

Mise en place d'une pare-feu open source dans une architecture sécurisée



Réalise par :

STIHI IBRAHIM

OTHMANE TAYBI

Encadré par :

Mr.KHARTOCH

SOMMAIRE

INTRODUCTION	3
LA SÉCURITÉ DES RÉSEAUX	44
a) Définition	3
b) Comment fonctionne la sécurité réseau ?	3
c) Les objectif.....	4
LES ATTAQUES	7
a) Qu'est-ce qu'une attaque réseau ?	7
b) Les types courants d'attaques réseau	8
c) Meilleures pratiques de protection du réseau	10
LES PARE-FEU.....	12
a) Technologies et Solutions de sécurité (pare-feu)	12
b) Les pare-feu fameux	14
c) Tableau comparatif	16
PFSENSE	19
a) PfSense comme solution :.....	19
b) Installation et configuration de PfSense	28
c) Ajouter des équipements Linux.....	36
d) Email Notification	40
CONCLUSION	44

INTRODUCTION

Le développement du réseau Internet, et de ses déclinaisons sous forme d'Intranets et d'Extranets, soulève des questions essentielles en matière de sécurité informatique. L'accroissement des trafics en télécommunication révèlent les besoins grandissants d'échanges privés et professionnels. Ces transmissions de données imposent une ouverture des systèmes d'information vers l'extérieur, notamment vers Internet. Celle-ci entraîne une certaine dépendance des entreprises et des personnes vis-à-vis des services qu'offre Internet. Ainsi conjuguées, cette ouverture et cette dépendance rendent l'entreprise vulnérable aux risques. C'est pour cela que la sécurité Internet est devenue un sujet de recherche très intense. Ces recherches ont permis le développement de certains dispositifs de sécurité comme les Pare-feux les antivirus et les systèmes de cryptographie pour protéger les systèmes informatiques.

✈ Étant donné l'importance et l'obligation de l'élaboration d'un pare-feu, chaque organisme doit établir un pare-feu pour la sécurité informatique afin d'identifier les sources de menace et les dommages informationnels.

LA SÉCURITÉ DES RÉSEAUX

A - Définition :

La sécurité des réseaux est un terme général qui couvre une multitude de technologies, d'appareils et de processus. Dans son expression la plus simple, il s'agit d'un ensemble de règles et de configurations conçues pour protéger l'intégrité, la confidentialité et l'accessibilité des réseaux informatiques et des données à l'aide de technologies logicielles et matérielles. Chaque organisation, quelle que soit sa taille, son secteur d'activité ou son infrastructure, a besoin d'un certain degré de solutions de sécurité réseau en place pour la protéger contre le paysage toujours croissant des cybermenaces dans la nature actuelle.



B - Comment fonctionne la sécurité réseau ? :

- Il y a plusieurs couches à prendre en compte pour gérer la sécurité réseau dans une organisation. Des attaques peuvent avoir lieu sur n'importe quelle couche du modèle de couche de sécurité du réseau. Vos politiques de sécurité hardware, software et network doivent donc être conçues pour gérer chaque domaine.

✈ La sécurité de réseau comprend généralement trois contrôles différents : physique, technique et administratif :

SÉCURITÉ DU RÉSEAU PHYSIQUE

Les contrôles de sécurité physique sont conçus pour empêcher le personnel non autorisé d'accéder physiquement aux composants du réseau tels que les routeurs, les armoires de câblage, etc. L'accès contrôlé, comme les serrures, l'authentification biométrique et d'autres dispositifs, est essentiel dans toute organisation.

SÉCURITÉ TECHNIQUE DU RÉSEAU

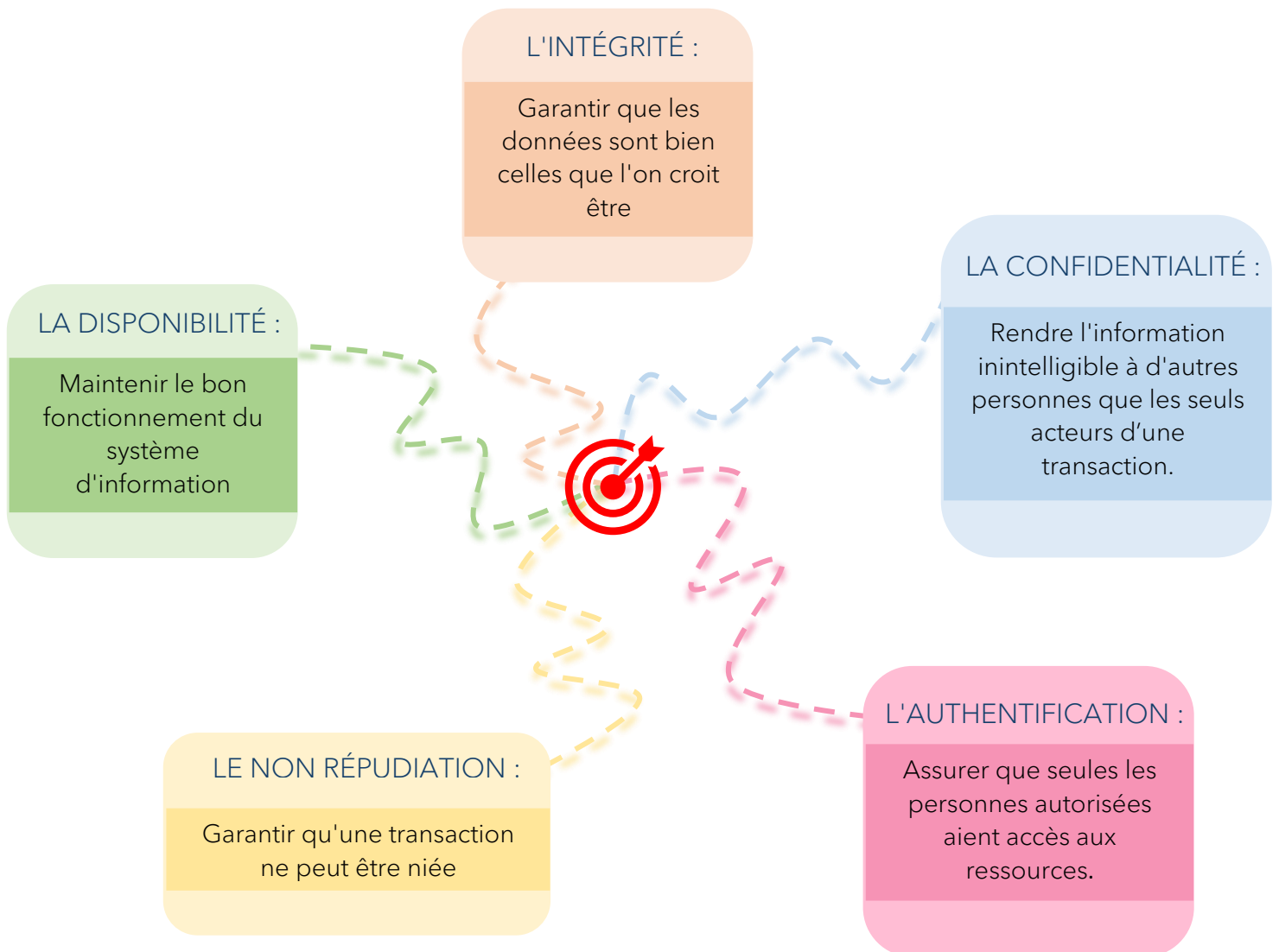
Les contrôles de sécurité techniques protègent les données qui sont stockées sur le réseau ou qui sont en transit à travers, vers ou hors du réseau. La protection est double ; il doit protéger les données et les systèmes contre le personnel non autorisé, et il doit également se protéger contre les activités malveillantes des employés.

SÉCURITÉ DU RÉSEAU ADMINISTRATIF

Les contrôles de sécurité administratifs consistent en des politiques et des processus de sécurité qui contrôlent le comportement des utilisateurs, y compris la manière dont les utilisateurs sont authentifiés, leur niveau d'accès et également la manière dont les membres du personnel informatique mettent en œuvre les modifications apportées à l'infrastructure.

C - Les objectif :

🔴 La sécurité informatique vise généralement cinq principaux objectifs :



LES ATTAQUES

A - Qu'est-ce qu'une attaque réseau ?

Une attaque réseau est une tentative d'obtenir un accès non autorisé au réseau d'une organisation, dans le but de voler des données ou d'effectuer d'autres activités malveillantes. Il existe deux principaux types d'attaques réseau :

PASSIF

Les attaquants accèdent à un réseau et peuvent surveiller ou voler des informations sensibles, mais sans apporter aucune modification aux données, en les laissant intactes.

ACTIF

Les attaquants obtiennent non seulement un accès non autorisé, mais modifient également les données, en les supprimant, en les cryptant ou en les endommageant d'une autre manière.

🔖 Nous distinguons les attaques réseau de plusieurs autres types d'attaques :

■ Attaques sur les terminaux :

Obtenir un accès non autorisé aux appareils des utilisateurs, aux serveurs ou à d'autres terminaux, les compromettant généralement en les infectant avec des logiciels malveillants.

■ Attaques de logiciels malveillants :

Infectant les ressources IT avec des logiciels malveillants, permettant aux attaquants de compromettre les systèmes, de voler des données et de causer des dommages.

■ Vulnérabilités, exploits et attaques :

Exploiter les vulnérabilités des logiciels utilisés dans l'organisation, pour obtenir un accès non autorisé, compromettre ou saboter les systèmes.

■ Menaces persistantes avancées :

Il s'agit de menaces multicouches complexes, qui incluent des attaques de réseau mais aussi d'autres types d'attaques.

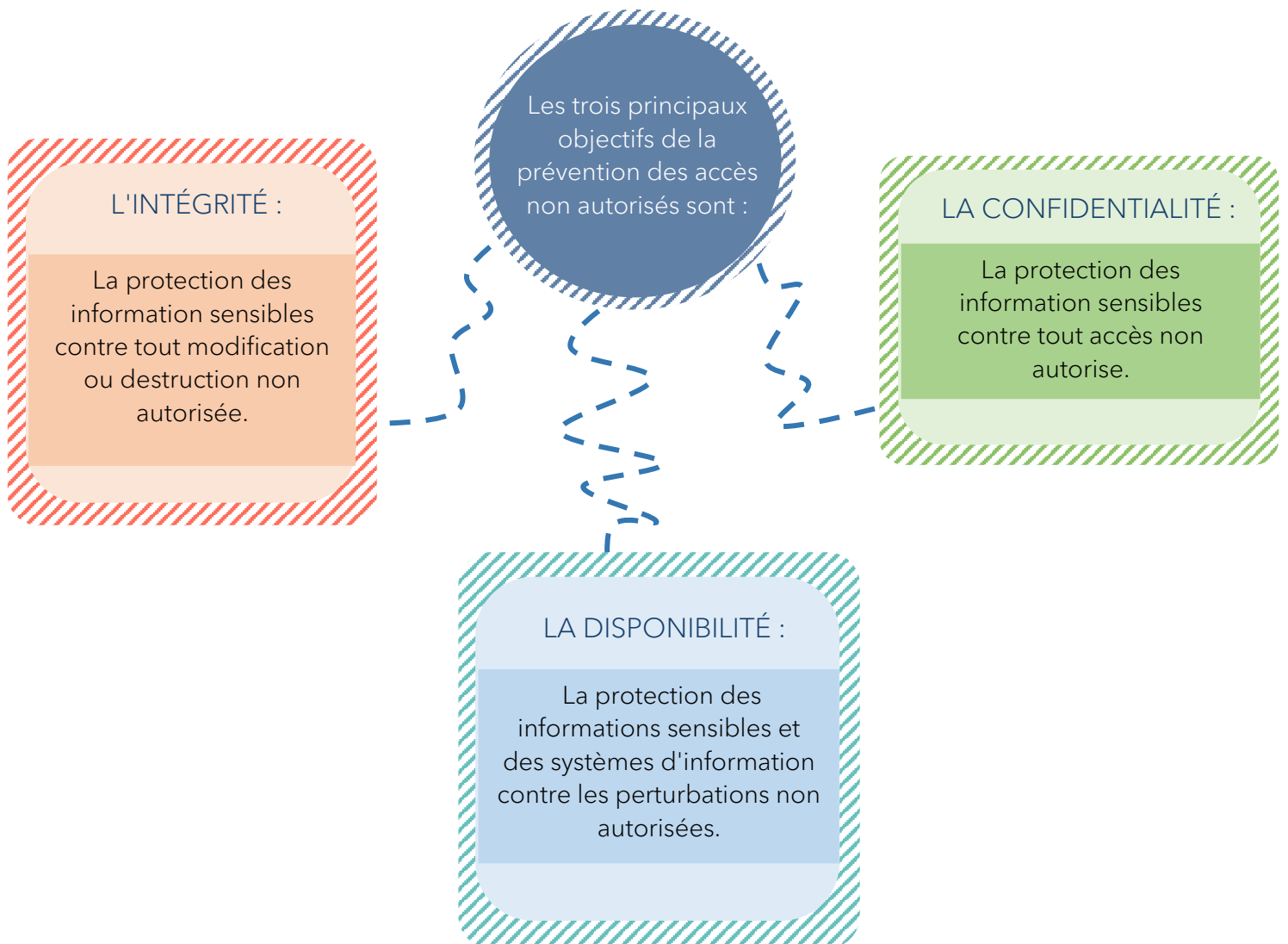
🔖 Lors d'une attaque réseau, les attaquants se concentrent sur la pénétration du périmètre du réseau de l'entreprise et l'accès aux systèmes internes. Très souvent, une fois à l'intérieur, les attaquants combinent d'autres types d'attaques, par exemple en compromettant un terminal, en propageant des logiciels malveillants ou en exploitant une vulnérabilité dans un système du réseau.

B - les types courants d'attaques réseau :

Voici les vecteurs de menace courants que les attaquants peuvent utiliser pour pénétrer un réseau :

1 - L'accès non autorisé :

L'accès non autorisé se produit lorsqu'une personne pénètre dans un réseau informatique, système, logiciel d'application, données, ou d'autres ressources sans autorisation.



Comment se produit l'accès non autorisé ?

- Deviner les mots de passe.
- Exploitation des vulnérabilités logicielles.
- Ingénierie sociale.

2 - Attaques par déni de service distribué (DDoS) :



Une attaque par déni de service [DOS] est une attaque destinée à arrêter une machine ou un réseau, le rendant inaccessible aux utilisateurs auxquels il est destiné. Les attaques DOS y parviennent en inondant la cible de trafic ou en lui envoyant des informations qui déclenchent un plantage. Dans les deux cas, l'attaque DOS prive les utilisateurs légitimes (c'est-à-dire les employés, les membres ou les titulaires de compte) du service ou de la ressource qu'ils attendaient.



Il existe deux méthodes générales d'attaques DOS :

FLOODING services ou CRASHING services

Les attaques par inondation :

Se produisent lorsque le système reçoit trop de trafic pour que le serveur puisse le mettre en mémoire tampon, ce qui les ralentit et finit par s'arrêter.

Les attaques d'inondation populaires incluent :

Attaque par débordement de tampon :

L'attaque DOS la plus courante. Le concept est d'envoyer plus de trafic vers une adresse réseau que les programmeurs n'ont conçu le système pour le gérer. Il comprend les attaques répertoriées ci-dessous, ainsi que d'autres conçues pour exploiter des bogues spécifiques à certaines applications ou réseaux.

ICMP Flood :

Exploite les périphériques réseaux mal configurés en envoyant des paquets usurpés qui envoient un ping à chaque ordinateur du réseau ciblé, au lieu d'une seule machine spécifique. Le réseau est alors déclenché pour amplifier le trafic. Cette attaque est également connue sous le nom d'attaque de schtroumpf ou ping de la mort.

SYN flood :

Envoie une demande de connexion à un serveur, mais ne termine jamais la poignée de main. Continue jusqu'à ce que tous les ports ouverts soient saturés de requêtes et qu'aucun ne soit disponible pour que les utilisateurs légitimes puissent se connecter

3 - L'accès non Attaque de l'homme du milieu :



Une attaque de l'homme du milieu implique que les attaquants interceptent le trafic, soit entre votre réseau et des sites externes, soit au sein de votre réseau. Si les protocoles de communication ne sont pas sécurisés ou si les attaquants trouvent un moyen de contourner cette sécurité, ils peuvent voler les données en cours de transmission, obtenir les informations d'identification des utilisateurs et détourner leurs sessions. L'exécution réussie de MITM comporte deux phases distinctes :

Interception :

La première étape intercepte le trafic utilisateur via le réseau de l'attaquant avant qu'il n'atteigne sa destination prévue. Les attaquants souhaitant adopter une approche plus active de l'interception peuvent lancer l'une des attaques suivantes :

IP spoofing :

Implique qu'un attaquant se déguise en application en modifiant les en-têtes de paquet dans une adresse IP. Par conséquent, les utilisateurs tentant d'accéder à une URL connectée à l'application sont renvoyés sur le site Web de l'attaquant.

ARP spoofing :

Est le processus consistant à lier l'adresse MAC d'un attaquant à l'adresse IP d'un utilisateur légitime sur un réseau local à l'aide de faux messages ARP. En conséquence, les données envoyées par l'utilisateur à l'adresse IP de l'hôte sont plutôt transmises à l'attaquant.

DNS spoofing :

Également connue sous le nom d'empoisonnement du cache DNS, consiste à infiltrer un serveur DNS et à modifier l'enregistrement d'adresse d'un site Web. En conséquence, les utilisateurs qui tentent d'accéder au site sont envoyés par l'enregistrement DNS modifié vers le site de l'attaquant.

Le déchiffrement :

Après interception, tout trafic SSL bidirectionnel doit être déchiffré sans alerter l'utilisateur ou l'application. Plusieurs méthodes existent pour y parvenir :

HTTPS spoofing :

Envoie un faux certificat au navigateur de la victime une fois la demande de connexion initiale à un site sécurisé effectuée. Il contient une empreinte numérique associée à l'application compromise, que le navigateur vérifie en fonction d'une liste existante de sites de confiance. L'attaquant peut alors accéder à toutes les données saisies par la victime avant qu'elles ne soient transmises à l'application.

SSL BEAST :

(Exploit de navigateur contre SSL/TLS) cible une vulnérabilité TLS version 1.0 dans SSL. Ici, l'ordinateur de la victime est infecté par du JavaScript malveillant qui intercepte les cookies cryptés envoyés par une application Web. Ensuite, le chaînage de blocs de chiffrement (CBC) de l'application est compromis afin de déchiffrer ses cookies et ses jetons d'authentification.

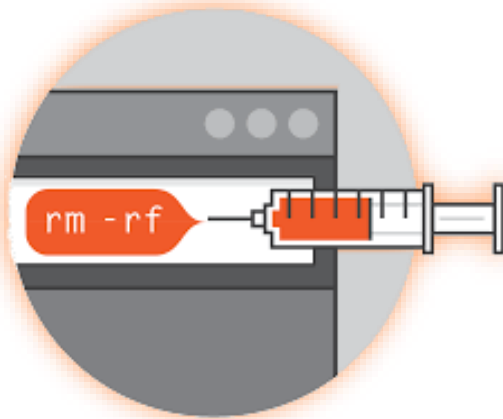
SSL hacking :

Se produit lorsqu'un attaquant transmet des clés d'authentification falsifiées à la fois à l'utilisateur et à l'application lors d'une poignée de main TCP. Cela établit ce qui semble être une connexion sécurisée alors qu'en fait, l'homme au milieu contrôle toute la session

SSL Stripping :

Rétrograde une connexion HTTPS vers HTTP en interceptant l'authentification TLS envoyée de l'application à l'utilisateur. L'attaquant envoie une version non chiffrée du site de l'application à l'utilisateur tout en maintenant la session sécurisée avec l'application. Pendant ce temps, toute la session de l'utilisateur est visible pour l'attaquant.

4 - Attaques par injection de code et SQL :



L'injection SQL, également connue sous le nom de SQLI, est un vecteur d'attaque courant qui utilise un code SQL malveillant pour la manipulation de la base de données principale afin d'accéder à des informations qui n'étaient pas destinées à être affichées. Ces informations peuvent inclure un certain nombre d'éléments, y compris des données sensibles de l'entreprise, des listes d'utilisateurs ou des détails privés sur les clients.

Types d'injections SQL :

Vous pouvez classer les types d'injections SQL en fonction des méthodes qu'ils utilisent pour accéder aux données backend et de leur potentiel de dommages.

Les injections SQL appartiennent généralement à trois catégories :

SQLI INTRABANDE [classique] :

L'attaquant utilise le même canal de communication pour lancer ses attaques et recueillir leurs résultats. La simplicité et l'efficacité de SQLI intrabande en font l'un des types d'attaque SQLI les plus courants.

Il existe deux sous-variantes de cette méthode :

Error-based SQLI.

Union-based SQLI.

SQLI inférentiel [aveugle] :

L'attaquant envoie des charges utiles de données au serveur et observe la réponse et le comportement du serveur pour en savoir plus sur sa structure. Cette méthode est appelée SQLI aveugle car les données ne sont pas transférées de la base de données du site Web à l'attaquant, de sorte que l'attaquant ne peut pas voir les informations sur l'attaque dans la bande.

Les injections SQL aveugles peuvent être classées comme suit :

Boolean.

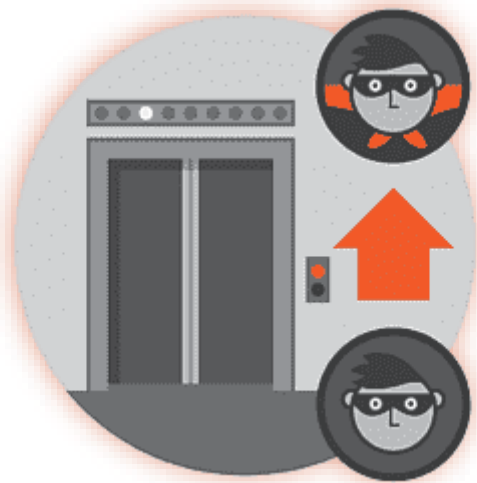
Time-Based.

SQLI hors bande :

L'attaquant ne peut effectuer cette forme d'attaque que lorsque certaines fonctionnalités sont activées sur le serveur de base de données utilisé par l'application Web. Cette forme d'attaque est principalement utilisée comme alternative aux techniques SQLI in-band et inférentielles.

5 - Escalade des privilèges :

L'élévation de privilèges peut être définie comme une attaque qui consiste à obtenir un accès illicite à des droits ou privilèges élevés, au-delà de ce qui est prévu ou autorisé pour un utilisateur. Cette attaque peut impliquer un acteur menaçant externe ou un initié. L'escalade de privilèges est une étape clé de la chaîne de cyberattaques et implique généralement l'exploitation d'une vulnérabilité d'escalade de privilèges, telle qu'un bogue système, une mauvaise configuration ou des contrôles d'accès inadéquats.



Les attaques par élévation de privilèges peuvent être séparées en deux grandes Catégories :

L'élévation horizontale des privilèges :

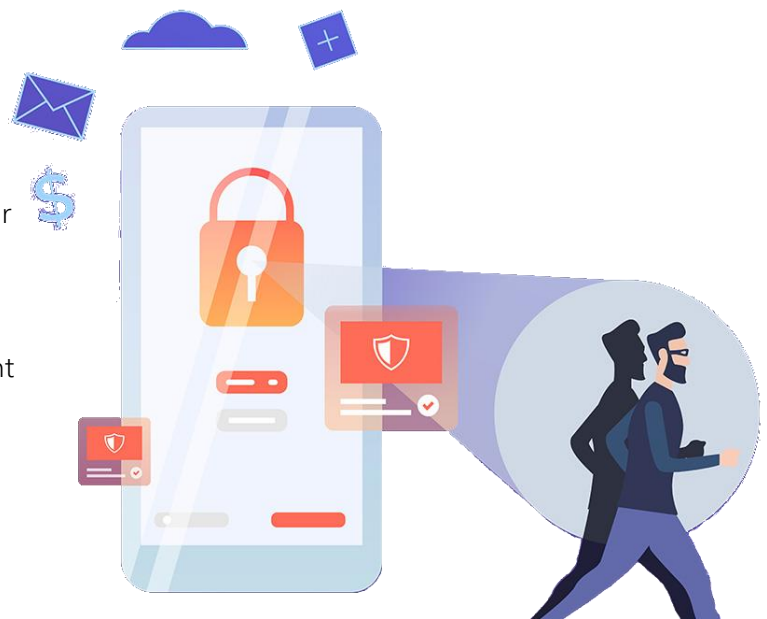
Implique d'accéder aux droits d'un autre compte, humain ou machine, avec des privilèges similaires. Cette action est appelée "prise de contrôle de compte". En règle générale, cela implique des comptes de niveau inférieur (c'est-à-dire un utilisateur standard), qui peuvent manquer de protection adéquate. Avec chaque nouveau compte horizontal compromis, un attaquant élargit sa sphère d'accès avec des privilèges similaires.

L'élévation verticale des privilèges :

Également connue sous le nom d'attaque d'élévation de privilèges, implique une augmentation des privilèges/accès privilégiés au-delà de ce qu'un utilisateur, une application ou un autre actif possède déjà. Cela implique de passer d'un faible niveau d'accès privilégié à un plus grand nombre d'accès privilégiés. L'élévation verticale des privilèges peut obliger l'attaquant à effectuer un certain nombre d'étapes intermédiaires (c'est-à-dire exécuter une attaque par débordement de la mémoire tampon, etc.) pour contourner ou outrepasser les contrôles de privilèges, ou exploiter les failles du logiciel, du micro logiciel, du noyau ou obtenir des informations d'identification privilégiées pour d'autres applications ou le système d'exploitation lui-même

6 - Menaces internes :

La menace interne est le potentiel pour un initié d'utiliser son accès autorisé ou sa compréhension d'une organisation pour nuire à cette organisation. Ce préjudice peut inclure des actes malveillants, complaisants ou involontaires qui affectent négativement l'intégrité, la confidentialité et la disponibilité de l'organisation, de ses données, de son personnel ou de ses installations.

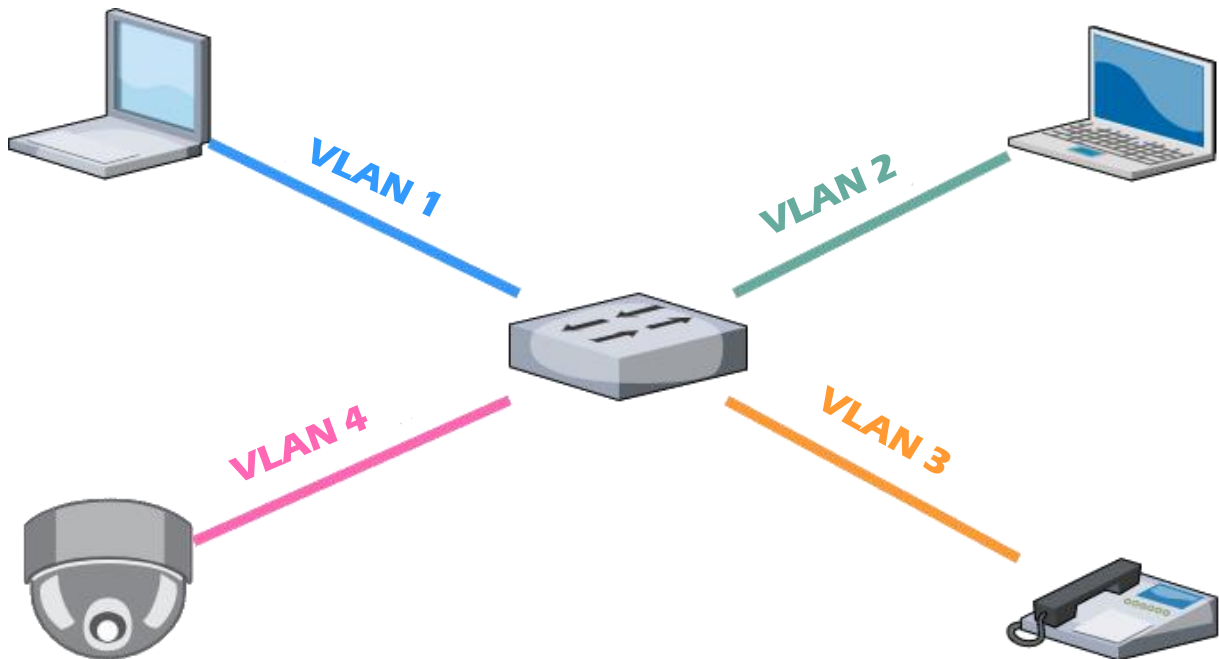


C - Meilleures pratiques de protection du réseau :

Séparez votre réseau :

Un élément fondamental pour éviter les menaces de sécurité réseau consiste à diviser un réseau en zones en fonction des exigences de sécurité. Cela peut être fait en utilisant des sous réseaux au sein du même réseau ou en créant des réseaux locaux virtuels (VLAN), chacun se comportant comme un réseau distinct complet. La segmentation limite l'impact potentiel d'une attaque à une zone et oblige les attaquants à prendre des mesures spéciales pour pénétrer et accéder à d'autres zones du réseau.

EX :



Réglementer l'accès à Internet via un serveur proxy :

N'autorisez pas les utilisateurs du réseau à accéder à Internet sans contrôle. Transmettez toutes les demandes via un proxy transparent et utilisez-le pour contrôler et surveiller le comportement des utilisateurs. Assurez-vous que les connexions sortantes sont effectivement effectuées par un humain et non par un bot ou un autre mécanisme automatisé. Ajoutez des domaines à la liste blanche pour vous assurer que les utilisateurs professionnels ne peuvent accéder qu'aux sites Web que vous avez explicitement approuvés.



Utiliser la traduction d'adresses réseau :

La traduction d'adresses réseau (NAT) vous permet de traduire les adresses IP internes en adresses accessibles sur les réseaux publics. Vous pouvez l'utiliser pour connecter plusieurs ordinateurs à Internet en utilisant une seule adresse IP. Cela fournit une couche de sécurité supplémentaire, car tout trafic entrant ou sortant doit passer par un périphérique NAT, et il y a moins d'adresses IP, ce qui rend difficile pour les attaquants de comprendre à quel hôte ils se connectent.

Placer correctement les dispositifs de sécurité :

Placez un pare-feu à chaque jonction de zones réseau, pas seulement à la périphérie du réseau. Si vous ne pouvez pas déployer de pare-feu complet partout, utilisez la fonctionnalité de pare-feu intégrée de vos commutateurs et routeurs. Déployez des dispositifs anti-DDoS ou des services cloud à la périphérie du réseau. Considérez soigneusement où placer les appareils stratégiques comme les équilibreurs de charge - s'ils se trouvent en dehors de la zone démilitarisée (DMZ), ils ne seront pas protégés par votre appareil de sécurité réseau.

LES PARE-FEU

A - Technologies et Solutions de sécurité [pare-feu] :

Un pare-feu est un dispositif qui permet à plusieurs réseaux de communiquer entre eux selon une politique de sécurité définie. Ils sont utilisés lorsqu'il est nécessaire que des réseaux de différents niveaux de confiance communiquent entre eux.



Les pare-feux sont utilisés principalement dans quatre buts :

**Protéger des
malveillances
externes**

**Surveiller les flux
internes/externes**

**Faciliter
l'administration
du réseau**

**Éviter la fuite
d'information non
contrôlée vers
l'extérieur.**

B - Les pare-feu fameux :

De nombreux Firewalls existent sous tous les systèmes d'exploitation. Le choix s'est fait en partie du fait de la contrainte des services offerts, sa fiabilité et qu'il soit très répandu dans le monde de l'entreprise.

Notre étude comparative se base sur les Firewalls suivants :22

1 - IPCOP :

Est à l'origine un fork de Smoothwall Express. Ceci signifie qu'IPCop est basé sur linux Redhat. La première version est sortie en décembre 2001. Aujourd'hui on est à la version 2.0.6. IPCop est distribué sous licence GPL.



2 - PfSense :

Est basé sur une distribution FreeBSD3 adapté pour être utilisé comme un pare feu et un routeur. Le projet débuta en 2004 avec le projet m0n0wall qui s'axer plus vers des installations sur ordinateur à part entière plutôt que la mise au point du matériel embarqué de m0n0wall. Pfsense inclue de nombreuses fonctions qui sont fournis par les pare feux commerciaux payants et d'autres qui ne sont disponibles que sur Pfsense :

- Pare feu
- Translation d'adresse et de port
- Redondance



C - Tableau comparatif :

Critère	PFsense	IP cop
Filtrage et sécurité		
Avec état	☑	☑
Filtrage d'URL	☑	☑
Filtrage contenu web	☑	☑
Temps d'accès par utilisateur	✖	✖
IDS	☑	☑
Antivirus WEB (HTTP/FTP)	☑	☑
Email Antivirus/Antispam	☑	☑
Routage		
NAT (dynamique)	☑	☑

Port adresse translation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Politique de routage (Policy Routing)	<input checked="" type="checkbox"/>	-
Licence	FreeBSD	GPL
Ergonomie		
Interface graphique	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Taille en Mo	88.8	47.23
Haute disponibilité		
Load Balance	<input checked="" type="checkbox"/>	x
Multi Wan	<input checked="" type="checkbox"/>	x
Capacité de failover	<input checked="" type="checkbox"/>	x
Facilité de configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Facilité de surveillance/journaux	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Performance et consommation réseau	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service		
Proxy web	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Proxy POP3	x	x
Proxy SIP	x	x
DHCP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DNS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TELNET	x	<input checked="" type="checkbox"/>
SSH	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VPN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
QoS		
Priorité selon type de trafic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Lissage de trafic (limitation)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Administration		
Recherche de mise à jour	<input checked="" type="checkbox"/>	x
Mise à jour automatique	<input checked="" type="checkbox"/>	x

PFSENSE

A - Pfsense comme solution :

Une solution de sécurité open-source avec un noyau personnalisé basé sur FreeBSD OS. PfSense est l'un des principaux pare-feu réseau avec un niveau commercial de fonctionnalités. PfSense est disponible en tant que périphérique matériel, Appliance virtuelle et binaire téléchargeable (édition communautaire).



À un niveau élevé, certaines des fonctionnalités PfSense qui méritent d'être mentionnées sont :

Pare feu :

Filtrage IP / port, limitation des connexions, capacité de couche deux, nettoyage.

Tableau d'état :

Par défaut toutes les règles sont avec état, plusieurs configurations disponibles pour la gestion des états.

Équilibrage de la charge du serveur :

LB intégrée à répartir la charge entre plusieurs serveurs backend.

NAT :

[Traduction d'adresse réseau] - redirection de port, réflexion.

HA :

[Haute disponibilité] - basculement vers le secondaire en cas de panne principale.

Multi-WAN :

[Réseau étendu] - utilisez plus d'une connexion Internet.

VPN :

[Un réseau privé virtuel] - prend en charge IP sec et OpenVPN.

Signalement :

Conserver l'historique des informations d'utilisation des ressources.

La surveillance :

Surveillance en temps réel.

DNS dynamique :

Plusieurs clients DNS sont inclus.

DHCP – Relais :

DHCP & Relais solutions.



Plus que certaines des fonctionnalités de pare-feu commerciales, vous obtenez GRATUITEMENT.



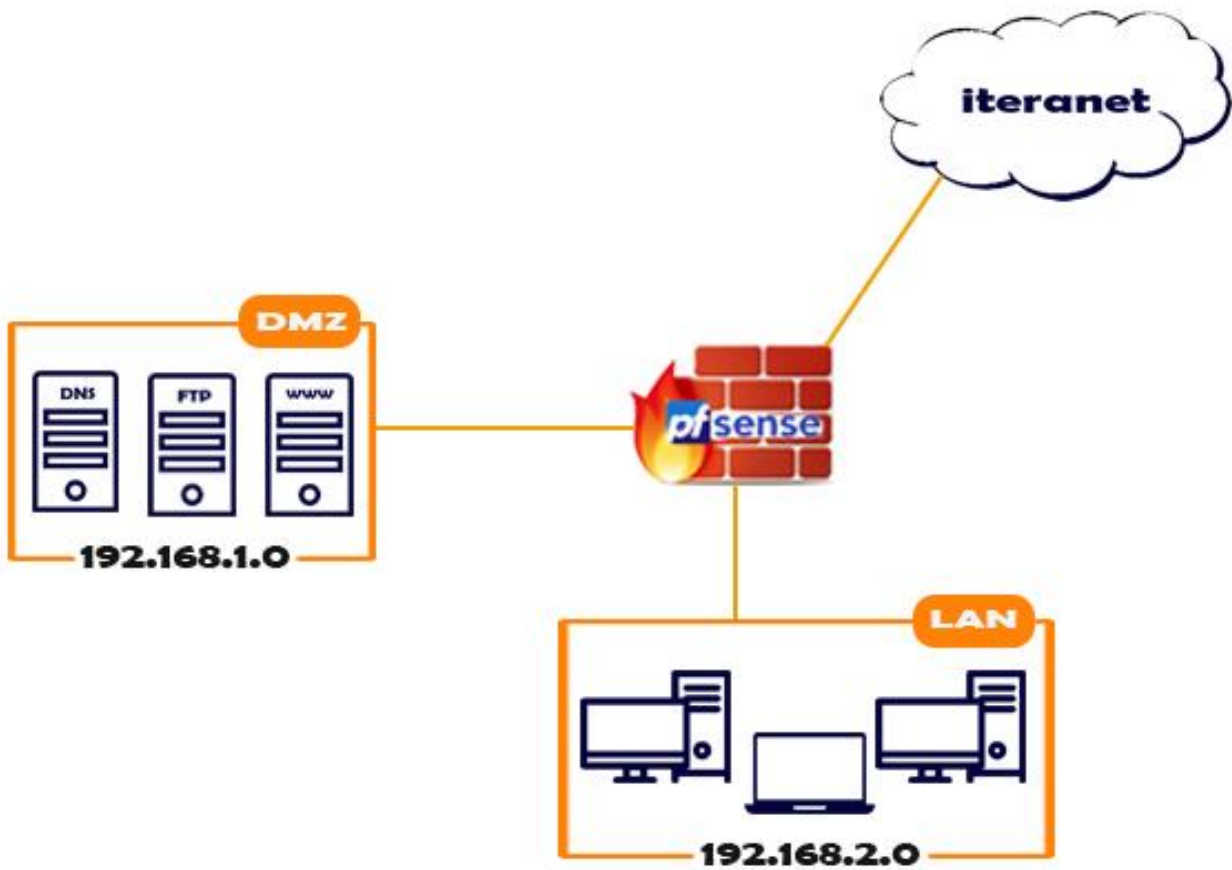
Non seulement cela, mais vous avez également la possibilité d'installer des packages en un seul clic.

EX :

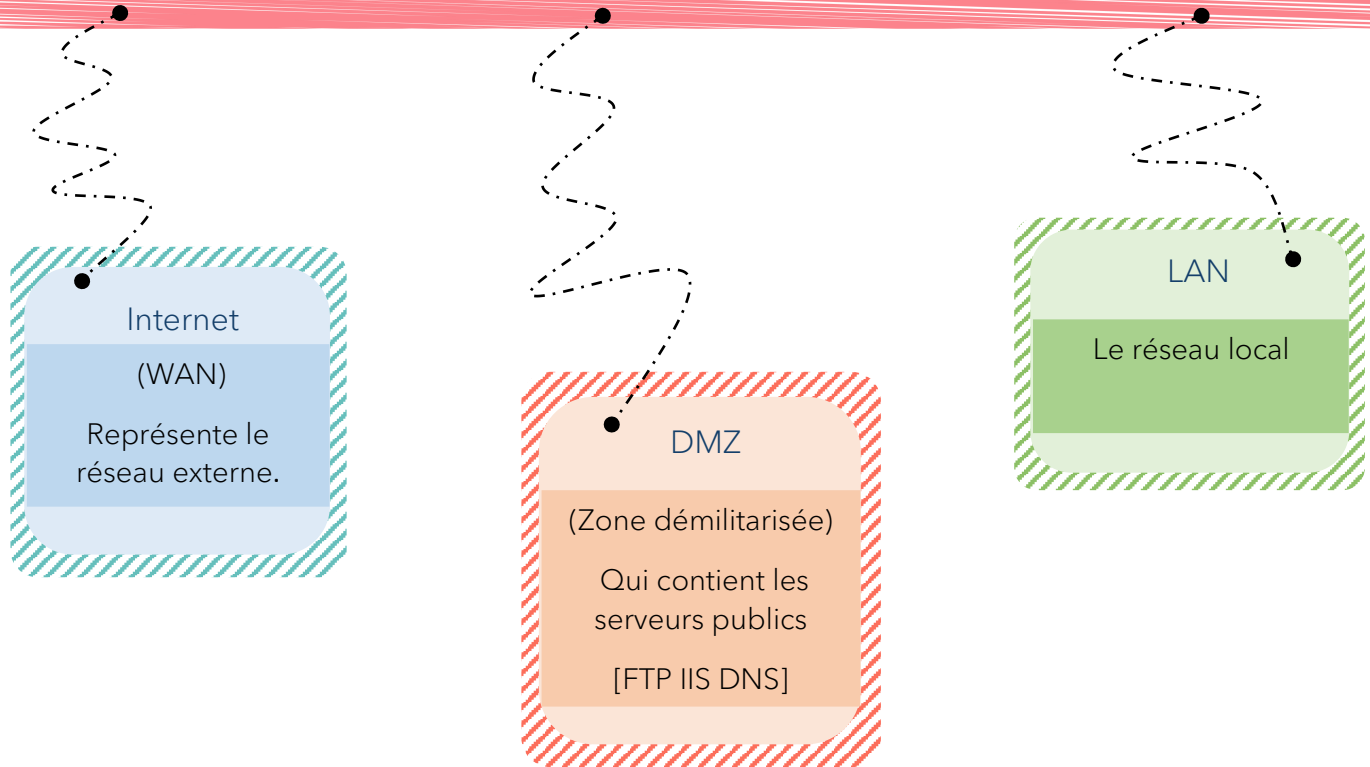
- Sécurité - un étourdissant, renifler, étain, nmap, arpwatsh.
- La surveillance - iftop, ntopng, softflowd, urlsnarf, darkstat, mailreport.
- La mise en réseau - netio, noix, Avahi.
- Routage - frr, olsrd, routé, OpenBGPD.
- Services - iperf, widentd, syslog-ng, bind, acme, inspector, git, dns-server.

A – Installation et configuration Pfsense :

1 - Architecture réseau :

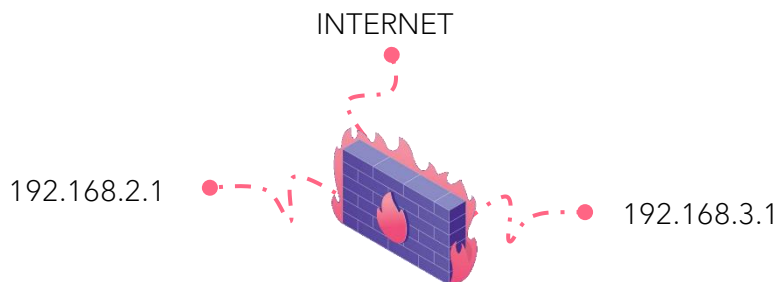


Cette topologie représente l'architecture réseau qu'on va l'implémenter. On y distingue :

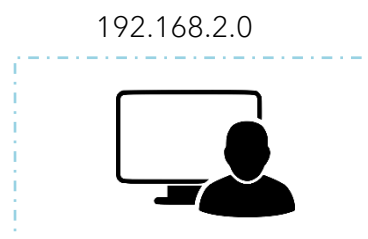


2 - plan d'adressage :

PfSense :



LAN :



DMZ :

192.168.3.0



3 - installation :

On installe PfSense sur GNS3, la configuration réseau, en effet, il faut paramétrer trois cartes réseaux sur notre PFsense, car j'ai une interface pour le réseau local, une pour le réseau externe et une pour la DMZ.

Avant de se lancer dans la configuration de PFsense, il faut configurer les VMNET de VMware Workstation.

Les **VMNET** sont des switches virtuels qui permettent de fournir trois modes de connexion :

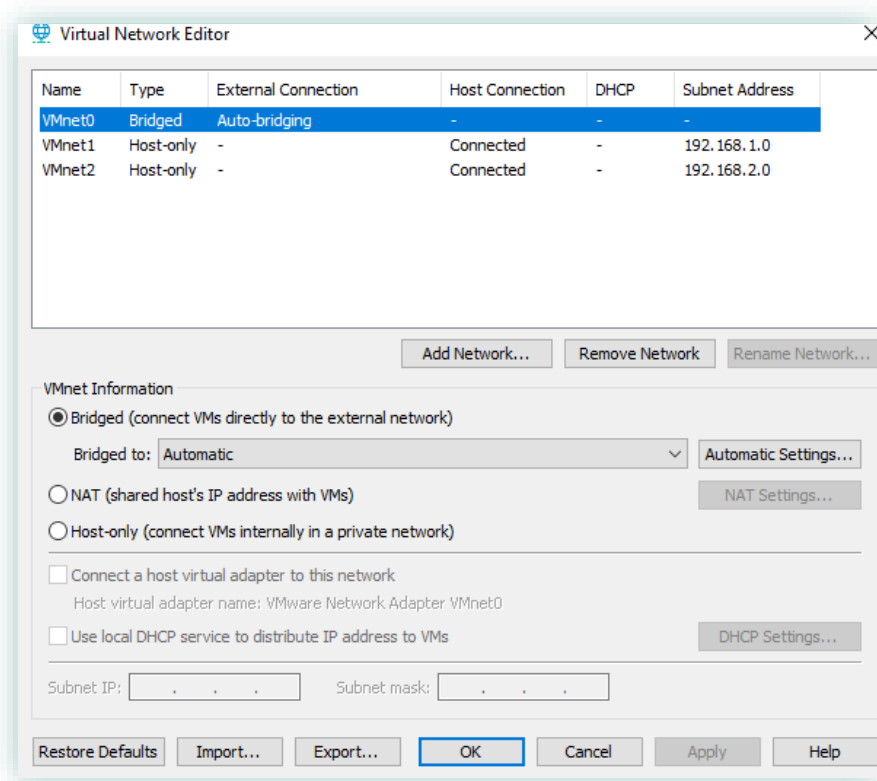
- Le mode Host-Only qui permet de connecter des machines virtuelles entre-elles ou/et avec la machine physique.
- Le mode Bridged qui permet de connecter une machine virtuelle au réseau externe.
- Le mode NAT qui permet de se cacher derrière la machine physique et de partager sa connexion internet avec la machine virtuelle.

Donc, si en réalité pour connecter plusieurs machines physiques on doit les brancher dans le même switch, dans VMware, pour connecter des machines entre-elles, il faut les mettre dans le même VMNET.

La configuration des VMNET se fait grâce à l'outil "Virtual Network Editor" qui vient avec l'installation de VMware Workstation.



On a besoin de 3 réseaux LAN, DMZ et WAN, on utilisera donc 3 VMNET [switches virtuels], soit VMNET 1, 2 et 3.



Une fois PfSense installé, on doit paramétrer les interfaces.

```

WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 192.168.2.1/24
DMZ (opt1)     -> em2      -> 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

```

On lance l'interface web de configuration à travers un poste de client.

Au niveau de la barre de navigation, on tape [HTTP://ADRESSE-IP-LAN](http://ADRESSE-IP-LAN). Ensuite, on doit s'authentifier pour accéder à l'interface de PfSense.

EX : On tape [HTTP://192.168.2.1](http://192.168.2.1):

The screenshot shows the pfSense Community Edition dashboard. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled 'Status / Dashboard' and features two primary panels. The 'System Information' panel on the left provides details about the system, including the name (PFE.ASR.home.arpa), user (admin@192.168.2.2), system type (VMware Virtual Machine), BIOS version (6.00), and the current version (2.5.2-RELEASE). It also displays CPU type, hardware crypto status, kernel PTI, MDS Mitigation, uptime, current date/time, DNS servers, last config change, and state table size. The 'Netgate Services And Support' panel on the right shows a message about retrieving support information. Below this, the 'Interfaces' panel lists three interfaces: WAN, LAN, and DMZ, each with its status (up), speed (1000baseT <full-duplex>), and IP address (0.0.0.0, 192.168.2.1, and 192.168.1.1 respectively).

System Information	
Name	PFE.ASR.home.arpa
User	admin@192.168.2.2 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 5c53335fd8e734db0ac5
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.5.2-RELEASE (amd64) built on Fri Jul 02 15:33:00 EDT 2021 FreeBSD 12.2-STABLE Unable to check for updates
CPU Type	Intel(R) Core(TM) i5-4300U CPU @ 1.90GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	01 Hour 55 Minutes 35 Seconds
Current date/time	Fri Feb 18 8:57:05 CET 2022
DNS server(s)	<ul style="list-style-type: none">127.0.0.18.8.8.88.8.4.4
Last config change	Fri Feb 18 8:20:31 CET 2022
State table size	0% (1/19000) Show states

Netgate Services And Support	
Retrieving support information	

Interfaces	
WAN	1000baseT <full-duplex> 0.0.0.0
LAN	1000baseT <full-duplex> 192.168.2.1
DMZ	1000baseT <full-duplex> 192.168.1.1

J'ai configuré les interfaces dans le menu

Interfaces ▼




Assignments

WAN : [DHCP]

LAN : 192.168.2.1/24

DMZ : 192.168.3.1/24

Adressage réseau des interfaces sur de PfSense :

Interfaces			
 WAN	↑	1000baseT <full-duplex>	0.0.0.0
 LAN	↑	1000baseT <full-duplex>	192.168.2.1
 DMZ	↑	1000baseT <full-duplex>	192.168.1.1

4 - Configurer le DHCP sur l'interface LAN :

Dans l'interface LAN, nous avons choisi d'utiliser le service DHCP pour allouer dynamiquement des adresses IP aux utilisateurs :

LA CONFIGURATION UTILISE :

LAN DMZ

General Options

Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny unknown clients	<div>Allow known clients from only this interface</div> <div>When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed on <i>any</i> scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.</div>
Ignore denied clients	<input type="checkbox"/> Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers	<input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Subnet	192.168.2.0
Subnet mask	255.255.255.0
Available range	192.168.2.1 - 192.168.2.254
Range	<div>192.168.2.10</div> <div>From To</div>

VÉRIFIER LE SERVICE DANS UNE MACHINE CLIENT :

```
C:\Users\stihi>ipconfig

Windows IP Configuration

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : PFE.local
    IPv4 Address. . . . . : 192.168.2.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

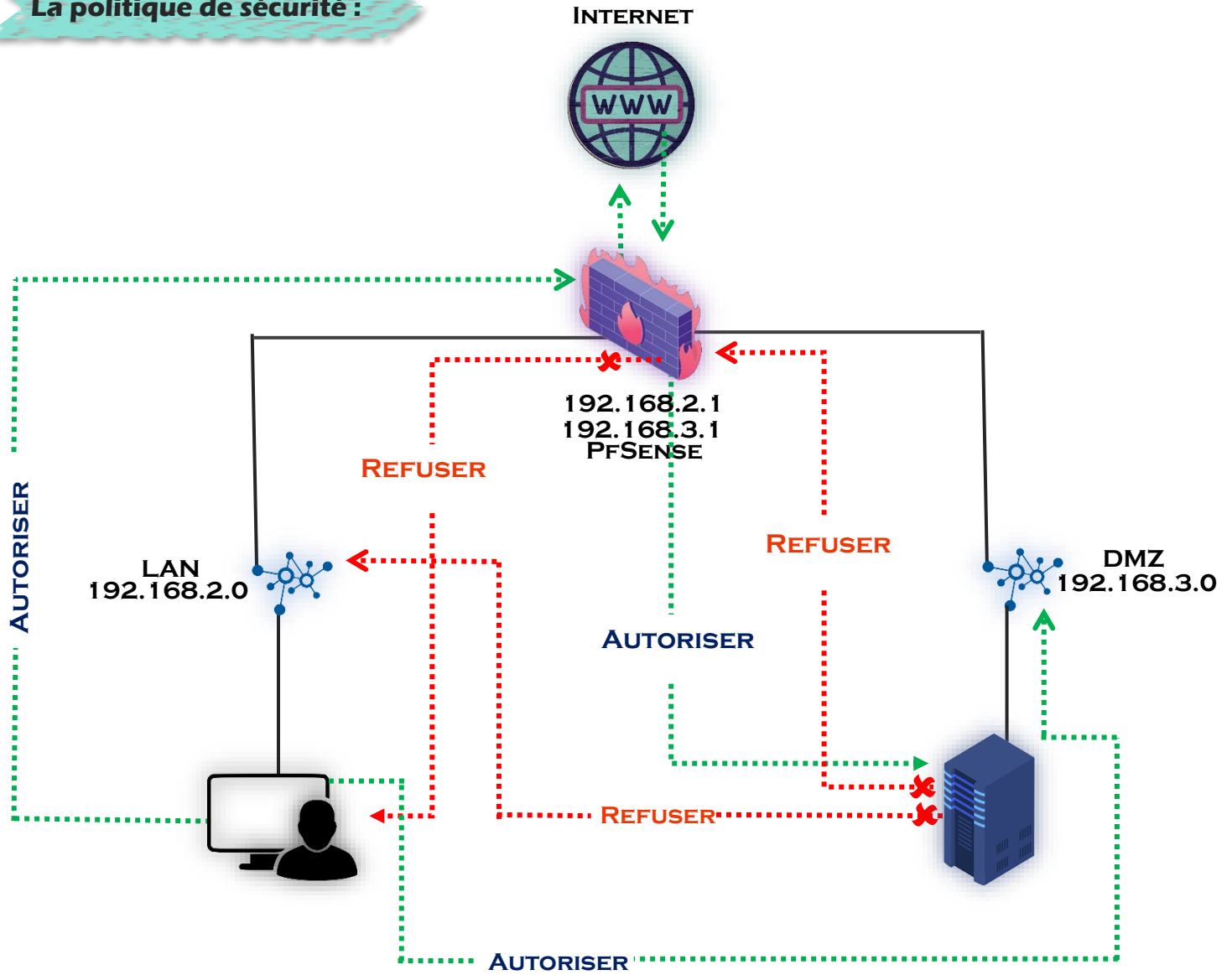
Tunnel adapter isatap.{3427D447-B2F8-40CA-B644-8CBA93AA81A6}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
Tunnel adapter isatap.PFE.local:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : PFE.local
```

5 - Configurer les règles du pare-feu :

La politique de sécurité :



La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Trafic du réseau externe vers la DMZ autorisé.
- Trafic du réseau externe vers le réseau interne interdit.
- Trafic du réseau interne vers la DMZ autorisé.
- Trafic du réseau interne vers le réseau externe autorisé.
- Trafic de la DMZ vers le réseau interne interdit.
- Trafic de la DMZ vers le réseau externe refusé.

Configuration de notre LAN :

Notre politique de sécurité. Pour garantir la sécurité de notre LAN, nous voulons :













Que le réseau de la DMZ, n'ait aucun accès vers le LAN.

Que LAN puisse naviguer sur le web.





Que LAN puisse accéder au serveur de la DMZ

De plus utilisateurs n'ont besoin d'accéder HTTP & HTTPS.

Ils n'ont donc besoin que des ports 80 443 et 53[DNS] :

public service		LAN							
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none	   
<input type="checkbox"/>	✓ 1 / 1.32 MiB	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none	   
<input type="checkbox"/>	✓ 0 / 608 B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none	   

Et n'oublier pas le Protocol ICMP pour tester la connectivité :

pour tester la connectivité		LAN							
<input type="checkbox"/>	✓ 0 / 2 KiB	IPv4 ICMP any	LAN net	*	*	*	*	none	   

Configuration de notre DMZ :

La DMZ, c'est la partie ouverte à Internet. Nous établirons en premier lieu, la politique de sécurité, puis vous la configurerez point par point.

La politique de sécurité :

- Les utilisateurs d'internet doivent avoir accès au serveur WEB.
- Le serveur Web doit pouvoir leur répondre
- Seuls les ports 80 et 443 [les ports HTTP et HTTPS] sont ouverts.

Rendez le serveur Web accessible depuis Internet :

Pour cela, il vous faut donc configurer le NAT :

The screenshot shows the Mikrotik WinBox interface for configuring NAT. The breadcrumb navigation at the top reads "Firewall / NAT / Port Forward". A yellow notification bar states: "The NAT configuration has been changed. The changes must be applied for them to take effect." with an "Apply Changes" button. Below the notification, there are tabs for "Port Forward", "1:1", "Outbound", and "NPt", with "Port Forward" being the active tab. A table titled "Rules" contains two entries:

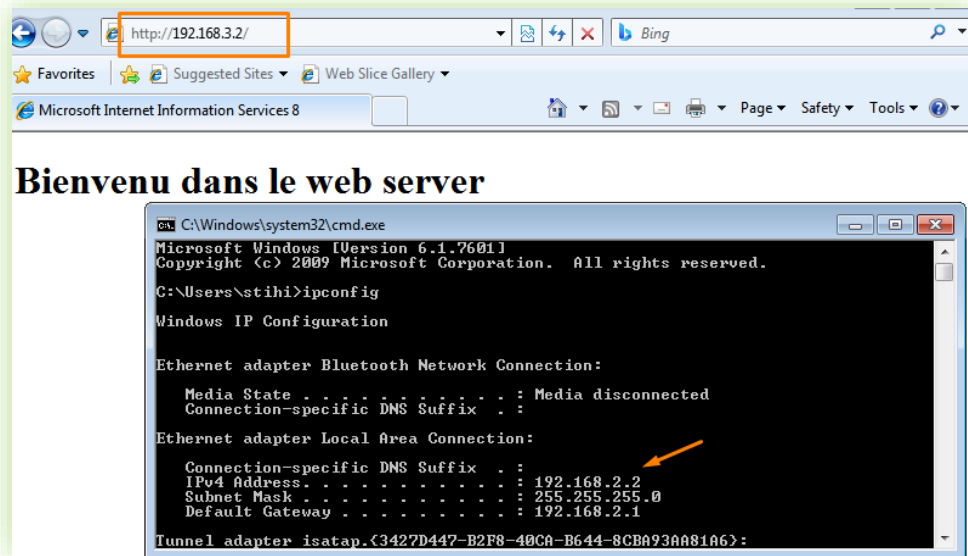
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions	
<input type="checkbox"/>	✓	WAN	TCP	*	*	DMZ address	80 (HTTP)	192.168.3.2	80 (HTTP)	pat server web	
<input type="checkbox"/>	✓	WAN	TCP	*	*	DMZ address	443 (HTTPS)	192.168.3.2	443 (HTTPS)	pat server web	

At the bottom of the table, there are buttons for "Add" (up arrow), "Add" (down arrow), "Delete", "Save", and "Separator".

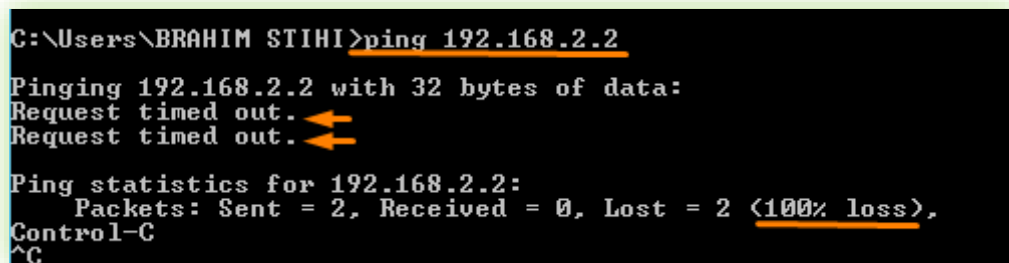
Il ne vous manque plus qu'à créer la règle firewall permettant l'accès à l'adresse WAN part le port 80

Teste la configuration :

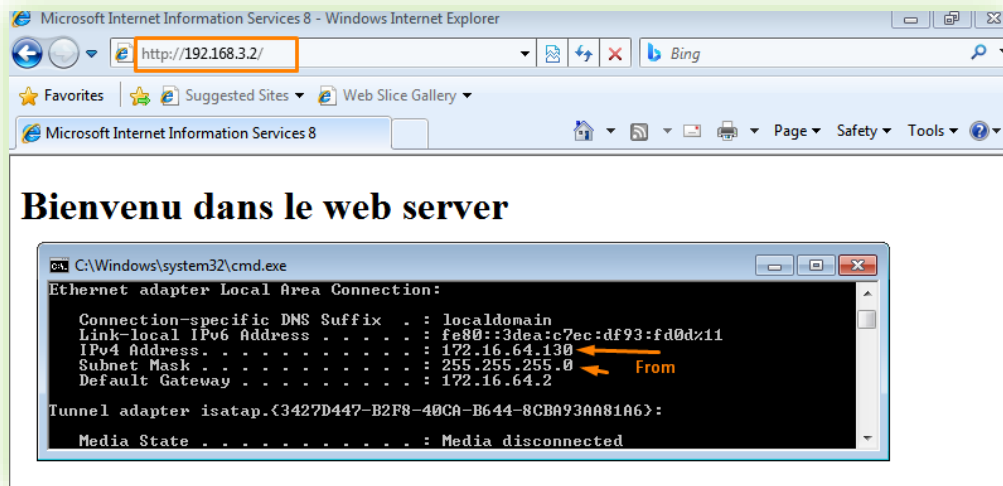
- Tester la connectivité à le LAN vers le DMZ :



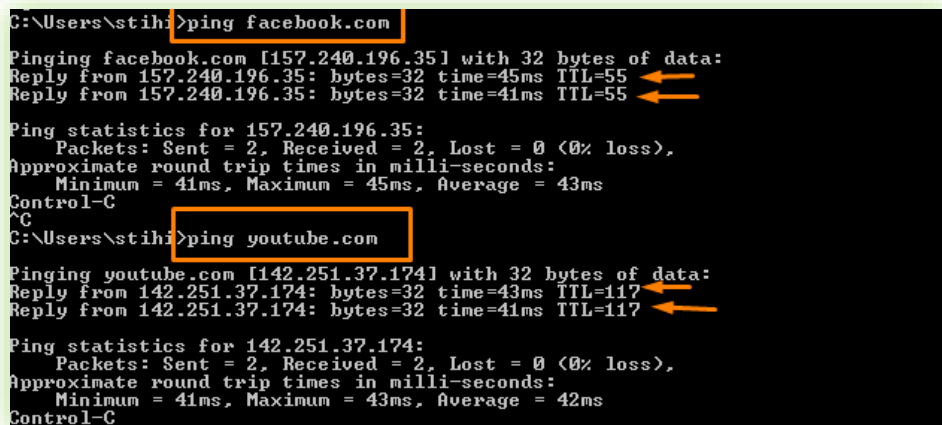
- Tester le DMZ vers le LAN :



- Tester l'utilisateur d'internet vers le DMZ :



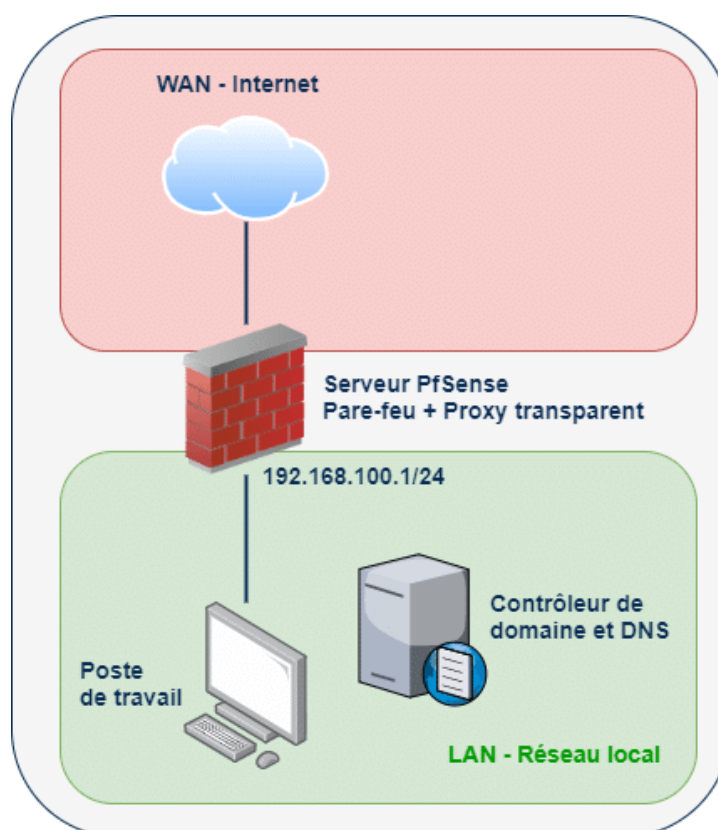
- Tester l'utilisateur de LAN vers le l'internet :



PROXY

L'objectif de la mise en place de ce proxy transparent, c'est de permettre l'accélération de la navigation Internet grâce à la mise en cache, mais aussi le filtrage des sites Internet, sans aucune configuration sur les postes clients.

Pour utiliser la fonctions proxy, on ajouter les packages `Squid` et `SquidGuard` et on le configurer.





Squid :


Squid est un serveur proxy/cache libre très connu du monde Open Source. Ce serveur est complet et propose une multitude d'options et de services qui lui ont permis d'être largement adopté par les professionnels. Il est capable de manipuler les protocoles HTTP, FTP, SSL, etc.



SquidGuard :

SquidGuard est un redirecteur d'URL, il utilise les listes noires avec le proxy [Squid] SquidGuard possède deux grands avantages : il est rapide et gratuit. Il est publié sous GNU Public License, licence gratuite.

SquidGuard est utilisé pour :

- 
- Limiter l'accès Internet pour certains utilisateurs à une liste de serveurs Web et /ou des URLs qui sont acceptés et bien connus.
 - Bloquer l'accès à des URLs correspondant à une liste d'expressions régulières ou des mots pour certains utilisateurs.
 - Imposer l'utilisation de nom de domaine et interdire l'utilisation de l'adresse IP dans les URLs.
 - Rediriger les URLs bloqués à une page d'informations relative à PfSense.
 - Avoir des règles d'accès différentes selon le moment de la journée, le jour de la Semaine, date, etc.

1 - Installation :

➤ Le serveur mandataire Squid et SquidGuard existent sur PfSense sous forme de package à installer :

À partir de l'interface graphique Web PfSense, il navigue vers :

➤ System > Package Manager > Available Packages et on Install le package squid :

The screenshot shows the 'Search' interface of the PfSense Package Manager. The search term 'squid' is entered in the search box. Below the search bar, there is a table of packages. The 'squid' package is highlighted with a red box. The table has columns for Name, Version, and Description. The 'squid' package is version 0.4.45_8 and is described as a high performance web proxy cache. It has several dependencies listed below it. The 'squidGuard' package is also visible in the list.

Name	Version	Description
Lightsquid	3.0.6_9	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.
squid	0.4.45_8	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.
squidGuard	1.16.18_20	High performance web proxy URL filter.

pfSense-pkg-squidGuard installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

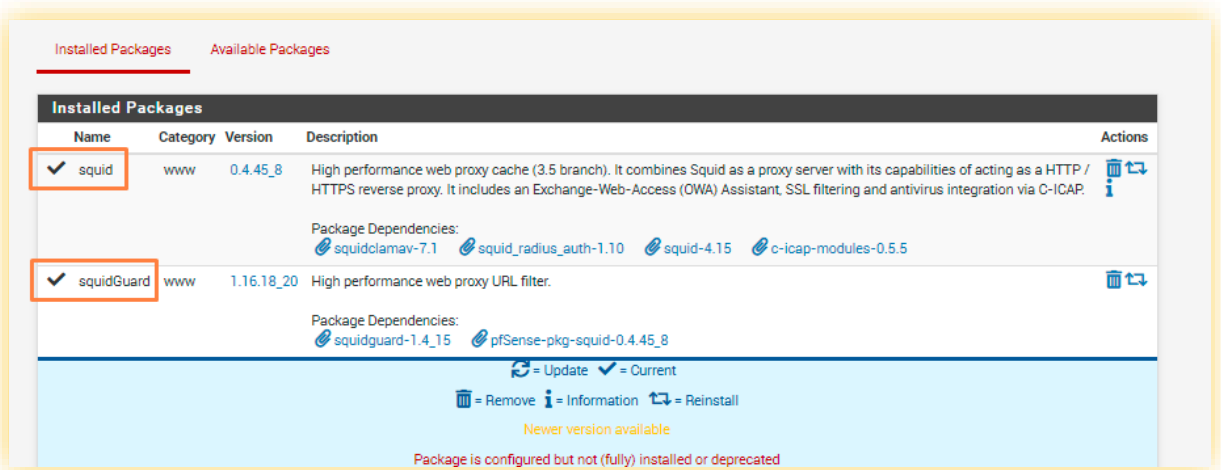
```
To activate the changes do a /usr/local/sbin/squid -k reconfigure
=====
Message from pfSense-pkg-squid-0.4.45_8:

--
Please visit Services - Squid Proxy Server menu to configure the package and enable the proxy.
=====
Message from pfSense-pkg-squidGuard-1.16.18_20:

--
Please visit Services - SquidGuard Proxy Filter - Target Categories and set up at least one category there before enabling SquidGuard. See
https://docs.netgate.com/pfsense/en/latest/packages/cache-proxy/squidguard.html for details.
>>> Cleaning up cache... done.
Success
```

Pour confirmer que les packages ont été installés, il est préférable de redémarrer les deux firewalls. Ensuite, on remarque que ces deux packages sont ajoutés au niveau de :

➤ System > Package > Installed Packages :



2 - Configuration de Squid :

➤ Une fois Squid et SquidGuard ont été installés, je vais configurer maintenant les paramètres du serveur proxy.

On choisit : Services > Proxy Server,

Dans l'onglet Général, on définit les paramètres suivants :

⚠ L'option d'interface proxy doit être réglé sur "LAN", et parce qu'on veut que Squid fonctionne avec authentification des clients, on choisit [Allow users on interface] :

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status Sync

Squid General Settings

Enable Squid Proxy ☒ Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data ☒ If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

Listen IP Version IPv4
Select the IP version Squid will use to select addresses for accepting client connections.

CARP Status VIP none
Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.
Important: Don't forget to generate Local Cache on the secondary node and configure **XMLRPC Sync** for the settings synchronization.

Proxy Interface(s) WAN LAN DMZ loopback
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

Outgoing Network Interface Default (auto)
The interface the proxy server will use for outgoing connections.

Proxy Port 3128
This is the port the proxy server will listen on. Default: 3128

ICP Port
This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

Allow Users on Interface ☒ If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.

Patch Captive Portal This feature was removed - see Bug #5594 for details!

Resolve DNS IPv4 First ☐ Enable this to force DNS IPv4 lookup first.
This option is very useful if you have problems accessing HTTPS sites.

Disable ICMP ☐ Check this to disable Squid ICMP pinger helper.

Use Alternate DNS

Ensuite, on choisit l'onglet **Local Cache**, par défaut, la taille du disque dur cache43 37 est réglé sur 100Mb :

Squid Hard Disk Cache Settings

Hard Disk Cache Size 100
Amount of disk space (in megabytes) to use for cached objects.

Hard Disk Cache System null
This specifies the kind of storage system to use.

Clear Disk Cache NOW Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron.
If you wish to clear cache **immediately**, click this button **once**: **Clear Disk Cache NOW**

Level 1 Directories 16
Specifies the number of Level 1 directories for the hard disk cache.

Hard Disk Cache Location /var/squid/cache
This is the directory where the cache will be stored. Default: /var/squid/cache

Minimum Object Size 0
Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)

Maximum Object Size 4
Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB)

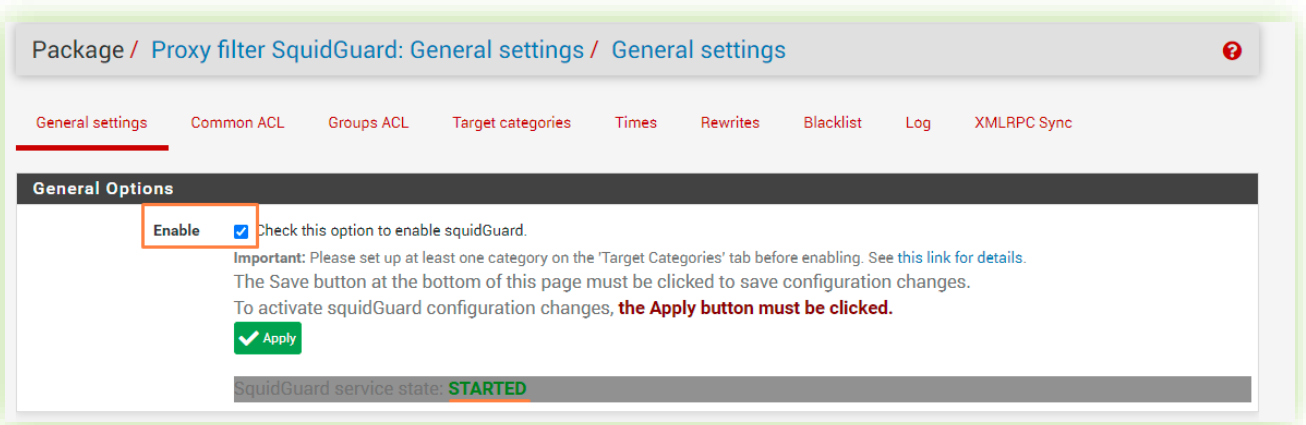
3 - Contrôle et filtrage de l'accès Web SquidGuard :

Le package **SquidGuard** permet un filtrage de contenu URL et un contrôle d'accès très puissants.

Il peut utiliser des listes noires ou des listes personnalisées de sites Web, et peut sélectivement autoriser ou refuser l'accès à ces sites.

SquidGuard est capable de bien plus que ce qui sera couvert dans cette section.

On navigue vers **Services > SquidGuard Proxy Filter** et dans **général setting** on coche sur enable ✓ pour activer le SquidGuard :



Target catégories :

Les catégories cibles sont des listes personnalisées de sites ou d'autres expressions qui définissent un groupe d'éléments pouvant être utilisés pour autoriser ou refuser l'accès. Elles sont gérées dans l'onglet Catégories cibles.

Dans l'onglet Target catégories on ajoute une catégorie qui s'appelle **blocked site** possède une liste des sites web on veut de bloquer :

Proxy filter SquidGuard: Target categories / Edit / Target categories

General settings Common ACL Groups ACL **Target categories** Times Rewrites Blacklist Log XMLRPC Sync

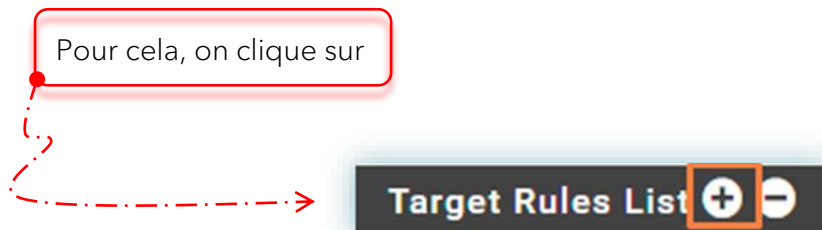
General Options

Name
 Enter a unique name of this rule here.
 The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter.

Order
 Select the new position for this target category. Target categories are listed in this order on ACLs and are matched from the top down in sequence.

Domain List

➤ On visite l'onglet Common ACL pour Choisir les actions pour nos catégories :



➤ Et on sélectionne les actions souhaitées dans la liste déroulante à la fin de la ligne pour chaque catégorie :

Package / Proxy filter SquidGuard: Common Access Control List (ACL) / Common ACL

General settings **Common ACL** Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

General Options

Target Rules

Target Rules List + -

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

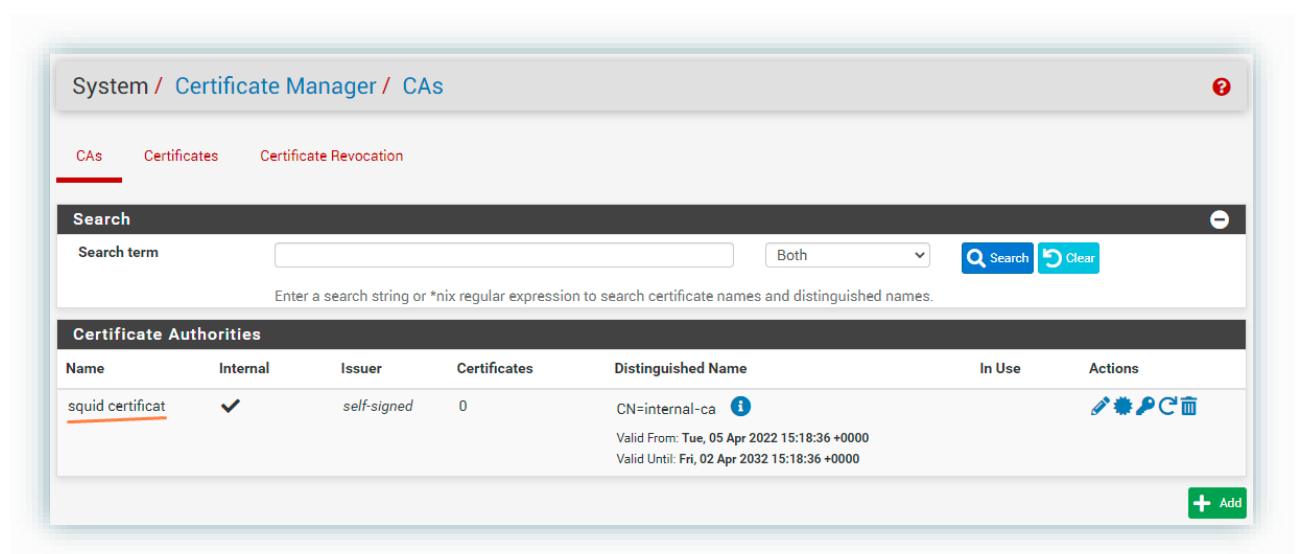
Target Categories	access	deny
<input type="text" value="Blocked_sites"/>	<input type="text" value="access"/>	<input type="text" value="deny"/>
Default access [all]	<input type="text" value="access"/>	<input type="text" value="allow"/>

Le choix default Access [all] contrôle ce qui se passe lorsqu'aucune correspondance n'a été trouvée dans aucune des catégories disponibles.

Proxise transparents et HTTP/HTTPS :

- Lors de l'utilisation d'un proxy, il est uniquement possible d'intercepter le trafic HTTP de manière transparente. Autrement dit, seul le trafic HTTP peut être saisi automatiquement et forcé via un proxy sans intervention de l'utilisateur ou de ses connaissances. C'est pratique, car il ne nécessite aucune configuration de paramètres sur le PC de l'utilisateur. L'inconvénient est que seul le trafic HTTP peut être capturé à l'aide de cette méthode ; il n'est pas possible d'intercepter HTTPS de la même manière.
- Tenter d'intercepter HTTPS de manière transparente romprait la chaîne de confiance créée par SSL, ce qui ferait que l'utilisateur serait accueilli par un avertissement de certificat effrayant lorsqu'il tenterait d'accéder à un site sécurisé. Cet avertissement serait valide dans ce cas, car le proxy effectue essentiellement une attaque de l'homme du milieu afin d'inspecter le trafic de l'utilisateur.
- Le package proxy Squid est capable d'intercepter HTTPS, mais cela ne peut pas être fait complètement à l'insu de l'utilisateur ou des modifications apportées à son ordinateur. Au minimum, l'interception de HTTPS nécessite l'installation d'une autorité de certification racine de confiance qui a été créée à cet effet, afin que le proxy puisse sembler utiliser des certificats valides.

Donc on va naviguer vers **System > Certificate Manager > CAs** et on crée une [internal certificat] :



Puis on navigue vers **Package > Proxy Server : General Settings > General** et dans Transparent Proxy Settings on coche ☒ sur enable et on choisit L'interface sur lesquelles le serveur proxy interceptera de manière transparente les requêtes :

Transparent Proxy Settings

Transparent HTTP Proxy ☒ Enable transparent mode to forward all requests for destination port 80 to the proxy server.

Transparent proxy mode works without any additional configuration being necessary on clients.

Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.

Hint: In order to proxy both HTTP and HTTPS protocols **without intercepting SSL connections**, configure WPAD/PAC options on your DNS/DHCP servers.

Transparent Proxy Interface(s)

WAN
LAN
DMZ

The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.

Après dans **SSL Man In the Middle Filtering**

SSL Man In the Middle Filtering

HTTPS/SSL Interception ☒ Enable SSL filtering.

SSL/MITM Mode **Splice All**

The SSL/MITM mode determines how SSL interception is treated when 'SSL Intercept Interface(s)' is set. Default: Splice Whitelist, Bump Otherwise. [Click Info for details.](#)

SSL Intercept Interface(s)

WAN
LAN
DMZ

The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.

SSL Proxy Port

This is the port the proxy server will listen on to intercept SSL while using SSL interception.

SSL Proxy Compatibility Mode Modern

The compatibility mode determines which cipher suites and TLS versions are supported.

DHPParams Key Size 2048 (default)

DH parameters are used for temporary/ephemeral DH key exchanges and DH key generation.

CA **squid certificat**

Select Certificate Authority to use when SSL interception is enabled.

Pour active SSL Filtering

Cette configuration convient si vous souhaitez utiliser le package SquidGuard pour le filtrage Web.

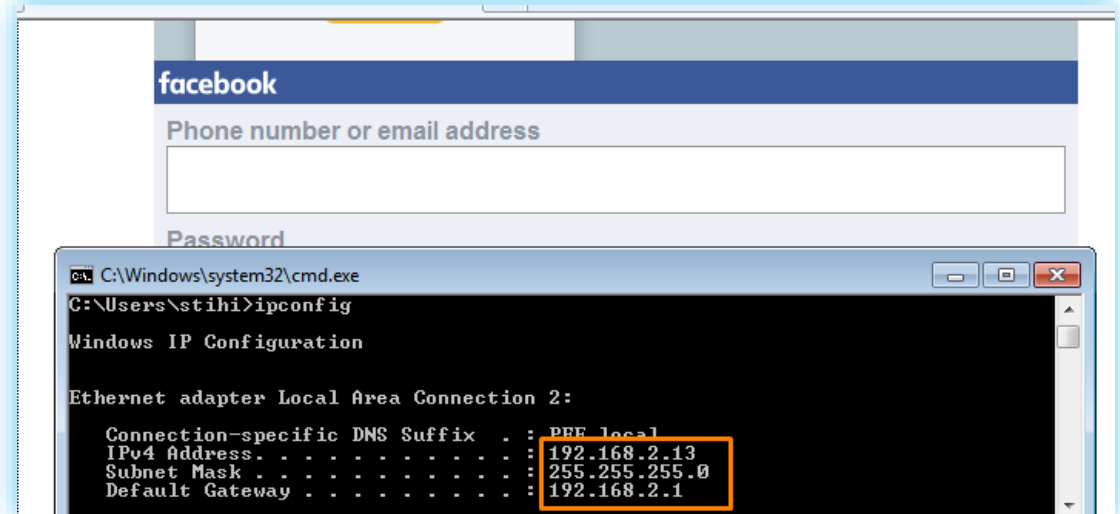
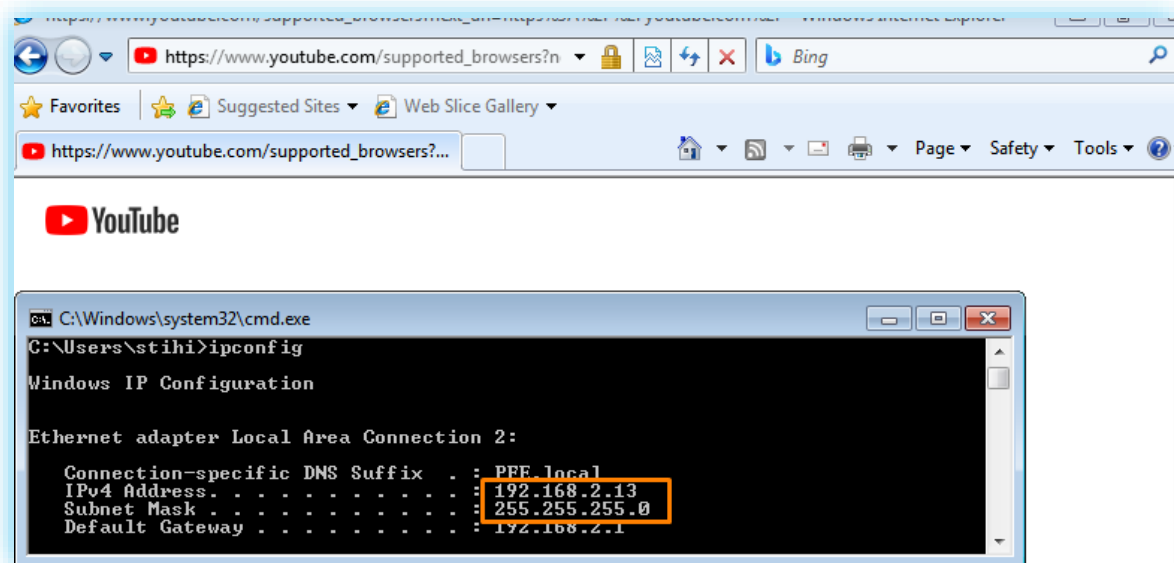
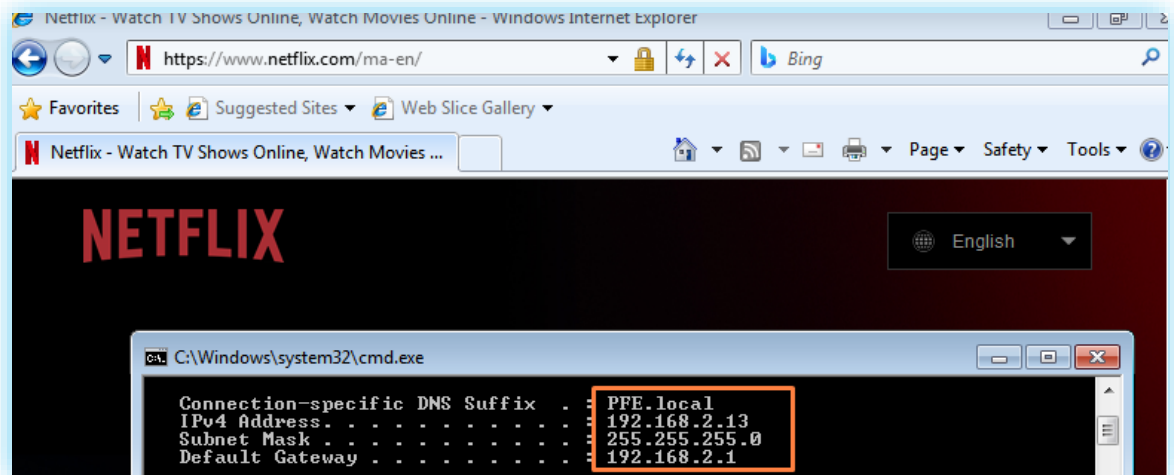
Toutes les destinations seront épissées. SquidGuard peut faire son travail en refusant ou en autorisant les destinations selon ses règles, comme il le fait avec HTTP.

Vous n'avez pas besoin d'installer le certificat CA configuré ci-dessous sur les clients

Le certificat ce qu'on a crée

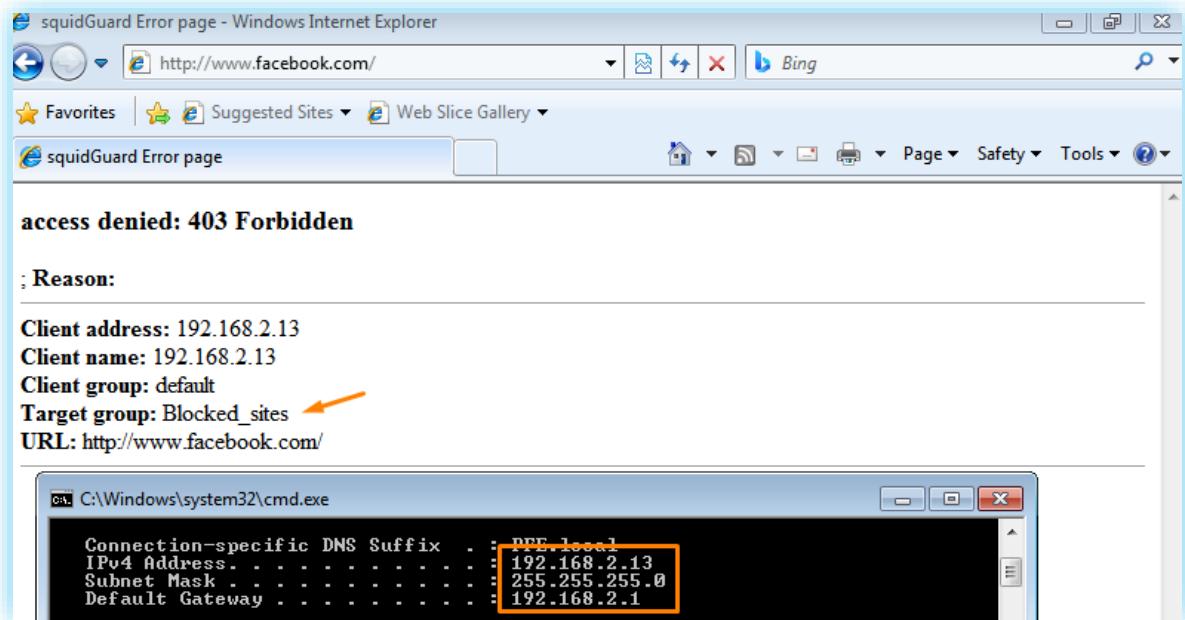
Teste de configuration de serveur proxy :

➤ Avant l'activation de proxy :



➤ Après l'activation de proxy :

HTTP :



HTTPS :

