

Fiche technique du système

Fiche technique décrivant la totalité des paramétrages système

Paul BURGNIARD - Merwan CHEHBI - Maxime GERARD - Malo BERGER - Taha CHAUDHRY

Sommaire:

- [Vue globale du projet :](#)
- [Configuration des VMs :](#)
- [Plan D'Adressage IP:](#)
- [Configuration OPNsense:](#)
 - [Règles De Pare Feu:](#)
 - [DMZ:](#)
 - [SERVEURS:](#)
 - [CLIENTS:](#)
 - [WAN:](#)
 - [NAT](#)
 - [Services:](#)
 - [Relay DHCPv4:](#)
- [Configuration Serveur Windows:](#)
 - [Script Powershell](#)
 - [Services:](#)
 - [Active Directory:](#)
 - [Ping Castle](#)
 - [GPO](#)
 - [DNS:](#)
 - [DHCP:](#)
- [Configuration Linux 1:](#)
 - [Service Reverse Proxy Nginx:](#)
- [Configuration Linux 2:](#)
 - [Service Docker:](#)

Vue globale du projet :

Création d'un réseau semblable à celui d'une entreprise séparée et mise en place de différents services internes et externes.

Cette approche est souvent utilisée pour améliorer la sécurité des communications au sein d'une entreprise. Une fois l'installation effectuée des services, il est nécessaire de tester et de valider que la configuration réseau soit fonctionnelle et sécurisée.

Lors de ce projet, nous travaillerons avec *Proxmox Virtual Environment* : Cela nous permettra de faciliter la coopération et l'installation des VMs.






Quelques abréviations afin de mieux comprendre :

- AD = Active Directory
- CLT = Client
- DHCP = Dynamic Host Configuration Protocol
- VMs = Virtual Machines
- DMZ = Demilitarized Zone

Voici la liste des VMs nécessaires au bon fonctionnement du projet (possible d'en ajouter si besoin) :

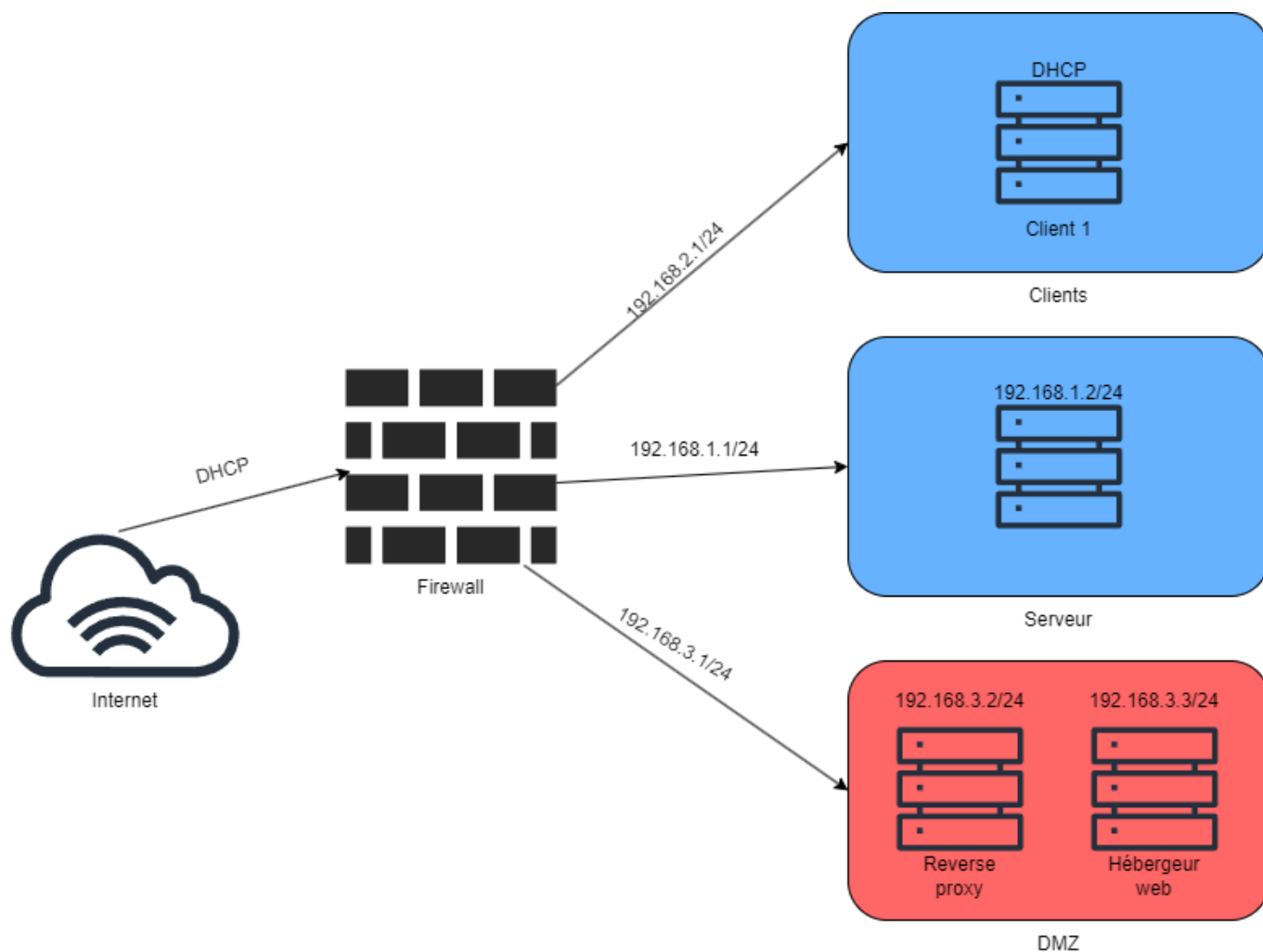
- OPNsense : Notre Firewall
- Windows Serveur : Contrôleur de domaine de l'AD, serveur DNS et serveur DHCP
- Windows Client : Servant à être le client de l'AD
- Serveur WEB : Permettant d'héberger notre site web (avec docker)
- Reverse Proxy : Servant de reverse proxy pour le Server WEB (avec nginx)

Configuration des VMs :

 Système D'Exploitation	 RAM	 Taille Disque	 Réseaux	 IP statique
Opnsense-Opnsense 23.7	2GB	32GB	tous	<i>Les gateway de chaque réseau</i>
Linux1-Debian 12.0	2GB	20GB	DMZ	<i>192.168.3.2</i>
Linux2-Debian 12.0	2GB	32GB	DMZ	<i>192.168.3.3</i>
WindSERV-Windows 10	8GB	32GB	SERVEURS	<i>192.168.1.2</i>
Wind1-Windows 10	2GB	30GB	CLIENT	✗

Plan D'Adressage IP:

 Réseaux	 Gateway	 DHCP
SERVEURS	192.168.1.1/24	✗
DMZ	192.168.3.1/24	✗
CLIENT	192.168.2.1/24	192.168.2.2 ➡ 192.168.2.254



Configuration OPNsense:

```
*** OPNsense.localdomain: OPNsense 23.7.12_5 ***

CLIENTS (vtnet3) -> v4: 192.168.2.1/24
DMZ (vtnet1)      -> v4: 192.168.3.1/24
SERVEURS (vtnet2) -> v4: 192.168.1.1/24
WAN (vtnet0)     -> v4/DHCP4: 10.1.91.33/23
```

Règles De Pare Feu:

DMZ:

Action	Source	Protocol	Destination	Port	Description
Pass	DMZ net	*	!192.168.0.0/16	*	Allow internet

SERVEURS:

Action	Source	Port	Destination	Port	Description
Pass	SERVEURS net	*	*	*	Allow To any

CLIENTS:

Action	Source	Protocol	Destination	Port	Description
Pass	CLIENTS net	TCP	192.168.1.2	53, 88, 135, 389, 445, 636, 5722, 1024:65535	Active Directory
Pass	CLIENTS net	UDP	192.168.1.2	53, 88, 123, 389 5722	Active Directory
Pass	CLIENTS net	TCP	192.168.3.2	80	Allow HTTP to Reverse Proxy
Pass	CLIENTS net	*	!192.168.0.0/16	*	Allow internet

WAN:

- Aucune règle

NAT

Interface	Protocol	Destination Address	Destination Port	NAT IP	NAT Port
WAN	TCP	192.168.3.2	80	10.1.91.33	80

Services:

Relay DHCPv4:

- Etat: Activé
- Réseau: CLIENTS
- Serveur: 192.168.1.2

Configuration Serveur Windows:

Script Powershell

Ce script permet de automatiser la création de nouveaux utilisateurs

```
Add-Type -AssemblyName System.Web
```

```
$CSVData = Import-Csv -Encoding UTF8 -Path ./Users.csv
```

```
$Output = @()
```

```
foreach(LineinCSVData){
```

```
    SamAccountName = (Line.Prénom.Substring(0,1) + $Line.Nom)
```

```
    if( -not (Get-ADUser -Filter "SamAccountName -eq '$SamAccountName'" -ErrorAction SilentlyContinue)){
```

```
        $Password = [System.Web.Security.Membership]::GeneratePassword(12,3)
```

```
        $Userparams = @{
```

```
            Name = (Line.Prénom + "" + Line.Nom)
```

```
            GivenName = $Line.Prénom
```

```
            Surname = $Line.Nom
```

```
            SamAccountName = $SamAccountName
```

```
            UserPrincipalName = (Line.Prénom.Substring(0, 1) + Line.Nom +  
"@fromageland.com")
```

```
            Path = "OU=Employes,DC=FROMAGELAND,DC=COM"
```

```
            AccountPassword = (ConvertTo-SecureString -AsPlainText -Force $Password)
```

```
ChangePasswordAtLogon = $true
```

```
Enabled = $true
```

```
}
```

```
New-ADUser @Userparams
```

```
$Output += [PSCustomObject]@{
```

```
    Login=(Line.Prenom.Substring(0,1)+Line.Nom)
```

```
    Password=$Password
```

```
}
```

```
}
```

```
}
```

```
$Output | Out-String | Add-Content Output.txt
```

Services:

Active Directory:

Ping Castle

Ping Castle est un outil d'audit d'AD, permettant de scanner automatiquement de multitudes de vulnérabilités et d'ensuite noter la sécurité de notre système selon un score de 0 à 100.

****Vulnérabilités rencontrées et réglées** :**

Authentification par NTLMv1 autorisée : désactivée par un GPO.

- Les utilisateurs non administrateurs sont autorisés à ajouter des ordinateurs AD : désactivé par un GPO.

- LAPS non installé : installation et configuration de LAPS sur le serveur et le client.

- Spooler activé : désactivation du service "spooler".

- Mise en place d'une stratégie d'audit : activée par un GPO

- Le compte administrateur peut être délégué : désactivé dans les propriétés du compte administrateur.

- Endurcissement du chemin : activation par un GPO

- Utilisateurs dans le groupe Administrateurs Schéma : Utilisateurs retirés

- Sous réseau non déclaré dans l'outil site: déclaration dans l'outil site

GPO

Un ****GPO**** (Group Policy Object) est un objet de stratégies de groupes permettant d'automatiser une tâche.

Ce dernier est utilisé dans les environnements ****Windows Server**** afin de gérer et appliquer des configurations sur les ordinateurs et utilisateurs d'un domaine AD.

Voici notre GPO :

`Configuration_ordinateur/Stratégies/Parametres_Windows/Parametres_de_Sécurité/Stratégies_locales/Comptes/Etat de compte administrateur= désactivé`

DNS:

- Zone: FROMAGELAND.com

Record	Nom		Adresse	
:----:	:--:		:-----:	
A	@		192.168.1.2	


```
| A | web1 | 192.168.3.2 |  
| A | web2 | 192.168.3.2 |
```

DHCP:

- Plage: 192.168.2.2 - 192.168.2.254
- Masque: 255.255.255.0
- Gateway: 192.168.2.1
- DNS: 192.168.1.2
- Nom DNS: FROMAGELAND.com

Configuration Linux 1:

Service Reverse Proxy Nginx:

```
```nginx  
server{
 listen 80;
 server_name web1.FROMAGELAND.com;

 location / {
 proxy_pass http://192.168.3.3:8080;
 proxy_set_header Host $host;
 proxy_set_header X-Real-IP $remote_addr;
 proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
 }
}

server{
 listen 80;
 server_name web2.FROMAGELAND.com;

 location / {
 proxy_pass http://192.168.3.3:8081;
 proxy_set_header Host $host;
 proxy_set_header X-Real-IP $remote_addr;
 proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
 }
}
```

## Configuration Linux 2:

---

### Service Docker:

Le service est défini par le stack compose suivant :

```
version: '3.8'
```

```
services:
```

```
 server1:
```

```
 image: httpd:alpine
```

```
 container_name: server1
```

```
 ports:
```

```
 - "8080:80"
```

```
 volumes:
```

```
 - ./server1:/usr/local/apache2/htdocs
```

```
 restart: always
```

```
 server2:
```

```
 image: httpd:alpine
```

```
 container_name: server2
```

```
 ports:
```

```
 - "8081:80"
```

```
 volumes:
```

```
 - ./server2:/usr/local/apache2/htdocs
```

```
 restart: always
```