Dorian Niclass & Ilan Ruiz-de-Porras

Projet système sur le sujet “Accès externe aux ressources d’entreprise”

Projet Système

Accès externe aux ressources d’entreprise

Table des matières

[1. Introduction 2](#_Toc534981864)

[2. Analyse du contexte 2](#_Toc534981865)

[3. Définition des critères 2](#_Toc534981866)

[4. Analyse des outils 3](#_Toc534981867)

[4.1 OpenVPN 3](#_Toc534981868)

[4.1.1 Description 3](#_Toc534981869)

[4.1.2 Avantages et inconvénients 4](#_Toc534981870)

[4.2 SSTP 4](#_Toc534981871)

[4.3 Centrify 4](#_Toc534981872)

[4.4 Cerberus FTP Server 5](#_Toc534981873)

[5. Mise en place pratique des outils 5](#_Toc534981874)

[5.1 Infrastructure 5](#_Toc534981875)

[5.2 Installation de l’AD 6](#_Toc534981876)

## 1. Introduction

Ce projet consiste à faire une étude concernant un principe de fonctionnement d’un outils/applications lié aux réseaux. Un exemple concret d’application au sein du CPNV doit être présenté. Des travaux pratiques seront mis en place pour appuyer et illustrer le fonctionnement de ces outils.

Notre sujet porte sur l’accès externe aux ressources d’entreprise, avec comme outils : SSTP (gratuit), OpenVPN (gratuit), Centrify (payant) et Cerberus (payant). Une analyse complète de chaque outil sera effectuée, une comparaison de ces outils sera ensuite faite pour en tirer des avantages/désavantage.

## 2. Analyse du contexte

Le contexte est de mettre en place un système utile pour le CPNV. Notre sujet portant sur l’accès externe aux ressources d’une entreprise, le but est de pouvoir accéder à certaines ressources de l’entreprise via un VPN. Les ressources pouvant être accessible sont par exemple : des fichiers (partages), les applications ou tout autres ressources hébergées sur les serveurs de l’entreprise. Il existe divers moyens et méthodes d’accéder à ces ressources à distance, les outils que nous avons sélectionnés sont diversifié sur les méthodes d’accès. Moyens d’accès pouvant être utilisé : VPN, FTP, HTTPS, SSH, SFTP.

Cas utile pour le CPNV : l’accès aux documents présent sur les différents partages (Commun, Perso, etc…) depuis l’extérieur (ex. depuis chez soi) et de fournir les applications utiles pour le travail à distance.

## 3. Définition des critères

Définir les critères de comparaisons des produits.

|  |  |
| --- | --- |
| **Critère** | **Définition** |
| Sécurité | La sécurité de l’outil (connexion sécurisée) |
| Prix | Prix de la solution |
| Rapidité de mise en place | La solution est-t-elle rapidement et facilement mise en place dans l’infrastructure ? |
| Facilité d’utilisation | Facile à utiliser pour les clients ? |
| Fonctionnalités | Les fonctionnalités mises à disposition sont-elles suffisantes ? Trop chargées ? |
| Compatibilité | L’outil est-il compatible avec toutes les plateformes, versions de l’OS ? |

## 4. Analyse des outils

Analyse des outils sélectionnés

Les outils que nous avons choisis sont les suivants :

|  |  |
| --- | --- |
| **Nom** | **Résumé** |
| OpenVPN | Logiciel gratuit et open source permettant la mise en place d’une connexion VPN |
| SSTP (VPN Windows Server) | SSTP est un protocole créé par Microsoft et utilisé par le rôle Accès à Distance de Windows Server. Protocole très sécurisé mais uniquement disponible sur Windows |
| Cerberus | Outil payant permettant de créer des serveur FTP accessible par HTTPS très facilement. Outil très complet et simple d’utilisation. |
| Centrify | Outil payant très complet et très sécurisé fournissant énormément de fonctionnalités. Son utilisation est surtout centré sur les grandes entreprises. |

### 4.1 OpenVPN

### 4.1.1 Description

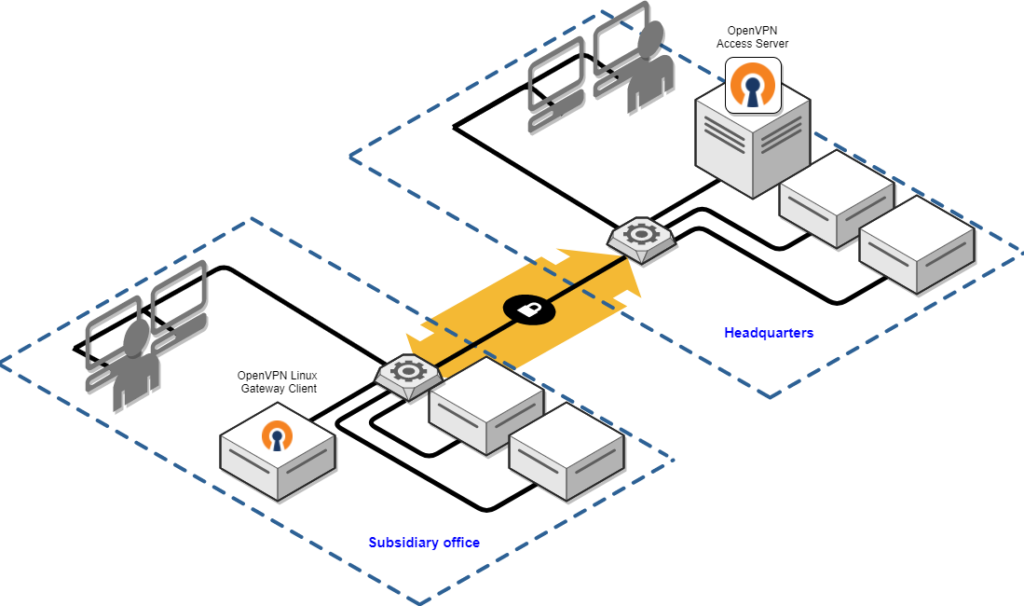
OpenVPN est un logiciel gratuit développer en 2001 par James Yonan

Ce logiciel utilise de manière intensive la bibliothèque d’authentification **OpenSSL**. Il utilise également le protocole **SSLv3/TLSv1**.

Il est disponible sur une multitude d’environnement tels que Windows, Linux et Mac OS X.

Il n’est par contre pas compatible avec **IPsec** ou d’autres logiciel VPN.

Ci-dessous un schéma de connexion au serveur OpenVPN:



### 4.1.2 Avantages et inconvénients

|  |  |
| --- | --- |
| **Avantages** | **Inconvénients** |
| - Gratuit  - Haute disponibilité | Incompatible avec d’autres logiciel VPN |

### 4.2 SSTP

#### 4.2.1 Description

SSTP (Secure Socket Tunneling Protocol) est un protocole de VPN créé par Microsoft, il est cependant uniquement disponible sur Windows. Il est reconnu comme l’un des protocoles les plus sécurisés.

Il utilise le canal sécurisé SSL (port 443), ce qui lui permet de passer plus facilement entre les pare-feu, du fait que les pare-feu autorisent le trafic SSL via le port 443. Cependant pour permettre cette connexion sécurisée, un certificat SSL est requis.

#### 4.2.2 Avantages et inconvénients

|  |  |
| --- | --- |
| **Avantages** | **Inconvénients** |
| - Très sécurisé  - Disponible nativement sur Windows | - Disponible uniquement sur Windows  - Mise en place peut être un peu plus difficile |

### 4.3 Centrify

#### 4.3.1 Description

Centrify propose plusieurs solutions dans la gestion des ressources et des utilisateurs d’une entreprise ainsi que dans sa sécurité.

Possède beaucoup de fonctionnalités et une mise en place pas trop compliquée. La quantité et la qualité des fonctionnalités ainsi que son prix conviennent mieux pour les grandes entreprises, ce qui ne serait pas rentable pour une école comme le CPNV.

#### 4.3.2 Avantages et inconvénients

|  |  |
| --- | --- |
| **Avantages** | **Inconvénients** |
| - Offre beaucoup de fonctionnalité  - Hautement sécurisé | - Payant  - Trop de fonctionnalités par rapport aux besoins |

### 4.4 Cerberus FTP Server

#### 4.4.1 Description

Cerberus permet de monter un serveur FTP sécurisé passant par HTTPS en utilisant une encryption SSL. C’est un outil très complet permettant une gestion complète des utilisateurs, des adresses IP autorisées et fournis des statistiques détaillées.

Les services peuvent être accéder par web (HTTP, HTTPS), FTP ou SSH. A noter que pour l’accès HTTPS un certificat SSL est requis.

Il peut être utilisé avec L’AD pour la gestion des comptes et des accès.

#### 4.4.2 Avantages et inconvénients

|  |  |
| --- | --- |
| **Avantages** | **Inconvénients** |
| - Très complet  - Sécurisé  - Gestion avancée  - Accès aux services très facilement via navigateur | - Payant |

## 5. Mise en place pratique des outils

Afin de pouvoir au mieux comparer les outils, nous allons les mettre en pratique dans la mesure du possible.

### 5.1 Infrastructure

Définition de l’infrastructure utilisée dans tous nos tests des outils.

VM utilisées :

|  |  |  |
| --- | --- | --- |
| **Nom** | **OS** | **Propriétés** |
| PRJS\_CLI1 | Windows 10 - Pro | - RAM : 2Go  - Nombre processeur : 1  - Espace disque : 60 Go |
| PRJS\_SRV1 | Windows Server 2012 r2 | - RAM : 2Go  - Nombre processeur : 1  - Espace disque : 60 Go |

### 

### 5.2 Installation de l’AD

Installer l’AD sur PRJS\_SRV1

Configuration :

* Ajouter une nouvelle forêt : PRJS.ch
* Niveau fonctionnel de la forêt : Windows Server 2012 R2
* Niveau fonctionnel du domaine : Windows Server 2012 R2
* Serveur DNS
* Nom NetBIOS : PRJS
* Dossier de la base de données : C:\Windows\NTDS
* Dossier des fichiers journaux : C:\Windows\NTDS
* Dossier SYSVOL : C:\Windows\SYSVOL