Documentation d’exploitation

Réalisé par :

Blondel Lucas

Caparros Maxime

Table des matières

[Introduction 3](#_Toc133394178)

[1. Schéma d’infrastructure 3](#_Toc133394179)

[2. Les différentes technologies utilisées 3](#_Toc133394180)

[3. Mise en place du firewall 4](#_Toc133394181)

[1. Configuration des interfaces : 4](#_Toc133394182)

# Introduction

Le projet consiste en la mise en place d'un intranet pour la gestion simplifiée de l'ensemble des services IT d'une entreprise, comprenant notamment un annuaire, une gestion de mails, une prise de notes, un agenda et une gestion de fichiers.

Le projet doit également proposer des applications internes telles qu'un serveur mail, un serveur web et une gestion d'agenda, ainsi qu'une gestion d'utilisateurs et de groupes via un annuaire, un portail captif, un VPN, etc. Le système doit mettre en œuvre un SSO fonctionnel, une interface "access management" pour les liens vers les applications internes et un accès distant (VPN).

# Schéma d’infrastructure

# Les différentes technologies utilisées

Pour le choix du firewall nous en avons choisi 3 puis nous avons effectué un tableau de pondération :

Une image contenant texte, capture d’écran, diagramme, ligne

Description générée automatiquement

Selon nos critères nous avons donc choisi pfsense.

Ensuite nous avons choisi notre solution pour héberger notre intranet, pour cela nous avons choisi plusieurs critères : Une image contenant capture d’écran, texte, ligne, Parallèle

Description générée automatiquement

Pour le serveur Active Directory nous avons pris serveur Windows 2019.

Pour tout mettre en place nous avons utilisé VMware.

# Mise en place du firewall

Pour mettre en place notre firewall nous avons choisi PFsense qui va nous servir de serveur VPN, de routeur et bien évidement de firewall.

## Configuration des interfaces :

Nous avons installé l’OS pfSense avec VMware puis nous l’avons lié au pc en bridged puis nous avons créé 3 lans :

* LAN-Serveurs       = 172.16.1.1/18      = Le réseau LAN pour les serveurs
* LAN-Users          = 172.16.64.1/18     = Le réseau LAN pour les Utilisateurs
* LAN-DMZ            = 172.16.128.1/18    = Le réseau de la DMZ

Ensuite nous avons utilisé 4 networks adaptateur réparti comme cela :

NetWork Adapter      = Bridged            = 192.168.1.41/24

NetWork Adapter 2    = LAN\_Serveurs       = 172.16.1.1/18

NetWork Adapter 3    = LAN\_Users          = 172.16.64.1/18

NetWork Adapter 4    = LAN\_DMZ            = 172.16.128.1/18

Dans la configuration du firewall nous avons assigné les 4 cartes réseaux a des interfaces :

Enter the WAN interface name or 'a' for auto-detection: **em0**

Enter the LAN interface name or 'a' for auto-detection

NOTE: this enables full Firewalling/NAT mode.

(em1 em2 em3 em4 a or nothing if finished): **em1**

Enter the Optional 1 interface name or 'a' for auto-detection

(em2 em3 em4 a or nothing when finished): **em2**

Enter the Optional 2 interface name or 'a' for auto-detection

(em3 em4 a or nothing when finished): **em3**

Enter the Optional 4 interface name or 'a' for auto-detection

( a or nothing when finished): **<Entrée>**

The interfaces will be assigned as follows:

WAN  -> em0

LAN  -> em1

OPT1 -> em2

OPT2 -> em3