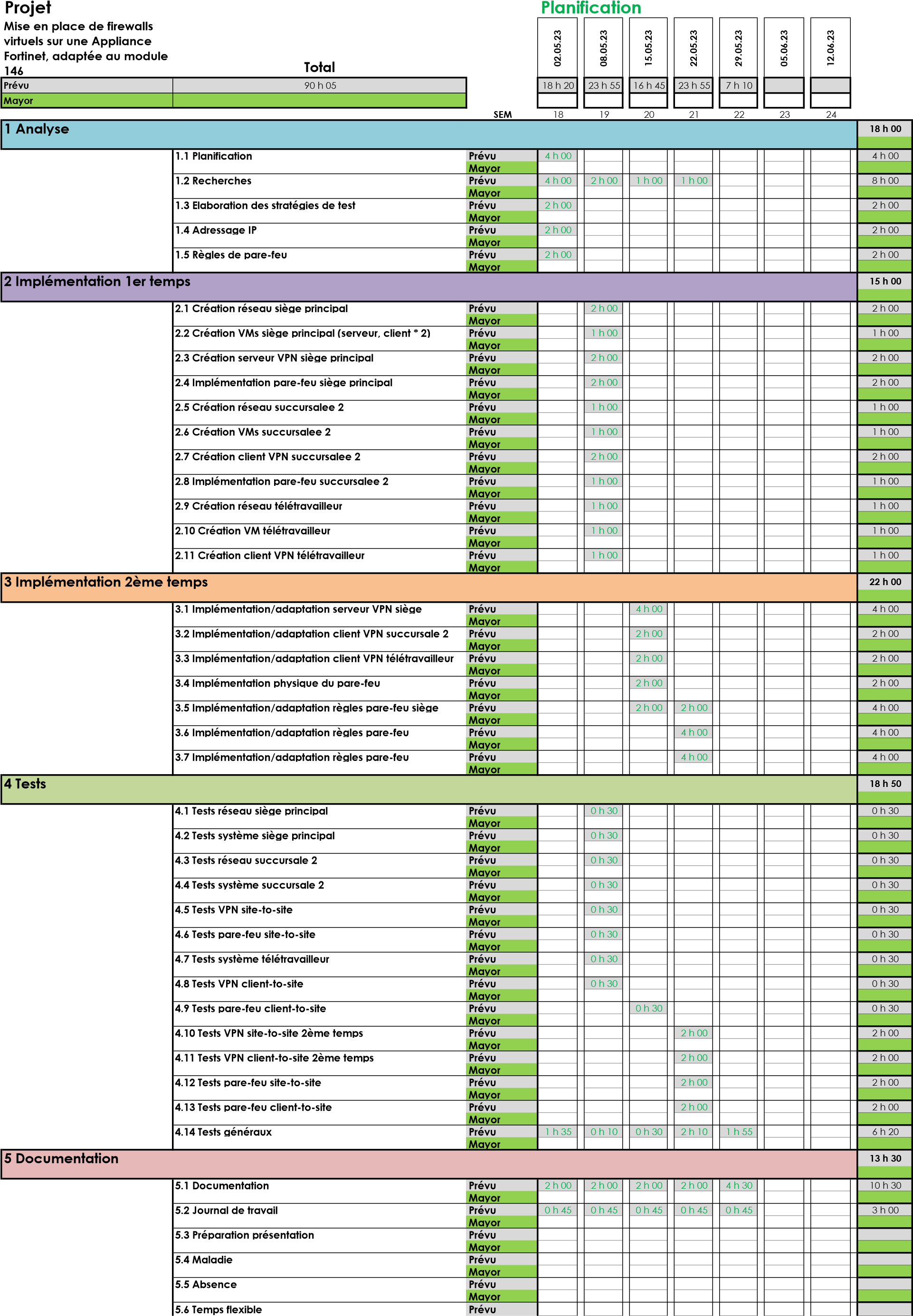
## Cahier des charges

Le cahier des charges est disponible à l'annexe 7.2 PAGE X

## 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 ficher d'identification du module est disponible à l'annexe 7.3 PAGE X

## 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.

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 ma planification initiale notamment sur la partie : "2 Implémentation 1er temps". Pour des raisons de temps et de respect d'esprit d'une planification initiale, j'ai pris la décision de ne pas modifier ladite planification.

# Analyse / Conception

## 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 linaire.

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](http://www.tpivd.ch), est bâtie sur ce modèle en cascade.

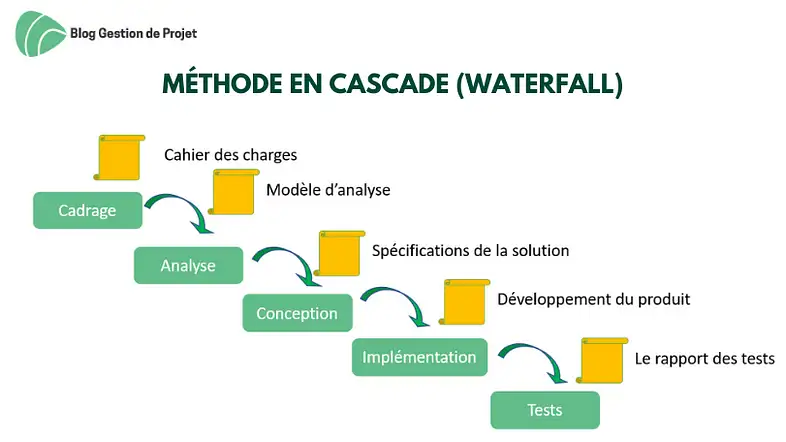


Figure 1 méthode en cascade. Source blog-gestion-de-projet.com

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.

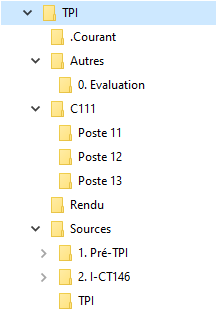
## Organisation du travail

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.

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 :

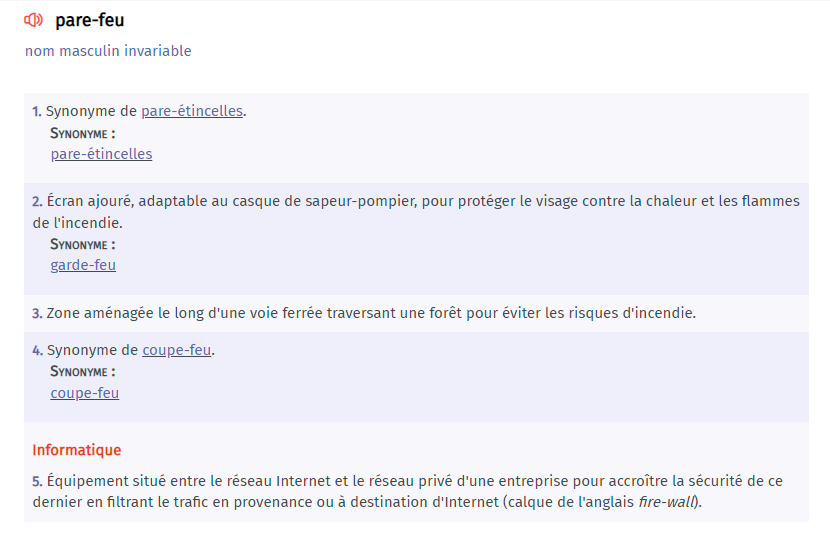
[http://damienmayorpmme.quickconnect.to](http://damienmayorpmme.quickconnect.to/)

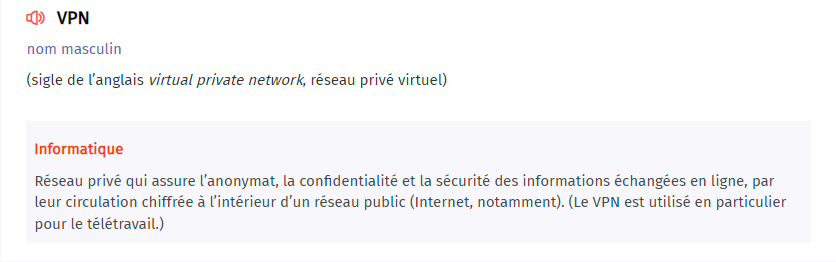
En ce qui concerne l'organisation de mes données, voici la nomenclature choisie :



## Informations générales

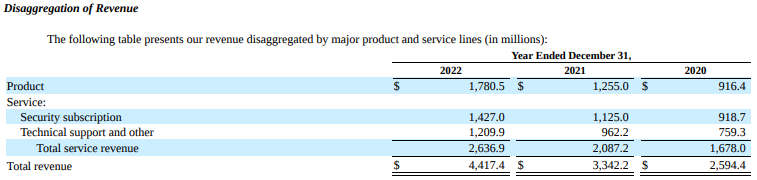
### Définitions





### Fortinet

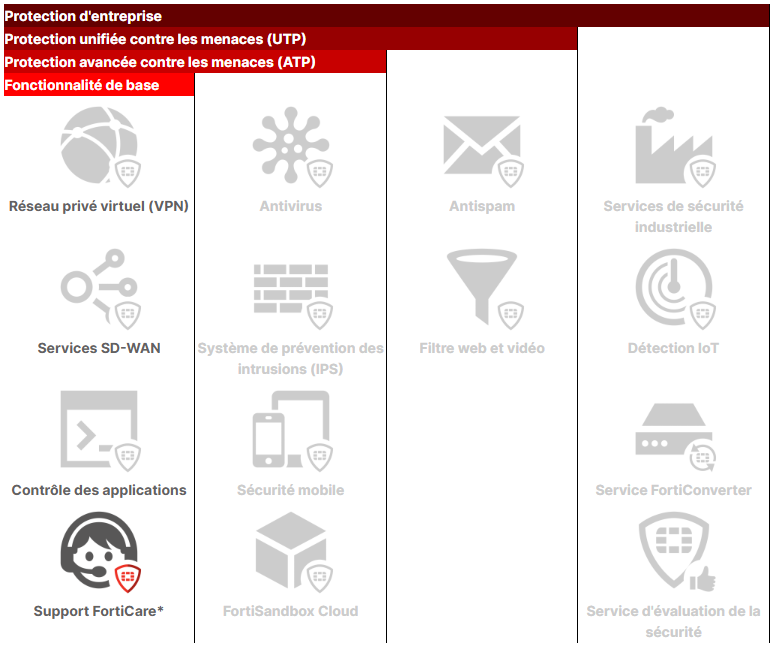
Fortinet, Inc. est une entreprise américaine fondée en 2000, basée à Sunnyvale en Californie et qui compte 13'000 employés. Cette société développe des appareils et des logiciels pour la sécurité de l'information tels que: pare-feu, programmes antivirus ou encore des systèmes de détection d'intrusion.



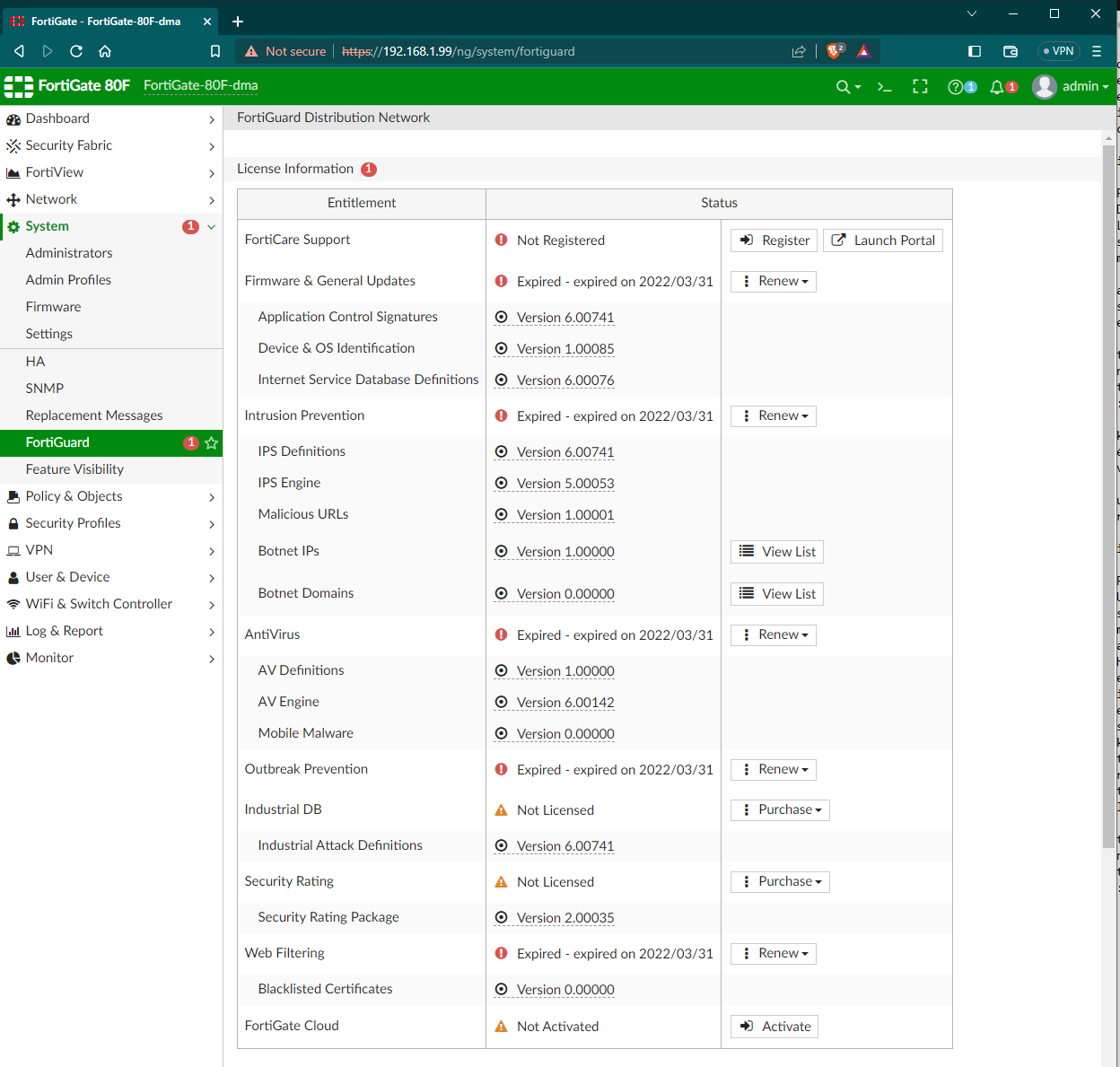
Avec des revenus supérieurs à 4 milliards de dollars, environ 60% viennent de la vente de services et les 40% restant proviennent de la vente de matériel.

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.

Voici en image ce à quoi donne droit les différents niveaux d'abonnements Fortinet : pour référence nous avons droit aux fonctionnalités de base.

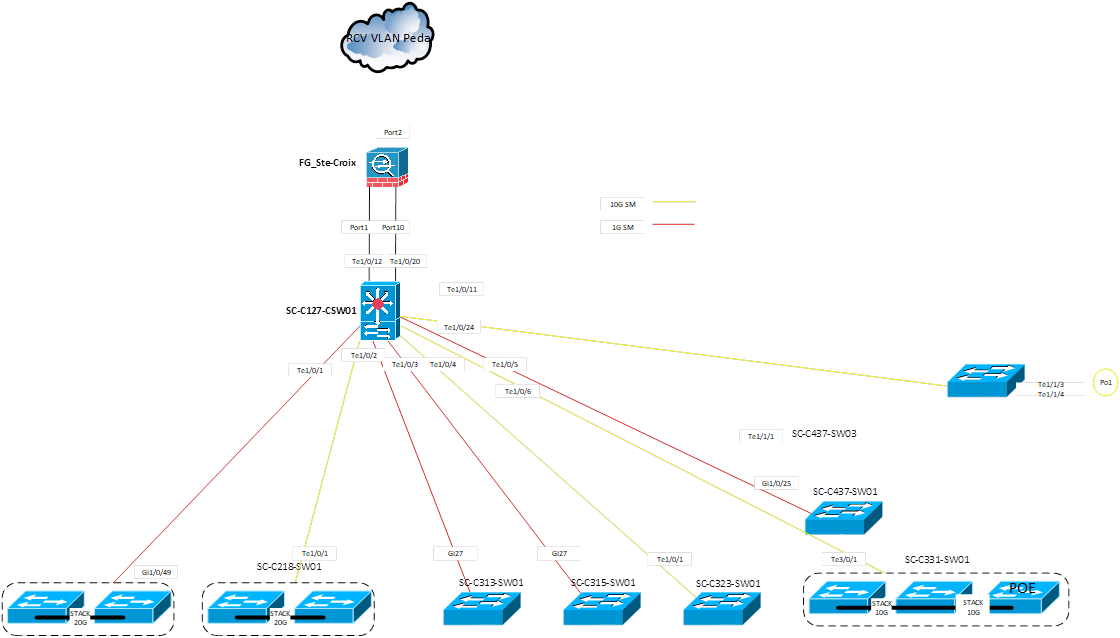


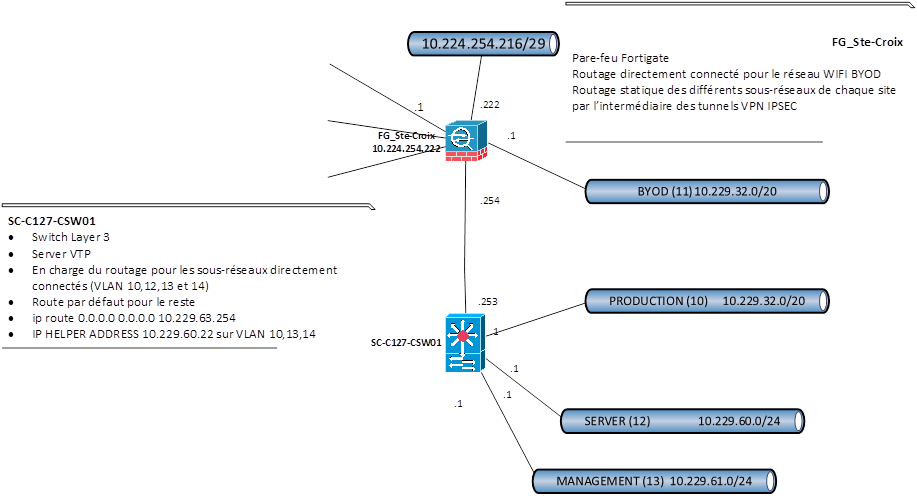
Ce tableau est confirmé par une capture d'écran de la section FortiGuard du FG-80F :



### Réseau CPNV

Nécessaire pour la seconde phase du projet :





## Concept

### 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-feux 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 travaille 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

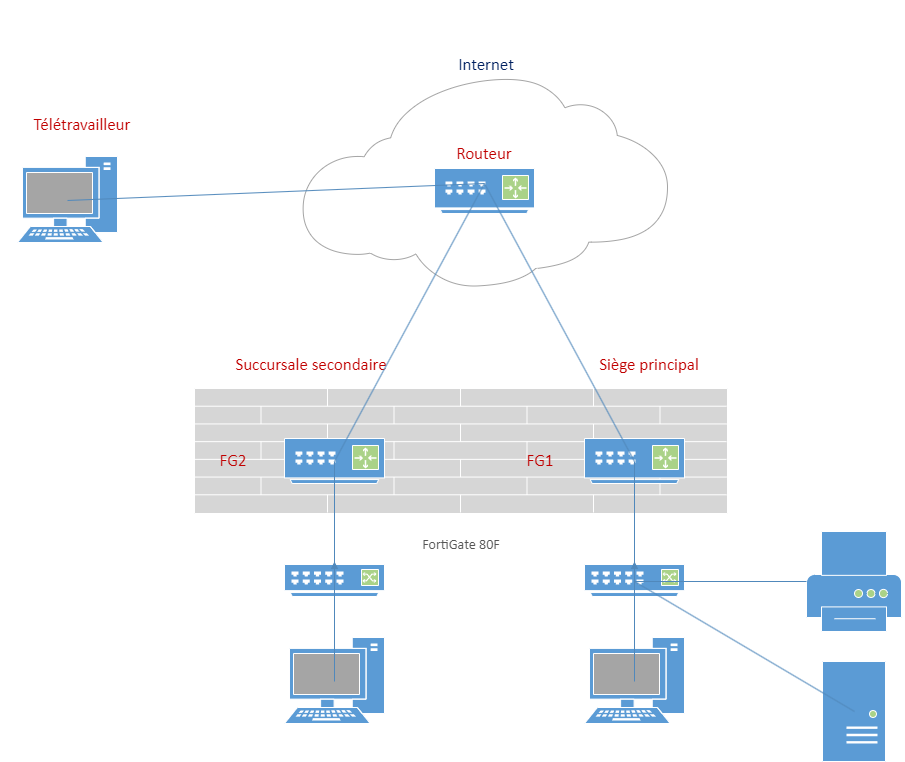
## Dossier de conception

### 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.

### Schéma :



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.

### Internet

Comme indiqué par le schéma trouvé au point 2.8.2, internet sera simulé par un routeur XXX

### 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** |
| *Site principal* | | | |
| 192.168.128.0/25 | 192.168.128.1/25 | 192.168.128.2-126/25 | 192.168.128.127/25 |
| *Succursale secondaire* | | | |
| 192.168.128.128/27 | 192.168.128.129/27 | 192.168.128.130-158/27 | 192.168.128.159/27 |
| *Télétravailleurs* | | | |
| 192.168.228.0/24 | 192.168.228.1/24 | 192.168.228.2-254/24 | 192.168.228.255/24 |
| *Tunnel pour télétravailleurs* | | | |
| - | - | 10.0.128.1-10/8 | - |

### Table de routage

|  |  |  |  |
| --- | --- | --- | --- |
| **Réseau destination** | **Masque de sous-réseau** | **Via** | **Interface FortiGate** |
| *Router Cisco 1900 (1.1)* | | | |
| 192.168.128.0 | 255.255.255.128 | 10.0.0.3 | - |
| 192.168.128.128 | 255.255.255.224 | 172.16.0.4 | - |
| *Switch-Routeur Cisco 3560 (1.2)* | | | |
| 192.168.128.0 | 255.255.255.128 | 10.0.0.3 | - |
| 192.168.128.128 | 255.255.255.224 | 172.16.0.4 | - |
| *VDOM Siège principal* | | | |
| 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 |
| *VDOM Succursale secondaire* | | | |
| 10.0.0.0 | 255.0.0.0 | 172.16.0.1 | WANSecondaire |
| 192.168.128.0 | 255.255.255.128 | - | IPSEC\_TO\_Princ |

## 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. Tous les tests 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 faire les tests 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.

La liste complète des tests, de leurs résultats ainsi que les preuves sont disponibles dans les annexes.

**Edit :** Au final, tant mes camardes et moi nous sommes retrouvés à court de temps. Les tests n'ont donc été réalisé que par moi.

## Risques techniques

### 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. Les connaissances 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.

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

### 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.

### 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.

Je me renseigne sur le protocole "Spanning Tree".

### Connaissances non-acquises pendant le pré-TPI

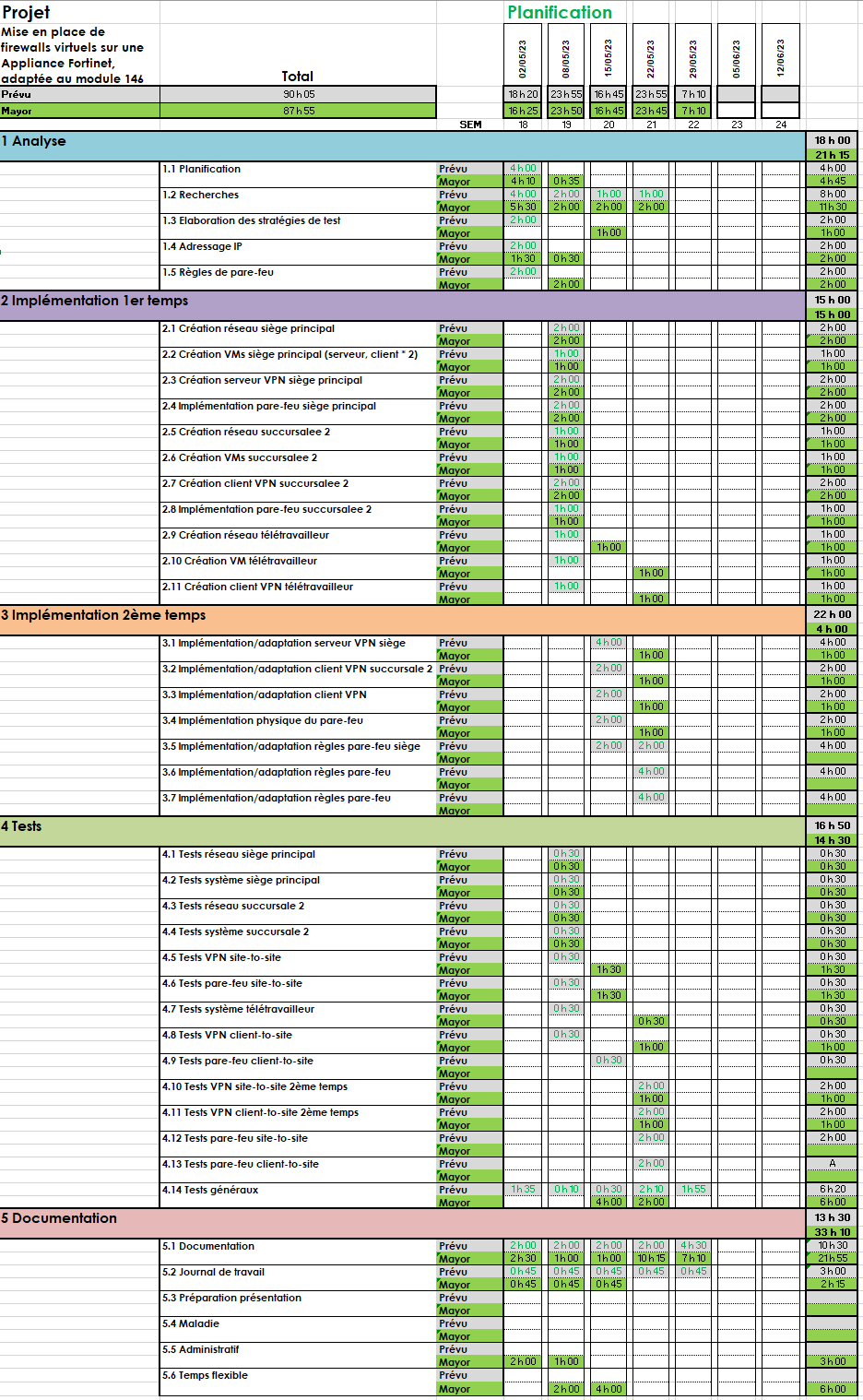
Ce point m'était inconnu au début du projet est c'est révélé être très important. En effet, ma planification initiale ainsi que la première semaine et demie de mon TPI s'est déroulée avec une solution ne permettant l'implémentation de firewalls virtuels.

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'apparait 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 à suffit à résoudre ce problème. Il aurait été nécessaire de faire un débrief complet entre le pré-TPI et le TPI pour s'assurer que cette connaissance fondamentale ait bien été apprise.

## Planification finale



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

Ces différences s'expliquent très facilement : l'implémentation du 2ème 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.

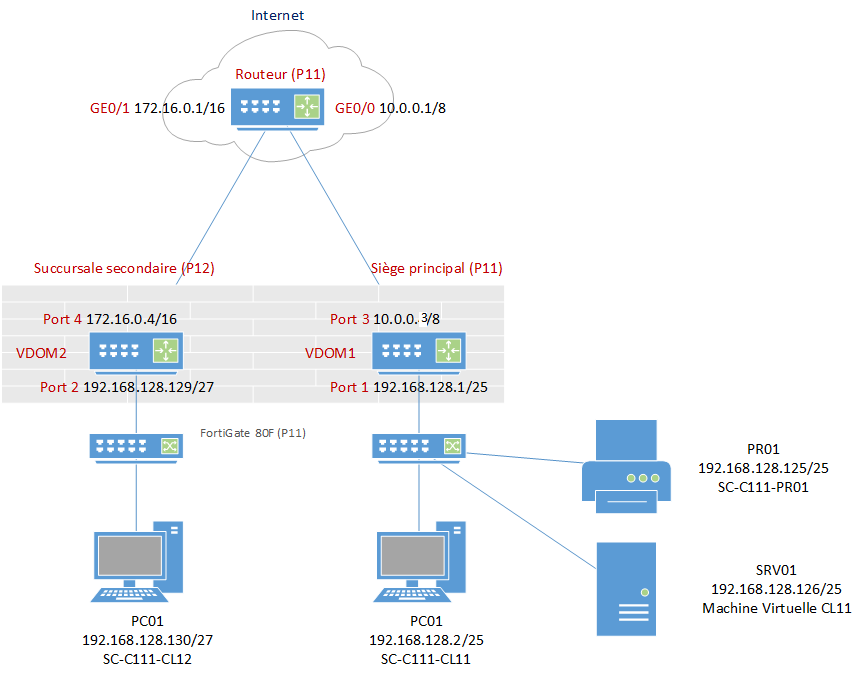
Une fois cette deuxième implémentation faite, tout le temps restant est passé dans la documentation.

# Réalisation

## Dossier de réalisation

### 1er temps

**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.



#### PC11 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

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

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

#### Firewall

Ouvrir browser 192.168.1.99

Username : admin

Password : (vide)

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

Se connecter

System : Settings

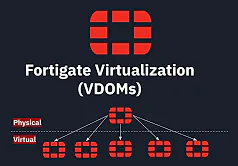
Time zone : GMT+1:00

Sync interval : 1

Apply

#### 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.



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

Dans le coin supérieur droite du GUI, clicker 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 disparaitre.

**Root** accueil 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

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

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

WHY PROF\_ADMIN?

Création des administrateurs

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

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

EXPLIQUER REGLES DE BASE

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

: 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

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

: 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 : WANSecondaire

OK

#### 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*

#### PC12 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

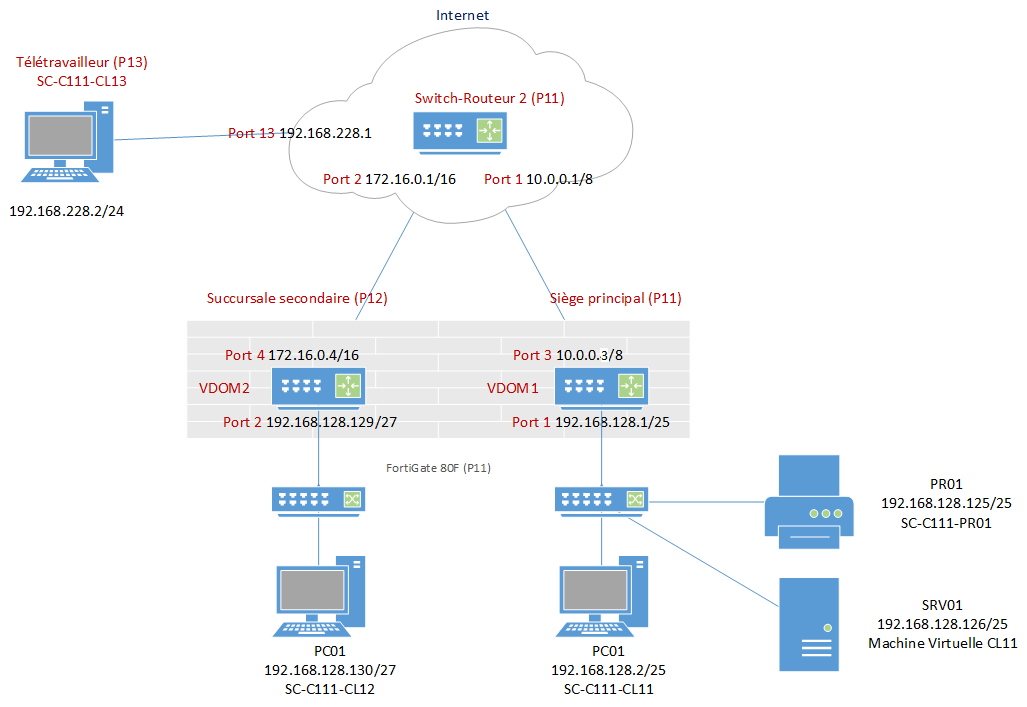
Relier le port Ethernet du PC au port 1 du switch Netgear

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

#### Tunnel site-à-site

Création du tunnel

**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*



#### 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*

#### 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

#### Tunnel client-à-site

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

#### FortiClient VPN

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

Installer FortiClient VPN

Configuration VPN:

VPN : VPN IPsec

Nom de la connexion : VPNtt

Passerelle distante : 10.0.0.3

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

Paramètres avancés

Se connecter:

Lancer l'application FortiClient VPN

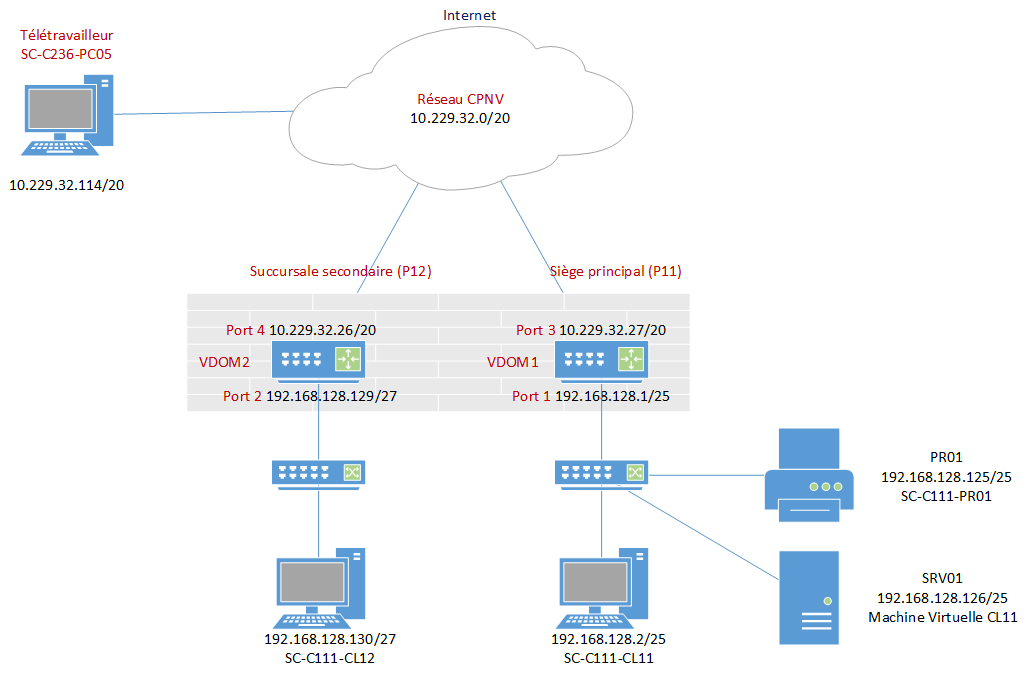
Nom du VPN : VPNtt

Nom d'utilisateur : teletravailleur

Mot de passe : Pa$$w0rd

Connecter

### 2ème temps



Pas oublier de passer de fixe à DHCP dans les interfaces

## Description des tests effectués

Voir annexe 7.4 PAGE X Manuel de tests

### 1er temps

### 2ème temps

Pour chaque partie testée de votre projet, il faut décrire :

• les conditions exactes de chaque test

• les preuves de test (papier ou fichier)

• tests sans preuve: fournir au moins une description

## Erreurs restantes

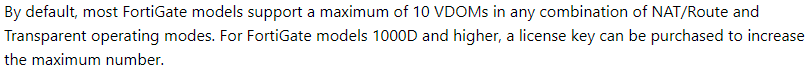
Toutes les demandes du cahier des charges ont été satisfaites. Néanmoins des améliorations sont possibles et ont été formulées au point 4.4

## Nombre maximal d’implémentations

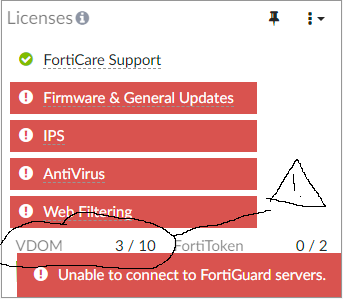
Sans tenir compte des performances, il existe deux facteurs qui pourraient impacter le nombre d’implémentations maximal :

### VDOM

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



L’interface du FortiGate confirme cette limitation :



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.

### 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.

## Liste des documents fournis

Lister les documents fournis au client avec votre produit, en indiquant les numéros de versions

• le rapport de projet

• le manuel d'Installation (en annexe)

• le manuel d'Utilisation avec des exemples graphiques (en annexe)

• autres…

# Conclusions

## 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.

## Points positifs / négatifs

### Négatif

J'ai trouvé très dur que la validation de la formation se joue sur ce seul projet. Evidemment, on ne peut se présenter à son travail de TPI si on ne satisfait à certaines exigences au niveau des notes. Mais qu'un TPI qui se passe mal puisse avoir un tel impact sur un formation amène une quantité de stress non négligeable et très désagréable.

Ceci dit, je suis conscient d'un être cas particulier par rapport à la majorités des élèves, même en ne prenant en compte que les élèves de FPA. Un échec dans mon cas aurait signifié la fin de ma tentative de reconversion.

Comme le rapporte ce document, tout ne ce n'est pas passé de la manière la plus douce possible, soit par des erreurs de ma part, soit par des détails manqués par le chef de projet et/ou moi-même. La réussite de la réalisation du projet c'est jouée sur les derniers jours du TPI et notamment grâce à une phase 2 qui n'a rencontrée aucuns problèmes.

Nous, les élèves, savons qu'il est tout à fait possible de réussir son TPI sans forcément réussir l'implémentation du projet. Ceci dit, la dynamique s'en trouve complétement changée.

### Positif

La satisfaction, l’intérêt pour les firewalls

## Difficultés particulières

-raté le vdom

-virtuel/physique

-abstraction

-routing table

-erreur plage ip

## Améliorations

-ip fixes recue du cpnv, imprimante fix fg, pc dhcp, serveur fix

-optimisation des règles du pare-feu

-montage rack

-review par quelqu’un de plus experimenté

## Retour personnel

# Remerciements

Merci à Madame Nicole Mayor pour les corrections de l'orthographe et la grammaire de ce document, tout en ayant des compétences limitées au niveau informatique.

# Table des illustrations

[Figure 1 méthode en cascade. Source blog-gestion-de-projet.com 6](#_Toc134102894)

[Figure 2 Nomenclature fichiers 7](#_Toc134102895)

# Annexes

## Résumé du rapport du TPI

1.

2.

3.

## Cahier des charges

**1 INFORMATIONS GENERALES**

|  |  |  |
| --- | --- | --- |
| Candidat : | Nom : **MAYOR** | Prénom : **Damien** |
|  : damien.mayor@cpnv.ch |  : +41 78 918 43 75 |
| Lieu de travail : | ☐ CPNV, Rue de la Gare 14, 1450 Sainte-Croix | |
| Orientation : | ☐ 88601 Développement d’application  ☒ 88602 Informatique d’entreprise  ☐ 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 : | Lundi 09h50-12h15 13h30-16h55  *Pentecôte 29 mai*  Mardi 08h00-12h15 13h30-16h55  Mercredi 08h00-12h15 -  Jeudi 08h00-12h15 13h30-16h55 *Ascension 18 mai*  Vendredi - - *Pont de l'Ascension 19 mai*  *Toutes les demi-journées ont une pause obligatoire de 15 minutes, sauf si elles se*  *commencent à 09h50.* | |
| 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 | |

# PROCÉDURE

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 débuter 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.

# TITRE

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

# MATÉRIEL ET LOGICIEL À DISPOSITION

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)

# PRÉREQUIS

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

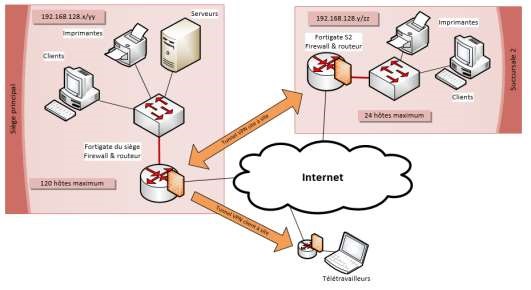
# DESCRIPTIF DU PROJET

Le module 146 abordant les grands réseau 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 1er 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 2ème 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’un tel 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 laissé au choix du candidat, en tenant compte que lors du 2ème temps se sera le réseau réel du CPNV qui sera utilisé.



# LIVRABLES

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

# POINTS TECHNIQUES ÉVALUÉS SPÉCIFIQUES AU PROJET

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 1er temps
2. Pertinence de la partie « Internet » proposée dans le 1er temps
3. A la fin du 1er 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 2ème temps
6. A la fin du 2ème 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’implémentions du schéma proposé qu’il est théoriquement possible de réaliser sans tenir compte des performances

# VALIDATION

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

## Identification du module

**Identification du module**



|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | 1 | | 2 | | 3 | | 4 | | 5 | | 6 | | |  | | --- | | Déterminer la liaison Internet selon les directives du client (sécurité, performance, disponibilité et maintenance). | | Classer les exigences selon priorité et signification pour l´entreprise, créer un cahier des charges pour l´évaluation d´un fournisseur de services (Provider). | | Représenter les résultats de l´évaluation sur la base du cahier des charges et des aspects économiques. | | Réaliser ou adapter le schéma et le plan du réseau. | | Déterminer les composants matériels et logiciels nécessaires, élaborer une demande d´acquisition. | | Planifier et réaliser la mise en exploitation avec les composants de la connexion Internet. Organiser et exécuter la remise de l´installation. | |

Objectifs opérationnels

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.

|  |
| --- |
| 1 |

|  |
| --- |
| Connaître les exigences (largeur de bande, disponibilité, ampleur du support, sécurité etc.) en matière de lien Internet |
| Connaître les mesures de surveillance et de sécurité lors de l’exploitation d’un réseau Internet. |
| Connaître les possibilités technologiques d´accès Internet ainsi que leur fournisseur (Provider). |
| Connaître des méthodes de classification des directives des clients. |
| Connaître l’organisation et le contenu d’un cahier des charges. |
| Connaître le déroulement d’un processus d’évaluation. |
| Connaître les critères principaux pour l’évaluation d’une offre. |
| Connaître les types de représentation pour l’évaluation d’une offre. |
| Connaître les règles pour l’élaboration d’un concept de dénomination et de numérotation. |
| Connaître la fonctionnalité d’un Firewall, DMZ, Proxy et DNS. |
| Connaître les types courants de représentation et symboles pour des schémas et plan de réseau. |
| Connaître l’organisation et le contenu d’une demande d’acquisition issue de l’évaluation. |
| Connaître le déroulement pour la planification et la mise en service de l’accès Internet. |
| Connaître le déroulement pour la remise du système dans l’exploitation opérationnelle. |
| Connaître l’organisation et le contenu d’un procès-verbal de remise. |

|  |
| --- |
| 1.1 |
| 1.2 |
| 2.1 |
| 2.2 |
| 2.3 |
| 2.4 |
| 3.1 |
| 3.2 |
| 4.1 |
| 4.2 |
| 4.3 |
| 5.1 |
| 6.1 |
| 6.2 |
| 6.3 |

|  |
| --- |
| 5 |
| 6 |

Objectifs opérationnels et connaissances opérationnelles nécessaires

2

3

4

Version du module 3.0

Créé le 11.02.2021

© ICT-Berufsbildung Schweiz 13.08.2021 Page 2 de 2

## Manuel de tests

A insérer à la fin du travail

## Sources – Bibliographie

A insérer à la fin du travail

Liste des livres utilisés (Titre, auteur, date), des sites Internet (URL) consultés, des articles (Revue, date, titre, auteur)… Et de toutes les aides externes (noms)

## Glossaire

A insérer à la fin du travail

## Journal de travail

A insérer à la fin du travail

## Archives du projet

Media, … dans une fourre en plastique