
Projet SISR5-4 : Pare-feu et VPN.

VEYNAND SAINT FIACRE Lucille

16/03/2021



Table des matières

1	Introduction	2
2	Contexte de travail et gestion des configurations	2
3	Gestion du travail en équipe et gestion du projet	2
4	Activités compétences du référentiel du BTSSIO	2
5	(reseaucerta.org)	2
6	La documentation.	2
7	Le Maquettage	2
8	Incident problème et assistance	2
9	Formation, autoformation et veille technologique.	2
10	Test et vérification	2



1 Introduction

Comment mettre en place un pare-feu logiciel ainsi qu'un VPN.

2 Contexte de travail et gestion des configurations

Voir contexte.doc

3 Gestion du travail en équipe et gestion du projet

	Date	Activité
VEYNAND SAINT FIACRE Lucille	16/03/2021	-Introduction -Étape 1 à 4 étape 2 (problème de proxy)
	22/03/2021	-Beaucoup de difficulté à faire l'étape 4-5-6 -Le travail est maintenant centralisé sur la VM du P14 car il faut la centraliser
	23/03/2021	

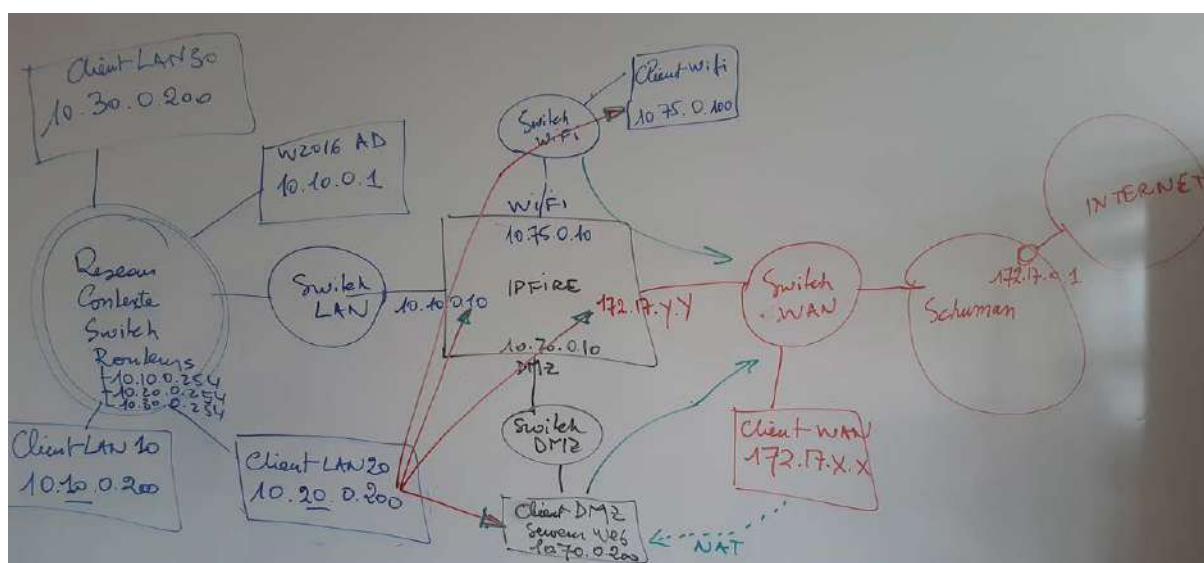
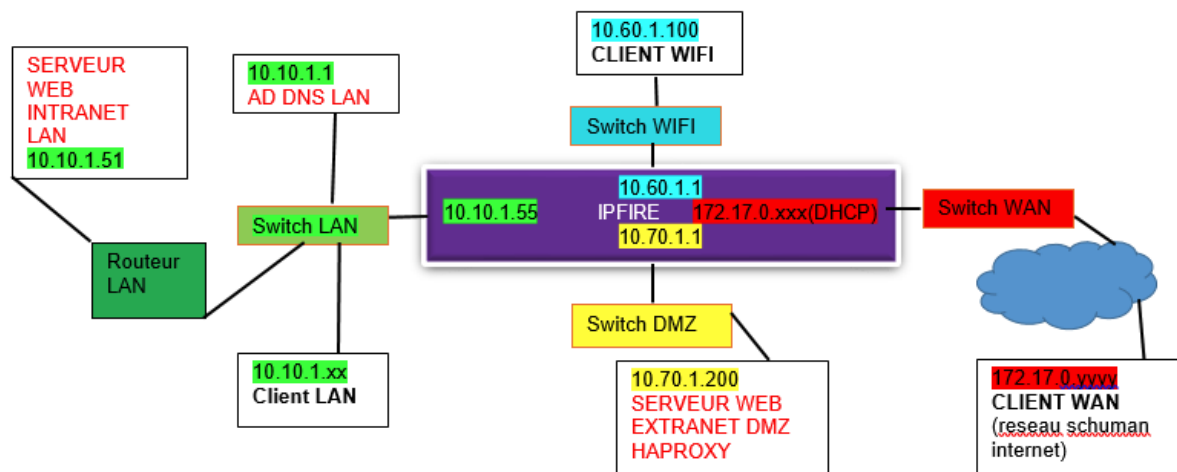
4 Activités compétences du référentiel du BTSSIO (reseaucerta.org)

A1.1.2 , Étude de l'impact de l'intégration d'un service sur le système informatique
A1.1.3 , Étude des exigences liées à la qualité attendue d'un service
A1.2.4 , Détermination des tests nécessaires à la validation d'un service
A1.3.1 , Test d'intégration et d'acceptation d'un service
A1.3.3 , Accompagnement de la mise en place d'un nouveau service
A1.3.4 , Déploiement d'un service
A1.4.1 , Participation à un projet
A1.4.2 , Évaluation des indicateurs de suivi d'un projet et justification des écarts
A2.2.1 , Suivi et résolution d'incidents
A3.1.2 , Maquettage et prototypage d'une solution d'infrastructure
A3.1.3 , Prise en compte du niveau de sécurité nécessaire à une infrastructure
A3.3.1 , Administration sur site ou à distance des éléments d'un réseau, de serveurs, ...
A5.2.2 , Veille technologique
A5.2.3 , Repérage des compléments de formation ou d'auto-formation ...
A5.2.4 , Étude d'une technologie, d'un composant, d'un outil ou d'une méthode

5 La documentation.

<https://wiki.ipfire.org/configuration/network/dnsforward>

6 Le Maquettage



7 Incident problème et assistance

Des problèmes avec le forward de DNS, résolu avec: <https://wiki.ipfire.org/configuration/network/dnsforward>



<https://www.ipfire.org/>
[http://reseaux85.fr/index.php?title=IPFire - Firewall/Proxy/Filtrage/Addons](http://reseaux85.fr/index.php?title=IPFire_-_Firewall/Proxy/Filtrage/Addons)
<https://drive.google.com/file/d/0BwtfbS0twOeXaDFWay1xbUdCd00/view>
<https://wiki.ipfire.org/start>
<https://www.commentcamarche.net/contents/992-firewall-pare-feu>
http://cerig.pagora.grenoble-inp.fr/Note/1999/Proxy_26-07-99.htm
https://www.memoireonline.com/07/11/4611/m_Mise-en-place-dun-proxy-Squid-securise-avec-authentification-LDAP3.html

Définir un pare-feu ?

Un pare-feu est un appareil de protection du réseau qui surveille le trafic entrant et sortant et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies.

IPFire : Type de logiciel ? OS ? Licence ?

IPFire est une distribution Linux, il suit une license libre, la GPL,

Fonctionnalité d'IPFire ?

IPFire a diverses fonctionnalités:

- Gestion de paquets : système léger pour un pare-feux, et modulable, il peut être mise à jour rapidement
- Parefeux
- Intrusion Detection System (Snort) de prévention des intrusions
- Serveur proxy avec filtrage de contenu et les fonctions de mise en cache des mises à jour (par exemple mises à jour Microsoft Windows, antivirus, et bien d'autres)
- Mise en cache
- Serveur de temps
- WOL (Wake up on LAN)
- VPN pour IPSec et serveur OpenVPN
- Serveur DHCP
- Dynamic DNS (DynDNS, No-IP)
- Analyse fonctions de surveillance du système et analyse des logs
- Qualité de service (QoS)



Définition de la sécurité garantie par IPFire ?

L'objectif principal d'IPFire est la sécurité. Son moteur de pare-feu et son système de détection d'intrusion, faciles à configurer, empêchent tout attaquant de pénétrer dans votre réseau. Dans la configuration par défaut, le réseau est divisé en différentes zones avec différentes stratégies de sécurité, telles qu'un réseau local et une zone démilitarisée, pour gérer les risques sur le réseau et disposer d'une configuration personnalisée pour les besoins spécifiques de chaque segment du réseau.

Mais même le pare-feu doit se protéger. IPFire est construit à partir de zéro et n'est basé sur aucune autre distribution. Cela permet aux développeurs de renforcer IPFire mieux que tout autre système d'exploitation serveur et de construire tous les composants spécifiquement pour une utilisation en tant que pare-feu.

Les mises à jour fréquentes maintiennent IPFire fort contre les vulnérabilités de sécurité et les nouveaux vecteurs d'attaque.

Quel type de pare-feu est IPFire ?

C'est un pare-feux logiciel cela veut dire qu'il n'est pas installé sur un matériel d'infrastructure dédié au pare-feux



Qu'est-ce que le système de détection et de prévention des intrusions

L'Intrusion Detection System est un système analysant le trafic réseau et détecte les exploits, s'il y a détection, des alertes sont faites et l'attaqueur est immédiatement bloqué

Comment utiliser un VPN avec IPFire ?

Il est utilisé en concordance avec OpenVPN ou IPSec.

Pour IPSec: <https://wiki.ipfire.org/configuration/services/ipsec>

Pour OpenVPN: <https://wiki.ipfire.org/configuration/services/openvpn/config>

Définir le filtrage simple de paquets

Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangée entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall:

- adresse IP de la machine émettrice ;
- adresse IP de la machine réceptrice ;
- type de paquet (TCP, UDP, etc.) ;
- numéro de port (rappel: un port est un numéro associé à un service ou une application réseau).

-Tout ce qui n'est pas explicitement interdit est autorisé

-Tout ce qui n'est pas explicitement autorisé est interdit

Définir le filtrage dynamique

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP

Pour remédier à l'absence d'autorisation des ports on se sert d'un système « stateful inspection » c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du pare-feu; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

Définir le filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application.

Il permet, comme son nom l'indique, de filtrer les communications application par application. Le filtrage applicatif suppose donc une bonne connaissance des applications présentes sur le réseau

Qu'est-ce qu'un serveur proxy

Un serveur proxy est un ordinateur connecté à Internet et dont votre ordinateur connaît l'adresse IP unique.

Lorsque vous envoyez une requête Web, celle-ci est d'abord dirigée vers le serveur proxy



Partie 1 : INSTALLATION de l'IPFire
--

Préparer votre machine virtuelle avec 4 cartes réseau (LAN, WAN, DMZ, WIFI).

Télécharger iso IPFire 2.15

Lancer l'installation de IPFire à partir de l'iso (IPFire 2.15).



Choisir la langue pour utiliser IPfire.

Lire et accepter la licence.

Préparer le disque dur pour être partitionner en autorisant la suppression des données du disque et l'installation des systèmes de fichiers.

Choisir le système de fichier "ext4". Le disque va ensuite être partitionné et redémarré.

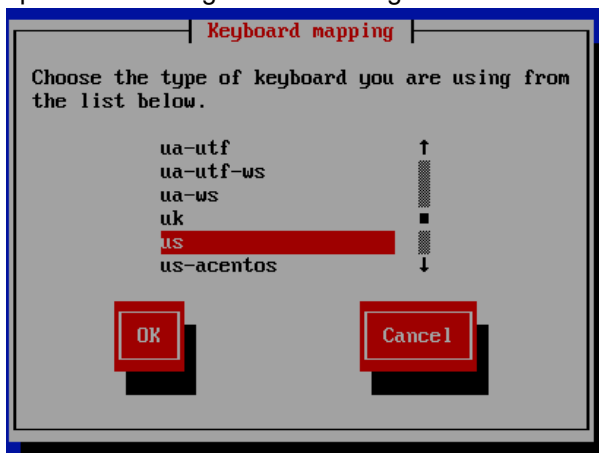
Appuyer sur OK pour redémarrer.



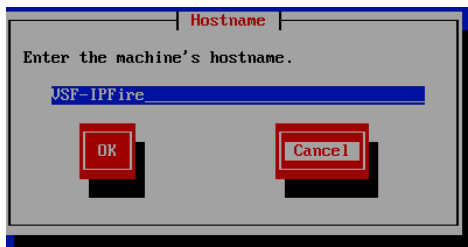
Partie 2 : Paramétrage d'IPFire



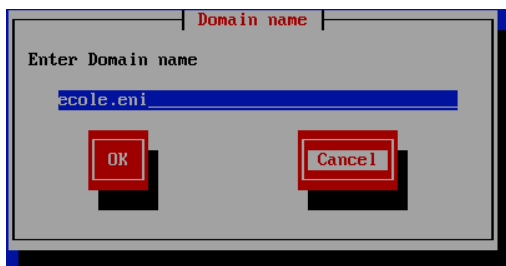
Après redémarrage choisir la langue du clavier et le fuseau horaire.



Donner le nom d'hôte de notre IPFire.



Rentrer le nom de domaine.



Saisir les mots de passe pour l'utilisateur "root" et pour l'administrateur "admin"
le mdp de root est root et d'amin azerty
Mot de passe : azerty

Configurer le réseau.



Assigned Cards

Please choose the interface you wish to change.

```

GREEN : "umbus: hv_netusc"
GREEN : (00:15:5d:1f:44:49)
RED   : "umbus: hv_netusc"
RED   : (00:15:5d:1f:44:4a)
ORANGE: "umbus: hv_netusc"
ORANGE: (00:15:5d:1f:44:4b)
BLUE  : "umbus: hv_netusc"
BLUE  : (00:15:5d:1f:44:4c)
    
```

GREEN
RED
ORANGE
BLUE

Select Remove Done

Interface - RED

Enter the IP address information for the RED interface.

☐ Static
☒ DHCP
☐ PPP DIALUP (PPPoE, modem, ATM ...)

DHCP Hostname: JSF-IPFire
Force DHCP MTU:

IP address:
Network mask: 255.255.255.0
Gateway:

OK Cancel

Interface - GREEN

Enter the IP address information for the GREEN interface.

IP address: 10.10.1.55
Network mask: 255.255.255.0

OK Cancel

Interface - BLUE

Enter the IP address information for the BLUE interface.

IP address: 10.60.1.55
Network mask: 255.255.255.0

OK Cancel

Interface - ORANGE

Enter the IP address information for the ORANGE interface.

IP address: 10.70.1.55
Network mask: 255.255.255.0

OK Cancel

DHCP server configuration

Configure the DHCP server by entering the settings information.

☒ Enabled

Start address:
End address:
Primary DNS: 10.10.1.55
Secondary DNS:
Default lease (mins): 60
Max lease (mins): 120
Domain name suffix: ecole.eni

OK Cancel

Attribuer une adresse IP (10.10.1.55/24 par exemple) à l'interface GREEN (LAN)
Configurer l'interface RED en DHCP (WAN).
Attribuer une adresse IP (10.70.1.55/24 par exemple) à l'interface ORANGE (DMZ).
Attribuer une adresse IP (10.75.1.55/24 par exemple) à l'interface BLUE (WIFI).

Paramétrer le DNS ainsi que la passerelle.
Terminer l'installation



Partie 3 : Test de connexion

Redémarrage d'IPfire.

```
bringing up the blue0 interface...
adding IPv4 address 10.75.0.1 to the blue0 interface... [ OK ]
bringing up the orange0 interface...
adding IPv4 address 10.70.0.1 to the orange0 interface... [ OK ]
bringing up the red0 interface...
starting dhcpd on the red0 interface... [ OK ]
DHCP Assigned Settings for red0:
  IP Address: 192.168.168.46
  Hostname: lhipfire
  Subnet Mask: 255.255.255.0
  Default Gateway: 192.168.168.254
  DNS Server: 192.168.168.254 00.67.169.12 00.67.169.40
Starting the Cyrus SASL Server... [ OK ]
initializing kernel random number generator... [ OK ]
Setting time on boot... [ OK ]
Starting ntpd... [ OK ]
Loading Sensor Modules: [ OK ]
Starting Collection daemon... [ OK ]
Starting Apache daemon... [ OK ]
Starting fcron... [ OK ]

IPFire v2.15 - www.ipfire.org
=====
IPFire running on Linux 3.10.44-ipfire 1686
IPFire login:
```

Connexion avec root

```
IPFire v2.25 - www.ipfire.org
=====
USF-IPFire.ecole.eni running on Linux 4.14.212-ipfire x86_64
USF-IPFire login: root
Password:
No mail.
[root@USF-IPFire ~]# _
```

Vérifier les configurations IP, MAC de chaque interface.

```
[root@USF-IPFire ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: green0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:15:5d:1f:44:49 brd ff:ff:ff:ff:ff:ff
    inet 10.10.1.55/24 scope global green0
        valid_lft forever preferred_lft forever
3: red0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:15:5d:1f:44:4a brd ff:ff:ff:ff:ff:ff
    inet 172.17.32.144/16 brd 172.17.255.255 scope global dynamic noprefixroute red0
        valid_lft 86145sec preferred_lft 75345sec
4: orange0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:15:5d:1f:44:4b brd ff:ff:ff:ff:ff:ff
    inet 10.70.1.55/24 scope global orange0
        valid_lft forever preferred_lft forever
5: blue0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:15:5d:1f:44:4c brd ff:ff:ff:ff:ff:ff
    inet 10.60.1.55/24 scope global blue0
        valid_lft forever preferred_lft forever
[root@USF-IPFire ~]# _
```

Configuration du client : vérifier son adressage IP. Et tester la communication entre le client et IPFire.

```
C:\Users\SIO1>ping 10.10.1.55

Envoi d'une requête 'Ping' 10.10.1.55 avec 32 octets de données :
Réponse de 10.10.1.55 : octets=32 temps<1ms TTL=64
```

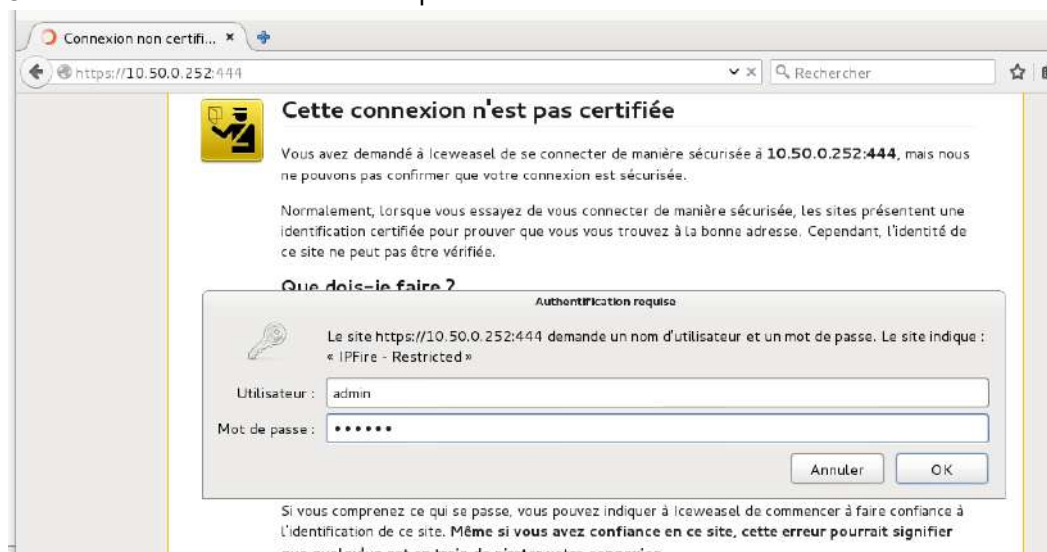
Vérifier la configuration du serveur proxy pour accéder à internet sur le navigateur du client.

Pour nous connecter sur le navigateur, il faut bien penser à désactiver le proxy (ou il faut le mettre dans les exceptions).

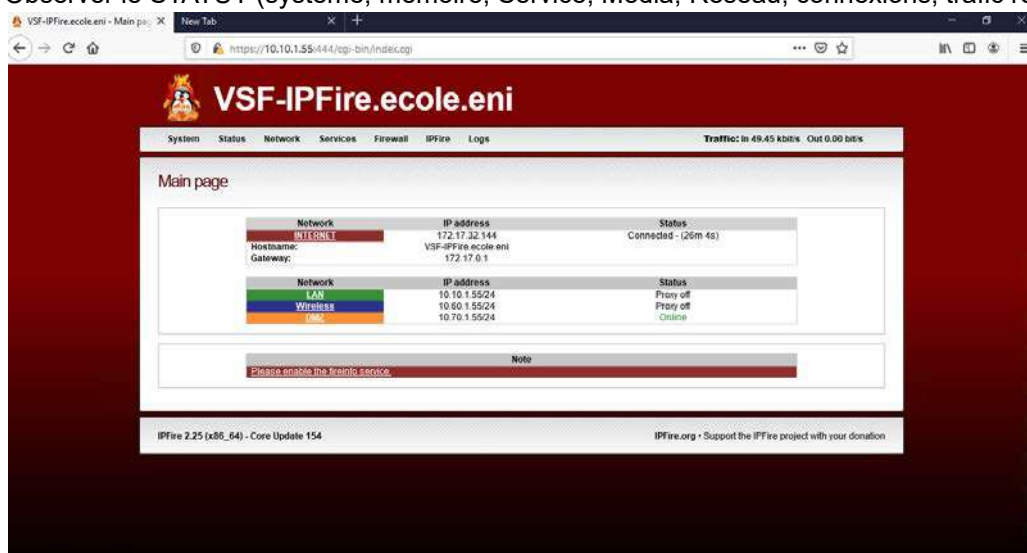
On se connecte avec l'adresse de IPfire <https://10.10.1.55:444>. Et accepter le certificat SSL.



Connexion sécurisée à distance à IPFire avec admin.



Vérifier la bonne configuration des interfaces sur la page principale de l'interface graphique d'IPFire. Observer le STATUT (système, mémoire, Service, Média, Réseau, connexions, trafic réseau)





Partie 4 : **Configuration d'IP FIRE**

Étape 1 : Joindre le domaine ecole.eni

Afin d'ajouter la machine IPFire au domaine, il faut configurer le **DNS Forwarding** en ajoutant l'entrée correspondant à la zone DNS **ecole.eni** avec l'adresse IP du serveur.

Afin que la redirection fonctionne, il a fallu suivre ces étapes:

<https://wiki.ipfire.org/configuration/network/dhcp>

Pour tester le **DNS Forwarding** il faut que **NSLOOKUP** sur le serveur IPFire de ecole.eni renvoie l'IP du serveur DNS du contexte.

```
[root@VSF-IPFire ~]# nslookup slam.ecole.eni
Server:      127.0.0.1
Address:     127.0.0.1#53

Non-authoritative answer:
Name:   slam.ecole.eni
Address: 10.10.1.51

[root@VSF-IPFire ~]#
```

Étape 2 : Fonction PROXY

Une fois IPFire dans le domaine et donc les zones directes et indirectes de la zone DNS, le proxy web sans authentification AD/LDAP peut être configuré dans Réseau/Webproxy.

Dans Paramètres communs, cocher **Actif sur Green** et choisir le port 800.

Configurer le proxy avec les identifiants pour accéder à internet.



Advanced Web Proxy

Common settings

Enabled on Green :	<input checked="" type="checkbox"/>	Proxy port: *	<input type="text" value="800"/>
Transparent on Green :	<input checked="" type="checkbox"/>	Transparent port: *	<input type="text" value="3128"/>
Enabled on Blue :	<input type="checkbox"/>	Visible hostname:	<input type="text"/>
Transparent on Blue :	<input type="checkbox"/>	Error messages language:	<input type="text" value="en"/>
Suppress version information:	<input type="checkbox"/>	Error messages design:	<input type="text" value="IPFire"/>
Squid cache version:	[4.13]		

URL filter

Enabled ☒

Update accelerator

Enabled ☐

Upstream proxy

Proxy address forwarding:	<input checked="" type="checkbox"/>	Upstream proxy (host:port):	<input type="text" value="172.17.0.1:3128"/>
Client IP address forwarding:	<input type="checkbox"/>	Upstream username:	<input type="text"/>
Username forwarding:	<input type="checkbox"/>	Upstream password:	<input type="text"/>
No connection oriented authentication forwarding:	<input type="checkbox"/>		

Les settings

Gestion du cache

Activer le gestionnaire de cache:	<input checked="" type="checkbox"/>	Cache e-mail administrateur: *	<input type="text"/>
Nombre de descripteurs de fichier:	<input type="text" value="16384"/>	Mot de passe administrateur du Cache: *	<input type="text"/>
Taille cache mémoire (MB):	<input type="text" value="2"/>	Taille du cache disque dur (MB):	<input type="text" value="50"/>
Volume d'objet minimal (KB):	<input type="text" value="0"/>	Volume d'objet maximal (KB):	<input type="text" value="4096"/>
Nombre de sous-dossier level-1:	<input type="text" value="16"/>	Ne pas mettre en cache ces domaines (un par ligne): *	<div></div>
Politique de remplacement de mémoire:	<input type="text" value="LRU"/>		
Politique du Cache de remplacement:	<input type="text" value="LRU"/>		
Autoriser mode hors connexion:	<input type="checkbox"/>		
Enable Cache-Digest Generation:	<input type="checkbox"/>		



Destination ports

Allowed standard ports (one per line): *

80 # http
21 # ftp
443 # https
563 # snews
70 # gopher
210 # wais
1025-65535 # unregistered ports

Allowed SSL ports (one per line): *

443 # https
563 # snews

Network based access control

Allowed subnets (one per line): *

10.10.1.0/24
10.60.1.0/24

Disable internal proxy access to **Green** ☐
from other subnets:
Disable internal proxy access from **Blue** ☐
to other subnets:

Unrestricted IP addresses (one per line):

Unrestricted MAC addresses (one per line):

Banned IP addresses (one per line):

Banned MAC addresses (one per line):

Classroom extensions Enabled: ☐

Web Proxy Auto-Discovery Protocol (WPAD) / Proxy Auto-Config (PAC)

Excluded IP Subnets (one per line):

e.g. 192.168.2.0/255.255.255.0

Excluded URL s (one per line):

e.g. *.ipfire.org*

Open PAC File: <http://10.10.1.55:81/wpad.dat>

Notice: For WPAD/PAC to work properly, further changes need to be made. Please see the [Wiki](#).

Time restrictions

Access MonTueWedThuFriSatSun From To
allow ☒ ☒ ☒ ☒ ☒ ☒ ☒ 00:00 24:00

Transfer limits

Max download size (KB): * 0 Max upload size (KB): * 0

Download throttling

Overall limit on **Green**: unlimited
Overall limit on **Blue**: unlimited
Limit per host on **Green**: unlimited
Limit per host on **Blue**: unlimited

MIME type filter Enabled: ☐

Privacy

Fake useragent submitted to external sites:

Fake referer submitted to external sites:

Authentication method

☒ None ☐ Local ☐ identd ☐ LDAP ☐ RADIUS

Save

Save and Reload

Save and Restart

Clear Cache

Tester si un client du réseau LAN accède à internet (WAN) à travers IPFire. (Vérifier la configuration du proxy dans le navigateur du client).

Configuration client :



Propriétés de : Protocole Internet version 4 (TCP/IPv4)

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP :

Masque de sous-réseau :

Passerelle par défaut :

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :

Serveur DNS auxiliaire :

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

Configuration du proxy

Paramètres du réseau local

Configuration automatique

La configuration automatique peut annuler les paramètres manuels. Pour garantir leur utilisation, désactivez la configuration automatique.

☒ Détecter automatiquement les paramètres de connexion

☐ Utiliser un script de configuration automatique

Adresse :

Serveur proxy

☒ Utiliser un serveur proxy pour votre réseau local (ces paramètres ne s'appliquent pas aux connexions d'accès à distance ou VPN).

Adresse : Port :

Avancé

☒ Ne pas utiliser de serveur proxy pour les adresses locales

OK Annuler



Bienvenu dans le site des Lekbouri



Étape 3 : Configuration du filtrage URL

Définir les éléments à filtrer :



URL filter configuration

URL filter settings

Block categories

ads: <input type="checkbox"/>	aggressive: <input type="checkbox"/>	audio-video: <input type="checkbox"/>	drugs: <input type="checkbox"/>
gambling: <input type="checkbox"/>	hacking: <input type="checkbox"/>	mail: <input type="checkbox"/>	porn: <input type="checkbox"/>
proxy: <input type="checkbox"/>	violence: <input type="checkbox"/>	warez: <input type="checkbox"/>	

Custom blacklist

Blocked domains (one per line)

Example: www.domain.com

https://www.youtube.com/

Enable custom blacklist



Blocked URLs (one per line)

Example: www.domain.com/ads/

Custom whitelist

Allowed domains (one per line)

Example: www.domain.com

https://www.metz.fr

Enable custom whitelist



Allowed URLs (one per line)

Example: www.domain.com/ads/

Custom expression list

Blocked expressions (as regular expressions)

video

Enable custom expression list



File extension blocking

Block executable files:



Block audio/video files:



Block compressed archive files:



Local file redirection

Enable local file redirection:



[Manage repository](#)

Network based access control

Unfiltered IP addresses

10.10.1.55

Banned IP addresses

10.10.1.51

Time based access control

[Set time constraints](#)

[Set user quota](#)

Block page settings

Redirect page template

legacy ▾

Show category on block page:



Redirect to this URL:

Show URL on block page:



Message line 1:

Show IP on block page:



Message line 2:

Use "DNS error" to block URLs:



Message line 3:

Advanced settings



Enable expression lists:	<input type="checkbox"/>	Enable log:	<input type="checkbox"/>
Block "ads" with empty window:	<input type="checkbox"/>	Log username:	<input type="checkbox"/>
Block sites accessed by it's IP address:	<input type="checkbox"/>	Split log by categories:	<input type="checkbox"/>
Block all URLs not explicitly allowed:	<input type="checkbox"/>	Allow custom whitelist for banned clients:	<input type="checkbox"/>

* Required field

Save

Save and Restart

URL filter maintenance

Blacklist update

The new blacklist will be automatically compiled to prebuilt databases. Depending on the size of the blacklist, this may take several minutes. Please wait for this task to be finished before restarting the URL filter.

To install an updated blacklist upload the .tar.gz file below:

Browse... No file selected.

Upload blacklist

Automatic blacklist update

Enable automatic update: ☐

Automatic update schedule: monthly ▾

Select download source: Shalla Secure Services ▾

Custom source URL:

Save update settings

Update now

Blacklist editor

Create and edit your own blacklist files

Blacklist editor

Backup URL filter settings

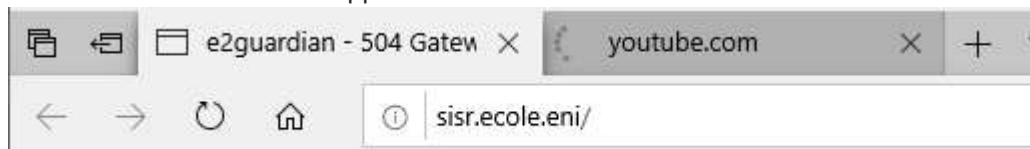
Include complete blacklist: ☐

Create backup file

Restore URL filter settings

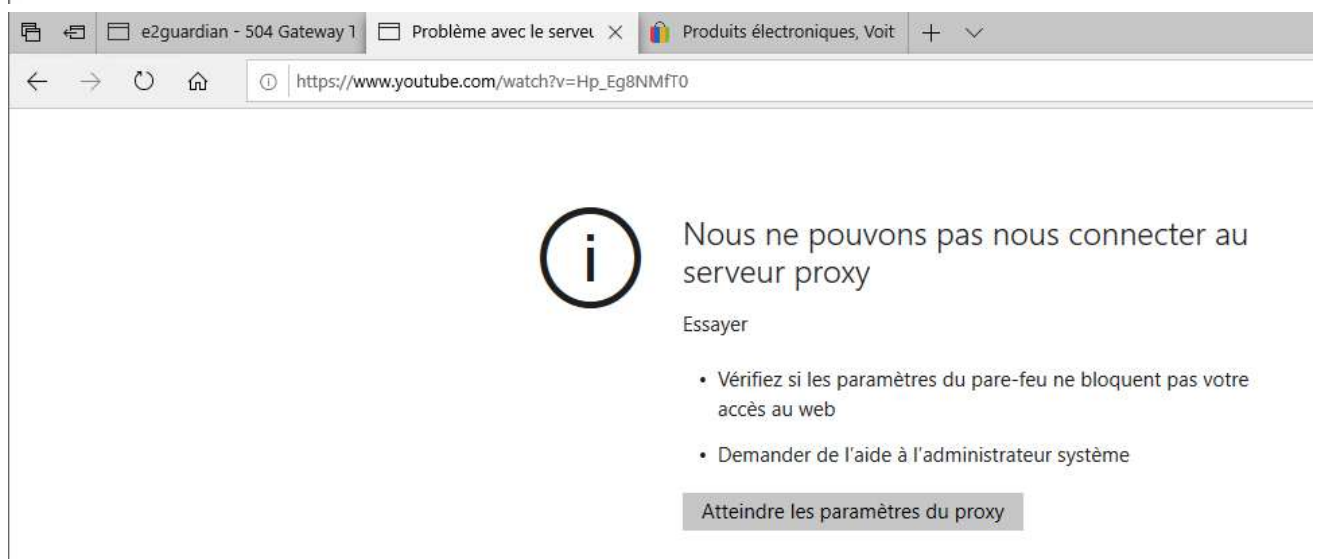
To restore a previously saved configuration upload the .tar.gz backup file below:

Valider le filtre et tester son application.



e2guardian - 504 Gateway Time-out

Unable to get response from upstream proxy (timeout)





ça ne sera pas possible !!!!

Access to the requested page has been denied

URL: <http://www.google.com/url?sa=1>

Please contact the Network Administrator if you think there has been an error

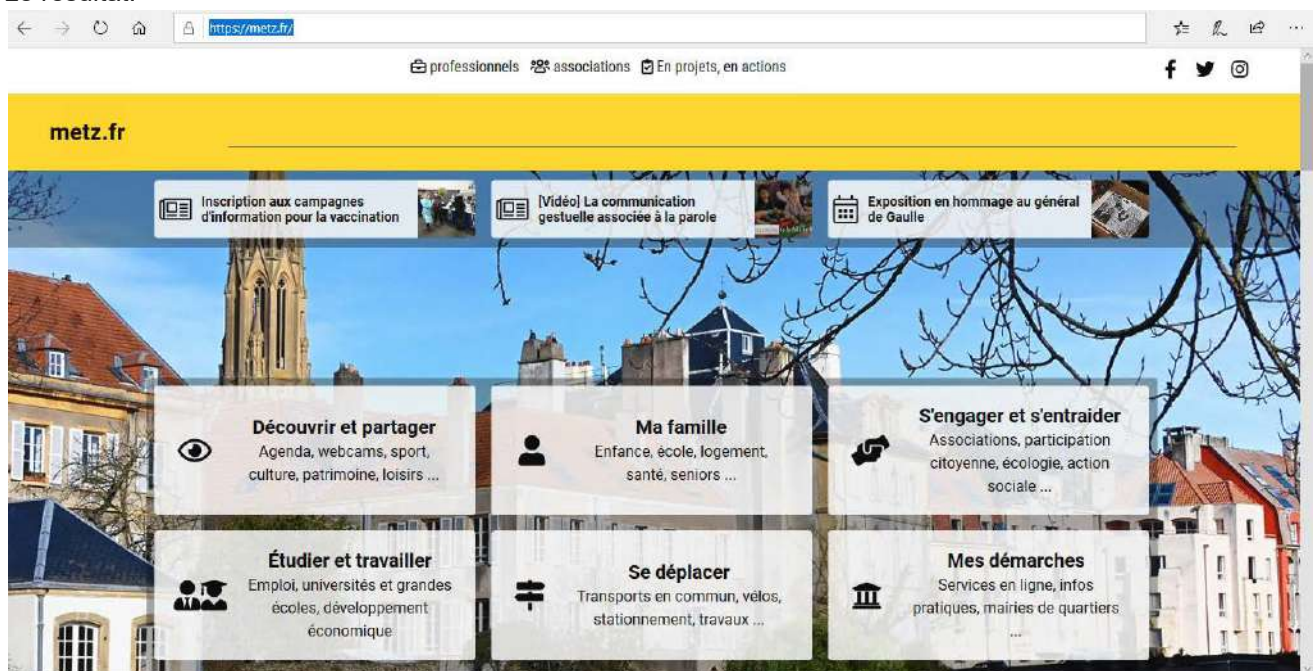
EXERCICE :

Filtrer ou interdire l'accès (totalement ou partiellement à des plages horaires) à des utilisateurs suivant leurs identification ou adresse IP ou adresse MAC.

La procédure

Unrestricted IP addresses (one per line): <input type="text" value="10.10.1.13"/>	Unrestricted MAC addresses (one per line): <input type="text"/>
Banned IP addresses (one per line): <input type="text"/>	Banned MAC addresses (one per line): <input type="text"/>
Classroom extensions Enabled: <input type="checkbox"/>	
Web Proxy Auto-Discovery Protocol (WPAD) / Proxy Auto-Config (PAC)	
Excluded IP Subnets (one per line): <input type="text"/> <p>e.g. 192.168.2.0/255.255.255.0</p>	Excluded URL s (one per line): <input type="text"/> <p>e.g. *.ipfire.org*</p>
Open PAC File: http://10.10.1.55:81/wpad.dat	
Notice: For WPAD/PAC to work properly, further changes need to be made. Please see the Wiki .	
Time restrictions Access Mon Tue Wed Thu Fri Sat Sun From To <input type="button" value="deny"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> 00 : 00 24 : 00	

Le résultat:





La procédure

Network based access control

Allowed subnets (one per line): *

10.10.1.0/24
10.60.1.0/24

Disable internal proxy access to Green ☐
from other subnets:
Disable internal proxy access from Blue ☐
to other subnets:

Unrestricted IP addresses (one per line):

Unrestricted MAC addresses (one per line):

Banned IP addresses (one per line):

10.10.1.13

Banned MAC addresses (one per line):

Classroom extensions Enabled: ☐

Web Proxy Auto-Discovery Protocol (WPAD) / Proxy Auto-Config (PAC)

Excluded IP Subnets (one per line):

e.g. 192.168.2.0/255.255.255.0

Excluded URL s (one per line):

e.g. *.ipfire.org*

Open PAC File: <http://10.10.1.55.81/wpad.dat>

Notice: For WPAD/PAC to work properly, further changes need to be made. Please see the [Wiki](#).

Time restrictions

Access Mon Tue Wed Thu Fri Sat Sun From To
allow ☒ ☒ ☒ ☒ ☒ ☒ ☒ 00 00 24 00

Le résultat:



ERROR: The requested URL
Problème avec le serveur pr
Nous ne pouvons pas atteindre
ERROR: The requested l

metz.fr/



ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: <http://metz.fr/>

Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is [webmaster](#).

Generated Mon, 22 Mar 2021 08:50:27 GMT by VSF-IPFire.ecole.eni (squid/4.13)

ERROR: The requested l
Nous ne pouvons pas atteindre
Nous ne pouvons pas atteindre
ERROR: The requested URL

sir.ecole.eni/



ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: <http://sir.ecole.eni/>

Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is [webmaster](#).

Generated Mon, 22 Mar 2021 08:51:11 GMT by VSF-IPFire.ecole.eni (squid/4.13)

On a mit à la fin:

Network based access control

Allowed subnets (one per line): *

10.10.1.0/24
10.60.1.0/24

Unrestricted IP addresses (one per line):
10.10.1.13

Banned IP addresses (one per line):

Classroom extensions Enabled ☐

Web Proxy Auto-Discovery Protocol (WPAD) / Proxy Auto-Config (PAC)

Excluded IP Subnets (one per line):

e.g. 192.168.2.0/255.255.255.0

Open PAC File: <http://10.10.1.55:81/wpad.dat>

Notice: For WPAD/PAC to work properly, further changes need to be made. Please see the [Wiki](#).

Time restrictions

Access: Mon Tue Wed Thu Fri Sat Sun From To

allow ☒ ☒ ☒ ☒ ☒ ☐ ☐ 00:00 24:00

Disable internal proxy access to Green ☐
from other subnets:
Disable internal proxy access from Blue ☐
to other subnets:

Unrestricted MAC addresses (one per line):

Banned MAC addresses (one per line):

Excluded URL s (one per line):

e.g. *.ipfire.org*



Étape 4 : Authentification Locale.

Pour mettre en place un proxy qui permet l'authentification des utilisateurs :
Il faut d'abord que la case « transparent » ne soit pas cochée :

Advanced Web Proxy

Common settings

Enabled on **Green**: ☒

Transparent on **Green**: ☐

Enabled on **Blue**: ☒

Transparent on **Blue**: ☐

Suppress version information: ☐

Squid cache version: [4.13]

Proxy port: *

Transparent port: *

Visible hostname:

Error messages language:

Error messages design:

URL filter

Enabled ☒

Update accelerator

Enabled ☐

Ensuite, dans la partie « Méthode d'authentification », il faut cocher « local », puis sauvegarder :

Méthode d'Authentification

☐ Rien
 ☒ Local
 ☐ identd
 ☐ LDAP
 ☐ Windows
 ☐ RADIUS

Paramètres d'authentification Global

Nombre de processus d'authentification:

Cache d'Authentification TTL (en minutes):

Limite d'adresses IP par utilisateur: *

Cache utilisateur/IP TTL (en minutes):

Exige l'authentification pour un accès sans restriction des adresses sources: ☒

Authentification du royaume invité: *

Domaines sans authentification (un par ligne): *

Authentification des utilisateurs locaux

Longueur minimale du mot de passe:

Redirection par contournement pour les membres du groupe 'Etendu': ☐

[Gestion des utilisateurs](#)

[Sauvegarder](#)
[Sauver et Recharger](#)
[Sauver et redémarrer](#)
[Effacer le Cache](#)

* Ce champ peut être vide.

En local, il faut ajouter un utilisateur local :



Transfer limits

Max download size (KB): * Max upload size (KB): *

Download throttling

Overall limit on Green: Limit per host on Green:

Overall limit on Blue: Limit per host on Blue:

MIME type filter Enabled: ☐

Privacy

Fake useragent submitted to external sites: Fake referer submitted to external sites:

Authentication method

☐ None ☒ Local ☐ identd ☐ LDAP ☐ RADIUS

Global authentication settings

Number of authentication processes: Authentication realm prompt:

Authentication cache TTL (in minutes): Domains without authentication (one per line):

Limit of IP addresses per user: User/IP cache TTL (in minutes):

Require authentication for unrestricted source addresses: ☒

Local user authentication

Minimum password length: Bypass redirection for members of the group 'Extended': ☐

User management

LHipfire.ecole.eni

Système Statut Réseau Services Pare-Feu IPFire Rapports Traffic: In 340.15 Bit/s Out 340.15 Bit/s

Configuration avancée du proxy Web

Authentification des utilisateurs locaux

Gestion des utilisateurs

Nom utilisateur: Groupe:

Mot de passe: Mot de passe (confirmez):

Comptes utilisateurs:

Aucun compte utilisateur disponible

IPFire 2.15 (i586) - Core Update 79 IPFire.org • Support the IPFire project with your donation

LHipfire.ecole.eni

Système Statut Réseau Services Pare-Feu IPFire Rapports Traffic: In 171.26 Bit/s Out 0.00 Bit/s

Configuration avancée du proxy Web

Authentification des utilisateurs locaux

Gestion des utilisateurs

Nom utilisateur: Groupe:

Mot de passe: Mot de passe (confirmez):

Comptes utilisateurs:

Nom utilisateur	Appartenance au groupe	
slor	Standard	<input type="button" value="Éditer"/> <input type="button" value="Enlever"/>

Légende:

IPFire 2.15 (i586) - Core Update 79 IPFire.org • Support the IPFire project with your donation



Advanced web proxy configuration

Local user authentication

User management

Username: Group:

Password: Password (confirm):

User accounts:

Username	Group membership		
administrateur	Extended		
utilisateur	Standard		

Legend: Edit Remove

Cette fois-ci, il faut entrer le proxy dans le navigateur. Soit il faut le faire en local, soit il faut créer une GPO pour tous mes utilisateurs.

Tester l'authentification local d'un client.

Authentication Required - Mozilla Firefox

The proxy moz-proxy://10.10.1.55:800 is requesting a username and password. The site says: "IPFire Advanced Proxy Server"

User Name:

Password:

☐ Use Password Manager to remember this password.

Authentication Required - Mozilla Firefox

The proxy moz-proxy://10.10.1.55:800 is requesting a username and password. The site says: "IPFire Advanced Proxy Server"

User Name:

Password:

☐ Use Password Manager to remember this password.

Étape 5 : Méthode d'Authentification LDAP

Il reste à synchroniser l'heure de l'AD et d'IPFIRE :

NTP Configuration

Common settings

☒ Obtain time from a network time server
Clock has not been synchronized

Primary NTP server: Secondary NTP server:

☒ Provide time to local network

☒ Force setting the system clock on boot

Synchronization

☒ Every Days

☐ Manually

Update the time:
To queue a synchronization event at any time (even while using a repeating schedule), press the **Set time now** button. Please note that you may have to wait for five minutes, or more, before a sync event occurs.

Waiting to synchronize clock...

* Required field

Activer Windows
Accédez aux paramètres

Test de connexion à internet du client à travers IPFIRE :



Étape 6 : Paramétrage des règles de connexion (routes statiques)

Il faut d'abord, pour que le réseau LOCAL puisse communiquer via IPFire. Pour cela, j'ai défini des routes statiques par VLAN, ayant pour passerelle le réseau 10 (celui des administrateurs). Dans « Réseau / Routes statiques » :

P14-IPFire.ecole.eni

Système Statut Réseau Services Pare-Feu IPFire Journaux Traffic: In 84.84 kbit/s Out 0.00 bits

Entrées de la table de routage :

Ajouter une route

Adresse IP de l'hôte / Réseau:

Passerelle:

Remarque:

Activé: ☒

Ajouter

Table de routage

Adresse IP de l'hôte / Réseau	Passerelle	Remarque	Action
10.30.1.0/24	10.10.1.254	reseau30	<input checked="" type="checkbox"/>
10.20.1.0/24	10.10.1.254	reseau20	<input checked="" type="checkbox"/>

Légende: ☒ Activé (décocher pour désactiver) ☐ Désactivé (cocher pour activer) Modifier Enlever

Dans « Réseau / Proxy Web » :

Contrôle d'accès réseau

Sous-réseaux autorisés (un par ligne) : *

10.60.1.0/24
10.70.1.0/24
172.16.0.0/16

Contrôle d'accès réseau

Sous-réseaux autorisés (un par ligne) : *

10.10.1.0/24
10.20.1.0/24
10.30.1.0/24
10.60.1.0/24

Sur les routeurs :

```
R12-CISCO1760(config)#ip route 10.60.1.0 255.255.255.0 10.10.1.76
R12-CISCO1760(config)#ip route 10.70.1.0 255.255.255.0 10.10.1.76
R12-CISCO1760(config)#ip route 172.17.0.0 255.255.0.0 10.10.1.76
R11-CISCO1760(config)#ip route 10.60.1.0 255.255.255.0 10.10.1.76
R11-CISCO1760(config)#ip route 10.70.1.0 255.255.255.0 10.10.1.76
R11-CISCO1760(config)#ip route 172.17.0.0 255.255.0.0 10.10.1.76
```

Résultat des tests ping d'un client du VLAN 10 à un autre du VLAN 60 :

```
C:\Users\SIO1>ping 10.60.1.176

Envoi d'une requête 'Ping' 10.60.1.176 avec 32 octets de données :
Réponse de 10.60.1.176 : octets=32 temps=2 ms TTL=127
Réponse de 10.60.1.176 : octets=32 temps=2 ms TTL=127
Réponse de 10.60.1.176 : octets=32 temps=1 ms TTL=127
Réponse de 10.60.1.176 : octets=32 temps<1ms TTL=127

Statistiques Ping pour 10.60.1.176:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 2ms, Moyenne = 1ms
```

Résultat des tests ping d'un client du VLAN 10 à l'interface locale de l'IPFire (dans VLAN 10) :



```
C:\Users\SIO1>ping 10.10.1.76

Envoi d'une requête 'Ping' 10.10.1.76 avec 32 octets de données :
Réponse de 10.10.1.76 : octets=32 temps<1ms TTL=64
Réponse de 10.10.1.76 : octets=32 temps<1ms TTL=64
Réponse de 10.10.1.76 : octets=32 temps=1 ms TTL=64
Réponse de 10.10.1.76 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.10.1.76:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

Résultat des tests ping d'un client du VLAN 10 à un autre du VLAN 70 :

```
C:\Users\SIO1>ping 10.70.1.176

Envoi d'une requête 'Ping' 10.70.1.176 avec 32 octets de données :
Réponse de 10.70.1.176 : octets=32 temps=2 ms TTL=127
Réponse de 10.70.1.176 : octets=32 temps=1 ms TTL=127
Réponse de 10.70.1.176 : octets=32 temps=1 ms TTL=127
Réponse de 10.70.1.176 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 10.70.1.176:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

Remarque : Sachant que le Proxy du lycée a des règles strictes (dû à une politique stricte du lycée), les pings ne marchent pas sur le réseau 172.17.0.0/16.

Étape 7 : Pare-feu

Pour établir les règles, j'ai procédé par une matrice des droits :

	RED	GREEN	ORANGE
RED		Autorisé	Autorisé NAT/PAT : 80
GREEN	Autorisé		Autorisé
ORANGE	Autorisé	Interdit	

- 1) J'ai, tout d'abord, mis en place les règles de filtrages, paramétrable dans "Pare-feu / Règles de pare-feu" :



Du WAN (rouge) au LAN (vert) :



Règles de pare-feu

Source

☐ Adresse source (adresse MAC/IP ou réseau) :
☐ Firewall

☒ Réseaux standards :
☐ Localisation :

NAT

☐ Utiliser la traduction d'adresses réseau (NAT)

Destination

☐ Adresse IP de destination (adresse IP ou réseau) :
☐ Firewall

☒ Réseaux standards :
☐ Localisation :

Protocole

☒ ACCEPTER
 ☐ IGNORER
 ☐ REFUSER

Paramètres additionnels

Remarque :

Position de règle :

☐ Log de règle
 ☐ Utiliser les contraintes horaires
 ☐ Limiter les connexions simultanées par adresse IP
 ☐ Limiter le nombre des nouvelles connexions

Ajouter Retour

Du WAN (rouge) à la DMZ (orange) :

Règles de pare-feu

Source

☐ Adresse source (adresse MAC/IP ou réseau) :
☐ Firewall

☒ Réseaux standards :
☐ Localisation :

NAT

☐ Utiliser la traduction d'adresses réseau (NAT)

Destination

☐ Adresse IP de destination (adresse IP ou réseau) :
☐ Firewall

☒ Réseaux standards :
☐ Localisation :

Protocole

☒ Services
☐ Groupes de service

☒ ACCEPTER
 ☐ IGNORER
 ☐ REFUSER

Paramètres additionnels

Remarque :

Position de règle :

☐ Log de règle
 ☐ Utiliser les contraintes horaires
 ☐ Limiter les connexions simultanées par adresse IP
 ☐ Limiter le nombre des nouvelles connexions

Du LAN (vert) au WAN (rouge) :



Règles de pare-feu

Source

☐ Adresse source (adresse MAC/IP ou réseau) :

☒ Réseaux standards :

☐ Localisation :

☐ Firewall :

NAT

☐ Utiliser la traduction d'adresses réseau (NAT)

Destination

☐ Adresse IP de destination (adresse IP ou réseau) :

☒ Réseaux standards :

☐ Localisation :

☐ Firewall :

Protocole

☒ ACCEPTER ☐ IGNORER ☐ REFUSER

Paramètres additionnels

Remarque :

Position de règle :

☐ Log de règle

☐ Utiliser les contraintes horaires

☐ Limiter les connexions simultanées par adresse IP

☐ Limiter le nombre des nouvelles connexions

Du LAN (vert) à la DMZ (orange) :

Règles de pare-feu

Source

☐ Adresse source (adresse MAC/IP ou réseau) :

☒ Réseaux standards :

☐ Localisation :

☐ Firewall :

NAT

☐ Utiliser la traduction d'adresses réseau (NAT)

Destination

☐ Adresse IP de destination (adresse IP ou réseau) :

☒ Réseaux standards :

☐ Localisation :

☐ Firewall :

Protocole

☒ ACCEPTER ☐ IGNORER ☐ REFUSER

Paramètres additionnels

Remarque :

Position de règle :

☐ Log de règle

☐ Utiliser les contraintes horaires

☐ Limiter les connexions simultanées par adresse IP

☐ Limiter le nombre des nouvelles connexions

De la DMZ (orange) au WAN (rouge) :



Règles de pare-feu

Source

☐ Adresse source (adresse MAC/IP ou réseau) :

☐ Firewall :

☒ Réseaux standards :

☐ Localisation :

NAT

☐ Utiliser la traduction d'adresses réseau (NAT)

Destination

☐ Adresse IP de destination (adresse IP ou réseau) :

☐ Firewall :

☒ Réseaux standards :

☐ Localisation :

Protocole

☒ ACCEPTER ☐ IGNORER ☐ REFUSER

Paramètres additionnels

Remarque :

Position de règle :

☐ Log de règle

☐ Utiliser les contraintes horaires

☐ Limiter les connexions simultanées par adresse IP

☐ Limiter le nombre des nouvelles connexions

De la DMZ (orange) au LAN (vert) :

Règles de pare-feu

Source

☐ Adresse source (adresse MAC/IP ou réseau) :

☐ Firewall :

☒ Réseaux standards :

☐ Localisation :

NAT

☐ Utiliser la traduction d'adresses réseau (NAT)

Destination

☐ Adresse IP de destination (adresse IP ou réseau) :

☐ Firewall :

☒ Réseaux standards :

☐ Localisation :

Protocole

☐ ACCEPTER ☐ IGNORER ☒ REFUSER

Paramètres additionnels

Remarque :

Position de règle :

☐ Log de règle

☐ Utiliser les contraintes horaires

☐ Limiter les connexions simultanées par adresse IP

☐ Limiter le nombre des nouvelles connexions

Voici un résumé des règles de pare-feu appliquées :



Règles de pare-feu

Nouvelle règle [Appliquer les changements](#)

Règles de pare-feu

#	Protocole	Source	Log	Destination	Action
1	Tous	ROUGE	<input checked="" type="checkbox"/>	VERT	<input checked="" type="checkbox"/>
2	TCP	ROUGE	<input checked="" type="checkbox"/>	ORANGE: HTTP	<input checked="" type="checkbox"/>
3	Tous	VERT	<input checked="" type="checkbox"/>	ROUGE	<input checked="" type="checkbox"/>
4	Tous	VERT	<input checked="" type="checkbox"/>	ORANGE	<input checked="" type="checkbox"/>
5	Tous	ORANGE	<input checked="" type="checkbox"/>	ROUGE	<input checked="" type="checkbox"/>
6	Tous	ORANGE	<input checked="" type="checkbox"/>	VERT	<input checked="" type="checkbox"/>
VERT ORANGE BLEU		Internet (Autorisé) Internet (Autorisé) Internet (Autorisé)		ORANGE (Autorisé) VERT (Bloqué) ORANGE (Bloqué)	BLEU (Autorisé) BLEU (Bloqué) VERT (Bloqué)
Politique: Autorisé					

- 2) Ensuite, j'ai vérifié les règles de connexions et de filtrage avec **IPTABLES** (dans "Pare-feu / Tables IP") :



Tables IP

Tables IP :

INPUT

Chain INPUT (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
35181	22M	BADTCP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	CUSTOMINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	P2PBLOCK	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	GUARDIAN	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	OVPNBLOCK	all	--	tun+	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	IPS_INPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	IPTVINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	ICMPINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
91716	30M	LOOPBACK	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
72409	25M	CAPTIVE_PORTAL	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
72409	25M	CONNTRACK	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
524	43080	DHCPGREENINPUT	all	--	green0*	*	0.0.0.0/0	0.0.0.0/0	
0	0	DHCPBLUEINPUT	all	--	blue0*	*	0.0.0.0/0	0.0.0.0/0	
53831	7361K	LOCATIONBLOCK	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
53831	7361K	IPSECINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
53831	7361K	GUIINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
53831	7361K	WIRELESSINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate NEW
53831	7361K	OVPNINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
53831	7361K	TOR_INPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
53831	7361K	INPUTFW	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
53816	7360K	REDINPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
51938	6736K	POLICYIN	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Table IP Mangle :

PREROUTING

pkts	bytes	target	prot	opt	in	out	source	destination
392K	63M	NAT_DESTINATION	all	--	*	*	0.0.0.0/0	0.0.0.0/0

Traduction d'adresses réseaux table IP :

PREROUTING

Chain PREROUTING (policy ACCEPT 15167 packets, 1726K bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
352K	40M	CUSTOMPREROUTING	all	--	*	*	0.0.0.0/0	0.0.0.0/0
352K	40M	CAPTIVE_PORTAL	all	--	*	*	0.0.0.0/0	0.0.0.0/0
352K	40M	SQUID	all	--	*	*	0.0.0.0/0	0.0.0.0/0
352K	40M	NAT_DESTINATION	all	--	*	*	0.0.0.0/0	0.0.0.0/0
352K	40M	UPNPFW	all	--	*	*	0.0.0.0/0	0.0.0.0/0



1. NAT / PAT

Définir un reverse-proxy.

Un **proxy** inverse (**reverse proxy**) est un type de serveur, habituellement placé en frontal de serveurs web. Contrairement au serveur **proxy** qui permet à un utilisateur d'accéder au réseau Internet, le **proxy** inverse permet à un utilisateur d'Internet d'accéder à des serveurs internes.

Exercice : Exonet Routeur NAT/PAT

L'entreprise SAGI externalisait ses serveurs HTTP, NNTP et SMTP pour l'Internet et l'extranet. Elle a décidé d'accueillir dans une zone démilitarisée ces serveurs. Ceci l'a conduit à revoir son architecture réseau et sa politique de sécurité.

Après avoir décidé dans un premier temps de créer une DMZ avec une adresse publique, l'administrateur décide d'utiliser aujourd'hui une adresse privée pour renforcer la sécurité.

Le routeur d'accès distant (R1) est un routeur filtrant, il permet d'interdire certains flux et en autoriser d'autres. Ce routeur prend aussi en charge la traduction d'adresses (NAT/PAT).

Les clients du réseau local ont un accès à Internet.

Vous trouverez en annexe 1 la structure schématique du nouveau réseau de l'entreprise.

Vous trouverez en annexe 2, des exemples de règles NAT/PAT appliquées par le routeur R1.

Vous trouverez en annexe 3 des exemples de règles de redirection appliquées par le routeur R1.

Première partie

1. Pourquoi le routeur R1 masque-t-il les adresses du réseau 192.168.50.0/24 ?

Le routeur masque les adresses du réseau 192.168.50.0/24 car il utilise le protocole NAT/PAT qui traduit des adresses IP privées en une adresse publique associée à un port pour chaque demande.

2. Expliquer le rôle des règles de l'annexe 3.

Ces règles permettent la communication des serveurs de la DMZ avec Internet, lors de demandes http sur l'adresse IP publique du routeur.

3. Le routage porte-t-il sur les adresses substituées ou sur les adresses réelles ?

Le routage porte sur les adresses substituées. (Traduction des adresses et ports par d'autres)

Deuxième partie

1. Pourquoi n'utilise-t-on pas le port standard 80 pour rediriger vers le serveur http partenaire de nom prive.sagi.fr ?

On n'utilise pas le port standard 80 pour rediriger vers le serveur HTTP partenaire de nom « prive.sagi.fr » car la communication n'est pas sécurisée. (Échanges non-cryptés par moyens de cryptage)

2. Comment les clients http des partenaires doivent-ils adresser leur requête pour accéder au serveur http partenaire prive.sagi.fr ?



Les clients HTTP des partenaires devraient adresser leur requête pour accéder au serveur HTTP partenaire « prive.sagi.fr » en utilisant un VPN et/ou un moyen de cryptage des échanges (TLS/SSL/cryptage asymétrique)

Troisième partie

L'administrateur décide d'appliquer une politique de sécurité plus restrictive. Il veut empêcher tout trafic entre l'Internet et l'Intranet. Pour cela, il va mettre en place un Proxy HTTP sur un serveur d'adresse 192.168.100.4 dans la DMZ qui écoutera sur le port 8080. Tous les utilisateurs devront passer par ce Proxy.

1. Comment fonctionne un Proxy-HTTP et quel est son intérêt ?

Un proxy est un dispositif informatique qui sert d'intermédiaire pour accéder à Internet (ou d'autres réseaux). De plus, il peut gérer le trafic venant de l'extérieur en l'autorisant ou l'interdisant selon la source du trafic, le type de trafic, la politique mise en place dans l'entreprise... mais aussi de l'intérieur en empêchant les fuites de données ou intrusions de logiciels malveillants.

Son intérêt est varié. Il peut permettre :

- L'accélération de l'affichage des pages web, grâce à son cache ;
- Bloquer l'accès à certains sites WEB ;
- Masquer son adresse IP ;
- Contourner la censure WEB...

2. Proposer une solution pour permettre aux postes de l'Intranet d'utiliser le Proxy-HTTP de façon transparente.

Pour permettre aux postes de l'Intranet d'utiliser le Proxy-HTTP de façon transparente, il faudrait :

- Régler l'option de serveur proxy sur son adresse IP (192.168.100.4) et un/des port(s) d'écoute ;
- Autoriser le trafic WEB entre le serveur Proxy http et les clients de l'Intranet en configurant des règles de filtrages sur le routeur ;
- Configurer une redirection de port entre l'interface du routeur ayant pour adresse IP publique 213.152.47.9 et le serveur Proxy.

3. Rédiger le(s) règle(s) permettant cette solution.

NAT/PAT

Numéro	Interface	Type	Protocole	Adresse publique	Port public	Adresse privée	Port privé
1	213.152.47.9	NP	TCP	213.152.47.9	*	192.168.100.0/24	*

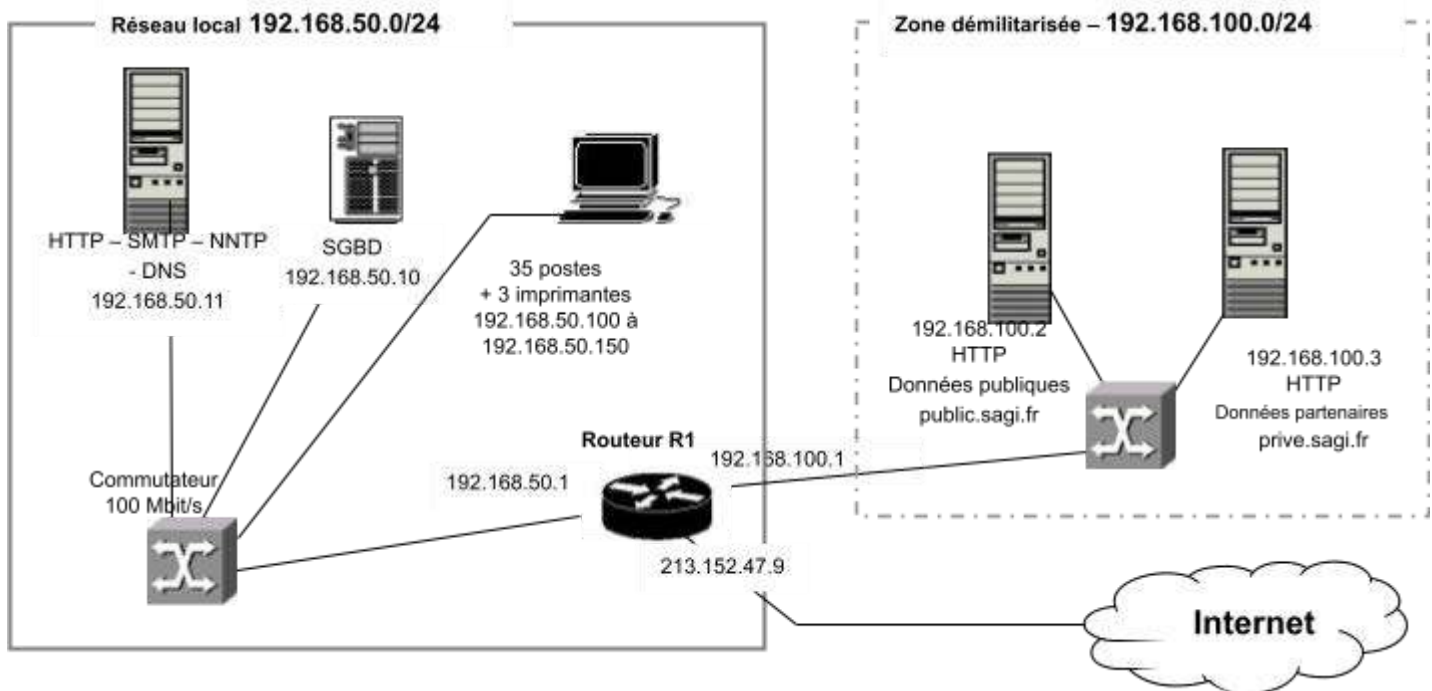
Redirection de ports

Numéro	Interface	Type	Protocole	Adresse publique	Port public	Adresse privée	Port privé
2	213.152.47.9	R	TCP	213.152.47.9	*	192.168.100.4/32	8080



Annexes

Annexe 1 : Structure schématique du réseau d'une entreprise



Annexe 2 : exemples de règles NAT/PAT

Le type NP (NAT/PAT) s'applique en sortie de l'interface et substitue l'adresse IP source et le port source privés par une adresse IP publique et un port public. Cette règle génère une entrée dans une table interne du routeur qui permettra de gérer la substitution inverse.

Numéro	Interface	Type	Protocole	Adresse publique	Port public	Adresse privée	Port privé
1	213.152.47.9	NP	TCP	213.152.47.9	*	192.168.50.0/24	*
2	213.152.47.9	NP	TCP	213.152.47.9	*	192.168.100.0/24	*

Annexe 3 : exemples de règles de redirection

Le Type R (Redirection) s'applique en entrée de l'interface et substitue l'adresse IP destination et le port de destination publics par une adresse IP privée et un port privé. Cette règle génère une entrée dans une table interne du routeur qui permettra de gérer la substitution inverse.

Numéro	Interface	Type	Protocole	Adresse publique	Port public	Adresse privée	Port privé
3	213.152.47.9	R	TCP	213.152.47.9	80	192.168.100.2	80
4	213.152.47.9	R	TCP	213.152.47.9	4500	192.168.100.3	80



Le serveur HAProxy de la DMZ équilibre la charge entre les serveurs web qui constituent l'extranet.

L'objectif est de rediriger les requêtes HTTP à destination de l'interface RED (**172.17.X.X donnée par DHCP**), GREEN et BLUE vers **P14_SerwebTest (qui sera changer par la suite par le serveur HAProxy et Serwebsecu1 et Serwebsecu2)** dans la DMZ (**10.70.1.77**).

- 1) Pour cela, j'ai été dans "Pare-Feu / Règles de pare-feu" et j'ai créé une nouvelle règle.
J'ai mis l'option "**Réseaux standards : Tous**" comme source.

Règles de pare-feu

Source	
<input type="radio"/> Adresse source (adresse MAC/IP ou réseau) :	<input type="radio"/> Firewall
<input checked="" type="radio"/> Réseaux standards :	Tous
<input type="radio"/> Localisation	A1 - Anonymous Proxy

- 2) J'ai, ensuite, activé le NAT (en cochant la case) et j'ai sélectionné "**Destination NAT**", avec l'option "**Rouge**" comme "**Interface de pare-feu**".

Règles de pare-feu

Source	
<input type="radio"/> Adresse source (adresse MAC/IP ou réseau) :	<input type="radio"/> Firewall
<input checked="" type="radio"/> Réseaux standards :	Tout
<input type="radio"/> Localisation	A1 - Anonymous Proxy

NAT	
<input checked="" type="checkbox"/> Utiliser la traduction d'adresses réseau (NAT)	
<input checked="" type="radio"/> Destination NAT (redirection de port)	Interface pare-feu: <u>ROUGE (172.17.30.94)</u>
<input type="radio"/> Source NAT	

- 3) Dans la catégorie "**Destination**", j'ai saisi l'adresse IP **10.70.1.77** de protocole TCP avec 80 (HTTP) comme "**Port de destination**" et 8080 comme "**Port externe (NAT)**" qui est accessible par les membres en dehors de la DMZ (ici, en WAN, LAN et WIFI). Le port source correspond au port sur lequel le client veut te parler.



Règles de pare-feu

Source	
<input type="radio"/> Adresse source (adresse MAC/IP ou réseau) :	<input type="radio"/> Firewall
<input checked="" type="radio"/> Réseaux standards :	Tous
<input type="radio"/> Localisation :	A1 - Anonymous Proxy

NAT	
<input checked="" type="checkbox"/> Utiliser la traduction d'adresses réseau (NAT)	
<input checked="" type="radio"/> Destination NAT (redirection de port)	Interface pare-feu: ROUGE (172.17.30.94)
<input type="radio"/> Source NAT	

Destination	
<input checked="" type="radio"/> Adresse IP de destination (adresse IP ou réseau) :	<input type="radio"/> Firewall
<input type="radio"/> Réseaux standards :	Tous
<input type="radio"/> Localisation :	A1 - Anonymous Proxy

Règles de pare-feu

Source	
<input type="radio"/> Adresse source (adresse MAC/IP ou réseau) :	<input type="radio"/> Firewall
<input checked="" type="radio"/> Réseaux standards :	Tous
<input type="radio"/> Localisation :	A1 - Anonymous Proxy

NAT	
<input checked="" type="checkbox"/> Utiliser la traduction d'adresses réseau (NAT)	
<input checked="" type="radio"/> Destination NAT (redirection de port)	Interface pare-feu: ROUGE (172.17.30.94)
<input type="radio"/> Source NAT	

Destination	
<input checked="" type="radio"/> Adresse IP de destination (adresse IP ou réseau) :	<input type="radio"/> Firewall
<input type="radio"/> Réseaux standards :	BLEU (10.60.1.0/24)
<input type="radio"/> Localisation :	A1 - Anonymous Proxy

Protocole	
TCP	
Port source :	
Port de destination :	80
Port externe (NAT) :	8080

4) J'ai donné un nom à la règle et je l'ai placé en première position.



Règles de pare-feu

Source

☐ Adresse source (adresse MAC/IP ou réseau) :
☐ Firewall :

☒ Réseaux standards :
☐ Localisation :

NAT

☒ Utiliser la traduction d'adresses réseau (NAT)

☒ Destination NAT (redirection de port)
 ☐ Source NAT

Interface pare-feu :

Destination

☒ Adresse IP de destination (adresse IP ou réseau) :
☐ Firewall :

☐ Réseaux standards :
☐ Localisation :

Protocole

Port source :

Port de destination :

Port externe (NAT) :

Paramètres additionnels

Remarque :

Position de règle :

☒ Activer la règle
 ☒ Log de règle
 ☐ Utiliser les contraintes horaires
 ☐ Limiter les connexions simultanées par adresse IP
 ☐ Limiter le nombre des nouvelles connexions

Mettre à jour
 Retour

Règles de pare-feu

#	Protocole	Source	Log	Destination	Action
1	TCP	Tout	<input checked="" type="checkbox"/>	Pare-feu (ROUGE): 8080 ->10.70.1.77: 80	<input checked="" type="checkbox"/>
Redirection INTERNET <-> DMZ					
2	Tous	ROUGE	<input type="checkbox"/>	VERT	<input type="checkbox"/>
3	TCP	ROUGE	<input type="checkbox"/>	ORANGE: HTTP	<input type="checkbox"/>
4	Tous	VERT	<input type="checkbox"/>	ROUGE	<input type="checkbox"/>
5	Tous	VERT	<input type="checkbox"/>	ORANGE	<input type="checkbox"/>
6	Tous	ORANGE	<input type="checkbox"/>	ROUGE	<input type="checkbox"/>
7	Tous	ORANGE	<input type="checkbox"/>	VERT	<input type="checkbox"/>
VERT		Internet (Autorisé)		ORANGE (Autorisé)	BLEU (Autorisé)
ORANGE		Internet (Autorisé)		VERT (Bloqué)	BLEU (Bloqué)
BLEU		Internet (Autorisé)		ORANGE (Bloqué)	VERT (Bloqué)
Politique: Autorisé					

Après l'avoir ajouté comme exception, nous pouvons atteindre l'Extranet en attaquant l'adresse IP de l'interface RED (depuis n'importe quel réseau dans notre cas).



Règles de pare-feu

Source

☐ Adresse source (adresse MAC/IP ou réseau) :

☐ Réseaux standards :

☐ Localisation :

☐ Firewall :

NAT

☒ Utiliser la traduction d'adresses réseau (NAT)

☒ Destination NAT (redirection de port)

☐ Source NAT

Interface pare-feu :

Destination

☒ Adresse IP de destination (adresse IP ou réseau) :

☐ Réseaux standards :

☐ Localisation :

☐ Firewall :

Protocole

Port source :

Port de destination :

Port externe (NAT) :

Paramètres additionnels

Remarque :

Position de règle :

☒ Activer la règle

☒ Log de règle

☐ Utiliser les contraintes horaires

☐ Limiter les connexions simultanées par adresse IP

☐ Limiter le nombre des nouvelles connexions

Activer Windows
Accédez aux paramètres
activer Windows.

Mettre à jour Retour

172.17.30.94:8080

Non sécurisé | 172.17.30.94:8080

Ceci est un test!

WEB

Remarque : Il ne faut pas oublier d'effacer l'historique des navigateurs WEB, entre les tests.



Partie 5 : **VPN**

Étape 1 : Principe

Les applications et les systèmes distribués font de plus en plus partie intégrante du paysage d'un grand nombre d'entreprises. Ces technologies ont pu se développer grâce aux performances toujours plus importantes des réseaux locaux.

Mais le succès de ces applications a fait aussi apparaître un de leur écueil. En effet si les applications distribuées deviennent le principal outil du système d'information de l'entreprise, comment assurer leur accès sécurisé au sein de structures parfois réparties sur de grandes distances géographiques ?

Afin d'assurer la confidentialité et l'intégrité des échanges, un VPN (Virtual Private Network) ou réseau privé virtuel met en place un système d'**authentification** et repose sur un **protocole d'encapsulation** (en anglais **tunneling**) permettant de sécuriser la transmission des données en les **chiffrant** (algorithmes de cryptographie).

Un système de Vpn doit pouvoir mettre en œuvre les fonctionnalités suivantes :

- **Authentification d'utilisateur.** Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.
- **Gestion d'adresses.** Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse.
- **Cryptage des données.** Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
- **Gestion de clés.** Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
- **Prise en charge multiprotocole.** La solution Vpn doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier Ip.

1 Typologie des VPN.

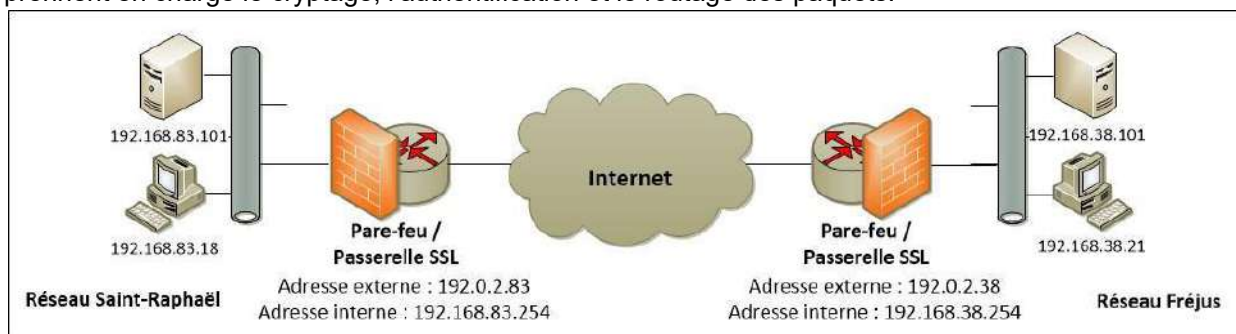
1.1 VPN d'entreprise

Dans ce cas, l'entreprise garde le contrôle de l'établissement des VPN.

VPN site à site

C'est un des cas les plus fréquents. Il s'agit de relier deux sites d'une même entreprise ou bien le site d'une entreprise et celui d'un fournisseur, d'un prestataire ou d'un client. Mais il faut également que tout ou partie des machines des deux réseaux puissent communiquer avec celles du réseau distant en utilisant les adresses privées de chaque réseau.

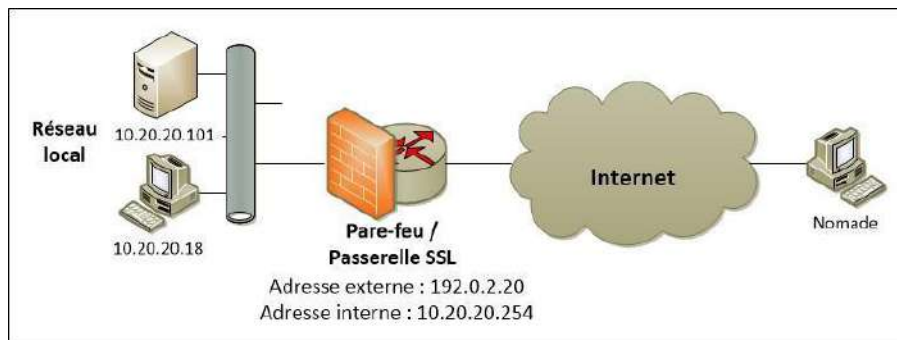
Généralement ce type de VPN est mis en place par l'interconnexion de deux éléments matériels (routeur/pare-feu) situés à la frontière entre le réseau interne et le réseau public de chaque site. Ces matériels prennent en charge le cryptage, l'authentification et le routage des paquets.



Cette solution n'assure aucune protection des données entre les postes et les firewalls puisque le tunnel n'est établi qu'entre les deux firewalls.

VPN poste à site

C'est également une utilisation très fréquente des VPN que celle consistant à permettre à des utilisateurs distants (nomades, travailleurs à domicile, commerciaux...) d'accéder aux ressources de l'entreprise via un VPN.



Pour construire cette solution, il faut sur le site central un matériel (firewall, routeur) constituant le point de terminaison de tous les VPN côté entreprise. Du côté des postes de travail distants, il faut un logiciel gérant le type de protocole choisi et compatible avec le matériel du site central. Dans certains cas ce logiciel est déjà présent dans le système d'exploitation de ces postes. Dans d'autres cas, il est nécessaire d'installer ce composant logiciel.

- La protection est totale du poste distant au site central.
- Le cryptage impose une charge non négligeable au poste distant, ce qui peut en dégrader les performances.
- Les protocoles utilisés pour le VPN doivent pouvoir traverser le firewall du réseau sur lequel est branché le poste distant. En effet, à l'exception des VPN SSL, les tunnels sont généralement établis à l'aide de ports ou de protocoles différents des ports classiquement autorisés (80, 21, 443...) et ces ports spécifiques sont souvent interdits par l'administrateur réseau.
- Le cryptage n'est pas assuré au-delà du firewall du site central.

VPN poste à poste

Dans ce cas, l'objectif est d'établir un canal sécurisé de bout en bout entre deux postes ou, plus couramment, entre un poste et un serveur. Le poste et le serveur peuvent être situés sur le même réseau ou sur deux réseaux distants reliés eux-mêmes par un VPN site à site.

Ici n'interviennent que des composants logiciels : un logiciel client sur le poste "demandeur" et un logiciel utilisé en serveur sur le poste "destinataire".

Quand les postes se situent sur des réseaux locaux séparés par Internet, il est nécessaire que les deux extrémités puissent échanger leurs messages sur des protocoles et des ports qui doivent être autorisés par les firewalls situés sur chaque site. Cela nécessite également des translations d'adresses puisque les machines concernées sont rarement dotées d'adresses IP publiques.

1.2. VPN opérateur

Lorsqu'il s'agit d'interconnecter plusieurs sites d'une même entreprise avec des besoins de performances et de disponibilité, il est plus judicieux, mais aussi plus coûteux, de faire appel à un opérateur qui va donc mettre en place un réseau privatif entre tous les sites. Ce réseau tient plus d'un réseau de tunnels que d'un véritable réseau VPN.

2. Principaux protocoles.

2.1. Niveau 2

Ces VPN encapsulent les données dans des trames et ce sont ces trames que va véhiculer le tunnel dans une communication point à point. Nous sommes ici au niveau 2 du modèle OSI. La plupart de ces protocoles sont progressivement délaissés au profit de protocoles plus souples comme peuvent l'être ceux des niveaux 3 à 7.

- **PPTP (Point to Point Tunneling Protocol)**

Ce protocole soutenu par Microsoft est très simple mais assez limité. Il est en fort déclin maintenant.

- **L2F (Layer 2 Forwarding)**

Cisco a développé ce protocole autour des années 1996. L'IETF en a fait un standard en 1998 avec la RFC 2341. Son fonctionnement est assez voisin de PPTP.

- **L2TP (Layer 2 Tunneling Protocol)**

Dérivé de PPTP et de L2F ce protocole est maintenant un des protocoles VPN implantés nativement sur les machines Windows, ce qui explique son succès.

2.2. Niveau 3 et +

IPsec

Ce protocole très populaire est un des plus robustes mais il est aussi un des plus complexes.

SSL/TLS

Ce protocole en plein essor est simple de mise en œuvre.

3. Mise en œuvre d'un VPN SSL.

3.1. Les types de VPN SSL/TLS



D'une façon générale, le VPN SSL est destiné principalement à interconnecter un poste à un site central. Il fonctionne donc essentiellement en mode client-serveur même s'il est parfois possible de trouver des VPN SSL site à site.

Il est classique de classer arbitrairement les VPN SSL dans trois grandes catégories :

- Le portail web pour accès à des sites web, utilisable avec un navigateur simple il est limité à des applications/sites accessibles en http ou https.
- Le portail applicatif qui permet, toujours à partir d'un navigateur, d'accéder à quelques types d'applications supplémentaires (ssh, rdp, ftp, telnet...).
- Le mode tunnel complet qui donne accès, sous réserve d'autorisation par les règles de filtrage, à la totalité d'un réseau local.

3.2. Mise en place d'un serveur OpenVPN (tunnel VPN complet).

OpenVPN est une solution qui se base sur SSL. Elle permet d'assurer l'authentification du client et du serveur ainsi que la sécurisation du canal de transmission.

OpenVPN s'utilise dans deux cas de figure :

- Le type **routed** pour mettre en relation des machines distantes par Internet (exploité dans ce projet).
- Le type **bridged** pour mettre en relation deux sous-réseaux différents.

4. Sites à visiter.

<https://www.frameip.com/vpn/>

<http://www.openmaniak.com/openvpn.php>

Étape 2 : Mise en place d'OPENVPN sur IPFIRE (serveur)

- Depuis l'interface Web : <https://adresse IP:444>
- Dans Services : OpenVPN,

LHipfire.ecole.eni

Système Statut Réseau Services Pare-Feu IPFire Rapports Traffic: In 0.00 Bit/s Out 0.00 Bit/s

4. Statut OpenVPN / Configuration :

Configuration générale

Statut actuel du serveur OpenVPN : **ARRETER**

☒ OpenVPN sur RED
☐ OpenVPN sur BLEU
☐ OpenVPN sur ORANGE

Nom d'hôte/IP du VPN local:

Sous-réseau OpenVPN (c.a.d. 10.0.10.0/255.255.255.0):

Périphérique OpenVPN:

Protocole:

Port de destination:

Taille du MTU:

Chiffrer:

Compression-LZO: ☐

Autorité de certification

Nom	Sujet	Action
Certificat root:	Absent	
Certificat hôte:	Absent	
Diffie-Hellman parameters:	Absent	
TLS-Authentication-Key:	Absent	

Envoyer un certificat CA

Nom CA: Aucun fichier sélectionné.

Diffie-Hellman parameters options

Upload new Diffie-Hellman parameters: Aucun fichier sélectionné.

Generate new Diffie-Hellman parameters:



- Commencer par générer les certificats de Root/Hôte

Générer des certificats Root/Hôte:

Nom Organisation:

Nom d'hôte d'IPFire:

Votre adresse de courriel:

Votre Département:

Ville:

Etat ou Région:

Pays:

Diffie-Hellman parameters length:

* Ce champ peut être vide.

ATTENTION: Generating the root and host certificates can take a long time. Creating DH parameters with lengths of 1024 or 2048 bits takes up to several minutes. Lengths of 3072 or 4096 bits might need several hours. Please be patient. For weak systems or systems with little entropy, it is recommended to upload long Diffie-Hellman parameters by usage of the upload function.

Sauver et Complétez la fenêtre principale en cochant la case « OpenVPN sur RED », en cliquant « Compression LZO » puis terminez en cliquant le bouton « Démarrer le serveur OpenVPN » de manière à obtenir ceci :

LHipfire.ecole.eni

Système Statut Réseau Services Pare-Feu IPFire Rapports Traffic: In 0.00 Bit/s Out 0.00 Bit/s

4. Statut OpenVPN / Configuration :

Configuration générale

Statut actuel du serveur OpenVPN: **EN FONCTION**

OpenVPN sur RED: ☒

OpenVPN sur BLEU: ☐

OpenVPN sur ORANGE: ☐

Nom d'hôte/IP du VPN local:

Sous-réseau OpenVPN (c.a.d. 10.0.10.0/255.255.255.0):

Périphérique OpenVPN:

Protocole:

Port de destination:

Taille du MTU:

Chiffrer:

Compression-LZO: ☒

Etat et contrôle de connexion :

Nom	type	Réseau	Remarque	Statut	Action
Ajouter Statistiques de connexions OpenVPN					

Autorité de certification

Nom	Sujet	Action
Certificat root	C=FR, S=Lorraine, L=Metz, O=lh, OU=Moselle, CN=lh CA	
Certificat hôte	C=FR, S=Lorraine, O=lh, OU=Moselle, CN=192.168.168.45	
Diffie-Hellman parameters	PKCS#3 DH Parameters: (1024 bit)	
TLS-Authentication-Key	2048 bit OpenVPN static key	

Légende: Montrer le certificat Téléchargez le certificat

- Dans Etat et contrôle de connexion, créer des connexions clients en cliquant sur « Ajouter »



LHipfire.ecole.eni

Système Statut Réseau Services Pare-Feu IPFire Rapports
Traffic: In 0.00 Bit/s Out 0.00 Bit/s

OpenVPN

Type de Connexion

Type de Connexion:

☒ Virtual Private Network (VPN) de l'hôte au net (RoadWarrior)
☐ Net-a-Net Réseau Privé Virtuel (VPN)
☐ Net-a-Net Réseau Privé Virtuel (VPN) (Upload Client Package)

Aucun fichier sélectionné.

Import Connection Name * Default: Client Packagename

- Puis encore Ajouter
- Saisir le nom du client et générer le certificat

LHipfire.ecole.eni

Système Statut Réseau Services Pare-Feu IPFire Rapports
Traffic: In 732.45 Bit/s Out 0.00 Bit/s

OpenVPN

Connection:

Nom:

Remarque : *

Actif : ☒

Choose network

☒ Dynamic OpenVPN IP address pool (10.100.110.0/255.255.255.0)



Authentification :

- ☐ Envoyer une demande de certificat :
☐ Envoyer un certificat :

Parcourir...

Aucun fichier sélectionné.

Générer un certificat :

Nom d'utilisateur complet ou nom d'hôte du système:

clientih

Adresse E-mail de l'utilisateur: *

Département de l'utilisateur: *

Moselle

Nom Organisation: *

lh

Ville: *

Metz

Etat ou Région: *

Lorraine

Pays:

France

Valide jusqu'à (days):

999

Fichier mot de passe PKCS12:

Fichier mot de passe PKCS12:
(confirmation)

* Ce champ peut être vide.

Advanced client options:

Redirect Gateway:

☐

Routing:

IPFire has access to these
networks on the client's site

Attention! If you change these settings, you have to restart the
OpenVPN server that the changes take effect!

Client has access to these
networks on IPFire's site

None
10.10.0.0/24
10.20.0.0/24
Bleu
ORANGE
VERT

DNS1:

DNS2:

WINS:

Sauvegarder

Annuler

Sauvegarder et télécharger le certificat ET le **package pour le client** (un point zip à décompresser).

Etat et contrôle de connexion :

Nom	type	Réseau	Remarque	Statut	Action
clientih	Hôte (Certif)	dynamic	client vpn	DECONNECTE	

Légende: ☒ Activé (cliquer pour désactiver) Montrer le certificat Editer Enlever
☐ Désactivé (cliquer pour activer) Téléchargez le certificat Téléchargez le paquet client (zip)

Ajouter

Statistiques de connexions OpenVPN

Autorité de certification

Nom	Sujet	Action
Certificat root	C=FR, S=Lorraine, L=Metz, O=lh, OU=Moselle, CN=lh CA	
Certificat hôte	C=FR, S=Lorraine, O=lh, OU=Moselle, CN=192.168.168.45	
Diffie-Hellman parameters	PKCS#3 DH Parameters (1024 bit)	
TLS-Authentication-Key	2048 bit OpenVPN static key	

Légende: Montrer le certificat Téléchargez le certificat



Autonote de certification

Nom	Sujet	Action
Certificat root	C=FR, S=Lorraine, L=Metz, O=Ih, OU=Moselle, CN=Ih CA	
Certificat hôte	C=FR, S=Lorraine, O=Ih, OU=Moselle, CN=192.168.168.45	
Diffie-Hellman parameters	PKCS#3 DH Parameters: (1024 bit)	
TLS-Authentication-Key	2048 bit OpenVPN static key	

Légende: Montrer le certificat Téléchargez le certificat

Envoyer un certificat CA

Nom CA: Aucun fichier sélectionné.

Diffie-Hellman parameters options

Upload new Diffie-Hellman parameters: Aucun fichier sélectionné.

Generate new Diffie-Hellman parameters:

Etat et contrôle de connexion :

Nom	type	Réseau	Remarque	Statut	Action
clientth	Hôte (Certif)	dynamic	client vpn	DECONNECTE	

Légende: ☒ Activé (cliquer pour désactiver) Montrer le certificat Edit Enlever

Autorité de

Nom	type	Réseau	Remarque	Statut	Action
Certificat root	Hôte (Certif)	dynamic	client vpn	DECONNECTE	
Certificat hôte	Hôte (Certif)	dynamic	client vpn	DECONNECTE	
Diffie-Hellman	Hôte (Certif)	dynamic	client vpn	DECONNECTE	
TLS-Authentication	Hôte (Certif)	dynamic	client vpn	DECONNECTE	

Légende: ☒ Activé (cliquer pour désactiver) Montrer le certificat Edit Enlever

Envoyer un ce

Nom CA: Aucun fichier sélectionné.

Diffie-Hellman parameters options

Upload new Diffie-Hellman parameters: Aucun fichier sélectionné.

Generate new Diffie-Hellman parameters:

Ajout d'une règle dans le pare feu d'ipFire pour la connexion au VPN
 Cliquez, dans le menu principal d'ipFire, sur « Pare feu » et « Firewall rules »
 Cliquez sur « New rule »
 Configurer la règle



LHipfire.ecole.eni

Système Statut Réseau Services Pare-Feu IPFire Rapports

Traffic: In 481.16 Bit/s Out 481.16 Bit/s

Firewall Rules

Source

☐ Source address (MAC/IP address or network):

☒ Standard networks:

☐ Firewall

Tous

NAT

☒ Use Network Address Translation (NAT)

☐ Destination NAT (Port forwarding)

☒ Source NAT

Firewall interface:

New source IP address:

Destination

☐ Destination address (IP address or network):

☒ Standard networks:

☐ Firewall

VERT (10.50.0.252)

Protocol

Source port:

Destination port:

External port (NAT):

Additional settings

Remarque:

Rule position:

☒ Activate rule

☒ Log rule

☐ Use time constraints

Update

Back



LHipfire.ecole.eni

Système Statut Réseau Services Pare-Feu IPFire Rapports

Traffic: In 0.00 Bit/s Out 0.00 Bit/s

Firewall Rules

New rule

Firewall Rules

#	Protocole	Source	Log	Destination	Action
1	TCP vpn	OpenVPN (10.100.110.0/24): 1194 ->VERT	<input checked="" type="checkbox"/>	VERT: 1194	<input checked="" type="checkbox"/>
		VERT (Allowed) ORANGE (Allowed) Bleu (Allowed)		ORANGE (Allowed) VERT (Blocked) ORANGE (Blocked)	Bleu (Allowed) Bleu (Blocked) VERT (Blocked)

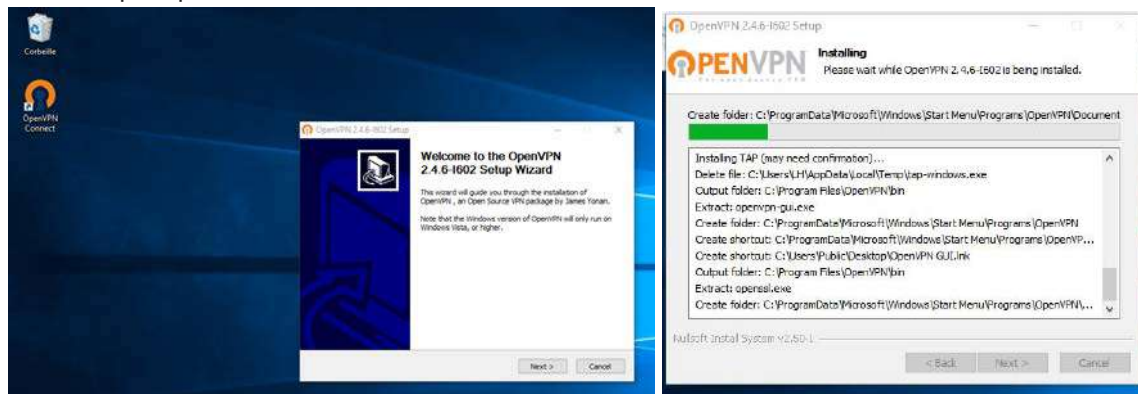
Politique: Allowed

Étape 3 : Mise en place du client OpenVPN sous Windows.

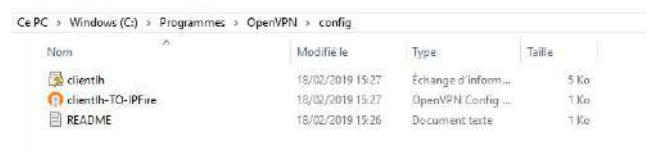
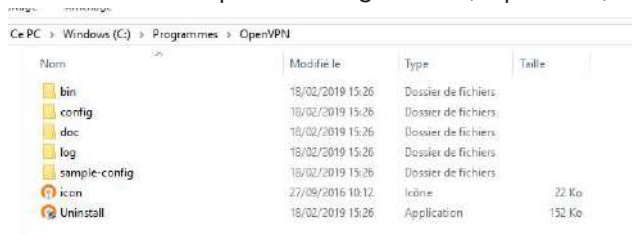
Télécharger OpenVPN



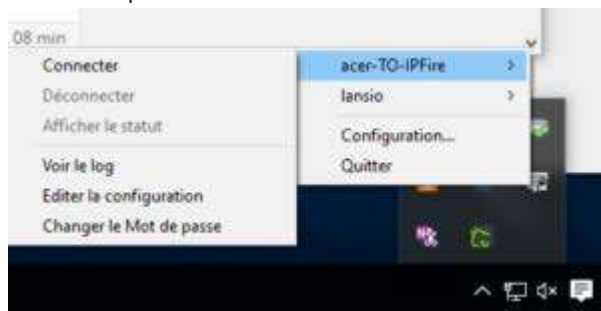
Installer openvpn



- Dans le répertoire Programmes, OpenVPN, config, mettez les fichiers du package



- Dans la zone des icônes en bas à droite de windows, vous aurez alors openVPn et via le bouton droit la possibilité de vous connecter



Puis via RDP, SSH ou HTTPS vous pouvez accéder aux hôtes sur réseau local interne.



Partie 6 : <u>Haute disponibilité de pare-feu</u>
--

<https://wiki.ipfire.org/addons/keepalived/start>

<https://docplayer.fr/5393879-Securisation-acces-reseau-internet.html>

En utilisant VRRP à travers KeeAlived qui est paquet Adons d'IPFire on mettre en place une redondance et une haute disponibilité d'IPfire.

Expliquer le principe, l'installation et la configuration de KeepAlived sur les serveurs IPFire.

Partie 7 : <u>IPSEC</u>

<https://wiki.ipfire.org/configuration/services/ipsec>

Expliquer le principe, l'installation et la configuration d'un VPN site à site avec IPSEC sur les serveurs IPFire.

Partie 8 : <u>Sauvegarde, mise à jour et WIFI</u>
--

<https://wiki.ipfire.org/configuration/system/backup>

<https://wiki.ipfire.org/addons/wireless/start>