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

Table des matières

[1 Analyse préliminaire 4](#_Toc134104851)

[1.1 Introduction 4](#_Toc134104852)

[1.2 Objectifs 4](#_Toc134104853)

[1.3 Cahier des charges 4](#_Toc134104854)

[1.4 Module 146 4](#_Toc134104855)

[1.5 Planification initiale 5](#_Toc134104856)

[2 Analyse / Conception 6](#_Toc134104857)

[2.1 Méthode de travail 6](#_Toc134104858)

[2.2 Organisation du travail 7](#_Toc134104859)

[2.3 Informations générales 7](#_Toc134104860)

[2.4 Concept 7](#_Toc134104861)

[2.4.1 1er temps 7](#_Toc134104862)

[2.4.2 2ème temps 7](#_Toc134104863)

[2.5 Stratégie de test 8](#_Toc134104864)

[2.5.1 1er temps 8](#_Toc134104865)

[2.5.2 2ème temps 8](#_Toc134104866)

[2.6 Risques techniques 8](#_Toc134104867)

[2.6.1 1er temps 8](#_Toc134104868)

[2.6.2 2ème temps 8](#_Toc134104869)

[2.7 Planification 8](#_Toc134104870)

[2.8 Dossier de conception 9](#_Toc134104871)

[2.8.1 1er temps 9](#_Toc134104872)

[2.8.2 2ème temps 9](#_Toc134104873)

[3 Réalisation 9](#_Toc134104874)

[3.1 Dossier de réalisation 9](#_Toc134104875)

[3.1.1 1er temps 9](#_Toc134104876)

[3.1.2 2ème temps 9](#_Toc134104877)

[3.2 Description des tests effectués 10](#_Toc134104878)

[3.2.1 1er temps 10](#_Toc134104879)

[3.2.2 2ème temps 10](#_Toc134104880)

[3.3 Erreurs restantes 10](#_Toc134104881)

[3.3.1 1er temps 10](#_Toc134104882)

[3.3.2 2ème temps 10](#_Toc134104883)

[3.4 Liste des documents fournis 10](#_Toc134104884)

[4 Conclusions 10](#_Toc134104885)

[5 Remerciements 11](#_Toc134104886)

[6 Table des illustrations 11](#_Toc134104887)

[7 Annexes 11](#_Toc134104888)

[7.1 Résumé du rapport du TPI 11](#_Toc134104889)

[7.2 Cahier des charges 11](#_Toc134104890)

[7.3 Identification du module 14](#_Toc134104899)

[7.4 Manuel de tests 16](#_Toc134104900)

[7.5 Sources – Bibliographie 16](#_Toc134104901)

[7.6 Glossaire 16](#_Toc134104902)

[7.7 Journal de travail 16](#_Toc134104903)

[7.8 Archives du projet 17](#_Toc134104904)

[8 A ne pas oublier : 17](#_Toc134104905)

# Analyse préliminaire

## Introduction

Ce chapitre décrit brièvement le projet, le cadre dans lequel il est réalisé, les raisons de ce choix et ce qu'il peut apporter à l'élève ou à l'école. Il n'est pas nécessaire de rentrer dans les détails (ceux-ci seront abordés plus loin) mais cela doit être aussi clair et complet que possible (idées de solutions). Ce chapitre contient également l'inventaire et la description des travaux qui auraient déjà été effectués pour ce projet.

Ces éléments peuvent être repris des spécifications de départ.

## Objectifs

*Tiré du cahier des charges :*

"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."

Liste:

Ce chapitre énumère les objectifs du projet. L'atteinte ou non de ceux-ci devra pouvoir être contrôlée à la fin du projet. Les objectifs pourront éventuellement être revus après l'analyse.

Ces éléments peuvent être repris des spécifications de départ

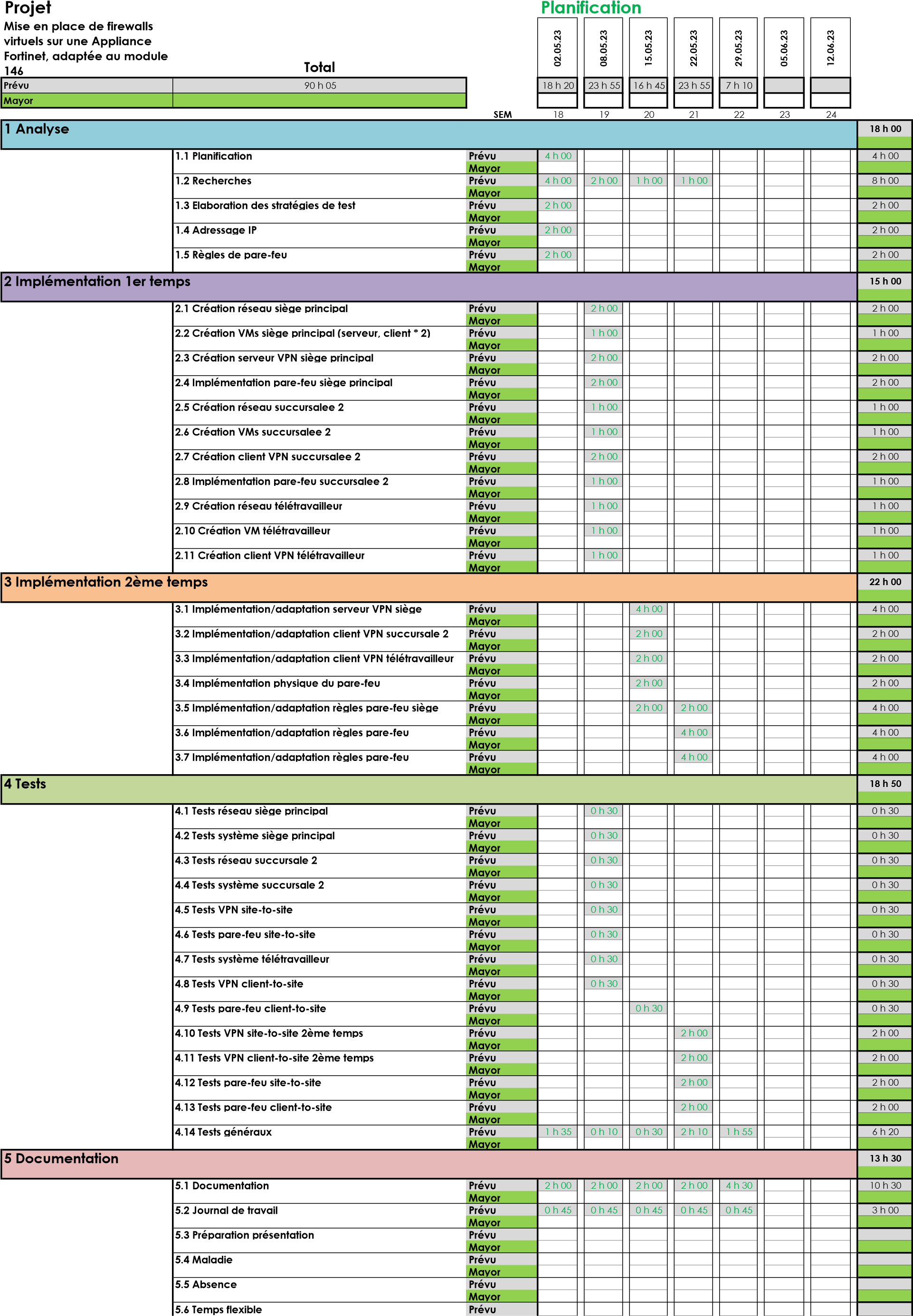
## Cahier des charges

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.

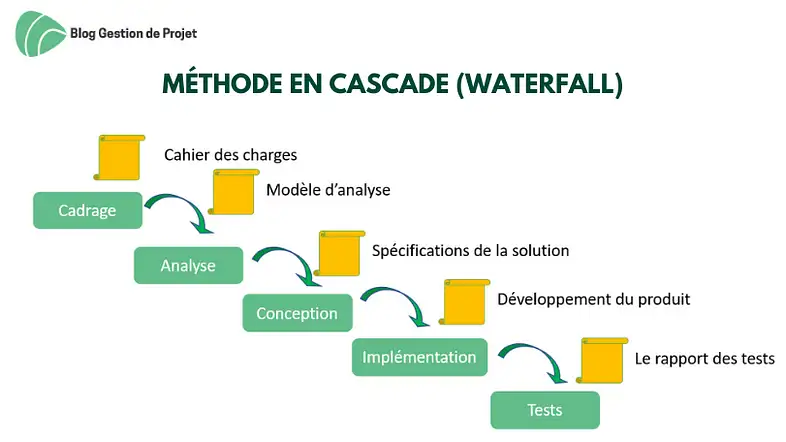


Figure 1 méthode en cascade. Source blog-gestion-de-projet.com

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 :

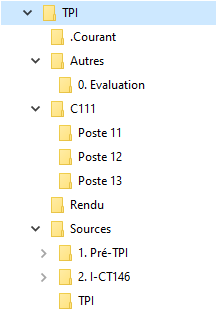


Figure 2 Nomenclature fichiers

## Informations générales

1. Fortinet
2. Réseau CPNV
3. Salle C11

## Concept

### 1er temps

### 2ème temps

Le concept complet avec toutes ses annexes:

Par exemple :

• Multimédia: carte de site, maquettes papier, story board préliminaire, …

• Bases de données: interfaces graphiques, modèle conceptuel.

• Programmation: interfaces graphiques, maquettes, analyse fonctionnelle…

• …

## Stratégie de test

### 1er temps

P

### 2ème temps

Décrire la stratégie globale de test:

• types de des tests et ordre dans lequel ils seront effectués.

• les moyens à mettre en œuvre.

• couverture des tests (tests exhaustifs ou non, si non, pourquoi ?).

• données de test à prévoir (données réelles ?).

• les testeurs extérieurs éventuels.

## Risques techniques

### 1er temps

Manque de connaissances en VPN

Manque de connaissances FortiGate

Faisabilité du projet

### 2ème temps

Complexité lié au réseau de l'école et à ses contraintes

• risques techniques (complexité, manque de compétences, …).

Décrire aussi quelles solutions ont été appliquées pour réduire les risques (priorités, formation, actions, …).

## Planification

Révision de la planification initiale du projet :

• planning indiquant les dates de début et de fin du projet ainsi que le découpage connu des diverses phases.

• partage des tâches en cas de travail à plusieurs.

Il s’agit en principe de la planification définitive du projet. Elle peut être ensuite affinée (découpage des tâches). Si les délais doivent être ensuite modifiés, le responsable de projet doit être avisé, et les raisons doivent être expliquées dans l’historique.

## Dossier de conception

### 1er temps

### 2ème temps

Fournir tous les document de conception:

• le choix du matériel HW

• le choix des systèmes d'exploitation pour la réalisation et l'utilisation

• le choix des outils logiciels pour la réalisation et l'utilisation

• site web: réaliser les maquettes avec un logiciel, décrire toutes les animations sur papier, définir les mots-clés, choisir une formule d'hébergement, définir la méthode de mise à jour, …

• bases de données: décrire le modèle relationnel, le contenu détaillé des tables (caractéristiques de chaque champs) et les requêtes.

• programmation et scripts: organigramme, architecture du programme, découpage modulaire, entrées-sorties des modules, pseudo-code / structogramme…

Le dossier de conception devrait permettre de sous-traiter la réalisation du projet !

# Réalisation

## Dossier de réalisation

### 1er temps

### 2ème temps

Décrire la réalisation "physique" de votre projet

• les répertoires où le logiciel est installé

• la liste de tous les fichiers et une rapide description de leur contenu (des noms qui parlent !)

• les versions des systèmes d'exploitation et des outils logiciels

• la description exacte du matériel

• le numéro de version de votre produit !

• programmation et scripts: librairies externes, dictionnaire des données, reconstruction du logiciel - cible à partir des sources.

NOTE : Evitez d’inclure les listings des sources, à moins que vous ne désiriez en expliquer une partie vous paraissant importante. Dans ce cas n’incluez que cette partie…

## 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

### 1er temps

### 2ème temps

S'il reste encore des erreurs:

• Description détaillée

• Conséquences sur l'utilisation du produit

• Actions envisagées ou possibles

## 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

Développez en tous cas les points suivants:

• Objectifs atteints / non-atteints

• Points positifs / négatifs

• Difficultés particulières

• Suites possibles pour le projet (évolutions & améliorations)

# Remerciements

Merci à Madame Nicole Mayor pour les corrections de l'orthographe et la grammaire de ce document, tout en ne comprenant absolument rien à son contenu.

# Table des illustrations

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

[Figure 2Nomenclature 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

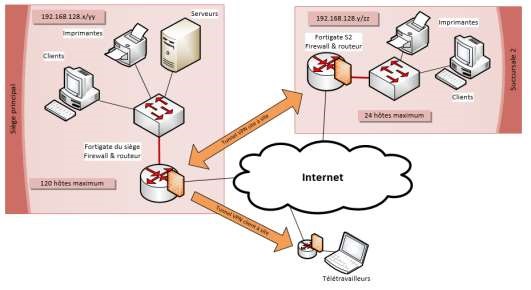
# DESCRIPTIF DU PROJET

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Durée** | **Activité** | **Remarques** |
|  |  |  |  |
|  |  |  |  |

## Archives du projet

Media, … dans une fourre en plastique

# A ne pas oublier :