

# PROJET HÉTÉROGÈNE

## Présentation :

**Projet Fin D'étude Collège Rosemont  
Gestion de Réseaux Linux et Windows**

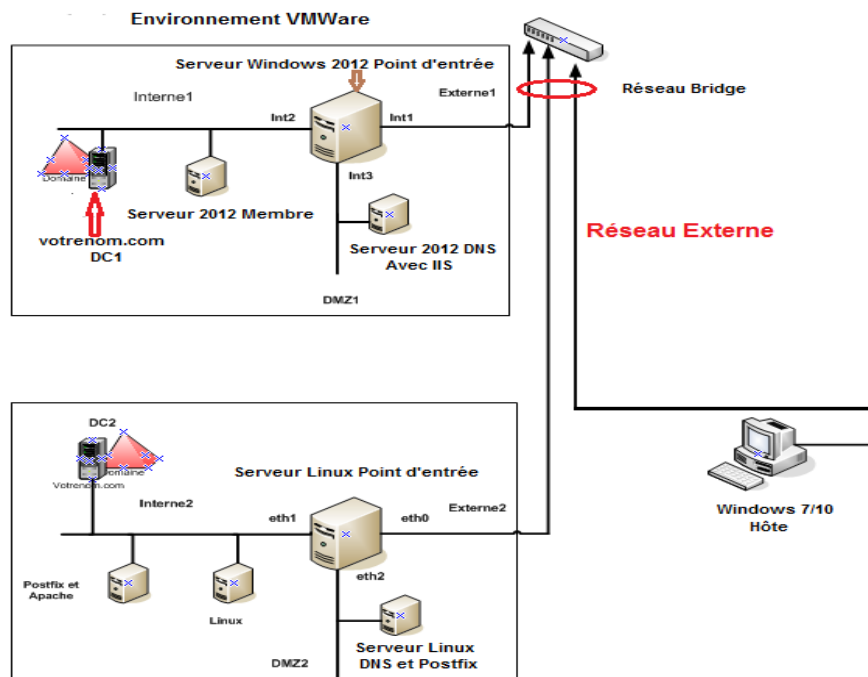
**Installation et Configuration de plusieurs services et Protocoles dans  
un Environnement hétérogène**

## Encadré Par:

***Dr Foudil HALITIM***

## Réalisé Par:

***Amine Hemissi***



## Topologie :

Nom VM	Adresse IP	Masque	Passerelle	DNS	VmNet	Site
SE 1	131.107.0.9	/16	-	-	3	Laval
	192.168.1.9	/24	-	192.168.1.12	2	Laval
	172.16.1.9	/16	-	172.16.1.11	5	Laval
	auto	auto	auto	auto	Bdg	Laval
MB 1	192.168.1.11	/24	192.168.1.9	192.168.1.12	2	Laval
DC 1	192.168.1.12	/24	192.168.1.9	-	2	Laval
DMZ 1	172.16.1.11	/24	172.16.1.9	-	5	Laval
SE 2	131.107.0.10	/16	-	-	3	Montréal
	192.168.2.10	/24	-	192.168.1.12	4	Montréal
	172.16.2.10	/16	-	172.16.1.11	6	Montréal
	auto	auto	auto	auto	Bdg	Montréal
MB 2	192.168.2.11	/24	192.168.2.9	192.168.2.12	4	Montréal
DC 2	192.168.2.12	/24	192.168.2.9	-	4	Montréal
WEB 2	192.168.2.13	/24	192.168.2.9	192.168.2.12	4	Montréal
DMZ 2	172.16.2.11	/24	172.16.2.9	-	6	Montréal
PC 0	auto	auto	auto	auto	3	-

## Partie 1:

### Étape 1 :

#### ■ Serveur d'entrée Windows :

- Installer le rôle Routage et accès distant
- Ajouter un itinéraire statique sur l'interface externe en spécifiant la destination comme le sous réseau interne 2 de passerelle l'interface externe du serveur d'entrée Linux.

#### ■ Serveur d'entrée Linux :

- Activer le Forwarding
- Ajouter une route vers Réseau interne 1 de passerelle l'interface externe du serveur d'entrée Windows :

```
# ip route add 192.168.1.0/24 via 131.107.0.9 dev ens33
```

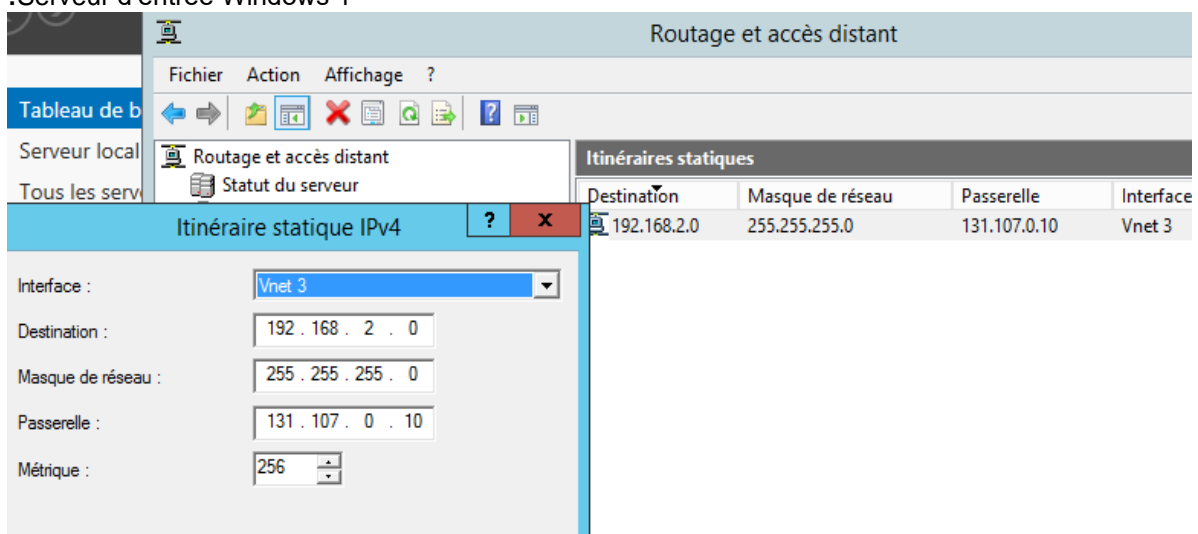
## ■ Serveur Membre Windows :

-Just ajouter une adresse IP avec passerelle par défaut l'interface interne du serveur d'entrée Windows.

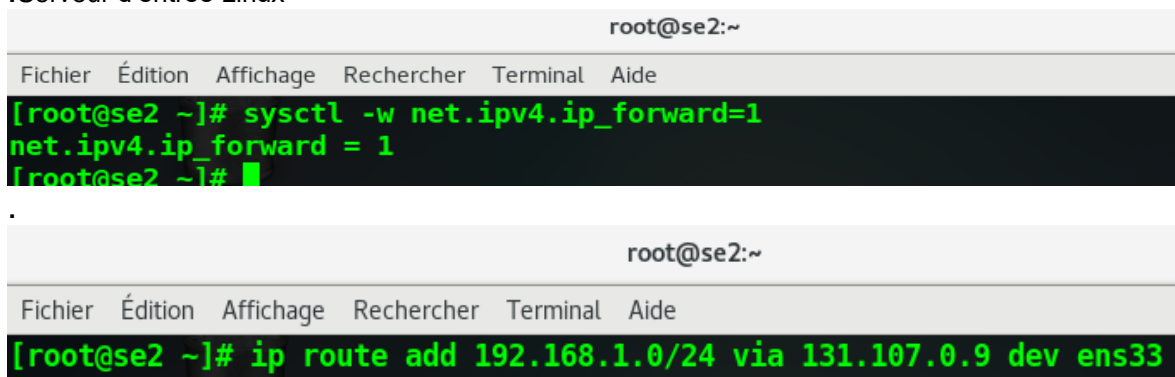
## ■ Serveur Membre Linux :

-Just ajouter une adresse IP avec passerelle par défaut l'interface interne du serveur d'entrée Linux.

.Serveur d'entrée Windows 1



.Serveur d'entrée Linux



## Étape 2 :

## ■ Serveur Membre Windows :

-Ajouter Rôle DHCP.  
 -Vérifier l'adresse IP et passerelle par défaut.  
 -Ajouter Étendue avec les options d'un sous-réseau spécifique, mettant Vmnet3.

## ■ Serveur d'entrée Windows :

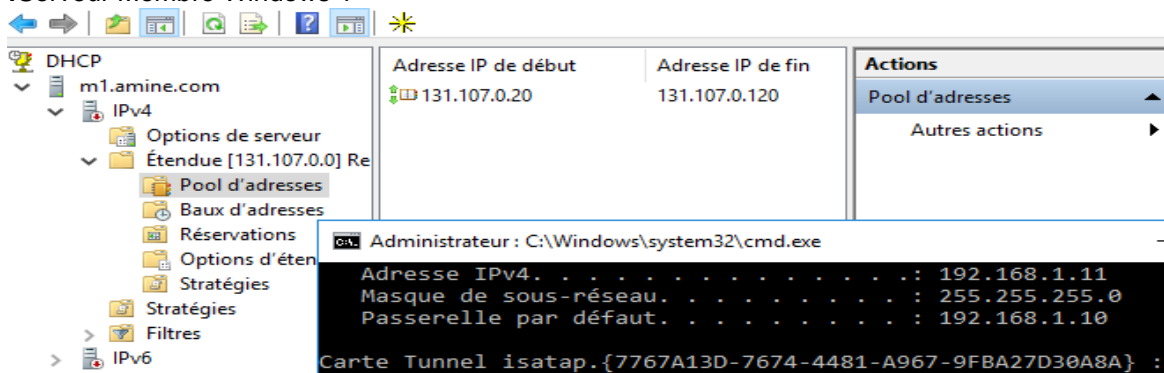
-Configurer l'interface externe dans le Vmnet3.  
 -Ajouter l'interface Externe a l'agent de relais DHCP dans Routage et Accès.

## ■ Client Externe Windows :

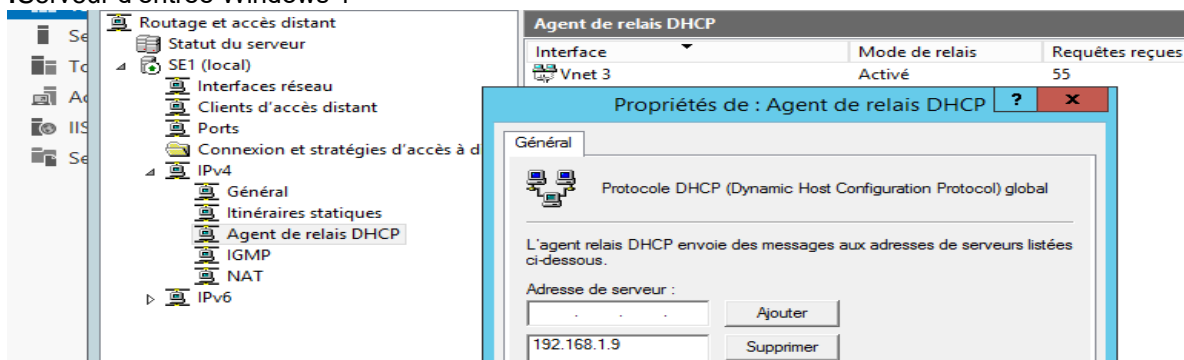
-Just Mettre le client dans le même réseau Vmnet3 et attendre, si ça ne marche pas  
Taper les commandes Shell Windows:

- > ipconfig /release
- > ipconfig /renew

.Serveur Membre Windows 1



.Serveur d'entrée Windows 1



## Étape 3:

### ■ Serveur Windows DC 1 :

- Ajouter le nouveau DC1 dans le Réseau interne 1.
- Vérifier l'adresse IP et passerelle par défaut.
- Ajouter le rôle ADDS.
- Ajouter une nouvelle forêt et un nouveau nom de domaine ( [hms.com](https://hms.com) ).
- Configurer zone inverse DNS.
- Ajouter réplication DNS avec Serveur DC 2.

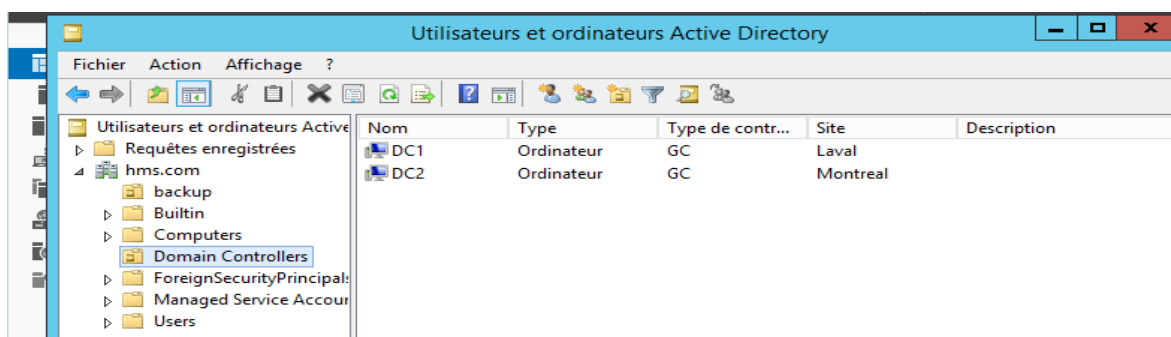
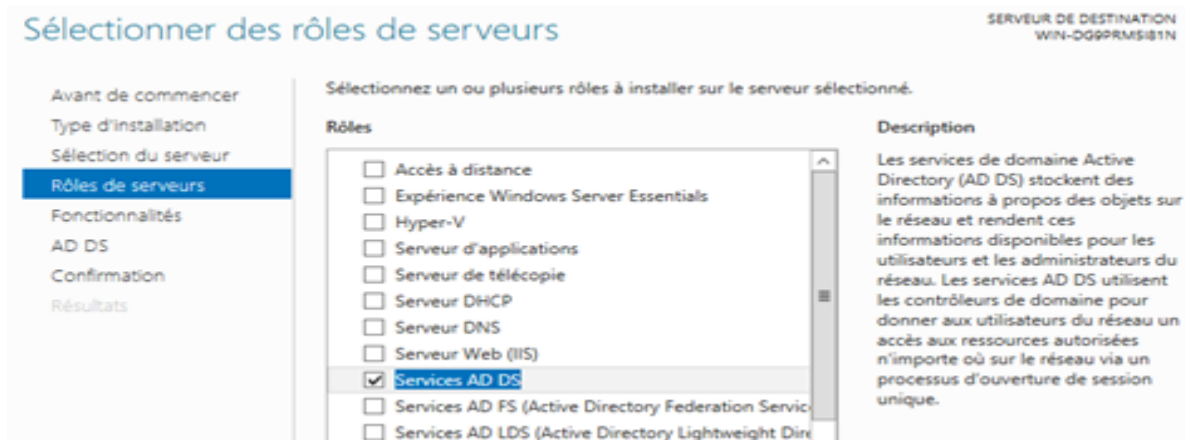
### ■ Serveur Windows DC 2 :

- Ajouter le nouveau DC2 dans le Réseau interne 2.
- Vérifier l'adresse IP et passerelle par défaut.
- Ajouter le rôle ADDS.
- Configurer dans la même forêt et le même nom de domaine ( [hms.com](https://hms.com) ).
- Ajouter ou actualiser la réplication DNS avec Serveur DC 1.

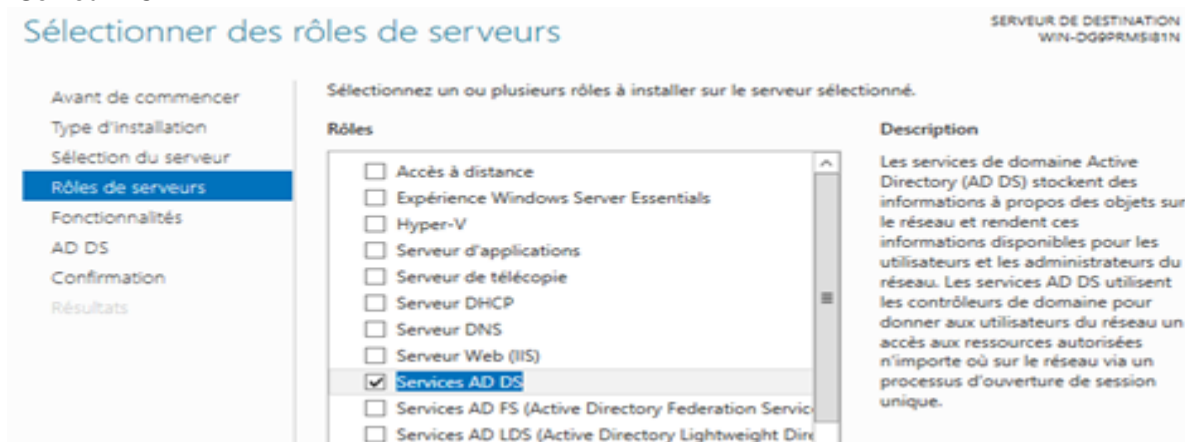
## ■ Serveur Membre Windows :

- Vérifier l'adresse IP et passerelle par défaut.
- S'assurer que son serveur DNS est le Serveur DC 1.
- Ajouter ce Serveur DHCP Déjà configuré au domaine [hms.com](https://hms.com).

.Serveur DC.1



.Serveur DC.2



## Étape 4 :

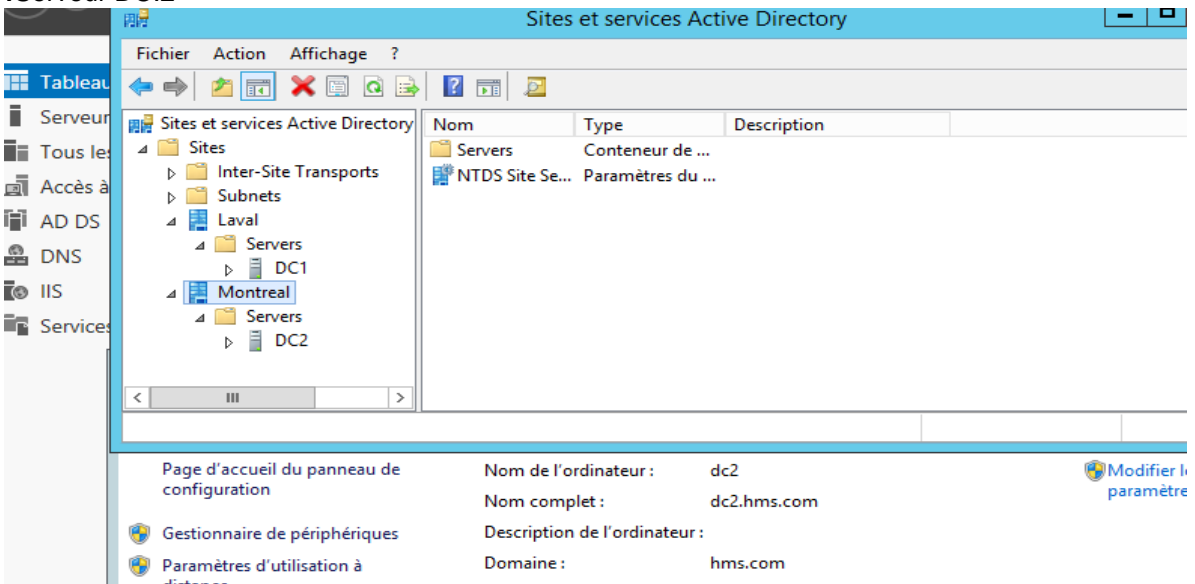
### ■ **Serveur Windows DC 1:**

- Vérifier les contrôleurs de domaines dans Utilisateurs et Ordinateurs Active Directory ou dans Domaine et Approbation A.D
- Dans Sites et Services A.D :
  - .Renommer et modifier le Site courant comme Laval.
  - .Déplacer DC 1 dans le site Laval.
  - .Cliquer sur NTDS Setting du DC 1.
  - .Vérifier la Topologie de Réplication dans toutes les tâches.
  - .Actualiser.
  - .Répliquer maintenant.
- Dans la Console MMC :
  - .Ajouter nouveau composant logiciel enfichable.
  - .Choisir Schéma Active Directory.
  - .Choisir un des Attributs, mettant le 1<sup>er</sup> *accountExpires*.
  - .Cocher Répliquer cet attribut dans le Catalogue Global.
  - .Cocher Indexer cet attribut pour des recherches en conteneur.
  - .ESSAYER avec un autre attribut.
  - .S'assurer qu'il était modifié aussi dans le Schéma de l'autre serveur DC 2.
- Vérifier la réplication entre les 2 sites en tapant la commande Shell Windows:  
    > *regsvr32 schmmgmt.dll*
- S'il n'y a pas d'erreur, alors les 2 sites répliquent bien.

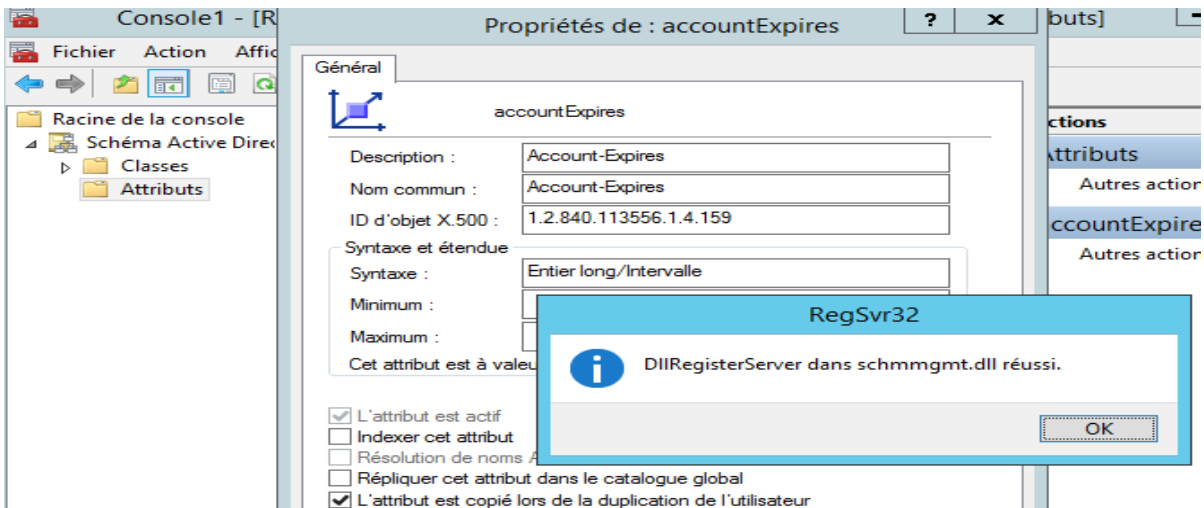
### ■ **Serveur Windows DC 2:**

- Vérifier les contrôleurs de domaines dans Utilisateurs et Ordinateurs Active Directory ou dans Domaine et Approbation A.D
- Dans Sites et Services A.D :
  - .Créer un nouveau Site comme Montréal.
  - .Déplacer DC 2 dans le site Montréal.
  - .Cliquer sur NTDS Setting du DC 2.
  - .Vérifier la Topologie de Réplication dans toutes les tâches.
  - .Actualiser.
  - .Répliquer maintenant.
- Dans la Console MMC :
  - .Ajouter nouveau composant logiciel enfichable.
  - .Choisir Schéma Active Directory.
  - .Choisir un des Attributs, mettant le 1<sup>er</sup> *accountExpires*.
  - .Cocher Répliquer cet attribut dans le Catalogue Global.
  - .Cocher Indexer cet attribut pour des recherches en conteneur.
  - .ESSAYER avec un autre attribut.
  - .S'assurer qu'il était modifié aussi dans le Schéma de l'autre serveur DC 1.
- Vérifier la réplication entre les 2 sites en tapant la commande Shell Windows:  
    > *regsvr32 schmmgmt.dll*
- S'il n'y a pas d'erreur, alors les 2 sites répliquent bien.

## .Serveur DC.2



## .Serveur DC.1

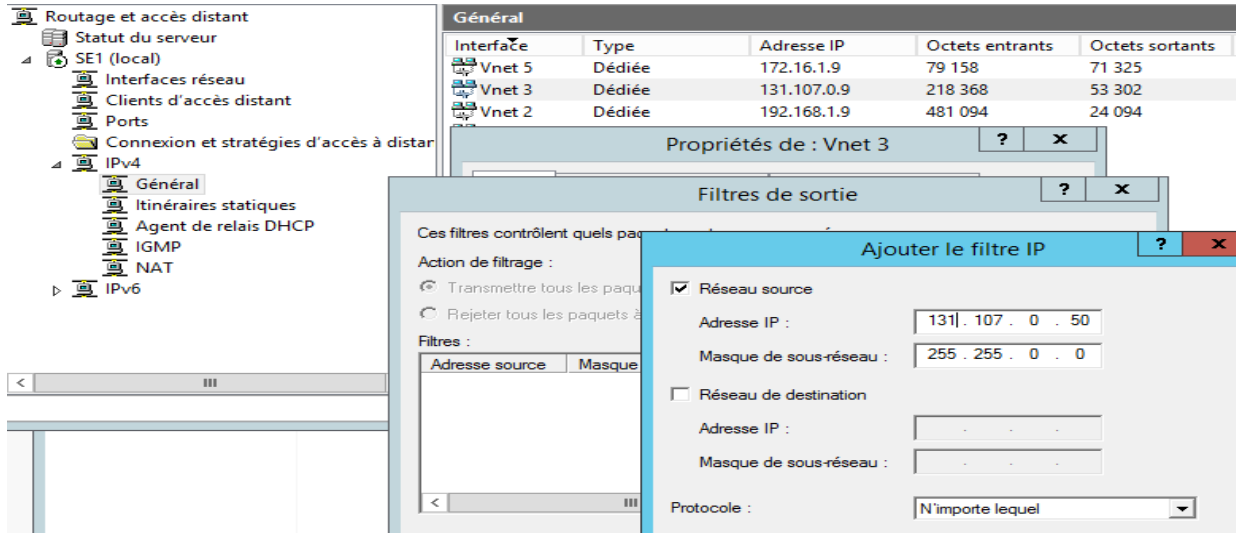


## Étape 5 :

- **Serveur DMZ 1 :**
  - Ajouter le rôle IIS et Configurer une page web et la publier
- **Serveur Membre Windows :**
  - Réserver l'adresse de la machine externe PC.0 dans le DHCP
- **Serveur d'entrée Windows :**
  - INT1: .Dans Routage Actées Distant / General / Interface Vmnet 2 / Propriété
    - .Choisir Filtre Entrée
    - .Vers n'importe quel Masque
    - .Vers n'importe quel Destination
    - .Rejeter tous sauf l'adresse Source de l'interface externe

- INT3: .Dans Routage Actées Distant / General / Interface Vmnet 2 / Propriété
- .Choisir Filtre Sortie
- .Vers n'importe quel Masque
- .Vers n'importe quel Destination
- .Rejeter tous sauf l'adresse Source de l'interface externe

.Serveur d'Entrée 1 Windows



## Étape 6 :

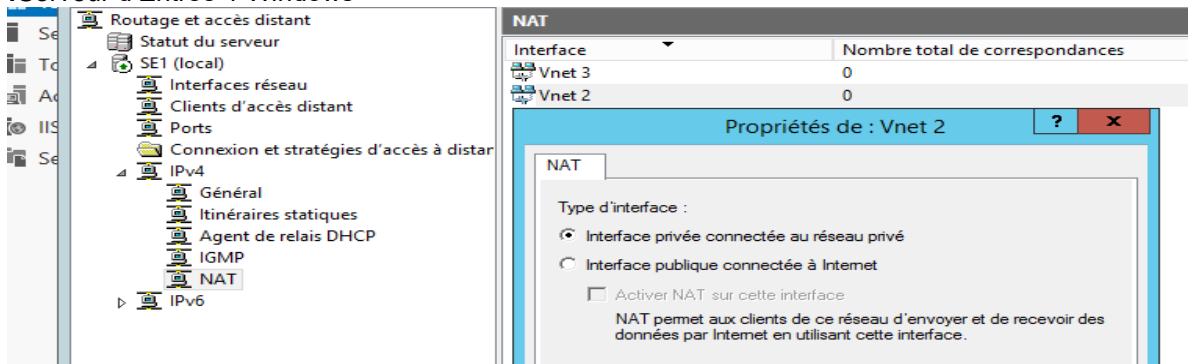
### ■ Serveur d'entrée Windows :

- Connecter l'interface externe au réseau Bridge ou NAT
- Ajouter au Protocole NAT l'interface externe dans le rôle Routage et accès distant en tant que sortie publique.
- Ajouter l'interface Interne comme interface privée afin de partager la connexion internet issue de la sortie publique à l'interne

### ■ Serveur Membre Windows :

- Configurer le proxy
- Vérifier la passerelle par défaut

.Serveur d'Entrée 1 Windows





## Étape 7:

### ■ Serveur Windows DC 2:

-Autoriser la Connexion a distance

### ■ Serveur d'entrée Linux :

-Configurer un Forward du port RDP 3389 vers le Serveur Membre Linux avec firewall En tapant la commande suivante :

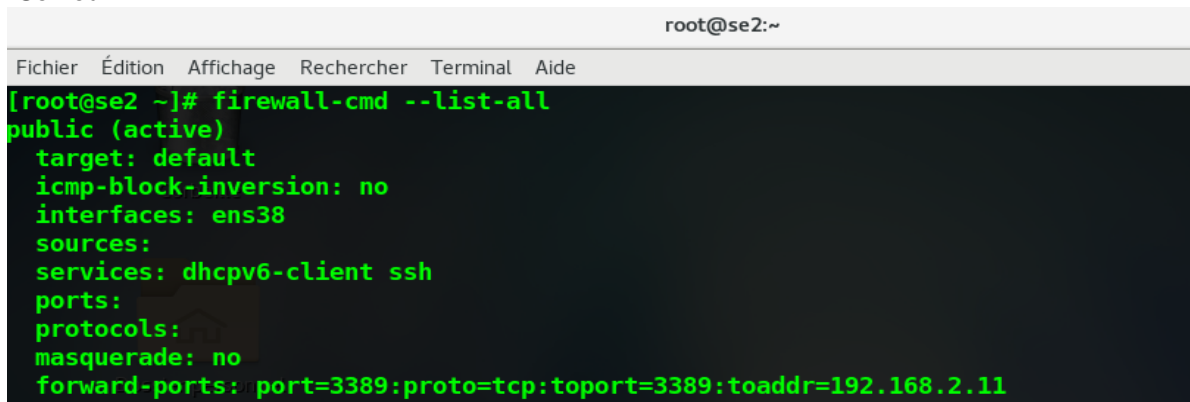
```
# firewall-cmd --permanent --add-forward-  
port=port=3389:proto=tcp:toport=3389:toaddr=192.168.2.11
```

### ■ Machine Externe PC.0:

-Configurer avec PUTTY une connexion ssh vers Serveur d'entrée Linux en spécifiant un tunnel local vers le serveur DC 2 (192.168.2.12 :3389) comme destination et comme source le port 8888

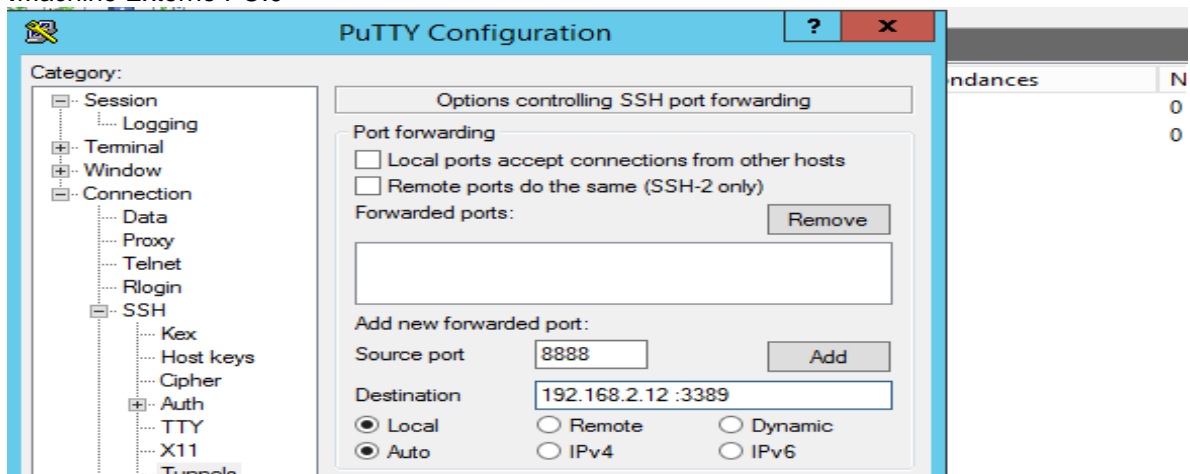
-Se Connecter comme localhost :8888

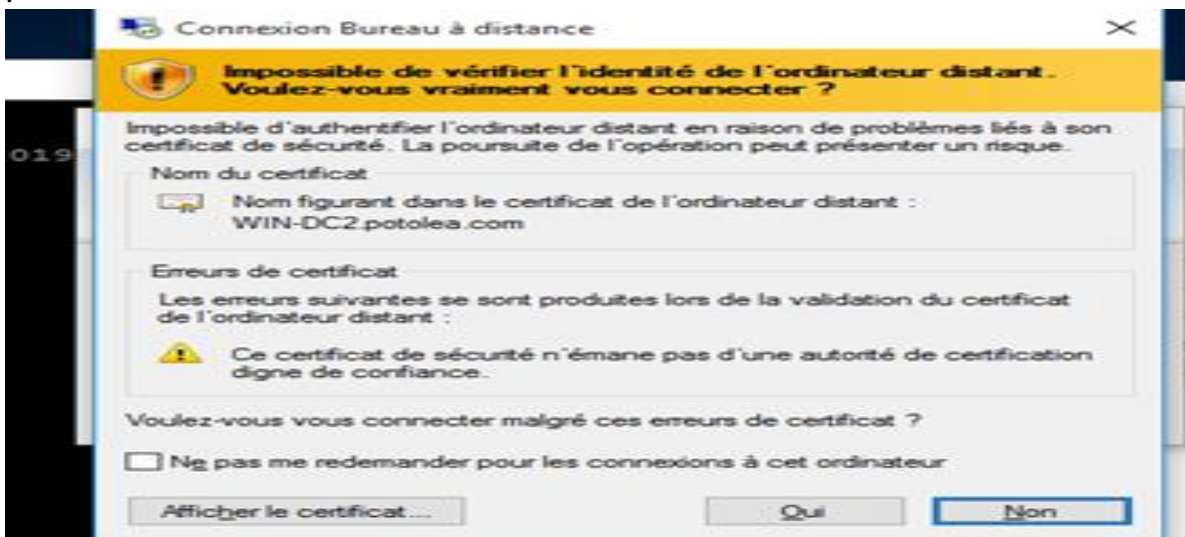
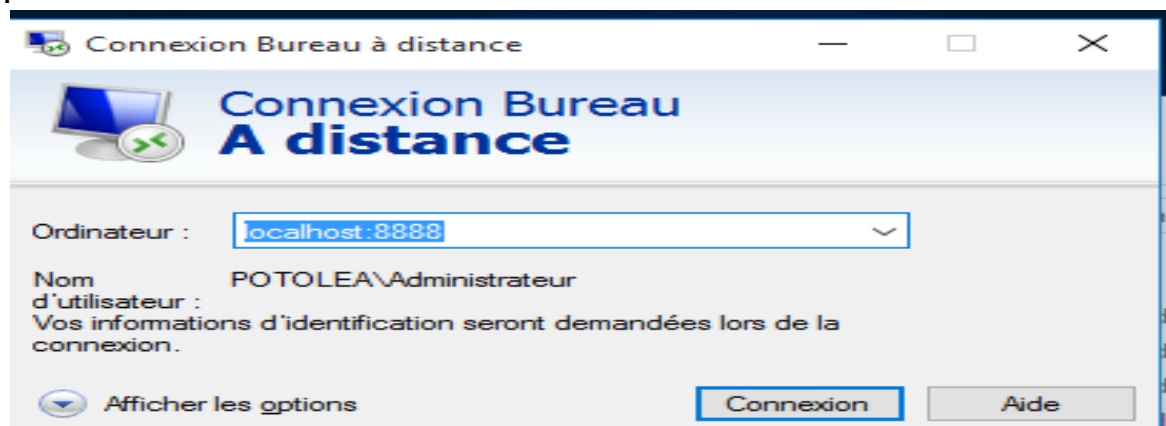
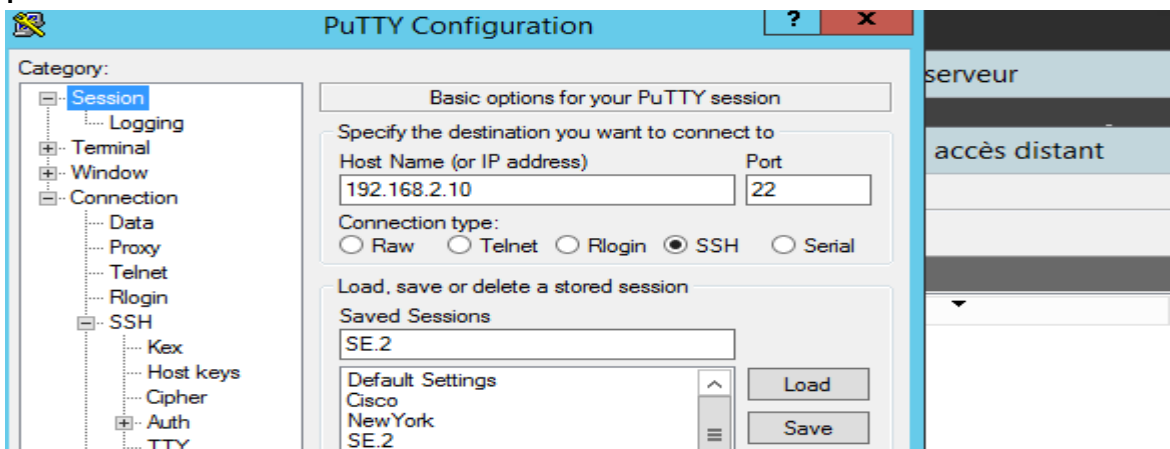
.Serveur d'Entrée Linux.2



```
root@se2:~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
[root@se2 ~]# firewall-cmd --list-all  
public (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: ens38  
  sources:  
  services: dhcpv6-client ssh  
  ports:  
  protocols:  
  masquerade: no  
  forward-ports: port=3389:proto=tcp:toport=3389:toaddr=192.168.2.11
```

.Machine Externe PC.0





## Étape 8:

### ■ Serveur Membre Windows :

- Installer et configurer le serveur mail IceWrap
- Ajouter 2 comptes Foudil et Habib et tester l'envoi et la réception

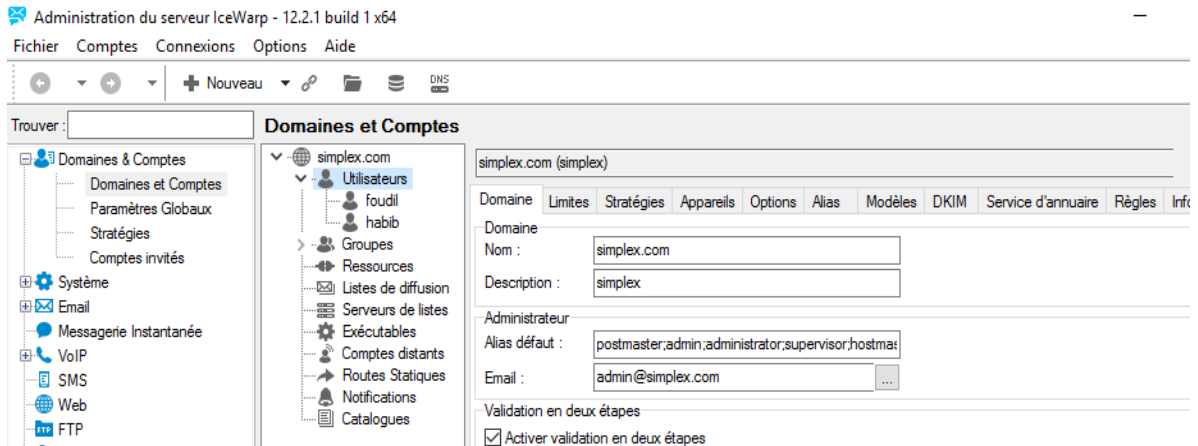
## ■ Machine Externe PC.0:

-Installer et Configurer le client de messagerie ThinderBird et spécifier l'adresse externe du Serveur d'entrée Windows comme adresse pour le serveur Mail

## ■ Serveur d'entrée Windows :

-Configurer dans Routage et Accès Distant / NAT / Interface Externe / Services et ports, le Forward de SMTP et POP3 vers l'adresse interne du Serveur Membre Windows qui le Serveur Mail

.Serveur Membre 1 Windows



## Étape 9:

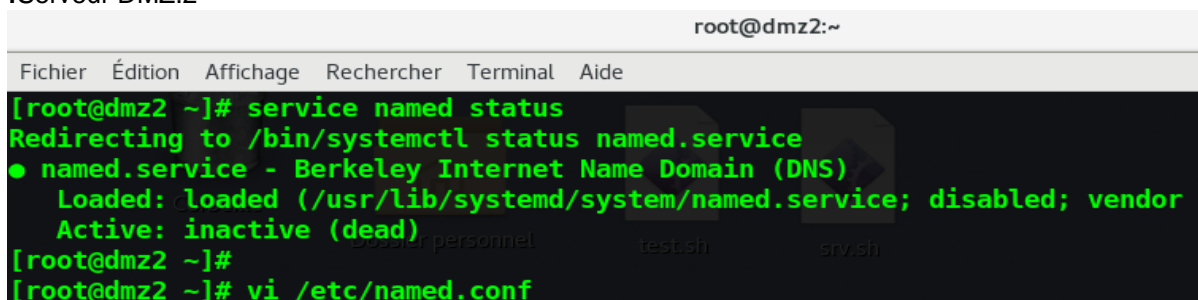
## ■ Serveur DMZ 2 :

-Installer le service BIND comme Serveur DNS  
-Configurer les 2 zones direct et inverse du domaine simplex.com  
-Ajouter l'enregistrement MX pour le Serveur Mail

## ■ Machine Externe PC.0:

-Configurer le DNS comme étant le Serveur DMZ 2  
-tester avec nslookup  
-Se connecter avec le client ThinderBird au Serveur Mail avec le nom du serveur (*mail.simplex.com*) et non pas avec l'adresse ip

.Serveur DMZ.2



```
root@dmz2:~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
#####  
zone "simplex.com" IN {  
    type master;  
    file "forward.simplex";  
    allow-update {none; };  
};  
  
zone "2.16.172.in-addr.arpa" IN {  
    type master;  
    file "reverse.simplex";  
    allow-update {none; };  
};  
#####
```

```
root@dmz2:~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
[root@dmz2 ~]#  
[root@dmz2 ~]# cat /var/named/forward.simplex  
$TTL 86400  
@ IN SOA dmz2.simplex.com. root.simplex.com. (  
2011071001;Serial  
3600      ;Refresh  
1800      ;Retry  
604800    ;Expire  
86400     ;Minimum TTL  
)  
  
@      IN      NS      dmz2.simplex.com.  
@      IN      A       172.16.2.11  
@      IN      MX      10      mail.simplex.com.  
dmz2   IN      A       172.16.2.11  
mail   IN      A       192.168.1.11
```

```
root@dmz2:~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
[root@dmz2 ~]# cat /var/named/reverse.simplex  
$TTL 86400  
@ IN SOA dmz2.simplex.com. root.simplex.com. (  
2011071001;Serial  
3600      ;Refresh  
1800      ;Retry  
604800    ;Expire  
86400     ;Minimum TTL  
)  
  
@      IN      NS      dmz2.simplex.com.  
@      IN      PTR     simplex.com.  
dmz2   IN      A       172.16.2.11  
11     IN      PTR     dmz2.simplex.com.
```

## Partie 2:

### Étape 1:

#### ■ Serveur d'entrée Linux :

-Installer et Activer le service SQUID (Proxy sous Linux)

-Modifier le fichier **squid.conf** comme suit:

```
.http_access allow localnet  
.http_access allow localhost  
.http_access allow all  
.http_port 3128  
.acl CONNECT method CONNECT  
.cache_peer 10.1.0.5 parent 8080 0 no-query default  
.never_direct allow all
```

#### ■ Serveur Membre Linux :

-Spécifier dans le navigateur le Serveur d'entrée Linux comme serveur proxy et le port 3128 ou exporter la variable proxy comme on vient de mentionner :

```
export http_proxy=http://192.168.2.10 :3128
```

-Vérifier la connexion

.Coté Serveur :



```
http_access deny all  
http_access allow all  
  
acl CONNECT method CONNECT  
  
auth_param basic program /usr/lib64/squid/basic_ncsa_auth /etc/squid/squid_passwd  
acl ncsa_users proxy_auth REQUIRED  
http_access allow ncsa_users  
  
cache_peer 10.1.0.5 parent 8080 0 no-query default  
never_direct allow all
```

### Étape 2:

#### ■ Serveur d'entrée Linux :

-Modifier le fichier **squid.conf** comme suit:

```
.acl blocksitelist dstdomain "/etc/squid/blockwebsites.lst"  
.http_access deny blocksitelist
```

-Créer le fichier **/etc/squid/blockwebsites.lst** comme suit:

```
.www.facebook.com  
.facebook.com
```

#### ■ Serveur Membre Linux :

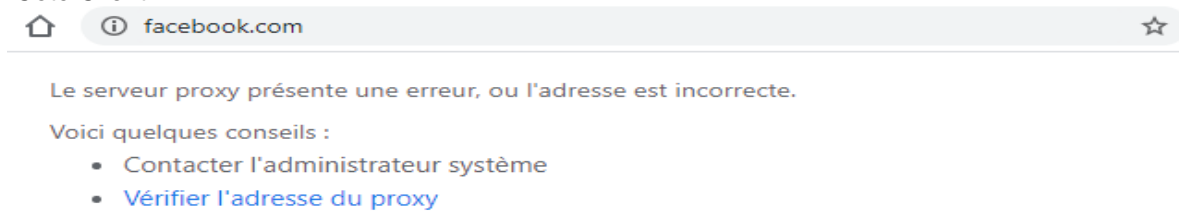
-Vérifier le l'accès refusé au site facebook.com

.Coté Serveur :

```
acl blocksitelist dstdomain "/etc/squid/blockwebsites.lst"  
http_access deny blocksitelist
```

```
root@se2:~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
[root@se2 ~]# vi /etc/squid/blockwebsites.lst  
[root@se2 ~]# cat /etc/squid/blockwebsites.lst  
www.facebook.com  
[root@se2 ~]#
```

.Coté Client :



### Étape 3:

#### ■ Serveur d'entrée Linux :

-Modifier le fichier **squid.conf** comme suit:

```
.auth_param basic program /usr/lib64/squid/bqsic_ncsa_auth  
/etc/squid/squid_passwd  
.http_access deny blocksitelist
```

-Ajouter L'utilisateur du proxy (exp : bob) lui donner un mot de passe et enregistrer son mot de passe dans un fichier qu'on va créer :

```
.# touch /etc/squid/squid_passwd  
.# htpasswd /etc/squid/squid_passwd bob  
.# taper le mot de passe de bob 2 fois
```

#### ■ Serveur Membre Linux :

-Se Connecter sur la navigateur avec l'utilisateur proxy crée

.Coté Serveur :

```
root@se2:~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
[root@se2 ~]#  
[root@se2 ~]# cat /etc/squid/squid_passwd  
bob:$apr1$EjRMjS8R$utp9X.rC7F.jUw5r3CHst1  
[root@se2 ~]#
```

```
#####
http_access deny all
http_access allow all

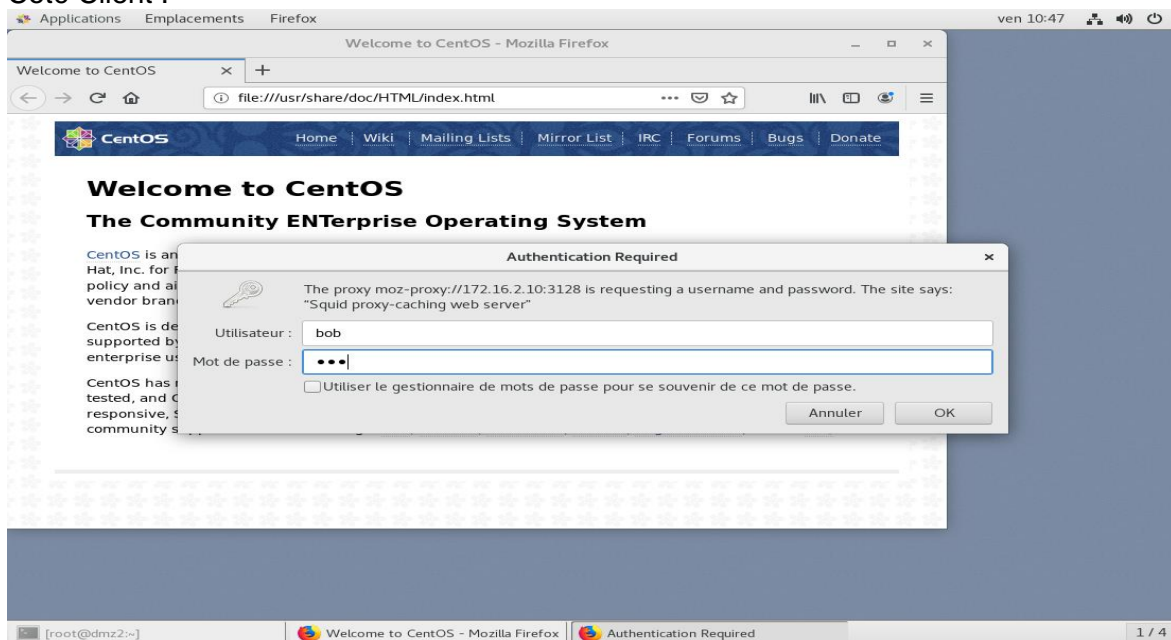
acl CONNECT method CONNECT

auth_param basic program /usr/lib64/squid/basic_ncsa_auth /etc/squid/squid_passwd
acl ncsa_users proxy_auth REQUIRED
http_access allow ncsa_users

cache_peer 10.1.0.5 parent 8080 0 no-query default
never_direct allow all

acl blocksitelist dstdomain "/etc/squid/blockwebsites.lst"
http_access deny blocksitelist
#####
```

Coté Client :



#### Étape 4:

##### ■ Serveur PFSENSE :

- Remplacer Serveur D'entrée Linux par une machine PFSENSE
- Installer et Configurer PFSENSE avec les adresses IP WAN et LAN appropriées
- Configurer le Proxy de l'école
- Ajouter 2 règles FIREWALL pour passer le flux http et https du WAN vers le LAN, d'où le partage de internet



## ■ Serveur Membre Linux :

-Configurer le Proxy de l'école dans le navigateur

.Coté Serveur :

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.4-RELEASE (Patch 3) amd64 Wed May 15 18:53:44 EDT 2019
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 92fb715c5fa6d99e00d8

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.17.0.72/25
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

The screenshot shows the pfSense web interface at the URL `https://192.168.2.10/firewall_rules.php?if=wan`. The interface is for the 'Firewall / Rules / WAN' section. A warning message at the top states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this, the 'Floating' tab is selected, showing a list of rules for the WAN interface. The rules are:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0 / 65536	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙️
✓ 1 / 0 B	IPv4 *	*	*	*	*	*	none			🔗 📄 🔄 🗑️
✓ 0 / 0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			🔗 📄 🔄 🗑️

At the bottom, there are buttons for 'Add', 'Delete', 'Save', and 'Separator'.



System / [Advanced](#) / [Miscellaneous](#)

[Admin Access](#) [Firewall & NAT](#) [Networking](#) [Miscellaneous](#) [System Tunables](#) [Notifications](#)

### Proxy Support

**Proxy URL**   
 Hostname or IP address of proxy server this system will use for its outbound Internet access.

**Proxy Port**   
 Port where proxy server is listening.

**Proxy Username**   
 Username for authentication to proxy server. Optional, leave blank to not use authentication.

**Proxy Password**    
 Password for authentication to proxy server. Confirm

## Étape 5:

### ■ Serveur PFSENSE :

- Se Connecter à partir de la machine client
- Installer le package OpenVPN-Client-Export
- Créer une Autorité de Certification
- Ajouter une **Règle** pour laisser passer le Traffic UDP dans FIREWALL
- Créer utilisateur OpenVPN PFSense ( *vpnuser* )
- Activer le Serveur VPN et le configurer pour accepter les connexions
- Exporter le client OpenVPN Vers la machine client

### ■ Machine Externe PC.0:

- Se Connecter au Serveur PFSENSE grâce au client déjà installé de l'externe

.Coté Serveur :

```

https://192.168.2.10/pkg_mgr_install.php

System / Package Manager / Package Installer

pfSense-pkg-openvpn-client-export installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation
[2/4] Installing zip-3.0_1...
[2/4] Extracting zip-3.0_1: ..... done
[3/4] Installing p7zip-16.02_1...
[3/4] Extracting p7zip-16.02_1: ..... done
[4/4] Installing pfSense-pkg-openvpn-client-export-1.4.19_2...
[4/4] Extracting pfSense-pkg-openvpn-client-export-1.4.19_2: ..... done
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Writing configuration... done.
>>> Cleaning up cache... done.
Success
  
```





pfSense  
COMMUNITY EDITION

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

System / Certificate Manager / CAs

CAs   Certificates   Certificate Revocation

### Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
OpenVPN_CA	✓	self-signed	0	ST=QC, OU=AEC, O=College-Rosemont, L=Montreal, CN=internal-ca, C=CA Valid From: Mon, 20 Jan 2020 04:05:30 -0500 Valid Until: Thu, 17 Jan 2030 04:05:30 -0500		   

+ Add





pfSense  
COMMUNITY EDITION


WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

System / User Manager / Users

Users   Groups   Settings   Authentication Servers

### Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	 vpnuser		✓		 

+ Add    Delete

https://192.168.2.10/vpn\_opensense\_server.php

**pfSense**  
COMMUNITY EDITION

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

### OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP4 / 1194	172.16.0.0/16	Crypto: AES-128-CBC/SHA256 D-H Params: 2048 bits	(tun)	

+ Add

https://192.168.2.10/vpn\_opensense\_server.php

Save as default

Search

Search term

Enter a search string or \*nix regular expression to search.

Servers configured with features that require OpenVPN 2.4 will not work with OpenVPN 2.3.x or older clients. These features include: AEAD encryption such as AES-GCM, X25519, and more.

### OpenVPN Clients

User

vpuser

Connexion OpenVPN (pfSense-UDP4-1194-vpuser-config)

Etat actuel: Connecté

```
Mon Jan 20 10:06:18 2020 OpenVPN 2.3.18 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [PKCS11] [IPv6] bu
Mon Jan 20 10:06:18 2020 Windows version 5.1 (Windows 7) 64bit
Mon Jan 20 10:06:18 2020 library versions: OpenSSL 1.0.2 25 May 2017, LZO 2.10
Mon Jan 20 10:06:30 2020 Control Channel Authentication: using 'pfSense-UDP4-1194-vpuser-tls.key' as a O
Mon Jan 20 10:06:30 2020 UDPv4 link local (bound): [undef]
Mon Jan 20 10:06:30 2020 UDPv4 link remote: [AF_INET]10.17.0.72:1194
Mon Jan 20 10:06:30 2020 WARNING: this configuration may cache passwords in memory -- use the auth-noc
Mon Jan 20 10:06:30 2020 [Server/OpenVPN] Peer Connection Initiated with [AF_INET]10.17.0.72:1194
Mon Jan 20 10:06:32 2020 do_fconfig, tt->ipv6=0, tt->did_fconfig_ipv6_setup=0
Mon Jan 20 10:06:32 2020 open_tun, tt->ipv6=0
Mon Jan 20 10:06:32 2020 TAP-WIN32 device [Connexion au réseau local] opened: \\Global\\{7BF1E204-
Mon Jan 20 10:06:32 2020 Set TAP-Windows TUN subnet mode network/local/netmask = 172.16.0.0/172.16
Mon Jan 20 10:06:32 2020 Notified TAP-Windows driver to set a DHCP IP/netmask of 172.16.0.2/255.255.0.0
Mon Jan 20 10:06:32 2020 Successful ARP Flush on interface [21] {7BF1E204-0914-46AF-BBF4-B2126CC9E7
Mon Jan 20 10:06:37 2020 Initialization Sequence Completed
```

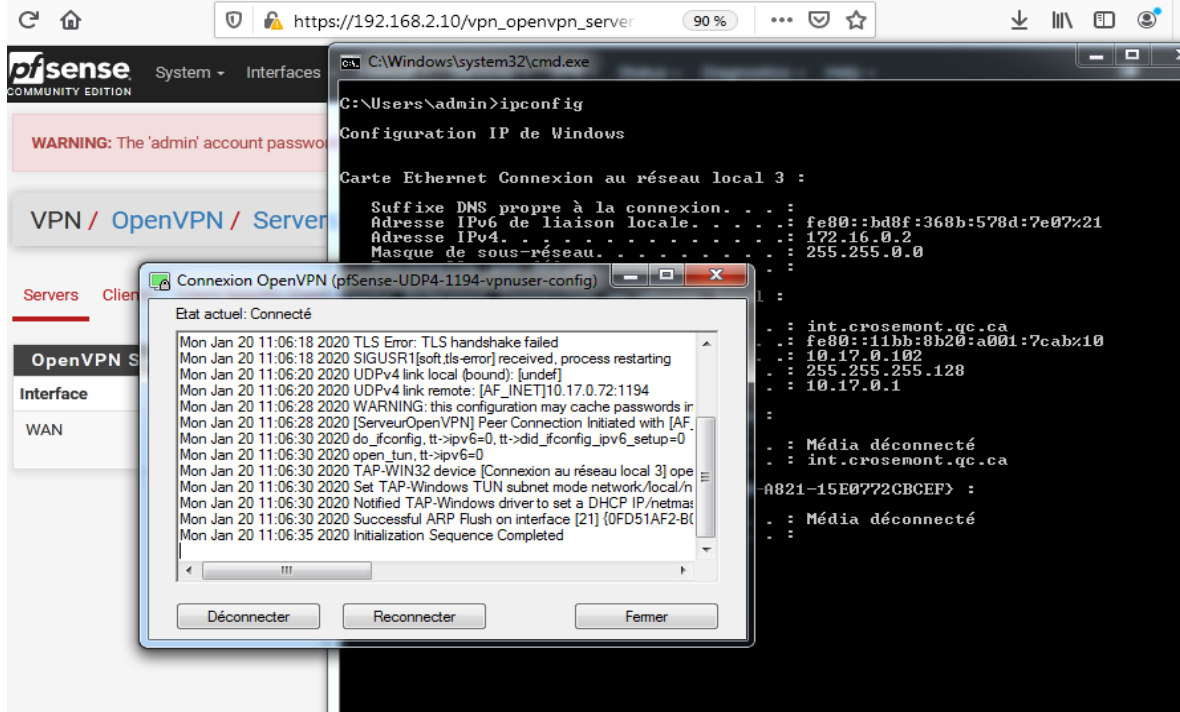
Only OpenVPN-compatible certificates are shown

If a client is missing from the list it is likely due to a CA mismatch between the OpenVPN server instance and the client certificate, the client certificate does not exist on this firewall, or a user certificate is not associated with a user when local database authentication is enabled.

OpenVPN 2.4.8 requires Windows 7 or later  
The "win6" Windows installers include the tap-windows6 driver which requires Windows Vista or later.  
The "XP" Windows installers work on Windows XP and later versions.

OpenVPN GUI  
Connecté à: pfSense-UDP4-1194-vpuser-config  
Connecté depuis: 20/01/2020 10:06  
Adresse IP assignée: 172.16.0.2

.Coté Client :



## Étape 6:

### ■ Machine Externe PC.2:

-Télécharger et Installer dsniff 2.4:

```
# wget https://centos.pkgs.org/6/epel-x86_64/dsniff-2.4-0.23.b1.el6.x86_64.rpm.html
```

```
# yum install dsniff
```

-Effectuer cette attaque arpspoof : `# arpspoof -i ens33 -t 10.17.0.72 10.17.0.1`

### ■ Serveur PFSENSE :

- Se Connecter et Vérifier dans le journal les attaques

-Vérifier que les clients derrières le Serveur PFSENSE n'ont plus internet

.Machine externe (Hacker)



```
[root@Cos8 ~]#
[root@Cos8 ~]# arpspoof -i ens33 -t 10.17.0.72 10.17.0.1
0:c:29:86:19:b6 0:c:29:43:86:3a 0806 42: arp reply 10.17.0.1 is-at 0:c:29:86:19:b6
0:c:29:86:19:b6 0:c:29:43:86:3a 0806 42: arp reply 10.17.0.1 is-at 0:c:29:86:19:b6
0:c:29:86:19:b6 0:c:29:43:86:3a 0806 42: arp reply 10.17.0.1 is-at 0:c:29:86:19:b6
0:c:29:86:19:b6 0:c:29:43:86:3a 0806 42: arp reply 10.17.0.1 is-at 0:c:29:86:19:b6
```

```
[root@Cos8 ~]#
[root@Cos8 ~]# arpspoof -i ens33 -t 10.17.0.72 10.1.0.5
0:c:29:86:19:b6 0:c:29:43:86:3a 0806 42: arp reply 10.1.0.5 is-at 0:c:29:86:19:b6
0:c:29:86:19:b6 0:c:29:43:86:3a 0806 42: arp reply 10.1.0.5 is-at 0:c:29:86:19:b6
0:c:29:86:19:b6 0:c:29:43:86:3a 0806 42: arp reply 10.1.0.5 is-at 0:c:29:86:19:b6
0:c:29:86:19:b6 0:c:29:43:86:3a 0806 42: arp reply 10.1.0.5 is-at 0:c:29:86:19:b6
```

#### .Serveur PFSENSE

Jan 20 06:06:23	check_reload_status	Syncing firewall
Jan 20 06:06:25	check_reload_status	Reloading filter
Jan 20 07:29:42	kernel	arp: 10.17.0.1 moved from d4:c1:9e:2d:73:80 to 00:0c:29:86:19:b6 on em0
Jan 20 07:29:47	kernel	arp: 10.17.0.1 moved from 00:0c:29:86:19:b6 to d4:c1:9e:2d:73:80 on em0
Jan 20 07:29:48	kernel	arp: 10.17.0.1 moved from 00:0c:29:86:19:b6 to d4:c1:9e:2d:73:80 on em0

#### .Client réseaux du Serveur

La connexion a été refusée par le serveur proxy

Firefox est configuré pour utiliser un serveur proxy mais celui-ci n'accepte pas les connexions.

- Vérifiez que les paramètres du proxy sont corrects ;
- Contactez votre administrateur réseau pour vous assurer que le serveur proxy fonctionne.

### Étape 7:

#### ■ Serveur PFSENSE :

- Modifier et Spécifier le Mac adresse d'une façon statique et permanente de la passerelle l'interface externe, comme ça on ne pourra plus la changer de l'externe, d'où mon ARP est permanent : `# arp -S 10.17.0.1 d4:c1:9e:2d:73:80`
- Vérifier dans le journal les attaques
- Vérifier que les clients derrières le Serveur PFSENSE ont l'accès à internet

## ■ Machine Externe PC.2:

- Refaire la même attaque arpspoof : `# arpspoof -i ens33 -t 10.17.0.72 10.17.0.1`

.Serveur PFSense

```
Enter an option: 8
[2.4.4-RELEASE][root@pfSense.localdomain]/root: arp -a
pfSense.localdomain (192.168.2.10) at 00:0c:29:43:86:44 on em1 permanent [ethernet]
? (10.1.0.75) at (incomplete) on em0 expired [ethernet]
? (10.17.0.49) at 64:00:6a:73:02:08 on em0 expires in 1091 seconds [ethernet]
? (10.17.0.72) at 00:0c:29:43:86:3a on em0 permanent [ethernet]
? (10.17.0.1) at d4:c1:9e:2d:73:80 on em0 expires in 1197 seconds [ethernet]
? (10.17.0.102) at 00:0c:29:a1:1a:08 on em0 expires in 1166 seconds [ethernet]
[2.4.4-RELEASE][root@pfSense.localdomain]/root:
[2.4.4-RELEASE][root@pfSense.localdomain]/root:
[2.4.4-RELEASE][root@pfSense.localdomain]/root: arp -S 10.17.0.1 d4:c1:9e:2d:73:80
10.17.0.1 (10.17.0.1) deleted
[2.4.4-RELEASE][root@pfSense.localdomain]/root:
```

.Machine externe (Hacker)

```
[root@Cos8 ~]#
[root@Cos8 ~]# arpspoof -i ens33 -t 10.17.0.72 10.17.0.1
0:c:29:86:19:b6 0:c:29:43:86:3a 0806 42: arp reply 10.17.0.1 is-at 0:c:29:86:19:b6
0:c:29:86:19:b6 0:c:29:43:86:3a 0806 42: arp reply 10.17.0.1 is-at 0:c:29:86:19:b6
0:c:29:86:19:b6 0:c:29:43:86:3a 0806 42: arp reply 10.17.0.1 is-at 0:c:29:86:19:b6
0:c:29:86:19:b6 0:c:29:43:86:3a 0806 42: arp reply 10.17.0.1 is-at 0:c:29:86:19:b6
```

. Serveur PFSense

https://192.168.2.10/status_logs.php		
Jan 20 08:04:58	login	login on ttyv0 as root
Jan 20 08:10:46	kernel	arp: 00:0c:29:86:19:b6 attempts to modify permanent entry for 10.17.0.1 on em0
Jan 20 08:10:48	kernel	arp: 00:0c:29:86:19:b6 attempts to modify permanent entry for 10.17.0.1 on em0
Jan 20 08:10:50	kernel	arp: 00:0c:29:86:19:b6 attempts to modify permanent entry for 10.17.0.1 on em0

## Étape 8:

### ■ Serveur PFSense :

- Installer le Package SNORT qui est le Détecteur d'intrusion sur PfSense
- Activer SNORT sur l'interface WAN
- Activer les Alertes Systèmes dans les Journaux de SNORT
- S'enregistrer a SNORT pour Mettre à jour la Base de Données des Signatures
- Configurer les paramètres de Mise à jour en utilisant notre code unique du compte
- Appliquer les Mises à jours et Démarrer SNORT
- Configurer les Règles et les alertes du WAN
- Modifier le fichier `/usr/local/etc/snort/snort.conf` en décommentant la ligne :  
`Preprocessor sfportscan : proto { all } memcap { 10000000 } sens_level { low }`
- Vérifier les Alertes et les Blocages après le NMAP lancé de la Machine Externe

## ■ Machine Externe PC.2:

-Lancer NMAP: *# nmap -sS 10.17.0.72*

### .Serveur PFSENSE

https://192.168.2.10/pkg\_mgr\_install.php

pfSense-pkg-snort installation successfully completed.

Installed Packages Available Packages **Package Installer**

#### Package Installation

Configuration files are located in `/usr/local/etc/snort` directory.

Please note that, by default, snort will truncate packets larger than the default `snaplen` of 15158 bytes. Additionally, `LRO` may cause issues with Stream5 target-based reassembly. It is recommended to disable `LRO`, if your card supports it.

This can be done by appending `'-lro'` to your `ifconfig` line in `rc.conf`.

=====

Message from pfSense-pkg-snort-3.2.9.10:

Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages at the Services - Snort - Global tab. Afterwards visit the Updates tab to download your configured `rulesets`.

>>> Cleaning up cache... done.

Success

https://192.168.2.10/snort/snort\_interfaces\_edit.php?id=0

#### General Settings

Enable	<input checked="" type="checkbox"/> Enable interface
Interface	<div>WAN (em0)</div> <div>Choose the interface where this Snort instance will inspect traffic.</div>
Description	<div>WAN</div> <div>Enter a meaningful description here for your reference.</div>
Snap Length	<div>1518</div> <div>Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.</div>

#### Alert Settings

Send Alerts to System Log	<input checked="" type="checkbox"/> Snort will send Alerts to the firewall's system log. Default is Not Checked.
System Log Facility	<div>LOG_AUTH</div> <div>Select system log Facility to use for reporting. Default is LOG_AUTH.</div>
System Log Priority	<div>LOG_ALERT</div> <div>Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.</div>
Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert
Kill States	<input checked="" type="checkbox"/> Checking this option will kill firewall states for the blocked IP. Default is checked.
Which IP to Block	<div>BOTH</div>

ofsense  
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Services / Snort / Interfaces

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
<input type="checkbox"/> WAN (em0)		AC-BNFA	ENABLED	DISABLED	WAN	

Add Delete

Services / Snort / Global Settings

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Snort Subscriber Rules

**Enable Snort VRT** ☒ Click to enable download of Snort free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rules Account](#)  
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

**Snort Oinkmaster Code**   
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Snort GPLv2 Community Rules

**Enable Snort GPLv2** ☒ Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

**Enable ET Open** ☒ Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

**Enable ET Pro** ☐ Click to enable download of Emerging Threats Pro rules

[Sign Up for an ETPro Account](#)  
ETPro for Snort offers daily updates and extensive coverage of current malware threats.

Sourcefire OpenAppID Detectors

**Enable OpenAppID** ☒ Click to enable download of Sourcefire OpenAppID Detectors



### Rules Update Settings

Update Interval	1 DAY
Please select the interval for rule updates. Choosing NEVER disables auto-updates.	
Update Start Time	00:05
Enter the rule update start time in 24-hour format (HH:MM). Default is 00:05. Rules will update at the interval chosen above starting at the time specified here. For example, using the default start time of 00:05 and choosing 12 Hours for the interval, the rules will update at 00:05 and 12:05 each day.	
Hide Deprecated Rules Categories	<input type="checkbox"/> Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.
Disable SSL Peer Verification	<input type="checkbox"/> Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

### General Settings

Remove Blocked Hosts Interval	1 HOUR
Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.	
Remove Blocked Hosts After Deinstall	<input checked="" type="checkbox"/> Click to clear all blocked hosts added by Snort when removing the package.
Keep Snort Settings After Deinstall	<input checked="" type="checkbox"/> Click to retain Snort settings after package removal.
Startup/Shutdown Logging	<input type="checkbox"/> Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

## Services / Snort / Update Rules

Snort Interfaces Global Settings **Updates** Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

### Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	c2975a2275f093e6efd8b7591fba37f3	Monday, 20-Jan-20 10:24:29 EST
Snort GPLv2 Community Rules	cbca669cfcb493afaab306a8bf6d997c	Monday, 20-Jan-20 10:24:30 EST
Emerging Threats Open Rules	976dbe685e71d5de5fc63bafb2250f5e	Monday, 20-Jan-20 10:24:30 EST
Snort OpenAppID Detectors	29c60f648df483ced689ee2fce1a0d20	Monday, 20-Jan-20 10:24:30 EST
Snort OpenAppID RULES Detectors	Not Enabled	Not Enabled

### Update Your Rule Set

Last Update	Jan-20 2020 10:24	Result: <b>Success</b>
Update Rules	<input checked="" type="button" value="Update Rules"/>	<input type="button" value="Force Update"/>
Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.		

Services / Snort / Interfaces

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
<input type="checkbox"/> WAN (em0)	<span style="color: green;">✔</span> <span style="color: blue;">🔄</span>	AC-BNFA	ENABLED	DISABLED	WAN	<span style="color: blue;">🔧</span> <span style="color: blue;">📄</span> <span style="color: red;">🗑️</span>

+ Add 🗑️ Delete

Select the rulesets (Categories) Snort will load at startup

✔ - Category is auto-enabled by SID Mgmt conf files  
✖ - Category is auto-disabled by SID Mgmt conf files

Select All Unselect All Save

Enable Ruleset: Snort GPLv2 Community Rules					
<input checked="" type="checkbox"/>	Snort GPLv2 Community Rules (Talos certified)				
Enable	Ruleset: ET Open Rules	Enable	Ruleset: Snort Text Rules	Enable	Ruleset: Snort SO Rules
<input checked="" type="checkbox"/>	emerging-activex.rules	<input checked="" type="checkbox"/>	snort_app-detect.rules	<input checked="" type="checkbox"/>	snort_browser-chrome.so.rules
<input checked="" type="checkbox"/>	emerging-attack_response.rules	<input checked="" type="checkbox"/>	snort_attack-responses.rules	<input checked="" type="checkbox"/>	snort_browser-ie.so.rules
<input checked="" type="checkbox"/>	emerging-botcc.portgrouped.rules	<input checked="" type="checkbox"/>	snort_backdoor.rules	<input checked="" type="checkbox"/>	snort_browser-other.so.rules
<input checked="" type="checkbox"/>	emerging-botcc.rules	<input checked="" type="checkbox"/>	snort_bad-traffic.rules	<input checked="" type="checkbox"/>	snort_browser-webkit.so.rules

Snort OPENAPPID rules are not enabled.

```
# Portscan detection. For more information, see README.sfportscan
preprocessor sfportscan: proto { all } memcap { 10000000 } sense_level { low }
```

. Machine externe (Hacker)

```
[root@Cos8 ~]# ifconfig |grep -w inet
inet 10.17.0.61 netmask 255.255.255.128 broadcast 10.17.0.127
inet 127.0.0.1 netmask 255.0.0.0
inet 192.168.122.1 netmask 255.255.255.0 broadcast 192.168.122.255
[root@Cos8 ~]#
[root@Cos8 ~]# nmap -sS 10.17.0.72
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-20 16:10 EST
Nmap scan report for pfSense.int.crosemont.qc.ca (10.17.0.72)
Host is up (-0.20s latency).
All 1000 scanned ports on pfSense.int.crosemont.qc.ca (10.17.0.72) are filtered
MAC Address: 00:0C:29:43:86:3A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.64 seconds
[root@Cos8 ~]#
```

. Serveur PFSENSE

https://192.168.2.10/snort/snort\_alerts.php

2020-01-20 11:32:50	2	TCP	Potentially Bad Traffic	10.17.0.61	59564	10.17.0.72	5432	1:2010939	ET SCAN Suspicious inbound to PostgreSQL port 5432
2020-01-20 11:32:50	2	TCP	Potentially Bad Traffic	10.17.0.61	59563	10.17.0.72	5432	1:2010939	ET SCAN Suspicious inbound to PostgreSQL port 5432

Services / Snort / Blocked Hosts

Snort Interfaces Global Settings Updates Alerts **Blocked** Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

**Blocked Hosts and Log View Settings**

**Blocked Hosts** [Download](#) [Clear](#)

All blocked hosts will be saved All blocked hosts will be removed

**Refresh and Log View** [Save](#) ☒ Refresh Default is ON

500 Number of blocked entries to view. Default is 500

**Last 500 Hosts Blocked by Snort**

#	IP	Alert Descriptions and Event Times	Remove
1	10.17.0.61 Q	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE – 2020-01-20 11:36:07 (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE – 2020-01-20 11:34:10 ET SCAN Suspicious inbound to MySQL port 3306 – 2020-01-20 11:32:34 ET SCAN Potential VNC Scan 5800-5820 – 2020-01-20 11:32:37 ET SCAN Potential VNC Scan 5900-5920 – 2020-01-20 11:32:38 ET SCAN Suspicious inbound to Oracle SQL port 1521 – 2020-01-20 11:32:44 ET SCAN Suspicious inbound to MSSQL port 1433 – 2020-01-20 11:32:46 ET SCAN Suspicious inbound to PostgreSQL port 5432 – 2020-01-20 11:32:50	<a href="#">Remove</a>

1 host IP address is currently being blocked Snort.

## Étape 9:

### ■ Serveur PFSENSE 1 (Client OpenVPN):

-Comme PFSense.2 on le transforme en Proxy:

- Remplacer Serveur D'entrée Windows par une machine PFSENSE
- Installer et Configurer PFSENSE avec les adresses IP WAN et LAN appropriées
- Configurer le Proxy de l'école
- Ajouter 3 Règles FIREWALL pour Autoriser Udp, Http et Https du WAN au LAN

### ■ Serveur PFSENSE 2 (Server OpenVPN):

-Ajouter un Serveur OpenVPN en spécifiant :

- .Server Mode: Peer to Peer (Shared Key) et Copier la Shared Key
- .Port 1195, Réseaux Tunnel 11.0.0.0/24, Réseaux Distant 192.168.1.0/24
- .Ajouter Règles FIREWALL OpenVPN pour autoriser tous IPv4
- . Vérifier Statut du Serveur

-Partager un dossier dans le Réseau 2 Puis autoriser l'accès au Réseau 1

### ■ Serveur PFSENSE 1 :

- Ajouter un Client OpenVPN en spécifiant :

- .Server Mode: Peer to Peer (Shared Key) et Coller la Shared Key
- .Port 1195, Réseaux Tunnel 11.0.0.0/24, Réseaux Distant 192.168.1.0/24
- .Server Host : 10.17.0.72 (ou 10.17.0.113) (IP Server OpenVPN)
- .Ajouter Règles FIREWALL OpenVPN pour autoriser tous IPv4
- .Vérifier Statut de la connexion avec le Serveur.

-Vérifier la Connexion Client-Serveur et l'accès au Réseau 2 avec : *tracert IP.r2*

-Vérifier l'accès au partage du Réseau 2, à partir du Réseau 1

[VPN](#) / [OpenVPN](#) / [Servers](#)

[Servers](#)
[Clients](#)
[Client Specific Overrides](#)
[Wizards](#)
[Client Export](#)
[Shared Key Export](#)

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP4 / 1194	172.16.0.0/16	Crypto: AES-128-CBC/SHA256 D-H Params: 2048 bits	(tun)	

Cryptographic Settings

Shared Key

```
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
12c72e350d8f5bc501b126b6d9fa362d
c5db20cd248a447a6ebf951ee70ffed6
8e7372306f16466d7dfcabab4d0d84da
```

Paste the shared key here

Encryption

AES-128-CBC (128 bit key, 128 bit block)

🏠

🔒 [https://192.168.2.10/vpn-openvpn\\_server.php?act=ne](https://192.168.2.10/vpn-openvpn_server.php?act=ne) 90% ... 📄 ⭐

Tunnel Settings

IPv4 Tunnel Network

11.0.0.0/24

This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

IPv6 Tunnel Network

This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

IPv4 Remote network(s)

192.168.1.0/24

IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.

Firewall / Rules / OpenVPN

Floating WAN LAN\_VNET\_4 LAN\_VNET\_6 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 0 B	IPv4 *	*	*	*	*	none			<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Save</a> <a href="#">Separator</a>

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

Status / OpenVPN

Server UDP4:1194 Client Connections

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent/Received
Status: <a href="#">✓</a> Actions: <a href="#">C</a> <a href="#">@</a>				

Peer to Peer Server Instance Statistics

Name	Status	Connected Since	Virtual Address	Remote Host	Bytes Sent / Received	Service
Server UDP4:1195					0 B / 0 B	<a href="#">✓</a> <a href="#">C</a> <a href="#">@</a>

## . Serveur PFSENSE 1 (Client)

VPN / OpenVPN / Clients

Servers Clients Client Specific Overrides Wizards

OpenVPN Clients

Interface	Protocol	Server	Description	Actions
<a href="#">+ Add</a>				

General Information

**Disabled** ☐ Disable this client  
Set this option to disable this client without removing it from the list.

**Server mode**

**Protocol**

**Device mode**   
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.  
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

**Interface**   
The interface used by the firewall to originate this OpenVPN client connection

**Local port**   
Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.

**Server host or address**   
The IP address or hostname of the OpenVPN server.

**Server port**   
The port used by the server to receive client connections.

→ ↻ 🏠 ⚠ Non sécurisé | 192.168.1.10/vpn\_openvpn\_client.php?act=new 🔍 ⭐ 👤

### Cryptographic Settings

Peer Certificate Authority No Certificate Authorities defined. One may be created here: [System > Cert. Manager](#)

Auto generate ☐ Automatically generate a shared key

Shared Key

```
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
12c72e350d8f5bc501b126b6d9fa362d
c5db20cd248a447a6ebf951ee70ffed6
```

Paste the shared key here

Encryption Algorithm AES-128-CBC (128 bit key, 128 bit block) ▼

The Encryption Algorithm used for data channel packets when Negotiable Cryptographic Parameter (NCP) support is not available.

→ ↻ 🏠 ⚠ Non sécurisé | 192.168.1.10/vpn\_openvpn\_client.php?act=new 🔍 ⭐ 👤

### Tunnel Settings

IPv4 Tunnel Network 11.0.0.0/24

This is the IPv4 virtual network used for private communications between this client and the server expressed using CIDR notation (e.g. 10.0.8.0/24). The second usable address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.

IPv6 Tunnel Network

This is the IPv6 virtual network used for private communications between this client and the server expressed using CIDR notation (e.g. fe80::/64). When set static using this field, the ::2 address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.

IPv4 Remote network(s) 192.168.1.0/24

IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.

→ ↻ 🏠 ⚠ Non sécurisé | 192.168.1.10/status\_openvpn.php 🔍 ⭐

### Status / OpenVPN

🔧 📊 📋 ?

#### Client Instance Statistics

Name	Status	Connected Since	Local Address	Virtual Address	Remote Host	Bytes Sent/Received	Service
Client UDP4:1194	up	Wed Jan 22 6:05:45 2020	10.17.0.32:1194	11.0.0.2	10.17.0.113:1194	544 B / 464 B	🟢 ↻ 🔄

→ ↻ 🏠 🔒 https://192.168.2.10/status\_openvpn 90 % ... 📋 ⭐

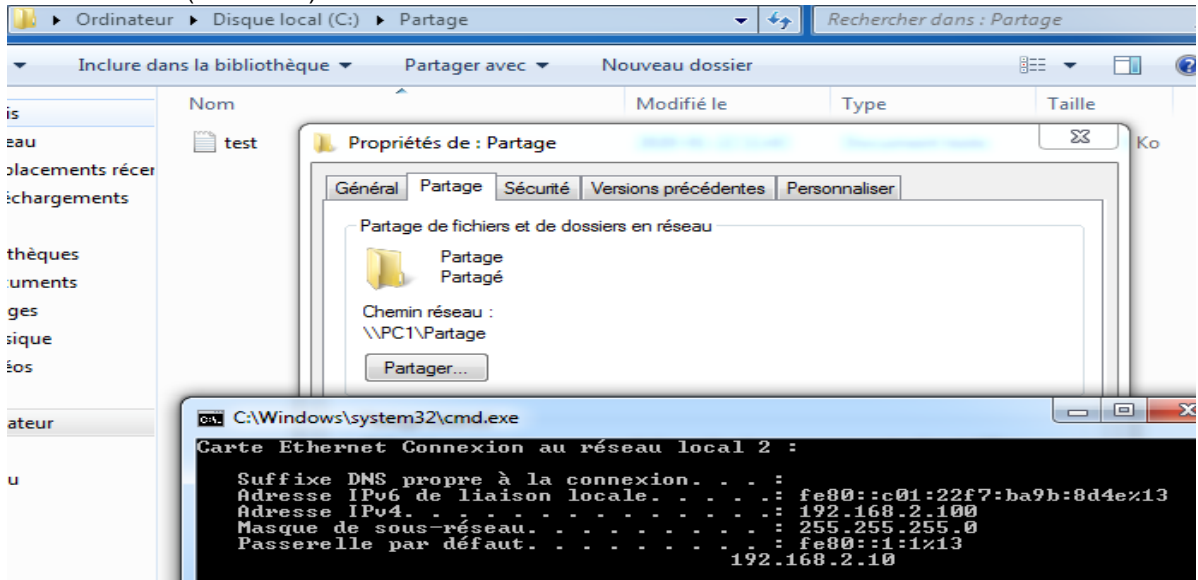
### Status / OpenVPN

🔧 📊 📋 ?

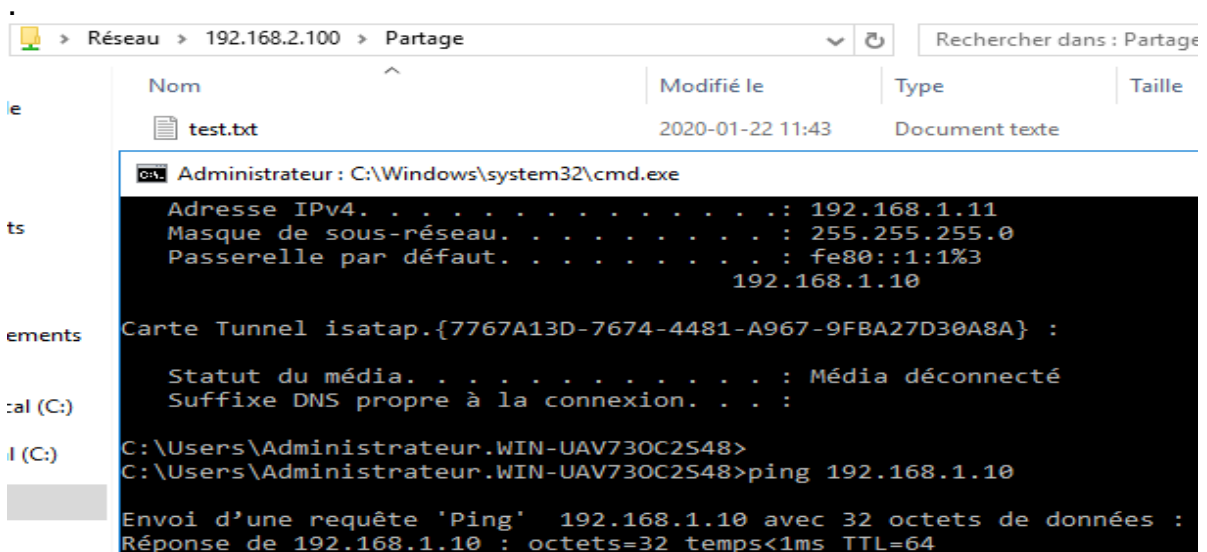
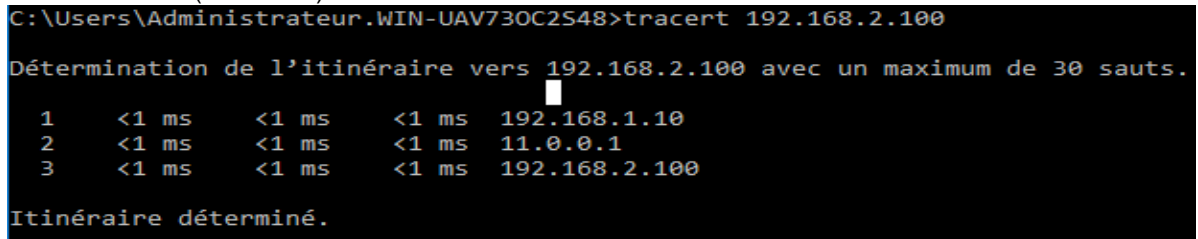
#### Peer to Peer Server Instance Statistics

Name	Status	Connected Since	Virtual Address	Remote Host	Bytes Sent / Received	Service
Server UDP4:1194	up	Wed Jan 22 6:05:42 2020	11.0.0.1	10.17.0.32	864 B / 944 B	🟢 ↻ 🔄

## .Serveur DC.2 (Réseau 2)



## . Serveur DC.1 (Réseau 1)



## Partie 3:

### Étape 1:

#### ■ Serveur Windows DC 1:

- Vérifier la Connectivité vi PFSENSE.2 avec le Réseau 2 et spécifiquement au *Serveur DC.2*
- Ajouter un disque de 20 Go pour le Sauvegarde
- Installer la Fonctionnalité Sauvegarde Windows Server
- Lancer une Sauvegarde Complete en spécifiant le disque ajouté
- Supprimer l'OU *backup*
- Redémarrer en Mode Réparation de Service d'Annuaire en utilisant **F8**
- Se connecter en admin local et lancer une Récupération de l'état du système en spécifiant l'emplacement d'origine
- Redémarrer encore en Mode Réparation de Service d'Annuaire en utilisant **F8**
- Se connecter en admin local et taper sur le Prompt ceci :
  - . *ntdsutil*
  - . *activate instance ntds*
  - . *authoritative restore*
  - . *restore subtree "OU=backup,DC=hms,DC=com"*
- Vérifie la Restauration
- Se Connecter en Admin du Domaine et vérifier la Restauration de l'OU *backup*

#### ■ Serveur Windows DC 2:

- Vérifier la Connectivité vi PFSENSE.1 avec le Réseau 1 et spécifiquement au *Serveur DC.1*
- Vérifier la suppression de l'OU backup puis sa restauration.

.Serveur DC.2

```
Adresse IPv4. . . . . : 192.168.2.12
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : fe80::1:1%12
                                192.168.2.10

Carte Tunnel isatap.{ACFF3FCF-FD76-413C-88A6-D1E399FB1172} :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

C:\Users\Administrateur.hms>tracert 192.168.1.12

Détermination de l'itinéraire vers dc1.hms.com [192.168.1.12]
avec un maximum de 30 sauts :

 1  <1 ms    <1 ms    <1 ms    192.168.2.10
 2  <1 ms    <1 ms    <1 ms    11.0.0.2
 3  <1 ms    <1 ms    <1 ms    dc1.hms.com [192.168.1.12]

Itinéraire déterminé.

C:\Users\Administrateur.hms>ping 192.168.1.12

Envoi d'une requête 'Ping' 192.168.1.12 avec 32 octets de données :
Réponse de 192.168.1.12 : octets=32 temps<1ms TTL=126
Réponse de 192.168.1.12 : octets=32 temps<1ms TTL=126
```



## .Serveur DC.1

```

Adresse IPv4. . . . . : 192.168.1.12
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : fe80::1:1%12
                                192.168.1.10

Carte Tunnel isatap.<B04CB679-FE68-4BD1-8598-BAAD390F89AC> :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . . . :

C:\Users\Administrateur>
C:\Users\Administrateur>
C:\Users\Administrateur>tracert 192.168.2.12

Détermination de l'itinéraire vers DC2 [192.168.2.12]
avec un maximum de 30 sauts :

  1  <1 ms    <1 ms    <1 ms    192.168.1.10
  2  <1 ms    <1 ms    <1 ms    11.0.0.1
  3  <1 ms    <1 ms    <1 ms    DC2 [192.168.2.12]

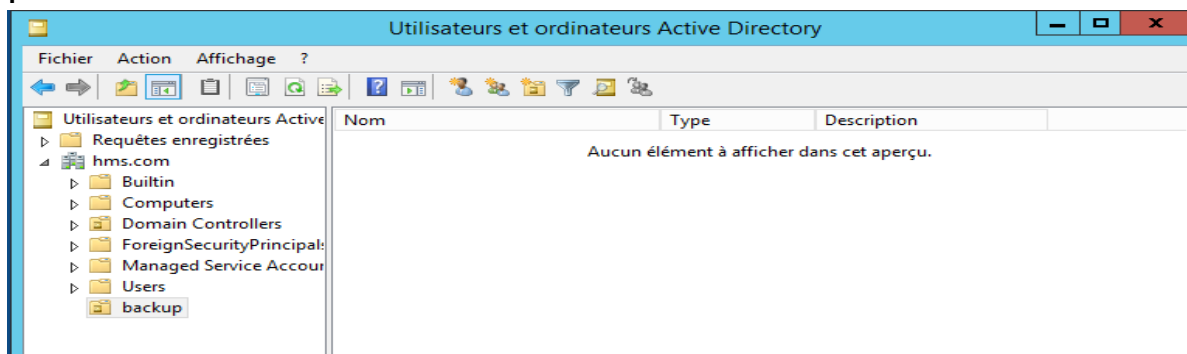
Itinéraire déterminé.

C:\Users\Administrateur>ping 192.168.2.12

Envoi d'une requête 'Ping' 192.168.2.12 avec 32 octets de données :
Réponse de 192.168.2.12 : octets=32 temps<1ms TTL=126
Réponse de 192.168.2.12 : octets=32 temps<1ms TTL=126

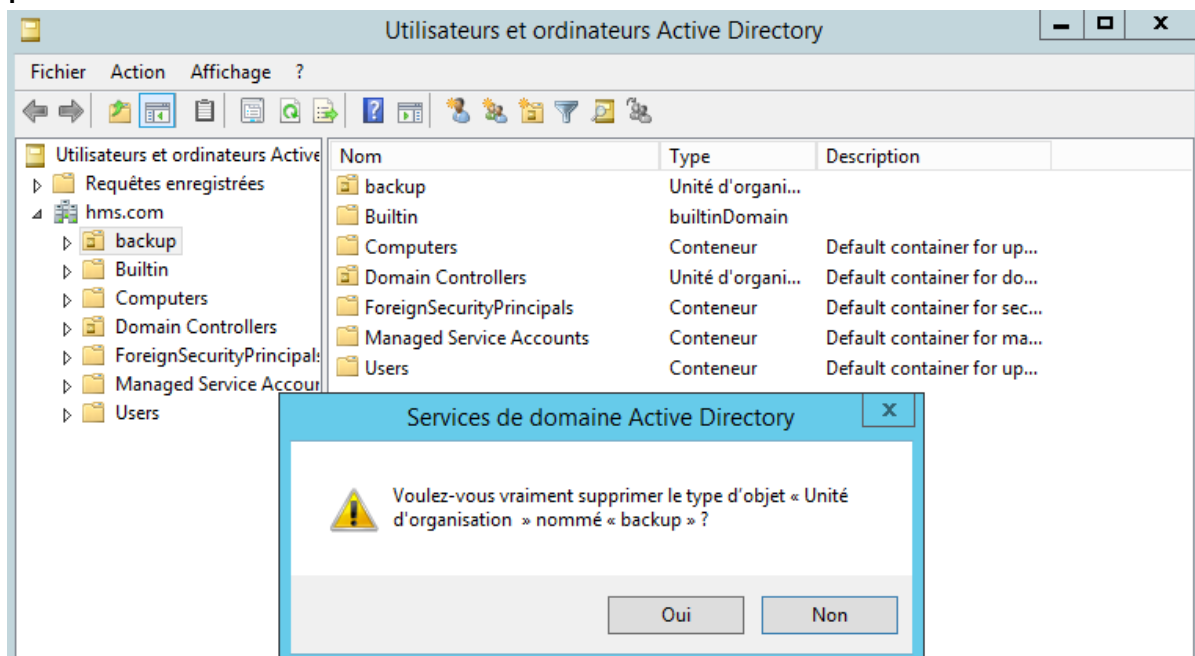
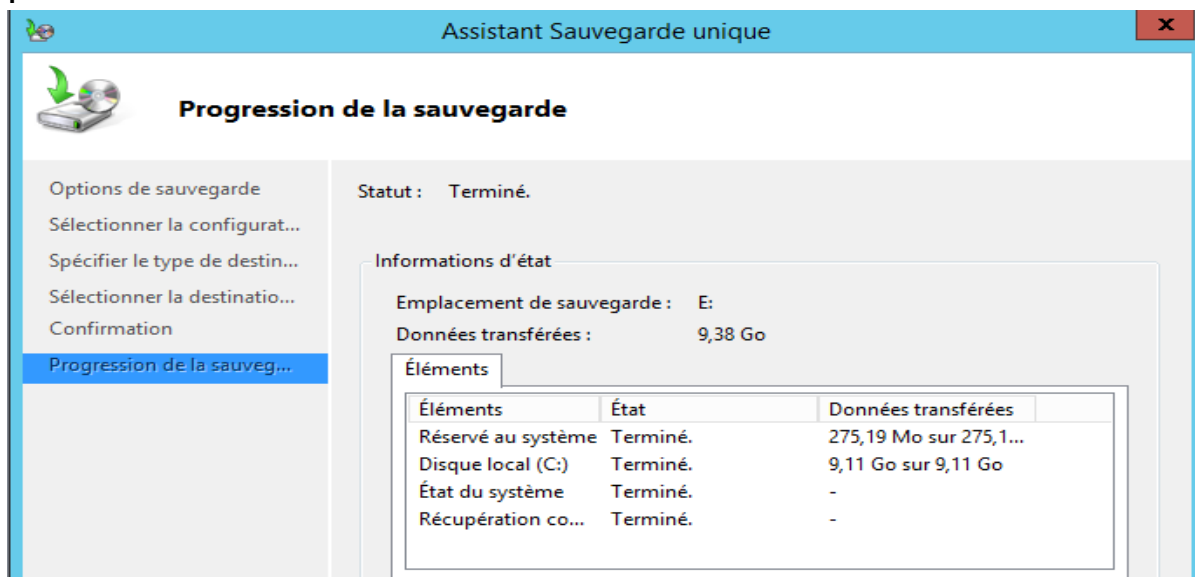
```

Fonctionnalités	
Confirmation	
Résultats	
	<input type="checkbox"/> Outils de migration de Windows Server <input checked="" type="checkbox"/> Prise en charge WoW64 (Installé) <input type="checkbox"/> Protocole PNRP <input type="checkbox"/> RPC sur proxy HTTP <input checked="" type="checkbox"/> Sauvegarde Windows Server <input type="checkbox"/> Serveur de gestion des adresses IP (IPAM) <input type="checkbox"/> Serveur SMTP



## Progression de la sauvegarde

Options de sauvegarde	Statut : Sauvegarde en cours...															
Sélectionner la configurat...																
Spécifier le type de destin...																
Sélectionner la destinatio...																
Confirmation																
Progression de la sauveg...	<div> <div></div> </div> <p>Informations d'état</p> <p>Emplacement de sauvegarde : E:</p> <p>Données transférées : 2,57 Go</p> <table border="1"> <thead> <tr> <th>Éléments</th> <th>État</th> <th>Données transférées</th> </tr> </thead> <tbody> <tr> <td>Réserve au système</td> <td>Terminé.</td> <td>275,19 Mo sur 275,1...</td> </tr> <tr> <td>Disque local (C:)</td> <td>Sauvegarde en cour...</td> <td>2,31 Go sur 9,11 Go</td> </tr> <tr> <td>État du système</td> <td>Sauvegarde en cour...</td> <td>-</td> </tr> <tr> <td>Récupération co...</td> <td>Sauvegarde en cour...</td> <td>-</td> </tr> </tbody> </table> <p>Vous pouvez fermer cet Assistant. L'exécution de l'opération de sauvegarde continuera en arrière-plan.</p>	Éléments	État	Données transférées	Réserve au système	Terminé.	275,19 Mo sur 275,1...	Disque local (C:)	Sauvegarde en cour...	2,31 Go sur 9,11 Go	État du système	Sauvegarde en cour...	-	Récupération co...	Sauvegarde en cour...	-
Éléments	État	Données transférées														
Réserve au système	Terminé.	275,19 Mo sur 275,1...														
Disque local (C:)	Sauvegarde en cour...	2,31 Go sur 9,11 Go														
État du système	Sauvegarde en cour...	-														
Récupération co...	Sauvegarde en cour...	-														



Inscrire les événements de démarrage dans le journal  
Activer la vidéo basse résolution  
Dernière configuration valide connue (option avancée)  
**Mode de réparation des services d'annuaire**  
Mode débogage  
Désactiver le redémarrage automatique en cas d'échec du système  
Désactiver le contrôle obligatoire des signatures de pilotes



## Sélectionner l'emplacement pour la récupération de l'état du système

Mise en route

Sélectionner une date de ...

Sélectionner le type de ré...

Sélectionner l'emplacement...

Confirmation

Statut de la récupération

Où voulez-vous récupérer l'état du système de cette sauvegarde Active Directory ?

☒ Emplacement d'origine

Cette option restaure l'état du système. Vous devez redémarrer l'ordinateur à la fin de l'opération de récupération.

☐ Effectuer une restauration faisant autorité des fichiers Active Directory

Cette option de récupération va rétablir tout le contenu répliqué sur ce contrôleur de domaine, y compris SYSVOL. Les autres dossiers répliqués sur ce serveur seront également concernés par cette récupération.

☐ Autre emplacement

Cette option copie l'état du système sous forme d'un jeu de fichiers à l'emplacement spécifié.

Parcourir

☐ Restaurer en tant que fichiers IFM (Installation à partir du support)

Activez cette case à cocher si vous utilisez la fonctionnalité Installation à partir du support (IFM) pour copier les fichiers de l'état du système et installer une base de données Active Directory.

< Précédent

Suivant >

Récupérer

Annuler

Administrateur : Invite de commandes - ntdsutil

```
C:\Users\Administrateur.DC1.000>ntdsutil
'ntdsutil' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\Administrateur.DC1.000>
C:\Users\Administrateur.DC1.000>ntdsutil
ntdsutil: activate instance ntds
Instance active définie à « ntds ».
ntdsutil: authoritative restore
authoritative restore: restore subtree "OU=backup,DC=hms,DC=com"

Ouverture de la base de données DIT... Terminé.

Il est actuellement 01-22-20 14:04.37.
Mise à jour la plus récente de la base de données effectuée à 01-22-20 13:57.18.

Incrémentation de l'attribut Numéros de version de 100000.

Dénombrement des données devant être mises à jour...
Nombre d'entrées : 0000000001
Terminé.

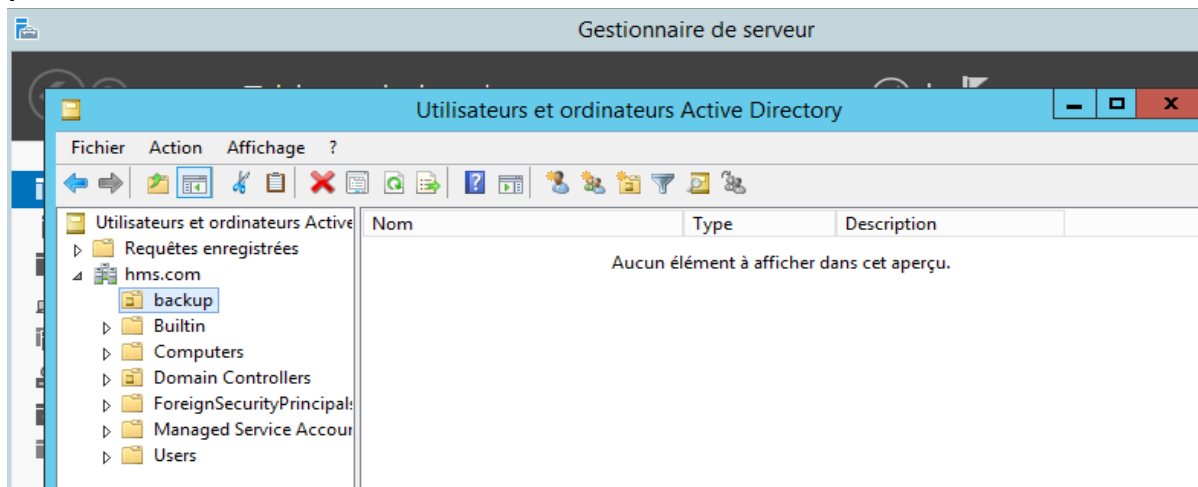
1 entrées doivent être mises à jour.

Mise à jour des entrées...
Entrées restantes : 0000000000
Terminé.

1 entrées ont été mises à jour.

Le fichier texte suivant doté d'une liste fiable d'objets restaurés a été créé
et se trouve dans le répertoire de travail :
ar_20200122-140437_objects.txt
Les objets indiqués n'ont aucun lien inverse dans ce domaine. Aucun fichier de
établissement de liens n'a été créé.

Restauration faisant autorité terminée correctement.
authoritative restore: _
```



## Étape 2:

### ■ Serveur DC.1 :

- Mettre à jour Windows Server 2012
- Installer .NET Framework 4.5.2
- Installer WindowsFeature RSAT-ADDS (powershell)
- Installer (UcmaR) Unified Communications Managed API 4.0, Core Runtime 64-bit.
- Étendre le schéma Active Directory pour Exchange Server 2016 :  
`.\Setup /PrepareSchema /IAcceptExchangeServerLicenseTerms`
- Préparer Active Directory pour Exchange Server 2016  
`.\Setup /PrepareAD /OrganizationName:"Foudil" /IAcceptExchangeServerLicenseTerms`
- Installer les pré-requis du rôle Mailbox Server :  
`.Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, Web-Mgmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation`
- Démarrer l'installation d'Exchange Server 2016
- Se Connecter au Centre d'administration Exchange via le web
- Créer l'Organisation et les Utilisateurs des boîtes mail
- Configurer les Connecteurs d'Envoi et de Réception SMTP et POP3
- Démarrer les Services Microsoft SMTP et POP3

## ■ Client Externe PC.0 :

-Installer ThinderBird d'un client Exchange et vérifier la réception d'un autre client

```
PS C:\Users\Administrateur.AIDE-SYS> Install-WindowsFeature AS-HTTP-Activation, Server-Media-Foundation, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, Web-Mgmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation, RSAT-ADDS

Success Restart Needed Exit Code      Feature Result
-----
True   Yes           SuccessRest... {Serveur d'applications, Activation HTTP, ...
AVERTISSEMENT : Vous devez redémarrer ce serveur pour terminer le processus d'installation.

PS C:\Users\Administrateur.AIDE-SYS>
```

MICROSOFT EXCHANGE SERVER 2016 MISE À JOUR CUMULATIVE 6

? X

### Téléchargement des mises à jour...

Aucune mise à jour trouvée, cliquez sur Suivant pour procéder à l'installation.

 Exchange

suivant

MICROSOFT EXCHANGE SERVER 2016 MISE À JOUR CUMULATIVE 6

? X

### Sélection du rôle serveur

Sélectionnez les rôles serveur Exchange à installer sur cet ordinateur :

☒ Rôle de boîte aux lettres

☒ Outils de gestion

☐ Rôle de transport Edge

☒ Installer automatiquement les rôles et les fonctionnalités Windows Server requis pour Exchange Server

 Exchange

retour

suivant

## Installation terminée

Félicitations ! L'installation s'est déroulée avec succès. Pour terminer l'installation de Microsoft Exchange Server, redémarrez l'ordinateur.

Vous pouvez afficher des tâches de post-installation supplémentaires en ligne en cliquant sur le lien suivant : <http://go.microsoft.com/fwlink/?LinkId=255372>. Vous pouvez également lancer le Centre d'administration Exchange à la fin du programme d'installation.

☒ Lancer le Centre d'administration Exchange une fois l'installation d'Exchange terminée.

 Exchange

terminer

https://exc-01/ecp/?ExchClientVer=15

ENTREPRISE Office 365

### Centre d'administration Exchange

destinataires

- autorisations
- gestion de la conformité
- organisation
- protection
- flux de messagerie
- mobile
- dossiers publics
- messaging unifiée
- serveurs
- hybride
- outils

boîtes aux lettres groupes ressources contacts boîte aux lettres partagée migration

+ - ✎ 🗑️ 🔍 ⋮

NOM D'AFFICHAGE	TYPE DE BOITE AUX LETTRES	ADRESSE DE COURRIER
Administrateur	Utilisateur	Administrateur@aide-sys.local

.....

### .Client Externe 1

Envoyés cool - Envoyés

Relever Écrire Messagerie instantanée Adresses Étiquette Filtre rapide Recherche

habib@amine.com

Courrier entrant

Envoyés

Corbeille

Dossiers locaux

Corbeille

Messages en attente

Filtrer ces messages <Ctrl+Maj+K>

Sujet	Correspondants	Date
cool	foudil@amine.com	14:28
signature	foudil@amine.com	14:50
qwdqwd	foudil@amine.com	14:51
Re: cool	foudil@amine.com	14:57

Répondre Transférer Archiver Indésirable Supprimer Autres

De Moi

Sujet cool 14:28

Pour foudil@amine.com

cool

27 Lun jan 2016

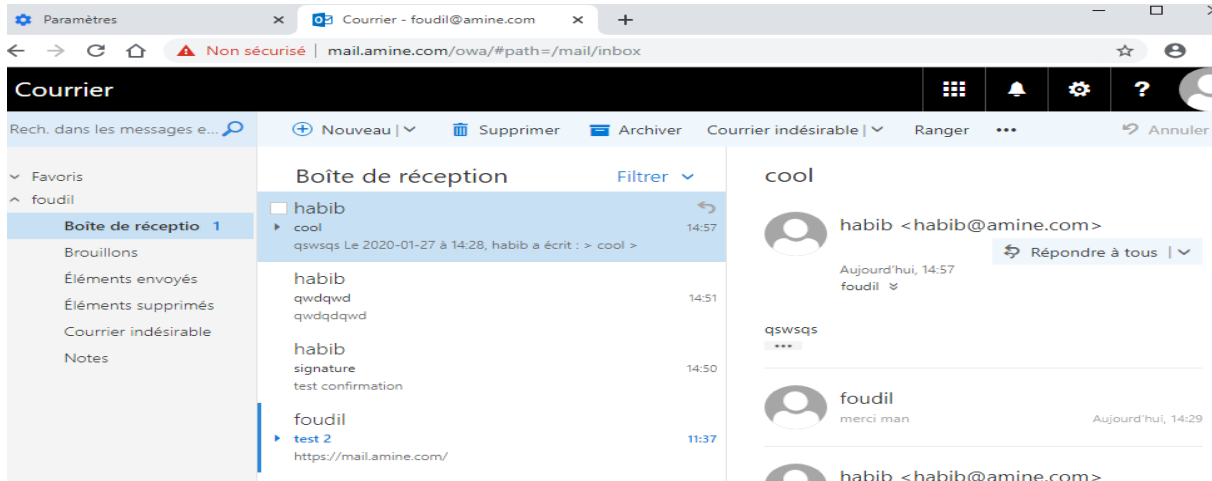
Nouvel évènement

Aujourd'hui

Demain

Prochainement

## . Client Externe 2



### Étape 3:

- **Serveur DC.1 :**  
-Autoriser Réplication
- **Serveur DMZ2 :**  
-Installer DNS

.Client Externe 1

.Client Externe 2