LYCÉE LOUIS PERGAUD
BTS SIO 2

SEPTEMBRE
2025

COMPTE RENDU

Mise en place d'un PortForward sur pare-feu OPNSENSE

RÉALISÉ PAR
GENSSE Mathéo

LYCÉELOUISPERGAUD

SOMMAIRE

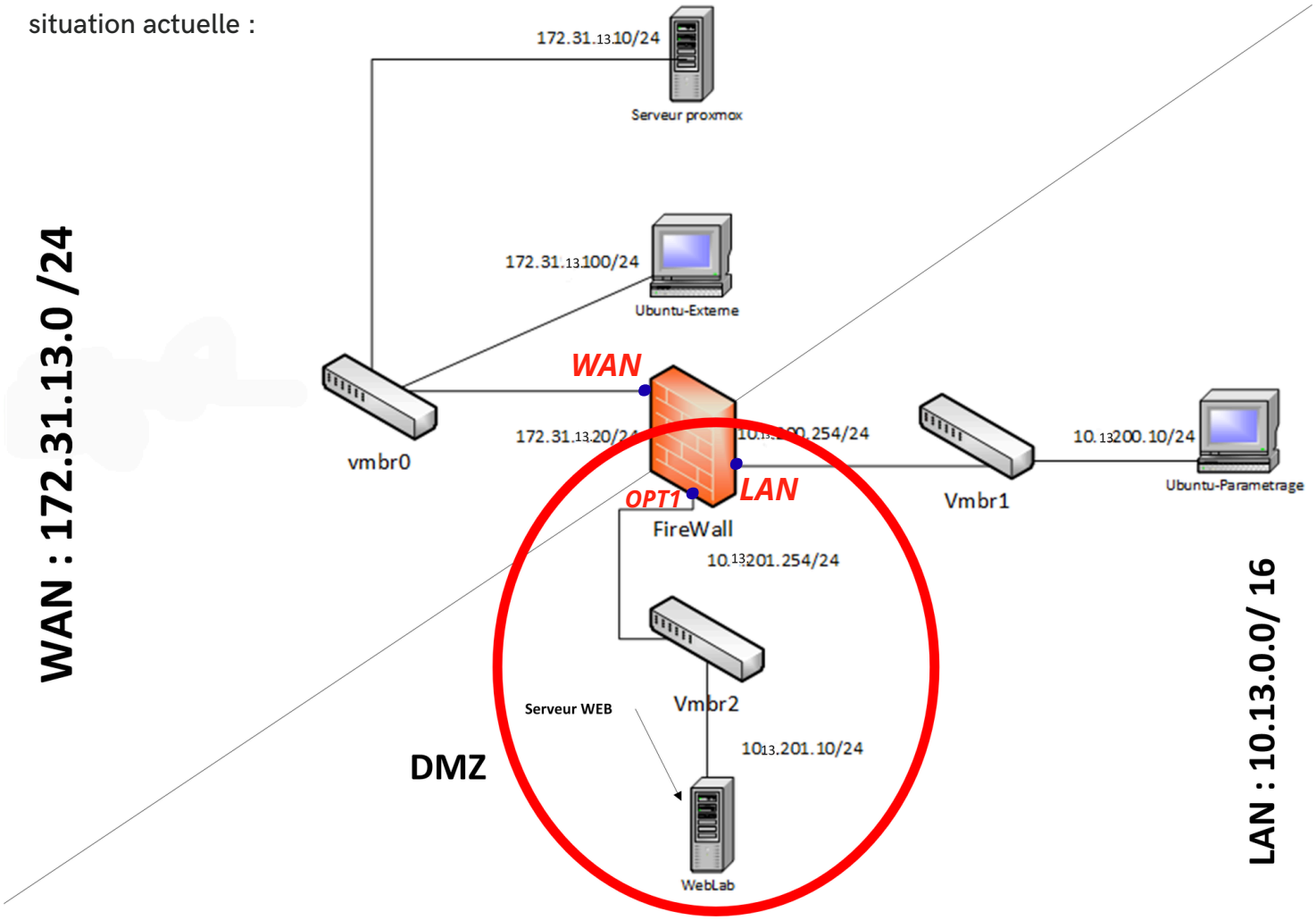
Définition des objectifs et schématisation de la situation		3
Qu'est-ce que le Port Forwarding et à quoi sert-il ?		4
Mise en place d'un Port Forwarding sur OPN Sense		5
	Mise en contexte	6
	Accès à l'interface OPNSense	7
	Vérification des interfaces réseau	8
	Accorder l'accès à Internet au serveur	9
	Ajout de la règle de redirection de port	10
Vérification du bon fonctionnement via une capture de trames		11
Conclusion		16

MISE EN PLACE D'UN PORTFORWARD SUR PARE-FEU OPNSENSE

DÉFINITION DES OBJECTIFS ET SCHÉMATISATION DE LA SITUATION

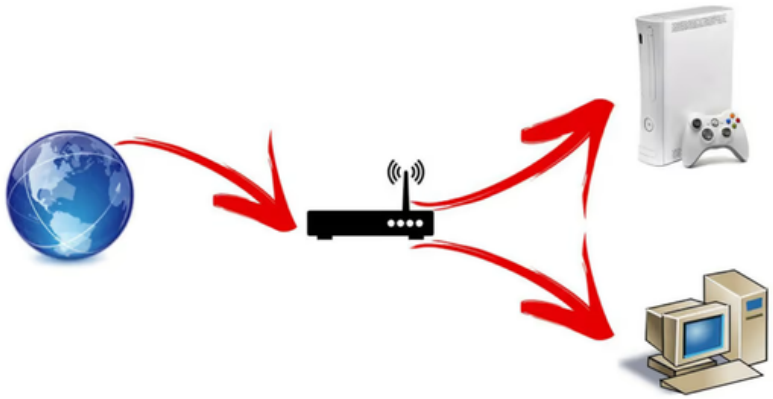
Dans ce compte rendu, nous allons chercher à comprendre le fonctionnement du port forwarding (ou redirection de port en français) ainsi que sa mise en place sur un pare-feu de type OPNsense.

L'objectif principal de ce travail est d'apprendre à configurer une zone démilitarisée (DMZ), dans laquelle l'ensemble du trafic destiné à un port spécifique du pare-feu sera redirigé vers une machine unique. Dans notre cas, il s'agira d'un serveur web. Pour comprendre tout cela, schématisons la situation actuelle :



MISE EN PLACE D'UN PORTFORWARD SUR PARE-FEU OPNSENSE

QU'EST-CE QUE LE PORT FORWARDING ET À QUOI SERT-IL ?



Le Port Forwarding, aussi appelé redirection de port, est une technique de configuration d'un routeur ou d'un pare-feu. Elle consiste à diriger le trafic entrant reçu sur un port précis de l'adresse publique (WAN) du réseau vers un appareil spécifique du réseau local (LAN). Par exemple, si un routeur reçoit des données sur le port 80, il peut les rediriger vers un ordinateur interne qui héberge un site web, comme on va le mettre en place dans le cas qui va suivre.

Cette technique est particulièrement utile lorsqu'on souhaite rendre accessible depuis l'extérieur un service qui fonctionne normalement uniquement à l'intérieur du réseau local. Grâce au Port Forwarding, il devient possible d'héberger un serveur web, un serveur de jeux en ligne, une caméra de surveillance ou tout autre service directement depuis chez soi, tout en permettant aux utilisateurs distants de s'y connecter.

Peut s'ajouter à cela la mise en place d'une DMZ (Demilitarized Zone), qui consiste à isoler un appareil ou un service accessible depuis l'extérieur dans une zone distincte du réseau local. Cette configuration permet de renforcer la sécurité, car même si le service exposé venait à être compromis, l'attaquant n'aurait pas accès directement aux autres machines du réseau interne.

MISE EN PLACE D'UN PORT FORWARDING SUR OPN SENSE

Mise en contexte

Avant de commencer la mise en place, récapitulons la situation… Au cours de ce travail, on partira du principe que les configurations de base des éléments ont bien été réalisées.

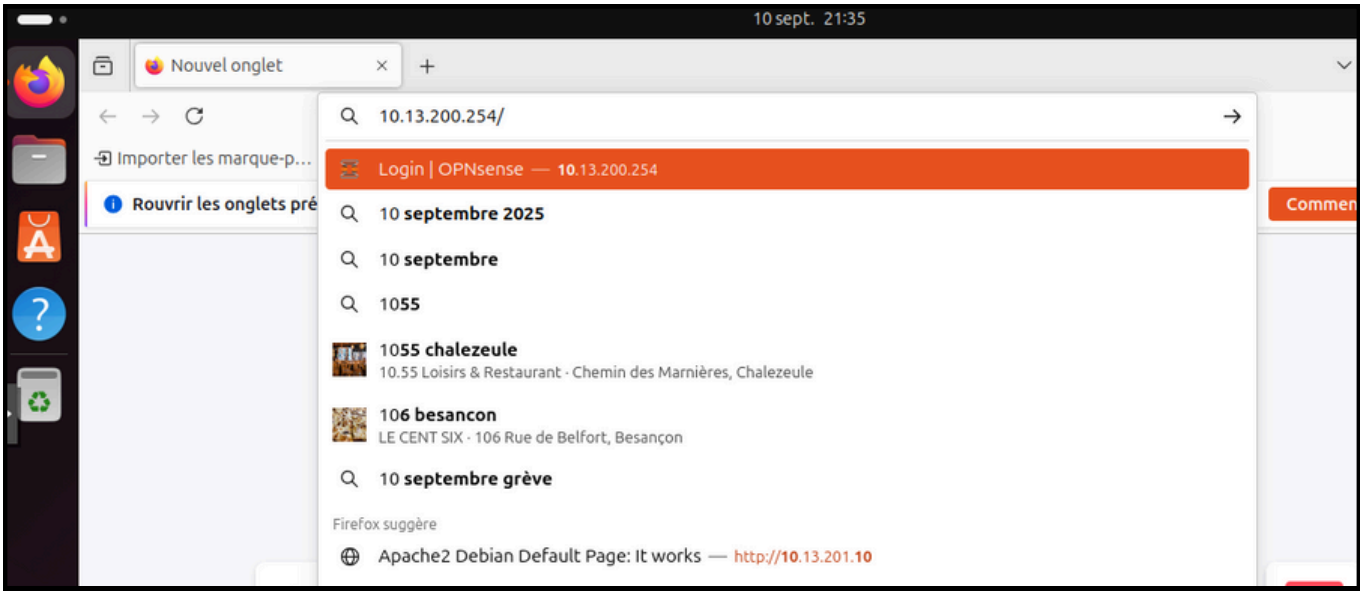
On possède… et on aura besoin… de :

- Un réseau LAN d'adresse 10.13.0.0 /16 divisé en deux sous-réseaux :
  - La DMZ d'adresse 10.13.201.0 /24 dont les occupants possèdent pour passerelle 10.13.201.254, qui est associée à l'interface OPT1 du FireWall ayant pour carte réseau vmbr2.
  - Le LAN d'adresse 10.13.200.0 /24 dont les occupants possèdent pour passerelle 10.13.200.254, qui est associée à l'interface LAN du FireWall ayant pour carte réseau vmbr1.
- Un réseau WAN d'adresse 172.31.13.0 /24 dont les occupants possèdent pour passerelle 172.31.13.254. MAIS… leurs cartes réseaux se trouvent sur le même réseau que l'interface WAN du FireWall ayant pour adresse 172.31.13.20. Il s'agit là de la carte réseau vmbr0.
- Un serveur WEB Apache2 qui se situe dans la DMZ du LAN et qui possède pour adresse 10.13.201.10. Le contenu WEB de ce serveur est donc accessible via HTTP sur le port 80 par tous les membres du réseau LAN 10.13.0.0 /16.
- Un poste se situant dans le réseau LAN et qui possédera l'adresse 10.13.200.10, qui nous permettra de manipuler le pare-feu depuis son interface WEB.
- Un poste se situant sur le réseau WAN 172.31.13.0 /24 ayant pour adresse 172.31.13.100, qui est en capacité de communiquer avec le FireWall via son interface WAN (172.31.13.20), mais qui, vous l'aurez compris, n'a pas la possibilité de communiquer avec les machines du réseau LAN 10.13.0.0 /16. L'objectif sera donc… si vous avez suivi… d'être en capacité, pour ce poste, d'entrer en contact avec le serveur WEB et uniquement le serveur WEB de ce réseau.

Enfin, inutile de préciser que nous aurons besoin d'un FireWall OPNsense. Il est le cœur de notre sujet. Si tout cela vous paraît abstrait, référez-vous au schéma en page 3.

MISE EN PLACE D'UN PORT FORWARDING SUR OPN SENSE

Accès à l'interface OPNSense



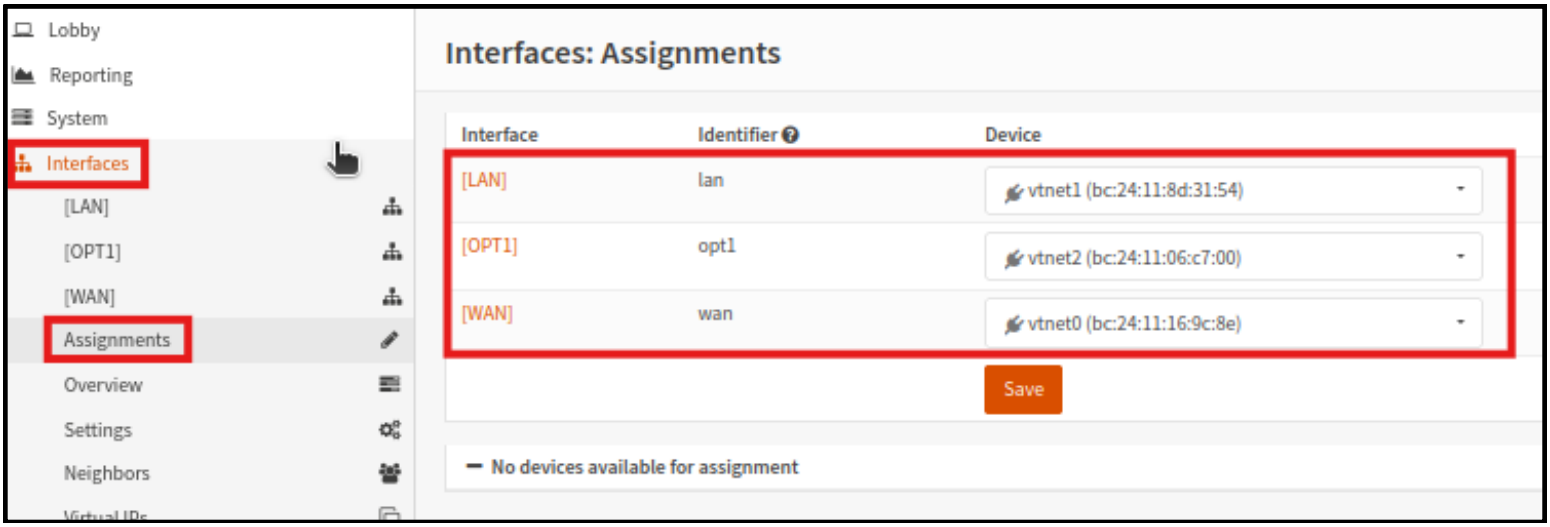
Pour mettre en place la redirection de port, rendez-vous tout d'abord sur votre poste/VM Ubuntu-Parametrage (10.13.200.10), puis ouvrez un navigateur.

Entrez l'adresse du FireWall, qui correspond à l'adresse de l'interface du réseau, donc ici LAN avec pour adresse 10.13.200.254.

La page de connexion OPNsense vous sera proposée, entrez alors les identifiants de connexion :
ID : root
MDP : root
Vous sera affiché ensuite le tableau de bord du FireWall.

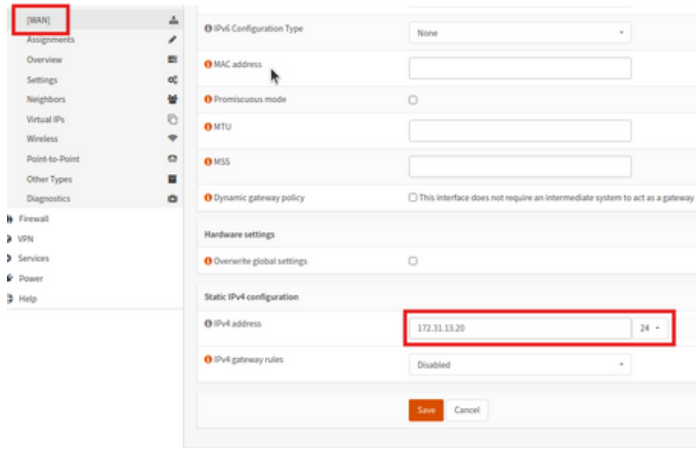
MISE EN PLACE D'UN PORT FORWARDING SUR OPN SENSE

Vérification des interfaces réseau



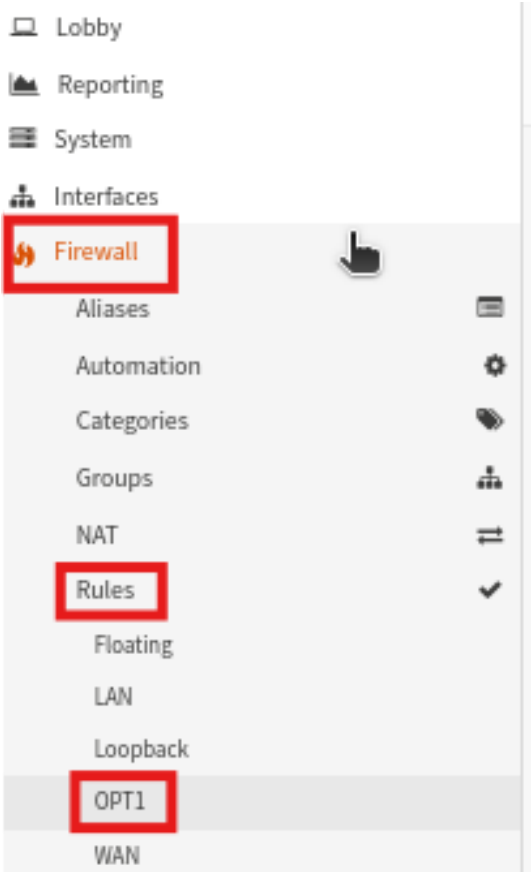
Avant toute chose, commencez par vérifier que vous possédez bien les 3 interfaces citées précédemment et qu'elles sont associées aux bonnes cartes réseaux. Le cas échéant, ajustez la configuration à votre guise.

N'hésitez pas à jeter un coup d'œil aux adresses IP associées aux interfaces. Il peut y avoir des erreurs.



MISE EN PLACE D'UN PORT FORWARDING SUR OPN SENSE

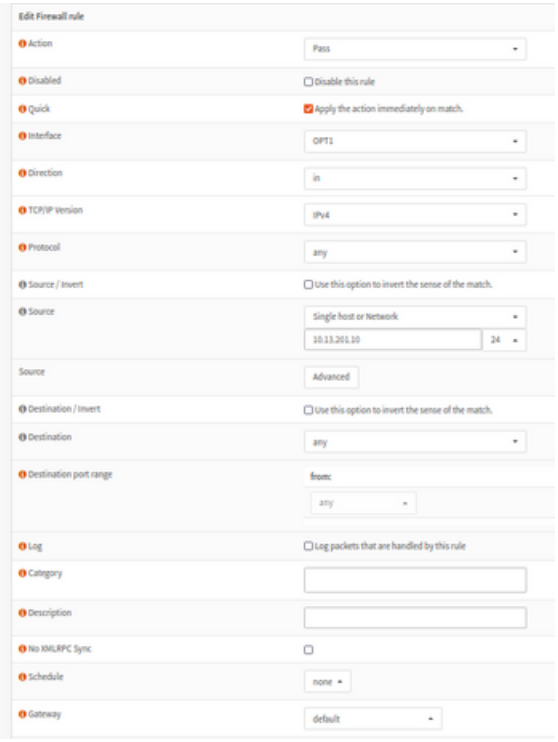
Accorder l'accès à Internet au serveur



En effet, pour que le serveur web renvoie son contenu à un client, il doit avant tout déjà lui-même être en capacité de sortir de son réseau DMZ. Pour cela, il faut donc ajouter une règle qui autorise les trames qui entrent sur OPT1 à passer de l'autre côté du FireWall.

Pour ceci, se rendre dans FireWall → Rules → OPT1, puis cliquer sur le + pour ajouter une règle et remplir comme ci-dessous :

N'OUBLIEZ PAS D'APPLIQUER LES CHANGEMENTS

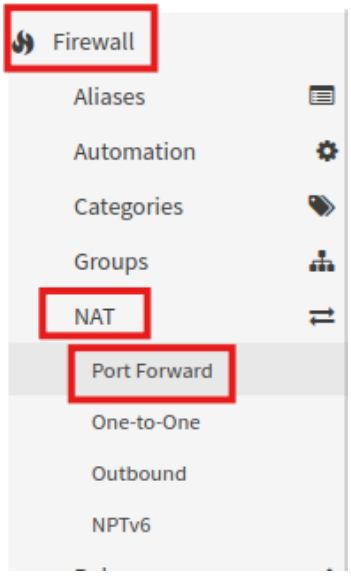


→ À NOTER : Il est également possible de n'entrer aucune IP, dans notre cas ça n'a pas vraiment de valeur. Cela indiquerait seulement au FireWall d'autoriser toutes les IP à passer sur l'interface OPT1.

MISE EN PLACE D'UN PORTFORWARD SUR PARE-FEU OPNSENSE

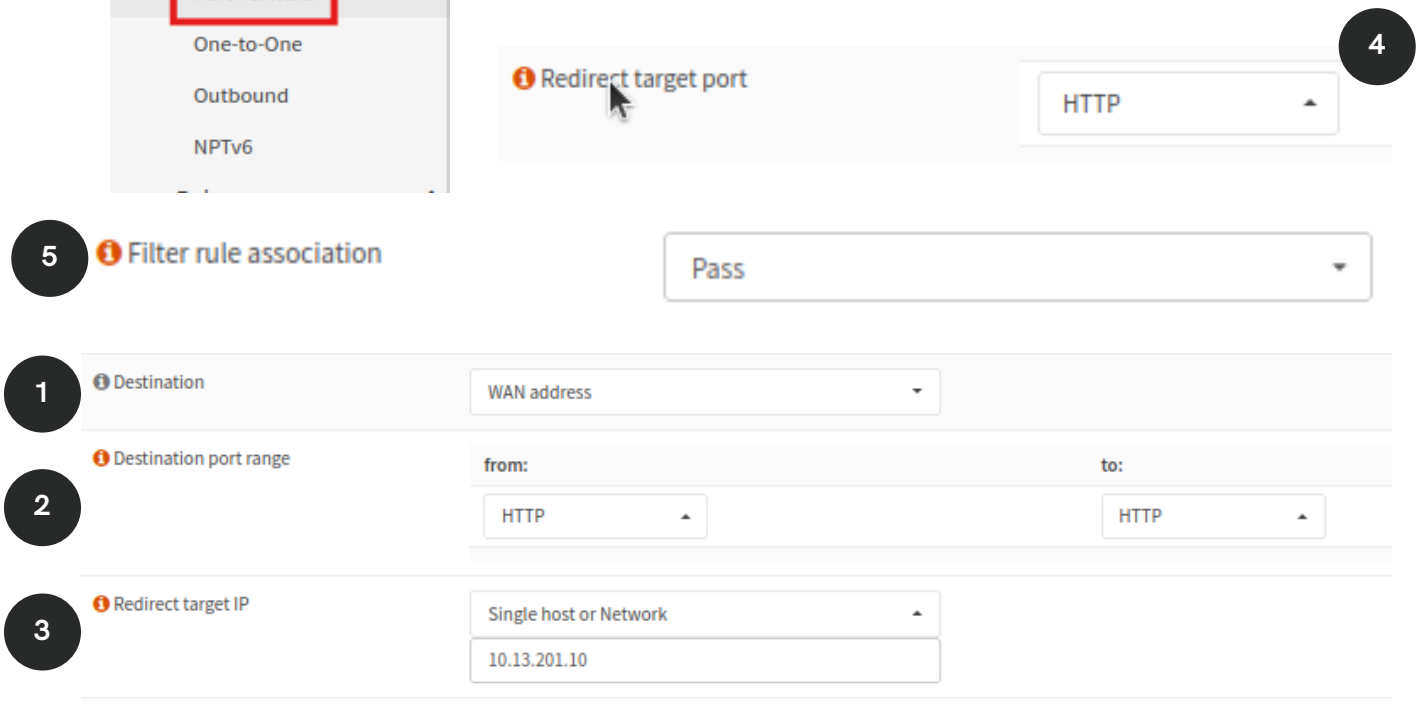
MISE EN PLACE D'UN PORT FORWARDING SUR OPN SENSE

Ajout de la règle de redirection de port



Pour mettre en place la redirection de port qui va permettre d'accéder au contenu du serveur WEB depuis le WAN, on va se rendre dans la section FireWall de l'OPNsense, puis NAT → Port Forward. Ensuite, cliquer sur le + pour ajouter une redirection de port.

Remplir les champs suivants :



MISE EN PLACE D'UN PORT FORWARDING SUR OPN SENSE

Ajout de la règle de redirection de port

Expliquons ce que fait chacun de ces paramètres :

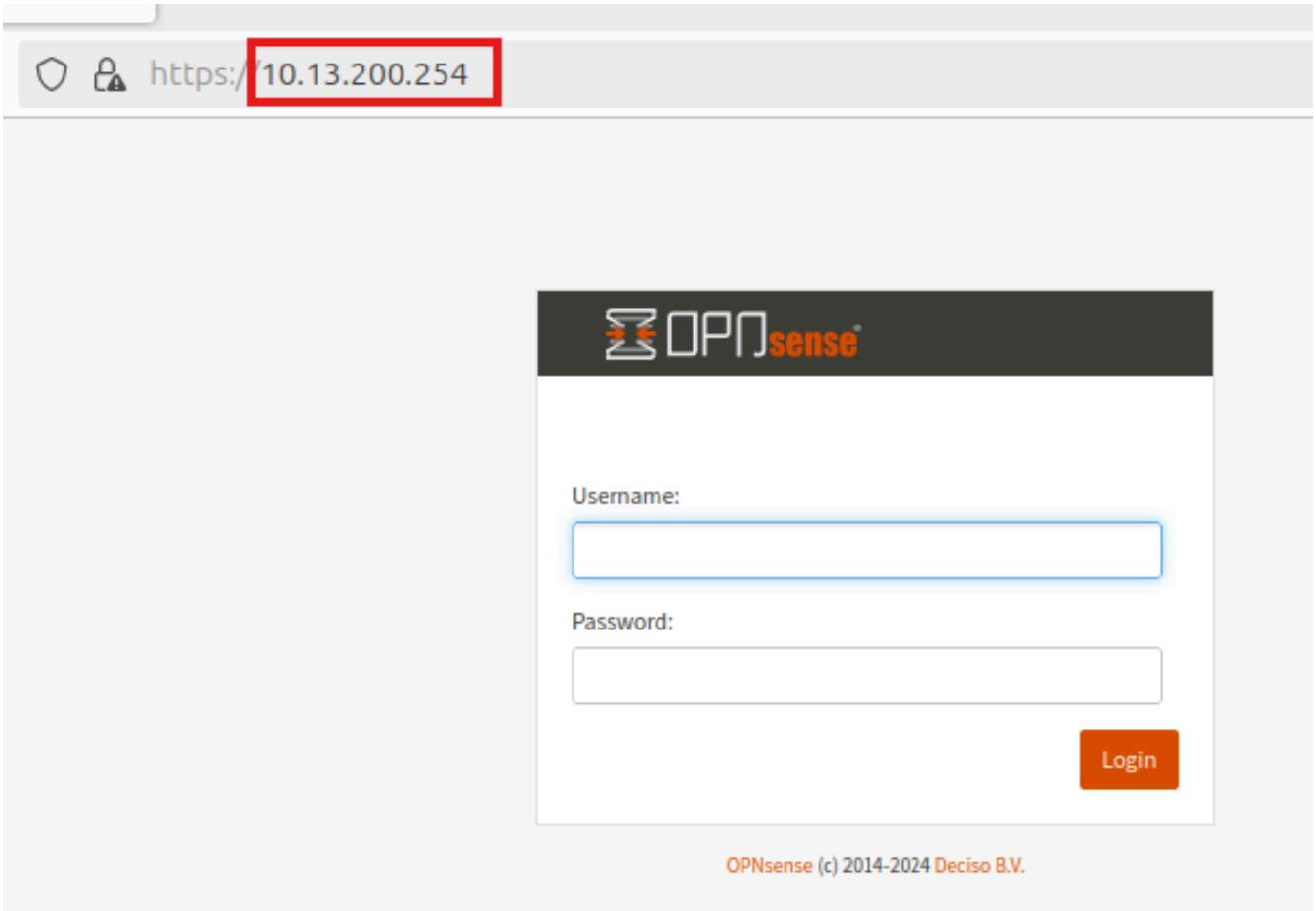
1. On définit sur quelle interface du pare-feu la trame qui va être redirigée arrive. Ici, elle arrive sur l'interface WAN.
2. On spécifie le port d'arrivée sur le pare-feu et le port de destination sur l'hôte de destination. Donc tout le trafic HTTP sera redirigé sur le port HTTP (80) du serveur WEB.
3. On dit où on redirige le paquet, sur un hôte (le serveur web), puis on indique son adresse IP.
4. On indique le port cible sur l'hôte cible, donc le HTTP, car on veut accéder au service WEB d'Apache2 qui se trouve sur le port 80 (HTTP).
5. On règle le trafic sur Pass pour permettre le passage/transfert des paquets.

On a maintenant mis en place la redirection de port. Donc, lorsque l'on entre l'adresse IP de l'interface WAN du pare-feu dans un navigateur WEB, le paquet arrive sur le port 80 (HTTP) et est redirigé sur le port HTTP (80) du serveur WEB. Le serveur WEB, grâce à son accès à Internet configuré précédemment, lui permet de renvoyer le contenu au client émetteur de la requête HTTP.

VÉRIFICATION DU BON FONCTIONNEMENT VIA UNE CAPTURE DE TRAMES

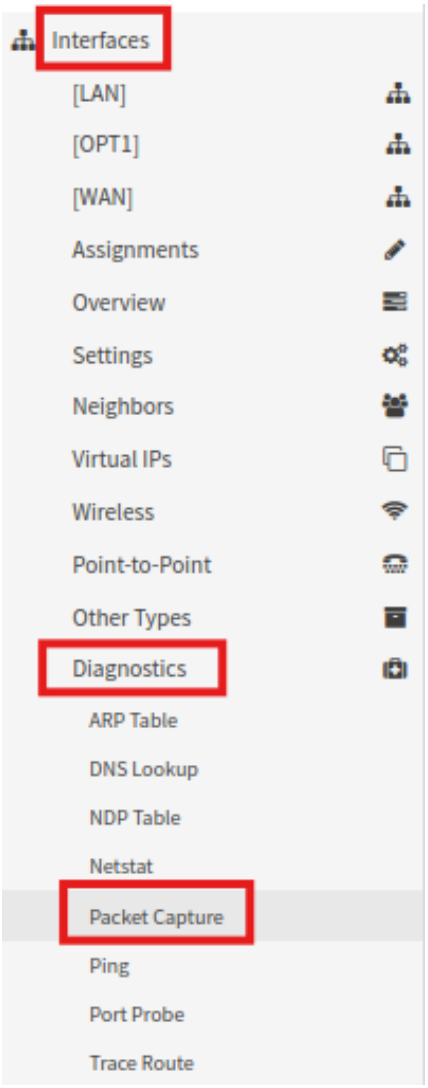
Maintenant que nous avons réussi à mettre en place notre redirection de port, prouvons donc qu'elle fonctionne bien, et ce grâce à une capture de trame. Pour ce faire, nous réaliserons les étapes qui suivent.

Ouvrir la Ubuntu-Paramétrage, puis se rendre sur l'interface du FireWall et se connecter (root/root):

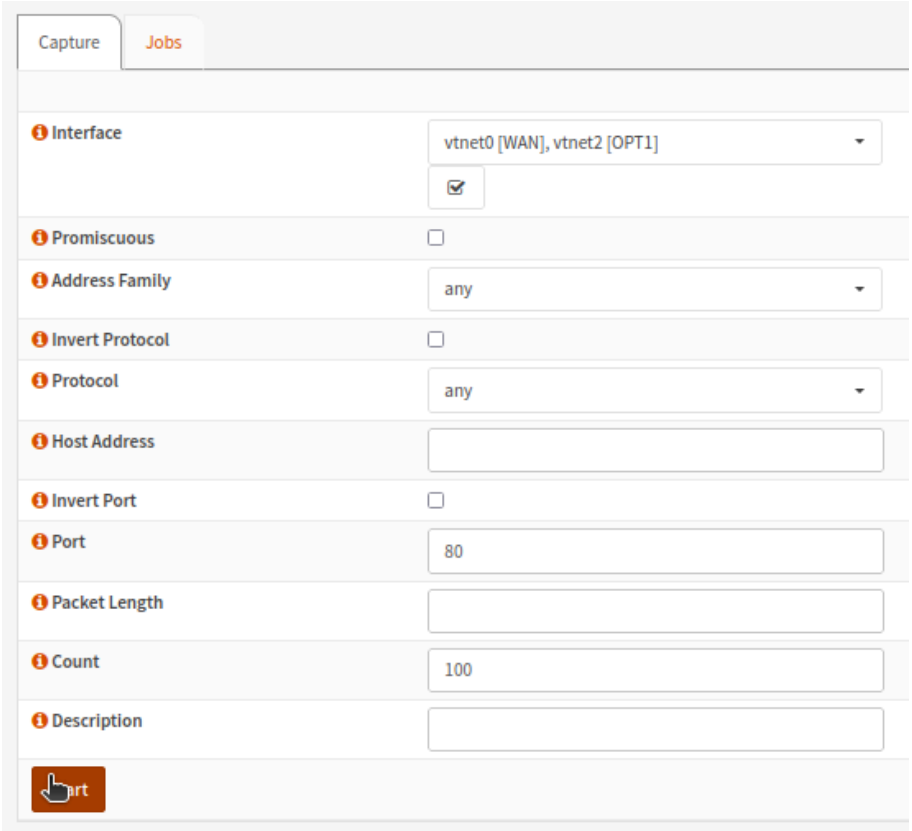


VÉRIFICATION DU BON FONCTIONNEMENT VIA UNE CAPTURE DE TRAMES

Se rendre ensuite dans Interfaces > Diagnostics > Packet Capture :



Remplissez ensuite comme ci dessous :



MISE EN PLACE D'UN PORTFORWARD SUR PARE-FEU OPNSENSE

VÉRIFICATION DU BON FONCTIONNEMENT VIA UNE CAPTURE DE TRAMES

Je m'explique :

1 - On note les interfaces sur lesquelles va transiter le paquet, donc WAN et OPT1, car le paquet arrive du réseau 172.31.0.0/16 et est redirigé vers le serveur WEB se situant dans le vtnet2 (OPT1).

2 - On entre le port 80, car il s'agit de requêtes HTTP arrivant sur le port HTTP du FireWall et étant redirigées sur le port HTTP du serveur WEB.

ATTENTION :

Avant de lancer la capture, veillez à avoir préparé votre autre poste/VM (Debian Externe) et à avoir une requête HTTP en direction du FireWall (interface WAN 172.31.13.20) prête à partir.

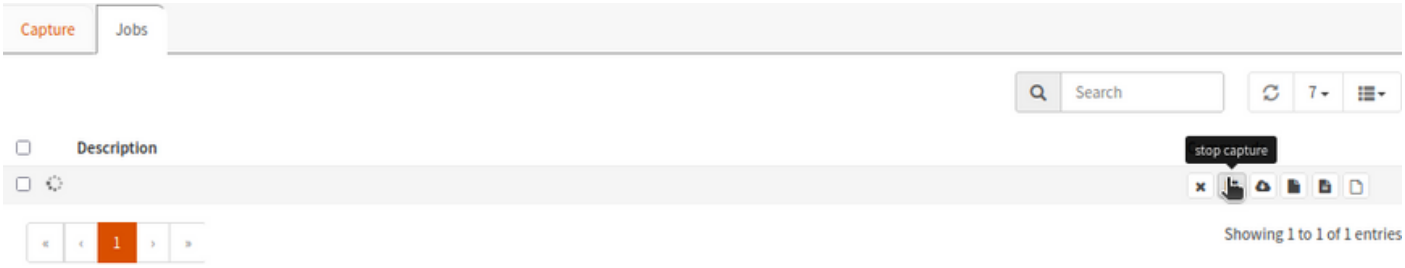
Lancer maintenant la capture avec START : Start

Dans la foulée, exécuter la requête HTTP en direction de 172.31.13.20 :

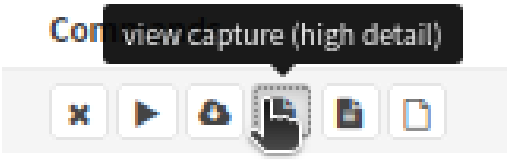
MISE EN PLACE D'UN PORTFORWARD SUR PARE-FEU OPNSENSE

VÉRIFICATION DU BON FONCTIONNEMENT VIA UNE CAPTURE DE TRAMES

Arrêtez ensuite la capture de trame sur le FireWall depuis l'interface WEB :



Affichez donc maintenant le contenu de la capture en cliquant sur View Capture :



On remarque ci-dessous que la trame HTTP a bien été reçue sur WAN (172.31.13.20) à 13:46:22 et qu'elle provenait de 172.31.13.100.

```
WAN     2025-09-12      bc:24:11:4d:f9:10 bc:24:11:16:9c:8e ethertype IPv4 (0x0800), length 511: (tos 0x0, ttl 64, id 21252, offset 0, flags [DF], proto TCP (6), length
vtnet0  13:46:22.332529                                     497)
    172.31.13.100.49118 > 172.31.13.20.80: Flags [P.], cksum 0x6516 (correct), seq 1:446, ack 1, win 502,
options [nop,nop,TS val 3240301958 ecr 1219586042], length 445: HTTP, length: 445
        GET / HTTP/1.1
        Host: 172.31.13.20
        User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
        Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
        Accept-Encoding: gzip, deflate
        Connection: keep-alive
        Upgrade-Insecure-Requests: 1
        If-Modified-Since: Wed, 10 Sep 2025 09:08:28 GMT
        If-None-Match: "29cd-63e6ec3955966-gzip"
        Priority: u=0, i
```

VÉRIFICATION DU BON FONCTIONNEMENT VIA UNE CAPTURE DE TRAMES

Puis, sur la trame qui suit, on voit que le FireWall a compris qu'il s'agissait d'une requête sur le port 80 et qu'il doit donc la transmettre au serveur 10.13.201.10, et que la requête provenait bien de 172.31.13.100.

```
OPT1    2025-09-12      bc:24:11:06:c7:00 bc:24:11:46:dd:af ethertype IPv4 (0x0800), length 511: (tos 0x0, ttl 63, id 21252, offset 0, flags [DF], proto TCP (6), length
vtnet2  13:46:22.332537                                     497)
    172.31.13.100.49118 > 10.13.201.10.80: Flags [P.], cksum 0x4b32 (correct), seq 1:446, ack 1, win 502,
options [nop,nop,TS val 3240301958 ecr 1219586042], length 445: HTTP, length: 445
        GET / HTTP/1.1
        Host: 172.31.13.20
        User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
        Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
        Accept-Encoding: gzip, deflate
        Connection: keep-alive
        Upgrade-Insecure-Requests: 1
        If-Modified-Since: Wed, 10 Sep 2025 09:08:28 GMT
        If-None-Match: "29cd-63e6ec3955966-gzip"
        Priority: u=0, i
```

Et donc ensuite on voir la trame que le serveur renvoie au poste client :

```
OPT1    2025-09-12      bc:24:11:46:dd:af bc:24:11:06:c7:00 ethertype IPv4 (0x0800), length 1514: (tos 0x0, ttl 64, id 2475, offset 0, flags [DF], proto TCP (6), length
vtnet2  13:46:22.350258                                     1500)
    10.13.201.10.80 > 172.31.13.100.49118: Flags [.], cksum 0x7bff (correct), seq 1:1449, ack 446, win 506,
options [nop,nop,TS val 1219586060 ecr 3240301958], length 1448: HTTP, length: 1448
        HTTP/1.1 200 OK
        Date: Fri, 12 Sep 2025 13:46:22 GMT
        Server: Apache/2.4.65 (Debian)
        Last-Modified: Wed, 10 Sep 2025 09:08:28 GMT
        ETag: "29cd-63e6ec3955966-gzip"
        Accept-Ranges: bytes
        Vary: Accept-Encoding
        Content-Encoding: gzip
        Content-Length: 3041
        Keep-Alive: timeout=5, max=100
        Connection: Keep-Alive
        Content-Type: text/html
```

CONCLUSION

En étudiant la mise en place du port forwarding sur le pare-feu OPNsense, on a pu voir concrètement comment il est possible de gérer efficacement l'accès à un serveur web situé dans une zone démilitarisée (DMZ) tout en maintenant la sécurité du réseau principal. La configuration nécessite une compréhension claire des différentes étapes : définir les interfaces concernées, ouvrir les bons ports, créer des règles de redirection, puis vérifier que tout fonctionne comme prévu à l'aide de captures de trames. Cela permet de s'assurer que le trafic destiné au port 80 (HTTP) est bien redirigé vers le serveur spécifique, et que le serveur peut répondre aux requêtes provenant d'un client externe.

Ce processus démontre aussi l'importance de bien paramétrer tant les règles de redirection que celles autorisant le trafic sortant, pour éviter toute faille de sécurité ou dysfonctionnement. La vérification via l'analyse des trames a été essentielle pour confirmer que la configuration est correcte et que le flux de données circule comme prévu. En somme, cette expérience montre que la configuration d'un port forwarding n'est pas uniquement une opération technique, mais aussi un équilibre entre accessibilité et sécurité, qui demande de la rigueur et une bonne compréhension du fonctionnement des réseaux. Cela permet d'assurer que les services web peuvent être accessibles en toute sécurité aux utilisateurs externes tout en protégeant les ressources internes contre d'éventuelles menaces.