

Projet MDL

(Maison des Ligues)

Sommaire

- Environnement technique	2
Mission 1 : installation du routeur-pare-feu pfsense	2
Objectif :.....	2
- Création du routeur pare-feu pfsense	3
- Schéma à réaliser	3
- Réalisation.....	3
- Configuration des interfaces réseau et attribution des étiquettes réseaux.....	4
Mission 2 : installation du contrôleur de domaine MDL.....	6
Objectif.....	6
- Schéma de l'infrastructure à réaliser.....	6
Réalisation	6
- Création de la machine.....	6
- Attribution et assignation de l'étiquette réseau.....	7
Mission 2 B: installation du poste client PC1	8
Mission 2 C: création des utilisateurs avec leur dossier personnel de base ; configuration d'autorisations spécifiques à certains dossiers (TP SI5 de référence : TP2A).....	8
Mission 3 : Inventaire du matériel avec GLPI/FusionInventory	11
Objectif.....	11
- Travail à faire	11
Mission 4 : Installation d'un VPN.....	12
Mission 5 : Installation d'un serveur hôte de session Bureau à distance	12
Mission 6 : Configuration d'un cluster de deux Pfsense redondants (en Haute Disponibilité).....	13
Mission 7 : Installation d'une machine Kali-Linux (intérieure au LAN) et d'un IPS sur le Pfsense	15
Définition	16
Aide	16

- Environnement technique

On utilise ici **VMware*** qui est un hyperviseur de type 1, celui-ci permet de créer des machines dites virtuelles.



VSphere* est un tableau de bord (celui de VMware) qui permet d'administrer toutes les machines virtuelles sur un serveur physique. On parle d'outil de gestion.



Mission 1 : installation du routeur-pare-feu pfSense

Objectif :

Le but de cette mission est d'installer un routeur pare-feu pfSense dans le but de segmenter les différents réseaux. On disposera de trois adresses physiques :

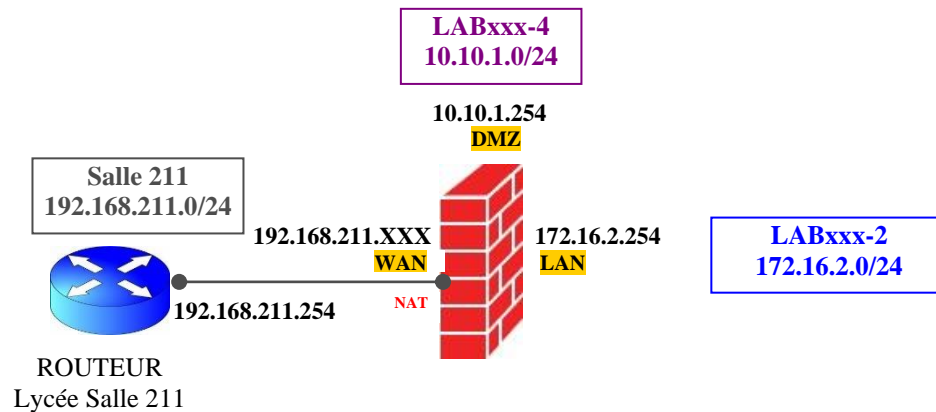
vmx0 qui correspond au réseau **WAN** c'est-à-dire le réseau étendu qui permet de se connecter à internet. Elle couvre généralement une zone assez large, c'est-à-dire un pays, un continent ou une planète. (Dans notre schéma le WAN est la salle 211)

vmx1 qui correspond au réseau **LAN** c'est-à-dire local, ce réseau permet de communiquer avec un réseau informatique interne à l'aide de trames sans forcément passer par internet.

vmx2 qui correspond au réseau **DMZ** (zone démilitariser), une zone démilitarisée est un réseau séparé du réseau informatique de base, pour éviter de lourde perte, ou pour plus simplement séparer les processus d'une entreprise.

- Création du routeur pare-feu pfsense

- Schéma à réaliser



Le réseau WAN permet d'accéder à internet à l'aide du **NAT***.

- Réalisation

- Créer une nouvelle machine virtuelle sous VMWare, de nom :

MH-MDL-PfSense
(XX étant les initiales du nom et prénom de l'étudiant)

- Avant de la démarrer lui rajouter des interfaces réseau, il faut que celle-ci dispose de trois interfaces : **WAN**, **LAN**, et **DMZ**.

> Adaptateur réseau 1	LAB-SISR-07-2 ▾	<input checked="" type="checkbox"/> Connecté
> Adaptateur réseau 2	LAB-SISR-07-4 ▾	<input checked="" type="checkbox"/> Connecté
> Adaptateur réseau 3	LAB-SISR-07-3 ▾	<input checked="" type="checkbox"/> Connecté
> Adaptateur réseau 4	SALLE - 211 ▾	<input checked="" type="checkbox"/> Connecté

- Les interfaces doivent être configurées de la sorte.
- La **salle 211** correspond à la salle du lycée on dispose d'une connexion internet sur cette interface réseau.

L'interface **DMZ** ne sera pas utilisée ici, mais on la configurera en vue d'une éventuelle installation d'une DMZ ultérieurement.

- Vérifier que la machine virtuelle **Pf sense** dispose de 3 cartes réseaux (si ce n'est pas le cas, mettre hors-tension la machine et ajouter les cartes nécessaires).

- Assigner les interfaces du Pfsense (fonction 1 : *Assign Interfaces* sur l'écran d'interface texte du Pfsense)

WAN : vmx0

LAN : vmx1

OPT1 : vmx2

```
WAN -> vmx0
LAN -> vmx1
OPT1 -> vmx2
```

Schéma du pf sense (pare-feu)



- Configuration des interfaces réseau et attribution des étiquettes réseaux

- Attribuer des adresses IP aux interfaces du Pfsense (fonction 2 : *Set Interface*, ne pas oublier la passerelle pour chaque interface).

Attention : ne pas configurer de DHCP (sur aucune interface) !

- Attribuer l'étiquette réseau adéquate à chaque interface réseau selon l'adresse MAC de la carte :

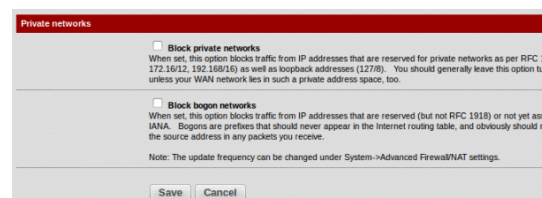
a) dans le tableau suivant, noter l'adresse MAC de chaque interface réseau.

b) retrouver (onglet *Résumé/modifier les paramètres*) le numéro d'adaptateur réseau correspondant à chaque adresse MAC de cette VM, et le noter dans le tableau

c) attribuer l'étiquette réseau adéquate à chaque adaptateur réseau (sous VMware Vsphere, onglet *Résumé, Modifier les paramètres*)

Interface physique	Interface logique	Adresse MAC	N° Adaptateur réseau	Etiquette réseau
vmx0	WAN	00 :50 :56 :90 :60 :51	4	Salle-211
vmx1	LAN	00 :50 :56 :90 :32 :a5	1	LAB-SISR-X-2
vmx2	OPT1 (DMZ)	00 :50 :56 :90 :49 :42	2	LAB-SISR-X-4

- Rendre accessible le Pfsense depuis un poste ayant une adresse IP privée en décochant la case *Block private networks* de l'interface WAN (sur l'écran d'interface graphique accessible via un navigateur de la machine physique hôte) :



- Modifier si besoin les règles de filtrage en entrée de l'interface LAN pour autoriser toute communication à partir de n'importe quel poste de n'importe quel VLAN de MDL.

Conseils :

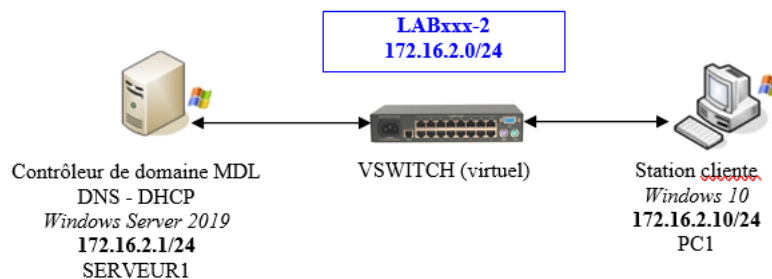
- L'interface graphique du Pfsense fonctionne très bien avec le navigateur Internet Explorer ; il peut poser des problèmes avec un autre navigateur (identifiant et mot de passe parfois non-reconnus).
- Il faut rendre accessible l'interface graphique uniquement par le port 80 (ou par le port 443), mais pas par les deux simultanément (peut poser des problèmes lors de la mise en cluster de ce Pfsense avec un autre).

Mission 2 : installation du contrôleur de domaine MDL

Objectif

Le but de cette mission est d'installer le domaine MDL sur un serveur contrôleur de domaine **Windows Server 2019**, et de tester l'installation via une station de travail cliente **Windows 10** :

- Schéma de l'infrastructure à réaliser



Réalisation




- Création de la machine

- Créer une nouvelle machine virtuelle sous VMWare, de nom :

MH-MDL-SERVEUR1-Contrôleur MDL.local-Windows 2019
(MH étant les initiales de mon nom et prénom)

Ne pas oublier de modifier par la même occasion le nom du serveur pour cela il existe deux manières de renommer une machine :

Windows  / paramètres  / Système  / Informations système  / renommer ce pc

Panneau de configuration  / Système et sécurité  / Système  / Paramètres système avancés / Nom de l'ordinateur

Cette capture d'écran montre la fenêtre de configuration du nom de l'ordinateur. Elle contient les champs suivants :
- **Description de l'ordinateur :** un champ de texte vide.
- **Nom complet de l'ordinateur :** SERVEUR1.MDL.local
- **Domaine :** MDL.local
En bas, il y a un bouton **Modifier...** et un message d'information : "Windows utilise les informations suivantes pour identifier votre ordinateur sur le réseau."

- Attribution de l'adresse IP et assignation de l'étiquette réseau.

Une fois le contrôleur de domaine renommé,

Attribuer l'étiquette réseau adéquate à l'interface réseau. Dans le cas présent « **LAB-SISR-07-02** ».

LAB-SISR-07-2 (connecté)

- Le 07 correspond à l'identification de l'étudiant, de plus le contrôleur de domaine dispose d'une adresse IP qui lui permet d'accéder à internet nous ne sommes donc pas en DHCP.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 172 . 16 . 2 . 1

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 172 . 16 . 2 . 254

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 172 . 16 . 2 . 1

Serveur DNS auxiliaire : 8 . 8 . 8 . 8

Sur le pfsense les interfaces doivent être configurées de la sorte conformément au schéma ci-dessus. :

WAN (wan)	-> VMX0	-> v4: 192.168.211.230/24
LAN (lan)	-> VMX1	-> v4: 172.16.2.252/24
OPT1 (opt1)	-> VMX2	-> v4: 10.10.1.254/24


- **VMX0** correspond à l'adresse du pare-feu pfsense A (primaire) coté **WAN** c'est-à-dire 192.168.211.230.

- **VMX1** correspond à l'adresse du pare-feu pfsense A (primaire) coté **LAN** c'est-à-dire 172.16.2.252.

- **VMX2** correspond à l'adresse du pare-feu pfsense A (primaire) coté **DMZ (OPT1)** c'est-à-dire 10.10.1.254.

- Installation du contrôleur de domaine sur la machine Windows 2019

Une fois les étapes précédentes réalisées, rendre la machine Windows server 2019 en contrôleur de domaine.

Pour cela se rendre dans gestionnaire de serveur  / gérer/ ajout de rôle et fonctionnalité/installation basée sur un rôle ou une fonctionnalité.

-Choisir le serveur MDL.local

SERVEUR1.MDL.local 172.16.2.1 Microsoft Windows Server 2019 Standard

- Puis installer le rôle serveur DNS, et le rôle AD DS (pour l'active directory et la gestion des utilisateurs).



Pour finir valider toutes les autres étapes jusqu'à que la machines Windows 2019 soit élevé en tant que contrôleur du domaine MDL.

Mission 2 B: installation du poste client PC1

- Créer une nouvelle machine virtuelle sous VMWare, de nom

MH-MDL-PC1-Client MDL.local-Windows 10
(MH étant les initiales du nom et prénom de l'étudiant)

- Attribuer l'étiquette réseau adéquate à l'interface réseau.

- Sur PC1, modifier le nom de l'ordinateur et sa configuration IP, puis connecter cette machine au domaine MDL.local (vérifier le bon fonctionnement du DHCP).

Mission 2 C: création des utilisateurs avec leur dossier personnel de base ; configuration d'autorisations spécifiques à certains dossiers (TP SI5 de référence : TP2A)

- Créer le dossier REPBASES et configurer ses autorisations de partage et ses autorisations de sécurité NTFS ; REPBASES contiendra les dossiers personnels de base de chaque utilisateur.

- Créer les utilisateurs suivants (chacun avec son dossier personnel) (pour plus de simplicité, le mot de passe de chaque utilisateur ne changera jamais) ; vérifier ensuite que chaque utilisateur a son dossier dans REPBASES et qu'il est le seul à pouvoir y accéder, hormis les administrateurs et le système :

Utilisateurs

Nom et prénom	Nom d'ouverture de session	Nom du dossier personnel	Mot de passe
Clément Ogier	cogier	cogier	Windows2019
Laure Dubreuil	ldubreuil	ldubreuil	Windows2019
Sylvie Pommier	spommier	spommier	Windows2019
Kevin Dalle	kdalle	kdalle	Windows2019

Le DSI demande ensuite de créer des dossiers (*Public*, *Football*, et *Basket*) pour la gestion des contrats et d'y affecter des droits d'accès NTFS différents à deux groupes d'utilisateurs (LigueFootball et LigueBasket).

- Créer les groupes d'utilisateurs et les dossiers, puis configurer les autorisations d'accès spécifiques suivantes :

Groupes d'utilisateurs

Nom de groupe	Membres du groupe
LigueFootball	Clément Ogier Laure Dubreuil
LigueBasket	Sylvie Pommier Kevin Dalle

C: \

↳ *Public*
↳ *Football*
↳ *Basket*

Chaque utilisateur du domaine doit pouvoir lire tous les fichiers et sous-dossiers (voir les noms des sous-dossiers, voir le contenu des fichiers) du dossier *Public* (ainsi que dans tous ses sous-dossiers, sous-sous-dossiers, ...), créer ses propres fichiers et sous-dossiers, mais ne doit pas pouvoir modifier ou supprimer les fichiers et les sous-dossiers des autres utilisateurs.

Chaque utilisateur de la ligue de football doit pouvoir lire tous les fichiers et sous-dossiers (voir les noms des sous-dossiers, voir le contenu des fichiers) du dossier *Football* (ainsi que dans tous ses sous-dossiers, sous-sous-dossiers, ...), mais ne doit pouvoir ni créer ses propres fichiers et sous-dossiers, ni modifier ou supprimer les fichiers et les sous-dossiers des autres utilisateurs. Seul Clément Ogier doit pouvoir créer, modifier ou supprimer des fichiers et des sous-dossiers dans *Football*.

Chaque utilisateur de la ligue de basket doit pouvoir lire tous les fichiers et sous-dossiers (voir les noms des sous-dossiers, voir le contenu des fichiers) du dossier *Basket* (ainsi que dans tous ses sous-dossiers, sous-sous-dossiers, ...), mais ne doit pouvoir ni créer ses propres fichiers et sous-dossiers, ni modifier ou supprimer les fichiers et les sous-dossiers des autres utilisateurs. Seul Kevin Dalle doit pouvoir créer, modifier ou supprimer des fichiers et des sous-dossiers dans *Basket*.

Attention : pour que ces droits prennent effet pour un utilisateur, il faudra ouvrir une session pour cet utilisateur après avoir attribué les droits.

Mission 3 : Inventaire du matériel avec GLPI/FusionInventory

(TP SI7 de référence : TP1 SI7).

Objectif

Le but de cette mission est de réaliser l'inventaire des matériels du réseau MDL, et de calculer leur TCO

- Travail à faire

- Installer GLPI sur le contrôleur de domaine, ainsi que le plugin FusionInventory.
- Installer l'agent FusionInventory sur chaque poste du réseau MDL (**SERVEUR1**, **PC1**, **Pfsense**) pour la remontée automatique des données des postes sur le serveur.
- Importer dans GLPI tous les utilisateurs du domaine MDL.local.
- Créer dans GLPI les opérations de maintenance suivantes sur le poste SERVEUR1, et vérifier l'exactitude des TCO et VNC de ce poste :

Clément Ogier travaille sur SERVEUR1 et constate que le lecteur de cdrom ne fonctionne plus du tout.

→ il déclare un ticket d'incident, en date du jour, d'urgence haute, sur SERVEUR1.

Laure Dubreuil travaille sur SERVEUR1 et constate que le logiciel Gantt Project n'est pas installé ; elle en a pourtant besoin.

→ elle déclare un ticket de demande, en date du jour, d'urgence haute, sur SERVEUR1.

L'utilisateur **glpi** attribue les tickets nouveaux au technicien **tech** qui va effectuer les travaux suivants :

→ Pour le premier ticket, il échange l'ancien lecteur de cdrom par un neuf (45 mn de main d'oeuvre à 160 €/h ; prix d'un lecteur : 80 €).

→ Pour le deuxième ticket, il installe le logiciel Gantt Project, et ne compte aucun temps passé.

SERVEUR1 a été acheté et mis en service le 01/01/2016. Son prix d'achat était de 1800 €. Son amortissement est linéaire sur 5 ans (aucune garantie connue).

Mission 4 : Installation d'un VPN

Le but de cette mission est de configurer un tunnel VPN type client nomade entre un PC de la salle R211 et le serveur OpenVPN installé sur le Pfsense (**TP SISR3 de référence : TP29**).

Le serveur VPN OpenVPN, configuré sur le PfSense qui intègre d'origine OpenVPN, gèrera sa propre autorité de certification ainsi que le certificat de l'autorité de certification.

Chaque machine Windows souhaitant se connecter au serveur OpenVPN utilisera le client VPN *OpenVPN GUI for Windows*.

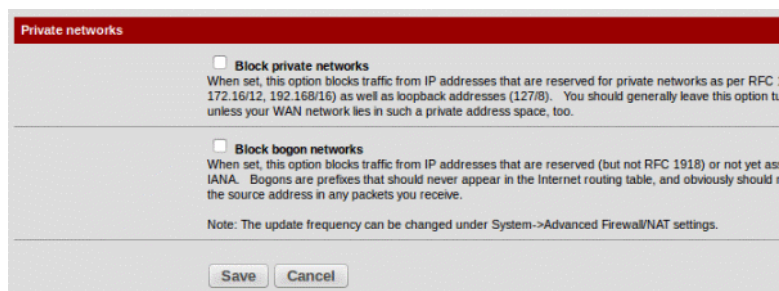
On configurera le serveur OpenVPN avec authentification des utilisateurs par un serveur LDAP (**SERVEUR1**).

L'adresse IP réseau du VPN sera **192.168.10.0/24**. On utilisera le port **1196** du Pfsense pour créer la liaison VPN.



Rappel préalable : le serveur OpenVPN sera accessible de l'extérieur via son interface WAN ; on devra pouvoir accéder à ce serveur à partir d'un poste de la salle R211 (qui a donc une adresse privée).

Il faut donc bien penser à rendre accessible le Pfsense depuis un poste ayant une adresse IP privée en vérifiant que la case *Block private networks* **de l'interface WAN** est décochée :



Mission 5 : Installation d'un serveur hôte de session Bureau à distance

Installer et configurer SERVEUR1 pour qu'il soit serveur hôte de session de bureau à distance (**TP SISR de référence : TP19**).

Configurer Cisco Packet Tracer en tant que application Remote App accessible aux deux utilisateurs Clément Ogier et Laure Dubreil (sur les postes distants, penser à ouvrir une session de bureau à distance en utilisant le nom du serveur et non son adresse IP).

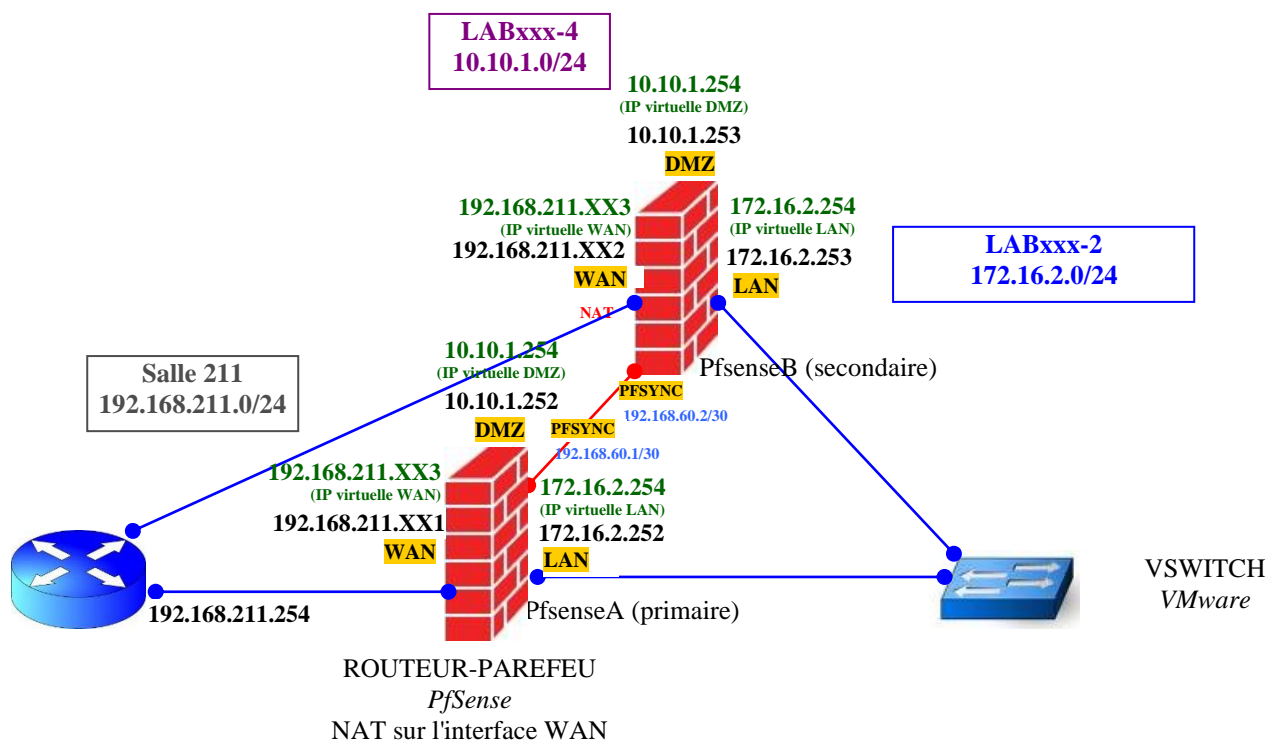
Mission 6 : Configuration d'un cluster de deux Pfsense redondants (en Haute Disponibilité)

Le but de cette mission est de configurer un cluster de deux Pfsense pour assurer une haute disponibilité du routeur pare-feu Pfsense : en cas de défaillance du premier pfSense (pfSenseA primaire), le deuxième pfSense (pfSenseB secondaire) prend le relais sans aucune interruption de service : la bascule du pfSenseA vers pfSenseB est totalement transparente.

PfSense communiquera sur les réseaux LAN, WAN, et DMZ avec ses adresses IP virtuelles.

Afin d'assurer la réplication du pfSenseA vers le pfSenseB, 3 éléments doivent être configurés : CARP, pfsync et XML-RPC :

- CARP (*Common Address Redundancy Protocol*) est un protocole permettant à plusieurs hôtes présents sur un même réseau de partager une même adresse IP virtuelle. C'est cette adresse IP virtuelle que pfSense va utiliser pour sa communication sur le réseau. Ainsi, en cas de défaillance du pfSense primaire (pfSenseA), le pfSense secondaire (pfSenseB) prendra le relais de manière transparente au niveau réseau (reprise de l'adresse IP virtuelle).
- PFSYNC est un protocole permettant de synchroniser entre deux pfSense l'état des connexions en cours. Ainsi, en cas de défaillance du Pfsense primaire, l'état des connexions en cours est maintenu sur le Pfsense secondaire. Il n'y a donc pas de coupure liée à la bascule des services du pfSenseA vers le pfSenseB.
Cette synchronisation sera effectuée sur une interface dédiée sur chacun des deux Pfsense (à défaut, le lien LAN aurait pu être utilisé).
- XML-RPC est un protocole permettant la réplication de données d'un Pfsense vers un autre. Il est utilisé dans pfSense afin de répliquer la configuration du Pfsense primaire vers le Pfsense secondaire.
Pour garantir son bon fonctionnement, il est important qu'il utilise la même interface que celle utilisée par le protocole pfsync.



Travail à faire

- Installer et configurer ce cluster de Pfsense.
- Rédiger une procédure complète et détaillée (avec copies d'écran) de cette installation.

Tutoriel : <https://notamax.be/pfsense-creation-dun-cluster/>

Conseil : Pour mener cette mission efficacement sous VMware, il est fortement conseillé de cloner le Pfsense primaire lorsque toutes les interfaces ont été correctement configurées, puis de configurer le clone comme Pfsense secondaire.

Mission 7 : Installation d'une machine Kali-Linux (intérieure au LAN) et d'un IPS sur le Pfsense

Le but de cette mission est d'installer et configurer une machine d'attaque Kali-Linux afin de mener des pentests.

On installera aussi un IPS (Snort) sur le Pfsense pour tenter de parer les attaques.

Travail à faire

- Installer et configurer cette machine Kali.
- Installer et configurer Snort sur Pfsense ; on installera les jeux de règles gratuites Snort VRT et Snort GPLv2 seulement pour ne pas surcharger le Pfsense.

Mission 7 A : attaque DOS vers le contrôleur de domaine

(TP de référence : TP4 Cybersécurité - Attaque par déni de service - Snort)

- Créer une attaque DOS depuis le Kali vers le serveur de domaine ; Snort peut-il détecter et arrêter cette attaque ?

Mission 7 B : attaque par malware du contrôleur de domaine, et élévation de privilèges

(TP de référence : TP5 Cybersécurité - Intrusion sur un serveur de domaine Windows)

Phase d'exploitation (préparation et mise en place de l'attaque)

- créer et envoyer un malware (cheval de Troie (trojan) dissimulé dans un programme existant et légitime (Putty par exemple)) au serveur de domaine SERVEUR1 de MDL. Ce malware permettra d'ouvrir une connexion *Meterpreter reverse_tcp* entre SERVEUR1 et KALI. Attention : ne pas créer de porte dérobée persistante sur le serveur cible afin de ne pas être repéré !
- via la connexion *Meterpreter reverse_tcp* :
 - lancer l'exécution du script PowerShell (*CreatAdminx.ps1* disponible sur DocsDeProfs) qui créera un nouvel utilisateur *adminx* qui sera membre du groupe *Administrateurs* du domaine MDL ;
 - installer sur SERVEUR1 un serveur SSH.

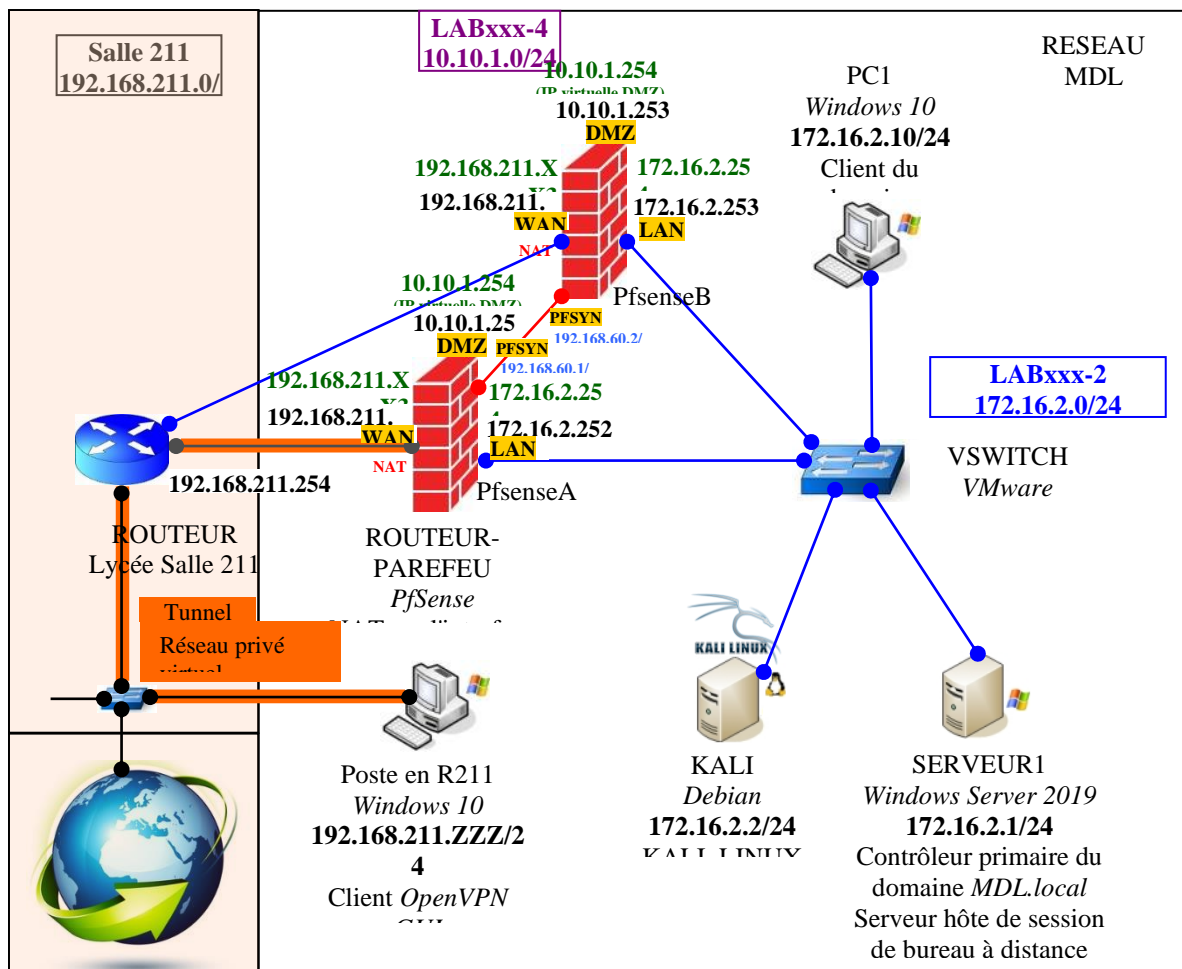
Phase de post-exploitation

- lancer une session SSH depuis Kali vers SERVEUR1 en utilisant le compte Administrateur illicite *Adminx*, et voler toutes les données souhaitées.

Mission 7 C : attaque ARP Poisoning du PC1

(TP de référence : TP6 Cybersécurité - Attaque d'empoisonnement ARP)

- Créer une attaque ARP Poisoning depuis le Kali vers le client PC1 ; détectez-vous les sites Web que PC1 consulte ?



Définition

NAT (Network address translation) : Le NAT permet à des machines disposant d'adresse privé de communiquer avec internet à l'aide d'adresse routable.

Aide

Pour se connecter à vSphere utiliser l'adresse suivante dans le navigateur Web :
192.168.216.230

Pour se connecter au Contrôleur de domaine : Windows2019