Date de création	23 Septembre 2025
Date de dernière mise à jour	29 Septembre 2025
Auteur(s)	CHAGNON Noah, LALIGANT Pierre-Louis, THOMASSINE Soann
Matière (E5-E6-E7-AP)	E6 - Solutions d'infrastructure, systèmes et réseaux
Compétence(s) validée(s)	- Sécuriser les équipements et les usages des utilisateurs

REDIRECTION DE PORT

Redirection de port avec Stormshield

SOMMAIRE

1. Introduction

1.1 Contexte ou cahier des charges

Mise en place d'une redirection de port avec le serveur web Apache2 pour permettre aux utilisateurs de ne pas accéder à la page web grâce à un pare-feu.

1.2 Ressources

Il faut avoir un pare-feu en place et un serveur Apache2 opérationnel.

1.3 Définitions

WAN : *Wide Area Network, représentant un réseau très grand, à l'échelle mondiale.*

TCP : *Le protocole TCP (Transmission Control Protocol) est une norme de communication qui permet aux programmes applicatifs et aux dispositifs informatiques d'échanger des messages sur un réseau. Il est conçu pour envoyer des paquets sur Internet et assurer la transmission réussie des données et des messages sur les réseaux.*

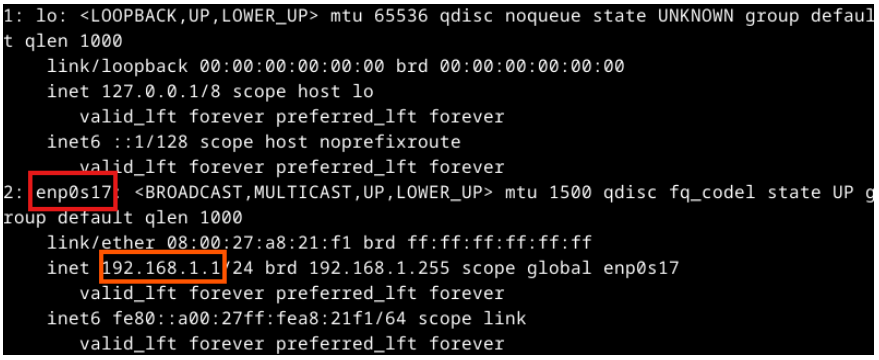
HTTP/HTTPS : *Le protocole HTTP transmet des données non chiffrées, ce qui signifie que les informations envoyées depuis un navigateur peuvent être interceptées et lues par des tiers. Ce processus n'étant pas idéal, il a été étendu au protocole HTTPS pour ajouter une couche de sécurité supplémentaire aux communications.*

2. Réalisation

2.1 Préparation

Pour réaliser correctement une redirection de port, on doit connaître son adresse IP de sa machine avec la commande dans le terminal :

```
ip a
```



NOTE: Il est important de noter qu'en fonction de chaque machine physique, le nom de la carte réseau (encadrée en rouge) peut être différent, ici *enp0s17*.

Pour configurer l'adresse IP et le DNS correctement, il faut effectuer dans le terminal :

```
sudo nano /etc/networks/interfaces
```

Une fois ouvert, s'assurer d'avoir les lignes suivantes inscrites et correctement configurées :

```
allow-hotplug {nom_carteRéseau}
iface {nom_carteRéseau} inet static
     address 192.168.1.1/24
     gateway 192.168.1.254
     dns-nameservers 192.168.1.254
```

Une fois ces lignes ajoutées et vérifiées de leur présence, effectuer la suite de manipulation : CTRL+O - ENTRER - CTRL+X

2.2 Configuration sur l'interface web du pare-feu

2.2.1 Se connecter à l'interface web

Se connecter à l'interface web du pare-feu, en l'occurrence https://192.168.1.254/

2.2.2 Créer une règle NAT

Accéder à l'onglet «*Firewall*» > «*NAT*» > «*Port Forward*».

Cliquez sur le bouton «*Add*» pour ajouter une nouvelle règle.

2.2.3 Configurer la règle de redirection

Pour configurer la règle de redirection, remplir les champs suivants :

Interface : Choisir l'interface sur laquelle le trafic arrive (Généralement WAN)

Protocol : Choisir le protocol (TCP pour HTTP/HTTPS)

Destination : Laisser le WAN address.

Destination port range : Spécifier le port (80 pour HTTP, 443 pour HTTPS)

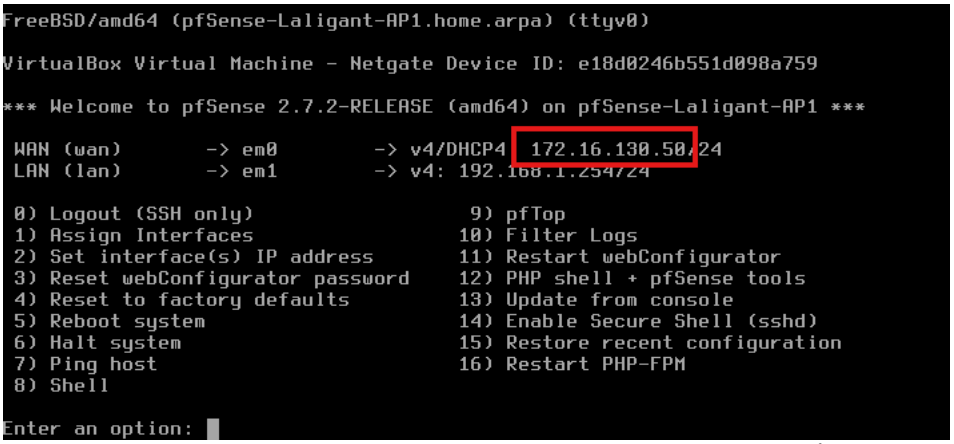
Redirect target IP : Entrer l'adresse IP du serveur web sur lequel diriger le trafic.

Redirect target port : Indiquer le port du serveur web (généralement 80 ou 443)

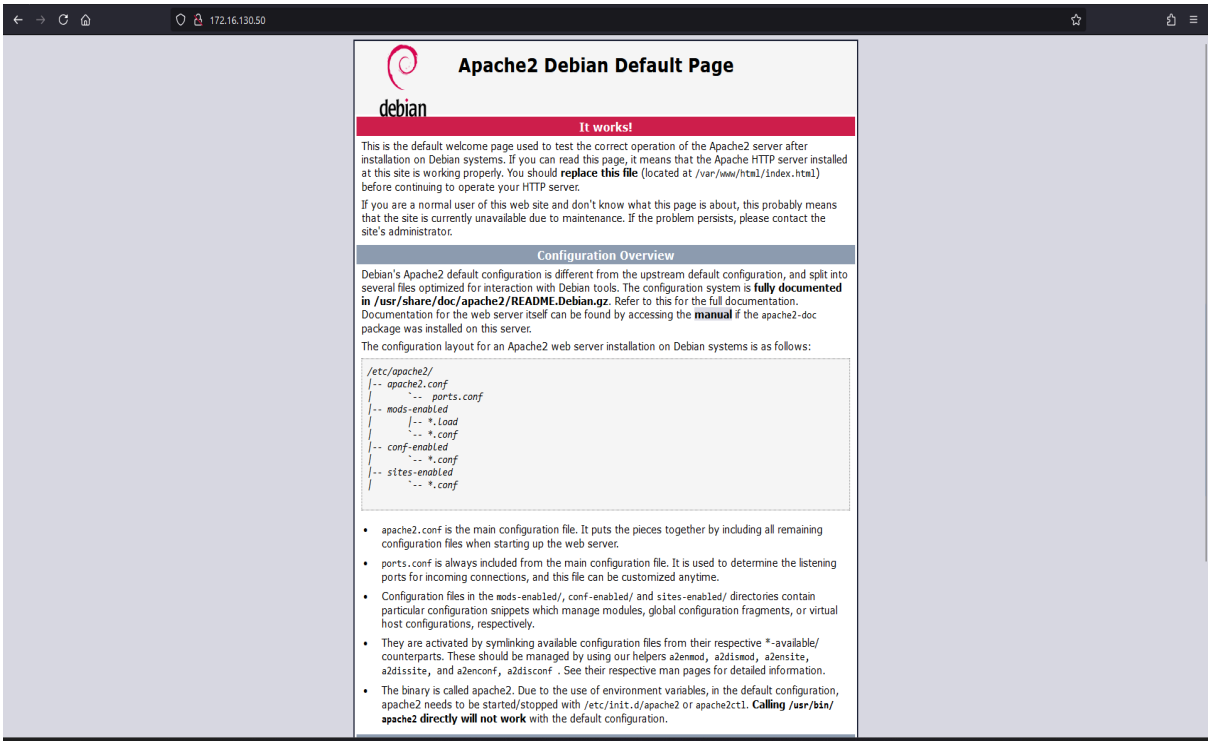
2.2.4 Tester la redirection

Pour tester la redirection, se rendre sur une machine tiers, et il suffit d'utiliser l'adresse IP définie sur le pare-feu :

L'adresse IP est encadrée en rouge



Une fois toutes les étapes terminées, lorsque vous entrez l'IP de redirection, sur votre machine, vous devriez avoir cette page web.


172.16.130.50
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed information.
The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not work with the default configuration.