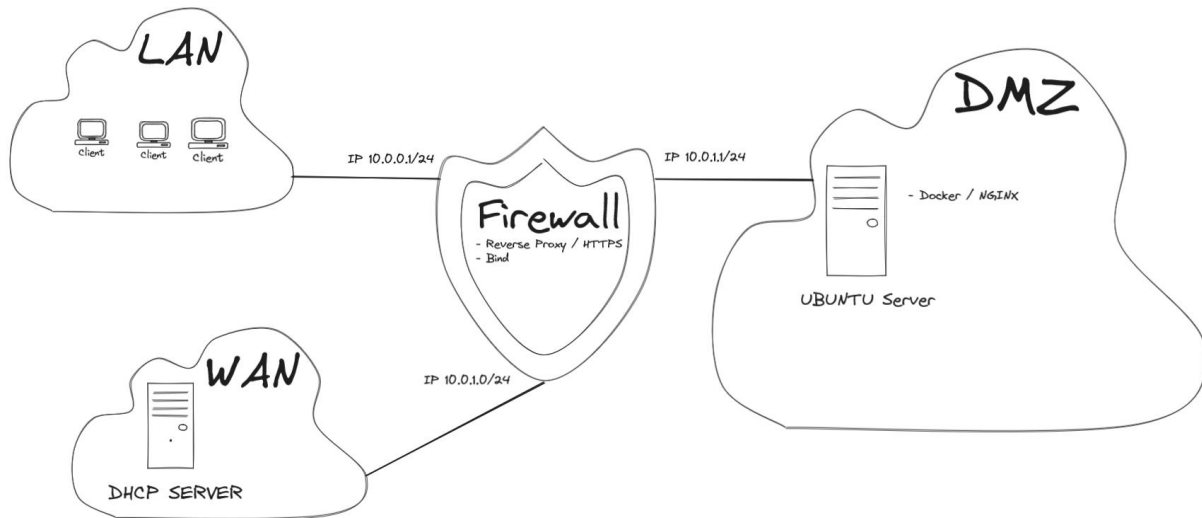

Labo 2 : Implémentation, administration et sécurisation d'une DMZ

Dans ce laboratoire, nous allons ajouter une DMZ au réseau que l'on a créé précédemment.



Une DMZ, ou zone démilitarisée, est une zone située entre le réseau interne et l'extérieur. Elle est utilisée pour héberger des services accessibles depuis l'extérieur, tels que des serveurs web, des serveurs de messagerie, etc., tout en fournissant une couche de sécurité supplémentaire en isolant ces services des réseaux internes.

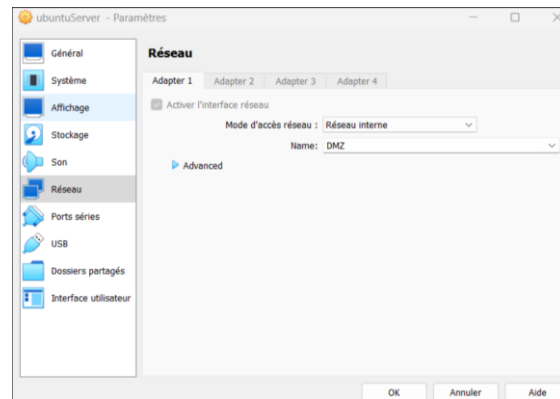
Nous allons ajouter différents services dont notamment un service web qui tournera en https sur lequel nous pourrons nous connecter depuis l'extérieur ainsi qu'un serveur autoritaire. 1.1

Installation de Ubuntu Server

On commence par installer Ubuntu Server qui est un système d'exploitation qui nous permettra de gérer le web server

Après avoir créé une nouvelle machine virtuelle, nous suivons les étapes relatives à l'installation présentes dans ce lien : <https://ubuntu.com/tutorials/install-ubuntu-server#1-overview>

Après avoir configuré Ubuntu Server dans virtualBox, on modifie l'interface réseau pour pouvoir se connecter à la DMZ.



Configuration du Firewall

2.1

On se rend dans l'interface de configuration du Firewall, on assigne l'interface em02 pour opt1 en lui attribuant l'IP 10.0.1.1, avec un range allant de 10.0.1.50 jusqu'à 10.0.1.200

2.2

```
Reloading routing configuration...
DHCPD...

The IPv4 OPT1 address has been set to 10.0.1.1/24

Press <ENTER> to continue.
VirtualBox Virtual Machine - Helgate Device ID: d6c19132939a9b828592

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)    -> em0      -> v4/DHCP4: 10.102.3.20/16
LAN (lan)    -> em1      -> v4: 10.0.0.1/24
OPT1 (opt1)  -> em2      -> v4: 10.0.1.1/24

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

Enter an option: 
```

Sur la page web de notre firewall, dans le menu, on clique sur Interface > OPT1 et on la renomme en DMZ

Configuration du service DHCP

Dans le menu on clique dans service > DHCP SERVER > DMZ > ADD Static mapping > Dans ip adresse, on ajoute l'ip 10.0.1.10.

Et dans Mac-adresse, on ajoute mac-adresse que nous avons récupérée via la commande : « ip a » dans notre Ubuntu. Et puis on SAVE.

DHCP Static Mappings				
Static ARP	MAC address	IP address	Hostname	Description
	08:00:27:4e:c8:27	10.0.1.10		
+ Add Static Mapping				

2.3

Configuration de l'accès à l'internet

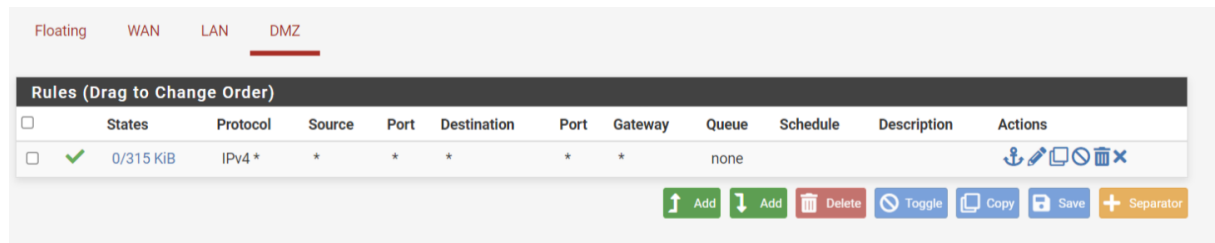
Nous allons à présent créer une règle qui va nous permettre d'accéder à l'internet depuis DMZ 3.1

Dans le menu on clique sur Firewall > rules > DMZ > ADD

Et puis on complète les paramètres suivants :

- Dans action : Pass
- Dans protocol : Any
- Dans Source : Any
- Dans destination : Any

Et on SAVE.



3.2

Installation de Docker

Docker est une plateforme open-source qui permet de créer, déployer et exécuter des applications dans des conteneurs logiciels. Les conteneurs sont des environnements légers et autonomes qui contiennent tout ce dont une application a besoin pour s'exécuter, y compris le code, les bibliothèques, les dépendances et les fichiers système, tout en étant isolés du reste du système.

Dans notre exercice, Docker nous permettra d'installer un container NGINX qui est un serveur web et qui va héberger notre application web.

L'installation de Docker se fait à l'aide de la commande « `sudo apt -get update install docker.io` »

Après avoir vérifié que notre version de docker est la plus à jour, on télécharge une image de NGINX par la commande : `docker pull NGINX`.

Puis, on lance cette image via la commande : `sudo docker run --name hourachiNginx -d -p 80:80 NGINX` et comme retour on reçoit l'ID de l'image. 3.3

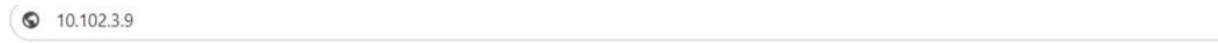
Configuration dans pfsense pour l'accès au serveur web depuis le réseau extérieur

4.1

Dans le Firewall, on va dans nat et on crée une entrée « port forward », on choisit le protocole TCP, on fait le redirect target IP dedans et on encode manuellement l'ip 10.0.1.10 et on save.

The screenshot shows the 'NAT Port Forward' rule configuration in pfSense. The rule is disabled. The 'Interface' is WAN, 'Address Family' is IPv4, and 'Protocol' is TCP. The 'Source' is set to 'Any/Any'. The 'Destination' is WAN address. The 'Destination port range' is HTTP (80). The 'Redirect target IP' is 10.0.1.10. The 'Redirect target port' is HTTP (80). The 'Description' is empty. The 'No XMLRPC Sync' checkbox is unchecked. The 'NAT reflection' is set to 'Use system default'. The 'Filter rule association' is 'Rule NAT'.

Ensuite pour vérifier que tout fonctionne correctement, on se connecte sur un browser extérieur :



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Création d'un reverse proxy

Un reverse Proxy est un serveur qui se place entre les utilisateurs et un ou plusieurs serveurs de backend (ceux qui contiennent les applications ou sites web). Il fonctionne comme un intermédiaire pour traiter les demandes des utilisateurs avant de les acheminer vers le serveur approprié.

4.2

Configuration des paramètres systèmes :

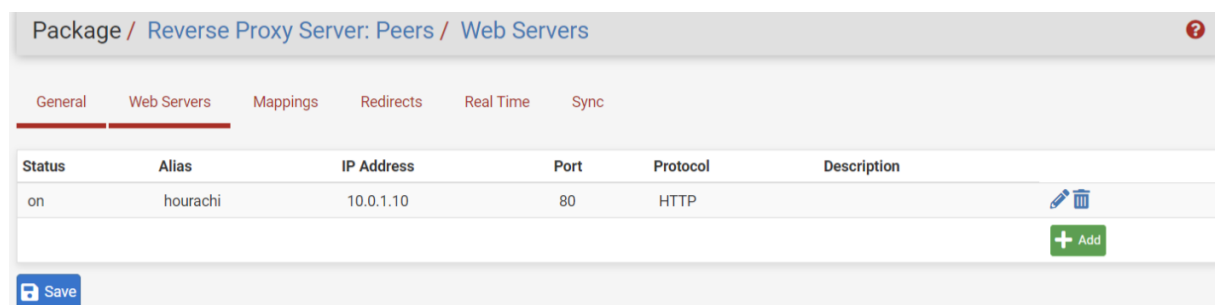
5.1

- On va dans System > Advanced > System Tunables.
- On crée une nouvelle entrée et dans tunable : net.inet.ip.portrange.reservedhigh et dans Value : 1 puis description : Reverse proxy
- On clique sur Enregistrer.

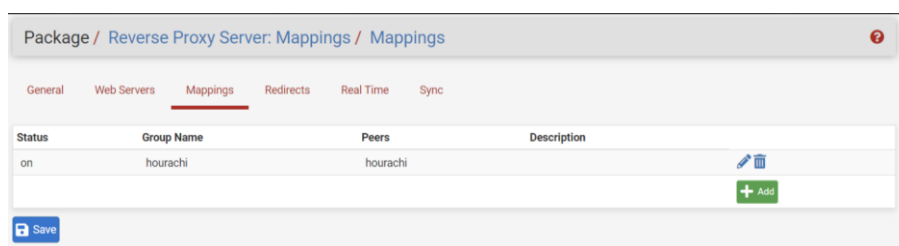
Configuration du reverse proxy et du HTTPS dans le firewall

Dans pfSense, on va dans « Squid reverse proxy » (Squid avait déjà installé lors du labo précédent)

- On accède à Services > Squid Reverse Proxy > Web Servers.
- On clique sur Ajouter.
- Active la case Enable This Peer.
- Dans Peer Alias, entre le nom de domaine de votre site web. <hourachi>
- Dans Peer IP, entre l'adresse IP privée de votre serveur web. 10.0.1.10
- Dans Peer Port, entre le port d'écoute de votre serveur web (généralement 80 ou 443).
- Dans Peer Protocol, sélectionne HTTP
- Dans Peer Description, entre un nom descriptif pour notre site web.
- Clique sur save.



- Sur la même page, on va dans Mappings > add.
- Dans Group Name, on entre le nom de domaine complet. hourachi
- Dans peers, on sélectionne le serveur web qu'on a créé à l'étape précédente.
- Dans l'URI on entre l'adresse IP public du WAN 10.102.3.6
- Dans l'URI entrez le nom de domaine www.hourachi.eu
- On clique sur save.

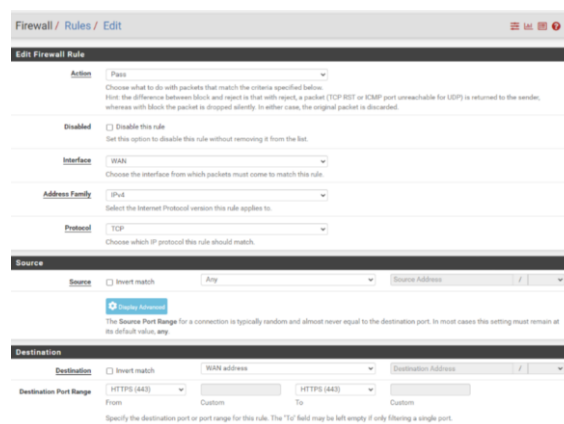


Autorisation du flux HTTPS dans le pare-feu:

Dans le menu, on clique sur Firewall > rules > WAN > add.

6.1

- Dans Action, on sélectionne pass.
- Dans Interface, on sélectionne WAN.
- Dans Protocol, on sélectionne TCP.
- Dans source : Any
- Dans destination, on sélectionne WAN adresse
- Dans Destination Port Range on sélectionne HTTPS
- Et on save.



Création d'une autorité de certification SSL:

- Allez dans System > Certificate > Authorities > add.
- On configure les paramètres selon nos besoins et on clique sur save.
- Génération d'un certificat SSL:
- On bascule vers Certificates > Add/Sign.
- On peut maintenant soit importer un certificat existant soit en générer un nouveau.
- Ici, on en génère un nouveau.
- Une fois créé, le certificat apparait dans la liste.

Certificates					
Name	Issuer	Distinguished Name	In Use	Actions	
GUI default (65d0736dd127d) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65d0736dd127d Valid From: Sat, 17 Feb 2024 08:50:54 +0000 Valid Until: Fri, 21 Mar 2025 08:50:54 +0000	webConfigurator Squid (1)		
HourachiCertificate User Certificate CA: No Server: No	HourachiCertificate	CN=www.hourachi.eu Valid From: Mon, 13 May 2024 19:30:47 +0000 Valid Until: Thu, 11 May 2024 19:30:47 +0000			

Ajout du certificat dans Squid Reverse Proxy:

- On accède à Services > Squid Reverse Proxy > General.
- Dans External FQDN, entrez votre nom de domaine complet. <www.hourachi.eu>
- On active l'option Enable HTTPS Reverse Proxy.
- On entre 443 comme Reverse HTTPS Port.

- Dans Reverse SSL Certificate, on sélectionne le certificat créé à l'étape précédente.
- Et dans « Ignore Internal Certificate Validation » on coche la case
- Cliquez sur save.

User Defined Reverse Proxy IPs
Squid will additionally bind to these user-defined IPs for reverse proxy operation. Separate entries by semi-colons (;) ⓘ

External FQDN
www.hourschi.eu
The external fully qualified domain name of the WAN IP address.

Reset TCP Connections on Unauthorized Requests
☐ If checked, the reverse proxy will reset the TCP connection if the request is unauthorized.

Squid Reverse HTTP Settings

Enable HTTP Reverse Proxy
☒ If checked, the proxy server will act in HTTP reverse mode.
Important: You must add a proper firewall rule with destination matching the 'Reverse Proxy Interface(s)' address.

Reverse HTTP Port
80
This is the port the HTTP reverse proxy will listen on. Default: 80

Reverse HTTP Default Site

This is the HTTP reverse proxy default site. Leave empty to use 'External FQDN' value specified above.

Squid Reverse HTTPS Settings

Enable HTTPS Reverse Proxy
☒ If checked, the proxy server will act in HTTPS reverse mode.
Important: You must add a proper firewall rule with destination matching the 'Reverse Proxy Interface(s)' address.

Reverse HTTPS Port
443
This is the port the HTTPS reverse proxy will listen on. Default: 443

Reverse HTTPS Default Site

This is the HTTPS reverse proxy default site. ⓘ

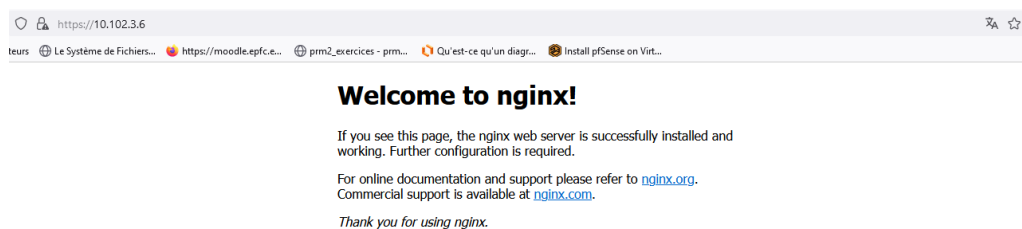
Reverse SSL Certificate
certificatHourschi
Choose the SSL Server Certificate here.

Intermediate CA Certificate (if Needed)

Paste a signed certificate in X.509 PEM format here.

Ignore Internal Certificate Validation
☒ If checked, internal certificate validation will be ignored.

On se connecte au browser en https depuis le WAN :



Serveur DNS BIND

BIND est un serveur DNS permettant de convertir des noms de domaine en adresses IP. Il est largement utilisé pour sécuriser les réseaux. Dans le cadre de pfSense, nous allons installer ce module pour configurer notre propre serveur DNS interne. Cela nous permettra de mettre en place un DNS autoritaire sur pfSense. Le port d'écoute sera configuré sur le WAN pour recevoir des requêtes externes vers le DNS autoritaire.

Installation du module Bind

Pour installer le module Bind, on suit ces étapes :

- On accède à l'interface Web de pfSense.
- On va dans Système > Gestionnaire de paquets > Paquets disponibles.
- On recherche "bind" et on clique sur Installer.

Création d'une vue

Une vue détermine comment le serveur DNS répond aux requêtes, en fonction de leur origine (interne ou externe). Pour notre cas, aucune configuration particulière n'est requise. Pour créer une vue, suivez ces étapes :

8.1

On accède à Services > BIND > Vues.

Dans Nom de la vue, saisissez "hourachi.eu".

Dans Correspondance des clients, sélectionnez Any.

Dans Autoriser la récursivité, sélectionnez None.

Services / Bind / Edit / Views

Settings ACLs Views Zones Sync

General Options

View Name hourachi.eu
Enter the name of the View.

Description
Enter a description of the View.

Recursion No
A recursive query occurs when your DNS server is queried for a domain that it currently knows nothing about, in which case it will try to resolve the given host by performing further queries (e.g. by starting at the root servers and working out, or by simply passing the request to yet another DNS server).

match-clients any
none
any
localhost
localnets
If either or both of match-clients are missing they default to any (all hosts match).
The match-clients statement defines the address_match_list for the source IP address of the incoming messages.

allow-recursion none
any
localhost
localnets
For example, if you have one DNS server serving your local network, you may want all of your local computers to use your DNS server.

Création d'une zone DNS

Une zone DNS correspond à notre nom de domaine, dans ce cas "hourachi.eu". Sa création permet d'améliorer la convivialité, la gestion et la sécurité du réseau. Pour la créer, on procède comme suit :

On accède à Services > BIND > Zones.

Dans Nom de zone, on saisit "hourachi.eu".

Dans Type de zone, sélectionne Master.

Dans Serveur de noms, saisit "ns".

Dans allow-query : any

Dans Enregistrements de domaine de zone, on ajoute les enregistrements suivants :

Record : www

Type : A (Adresse)

Alias ou adresse IP : 10.102.3.9 (adresse IP du pare-feu)

Services / Bind / Zones

Settings ACLs Views Zones Sync

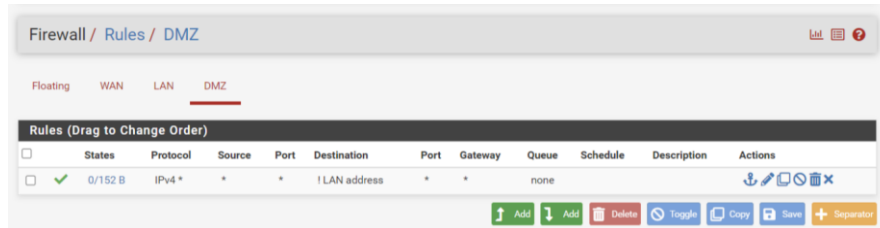
Status	Name	Type	View(s)	Serial	Description
Enabled	hourachi.eu	master	HourachiView	2714212157	

+ Add

Séparation des réseaux LAN et DMZ

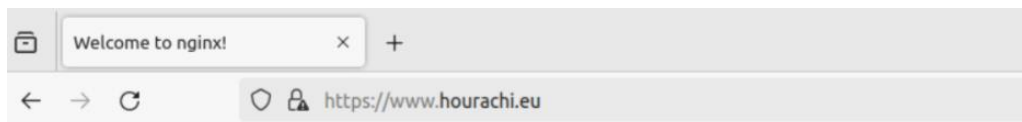
Séparer un réseau LAN et une DMZ est essentiel pour protéger les systèmes internes critiques des attaques externes, en contrôlant strictement le trafic entre eux et en réduisant la surface d'attaque. Cette séparation permet également de faciliter la gestion des incidents.

Et pour séparer les réseaux, on est retourné dans rules > firewall > DMZ et on a modifié la règle qu'on avait créé au début du labo et en destination on a coché « invert match » et on a sélectionné LAN adress



Conclusion :

Dans ce laboratoire, nous avons mis en place une DMZ pour ajouter une couche de sécurité supplémentaire au réseau, en isolant les services accessibles depuis l'extérieur des réseaux internes. Nous avons installé Ubuntu Server, configuré le firewall et le serveur DHCP pour la DMZ, et mis en place l'accès à Internet depuis cette zone. Ensuite, nous avons installé Docker et configuré un serveur NGINX pour héberger une application web. Nous avons également configuré pfSense pour permettre l'accès au serveur web depuis l'extérieur via un reverse proxy sécurisé avec HTTPS, en utilisant un certificat SSL généré. Enfin, nous avons installé et configuré BIND pour créer un serveur DNS autoritaire interne. Cette séparation entre le LAN et la DMZ protège les systèmes internes des attaques externes et facilite la gestion des incidents, assurant une sécurité et une gestion optimales du réseau.



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Index des commentaires

- 1.1 Il me semble que votre DNS autoritaire tourne sur le FW?
- 2.1 Vous n'avez pas du ajouter une interface au firewall?
- 2.2 Un range de quoi? DHCP!
- 2.3 Vous avez vérifier que c'était bon? Si oui, une capture de la commande "ip a" du serveur aurait été pertinente.
- 3.1 Peut-être intéressant de préciser que sans règle, le firewall bloque tout.
- 3.2 Et montrer que cela fonctionne (ping vers l'internet depuis le serveur...)
- 3.3 Que fait la commande exactement?
- 4.1 Quel port? A quoi ça sert?
- 4.2 Pourquoi on ajoute un reverse proxy ici?
- 5.1 Précisez pourquoi vous avez du faire cette manipulation.
- 6.1 A quoi cela sert?
- 8.1 Ben si! recursion NO!