GSB

TP 10

Version <1.0>

Pare-feu pfSense

Table des matières

Pare-feu pfSense

1. Introduction

1.1 Définitions, Acronymes et Abréviations

Pare-feu : Système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne) ; -
  une interface pour le réseau externe.

pfSense : pfSense est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD. À l'origine un fork de m0n0wall, il utilise le pare-feu à états Packet Filter, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. pfSense convient pour la sécurisation d'un réseau domestique ou de petite entreprise.

TinyWeb : Permet de démarrer un serveur Web tout simple supportant les CGI, SSL mais ni SQL et ni PHP. L'idée est de proposer un serveur Web de base destiné à tester quelques pages Web ou un gestionnaire de contenu genre blog fonctionnant sans base de données comme Guppy.

Nmap : Nmap est un scanner de ports libre créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant. Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de Nmap fournit des indications sur la sécurité d'un réseau. Il est disponible sous Windows, Mac OS X, Linux, BSD et Solaris.

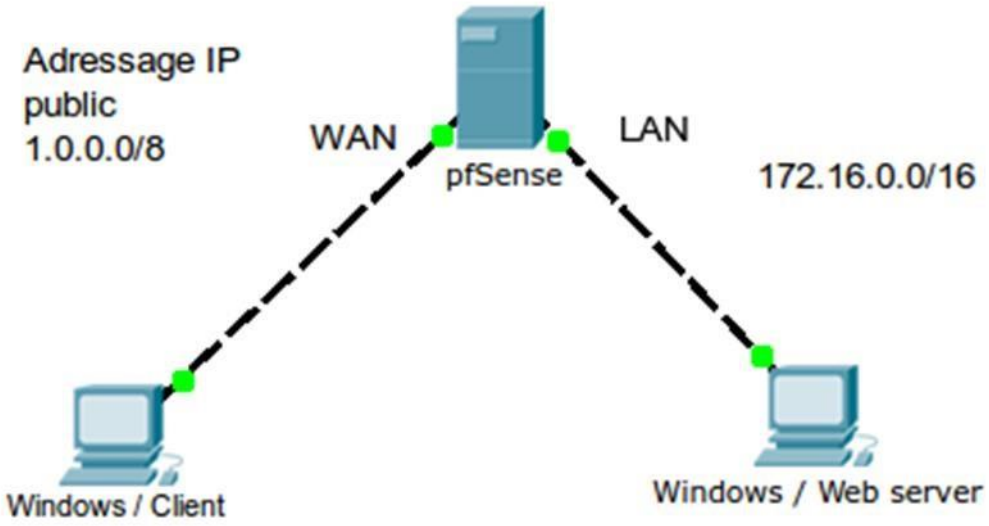
TSE (Terminal Services) : composant de Microsoft Windows (dans les versions clientes et serveur) qui permet à un utilisateur d'accéder à des applications et des données sur un ordinateur distant, via n'importe quel type de réseau. Son utilisation est optimisée sur des réseaux locaux (Local Area Network) ou régionaux Metropolitan Area Network, fournissant des meilleurs latences et débits que des réseaux plus larges comme Internet. Terminal Services consiste en la mise en œuvre par Microsoft du client léger Terminal Services, où les applications Windows ou même également le bureau entier de l'ordinateur exécutant Terminal Services sont rendus disponibles à l'aide d'un client à distance. Le client peut aussi bien être un ordinateur à part entière exécutant n'importe quel Système d'Exploitation tant que le protocole du service de Terminal est supporté, ou un ordinateur de type bare-bones assez puissant pour supporter le protocole (tel que Windows FLP). Avec les Services de Terminal, seule l'interface utilisateur d'une application est présentée au poste client. Chaque opération est redirigée au travers du réseau vers le serveur où toutes les opérations des applications sont effectuées. Le Service de Terminal représente un contraste avec les systèmes de virtualisation d'applications tel que Microsoft Softgrid, avec lesquels les applications (stockées sur un serveur central) sont diffusées sur les postes clients à la demande et ensuite gérées par le poste client.

1.2 Références

http://delphi.icm.edu.pl/ftp/d20free/tinyweb2.htm
https://tic-et-net.org/2014/04/16/tutoriel-installer-tinyweb-le-micro-serveur-web-sur-cle-usb/

2. Éléments de configuration

2.1 Schéma réseau



3. Tests / Validations

A. Pare-feu

Question 2

Sur pfSense, créer la règle de pare-feu qui laisse passer les pings.
Tester.
Relancer le nmap. Quelles différences ?

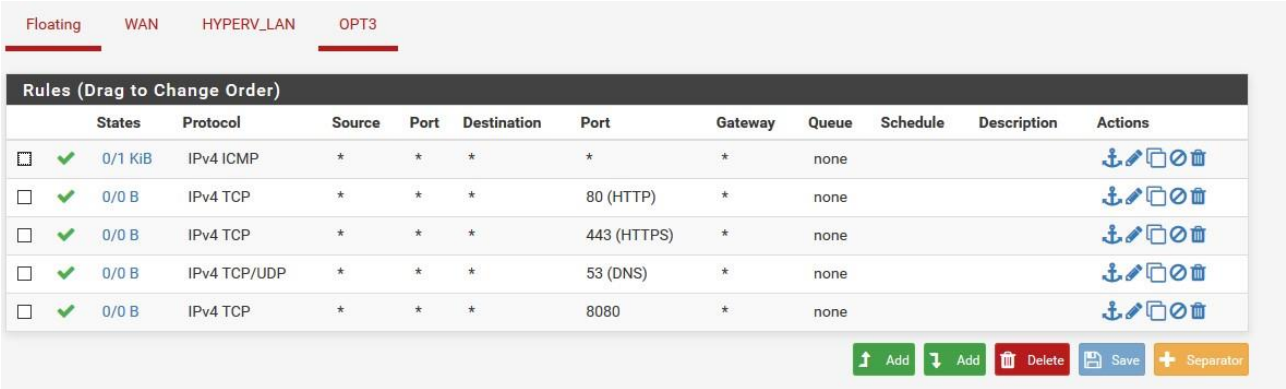
Si les pings sont désactivés sur le pare-feu, nmap considère l'autre comme inactif.

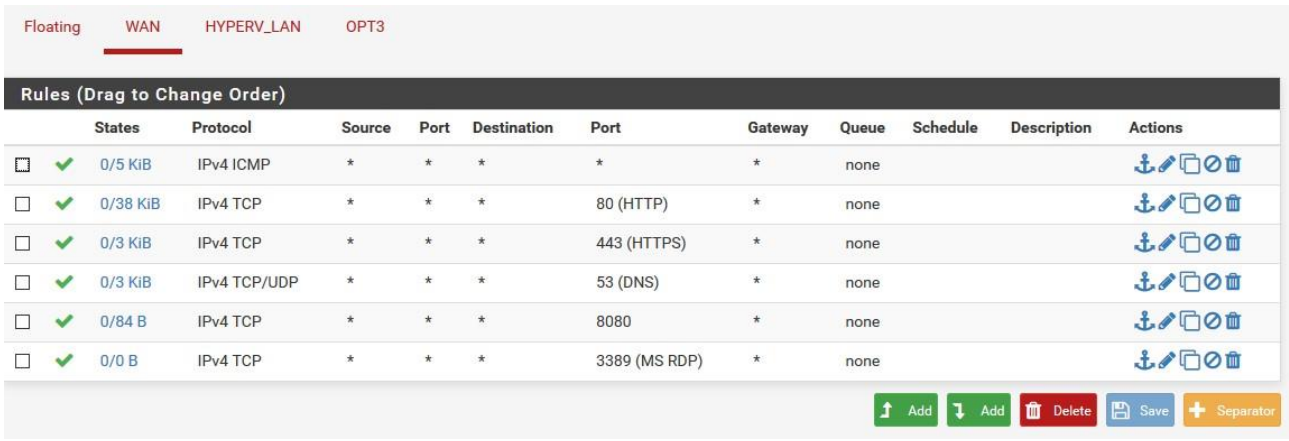
```
PORT     STATE  SERVICE           VERSION
53/tcp   closed domain
80/tcp   closed http
443/tcp  closed https
3389/tcp open   ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=B303-HP06.sio-savary-85.local
| Issuer: commonName=B303-HP06.sio-savary-85.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-01-18T13:16:40
| Not valid after:  2017-07-20T13:16:40
| MD5:   2c5f be3b a7b4 6499 b593 d948 fd3a 4102
|_SHA-1: 360c 51ac 8f1b 6b1b ffb7 ec31 633c b07e d4a4 9a92
|_ssl-date: 2017-02-28T14:36:15+00:00; -1s from scanner time.
8080/tcp open   http              Tinyweb httpd 1.93
|_http-generator: OpenOffice 4.0.1  (Win32)
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: TinyWeb/1.93
|_http-title: Site doesn't have a title (text/html).
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|2008 (88%), FreeBSD 6.X (87%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows Vista SP2 (88%), FreeBSD 6.2-RELEASE (87%), Microsoft Windows Server 2008 R2 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 35.942 days (since Mon Jan 23 17:00:07 2017)
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Question 3

Créer la règle de pare-feu qui autorise le client à accéder au serveur Web. Pour constater que la règle fonctionne correctement, nmap doit montrer le port 80 ouvert et on peut accéder à la page d'accueil du site.

Réponses :





Question 4

Quelle règle faut-il ajouter pour autoriser les flux DNS entre le client et le serveur Windows (on suppose que Windows est serveur DNS) ?

Il faut autoriser le port 53 (DNS)

Question 5

Même question avec les flux TSE (on veut pouvoir se connecter depuis le WAN en bureau à distance sur le serveur Windows)

Il faut autoriser le port 3389 (Microsoft Terminal Server/RDP)

Question 6

On a besoin maintenant de faire fonctionner le serveur Web non plus sur le port TCP standard (80) mais sur le port TCP 8080.
Arrêter Tinyweb et le redémarrer sur le port 8080.

Question 7

Supprimer la règle du pare-feu qui donne accès au port 80.
Créer une règle qui autorise les flux TCP sur le port 8080.
Vérifier que le navigateur et nmap fonctionnent

B.
Redirection de ports

On veut maintenant que le serveur Web continue à écouter sur le port 8080 mais que depuis le client on y accède sur le port 80. On veut mettre en place de la **redirection de port**.

Question

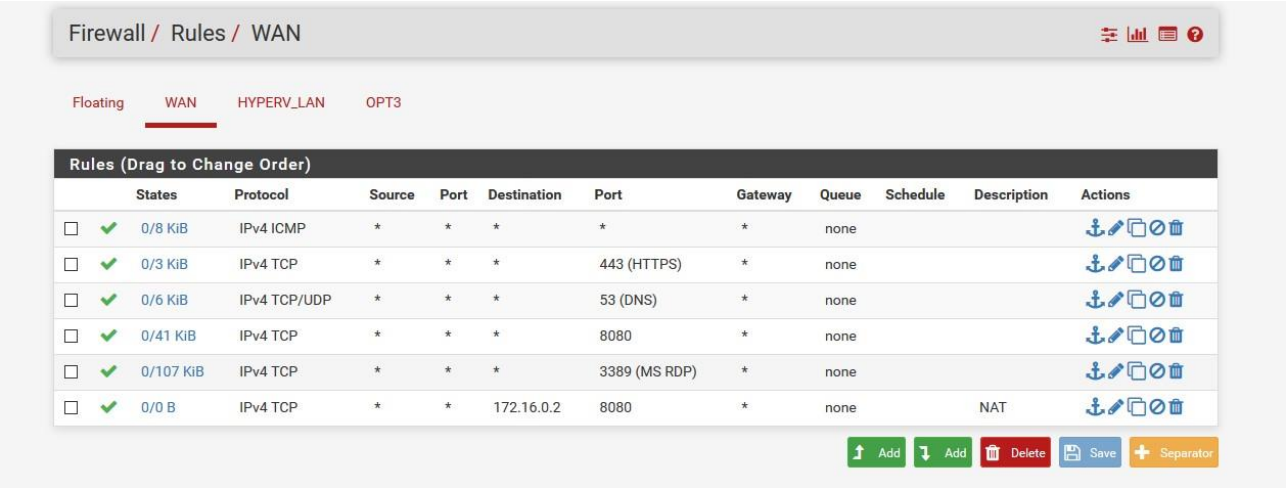
Supprimer la règle de pare-feu qui donne accès au port TCP 8080

Mettre en place une règle de redirection de port qui transforme une adresse de type 172.16.0.101:80 en 172.16.0.101:8080

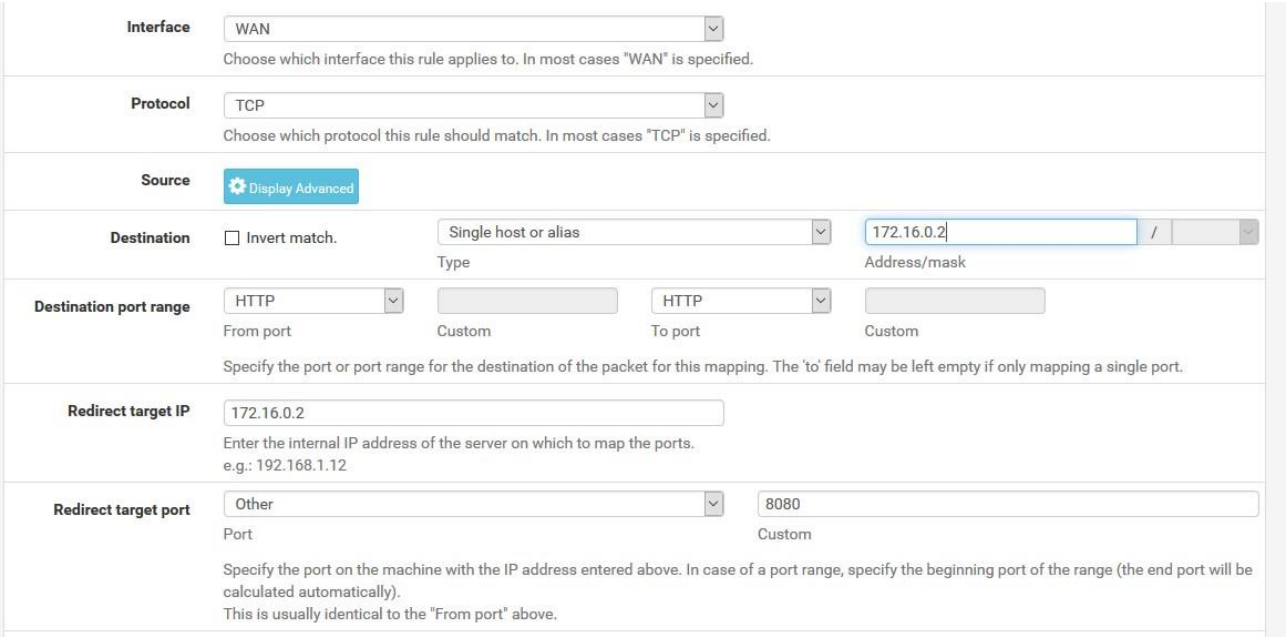
Depuis le client, on accède au site web comme avant sur le port 80 (mais le serveur fonctionne sur le port 8080 !).

Indice :

Il faut faire une règle de "NAT port forwarding"



C.



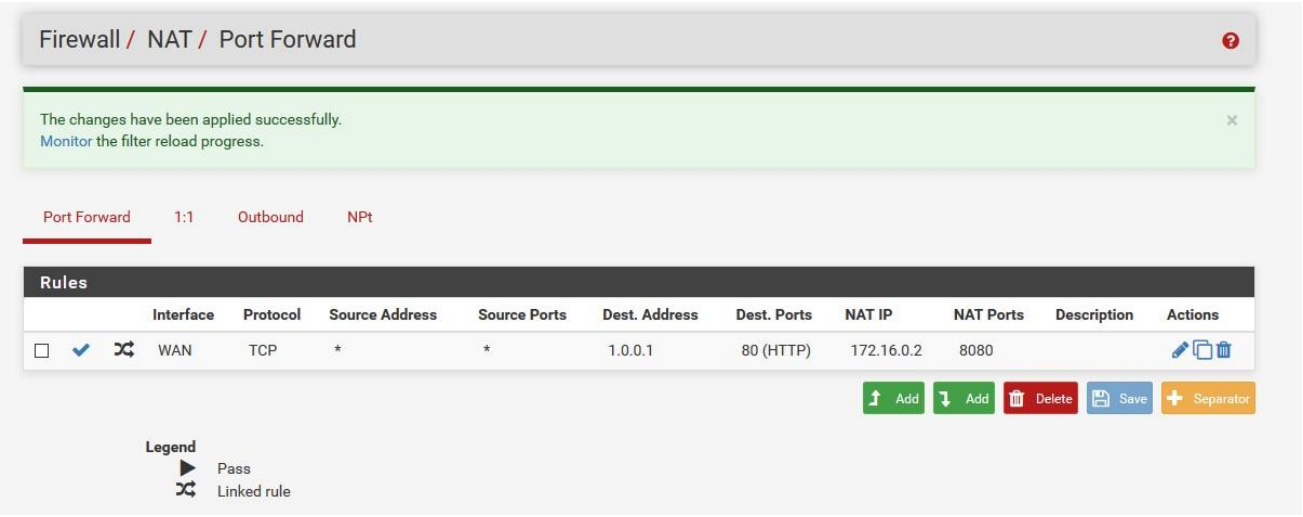
Translation d'adresse

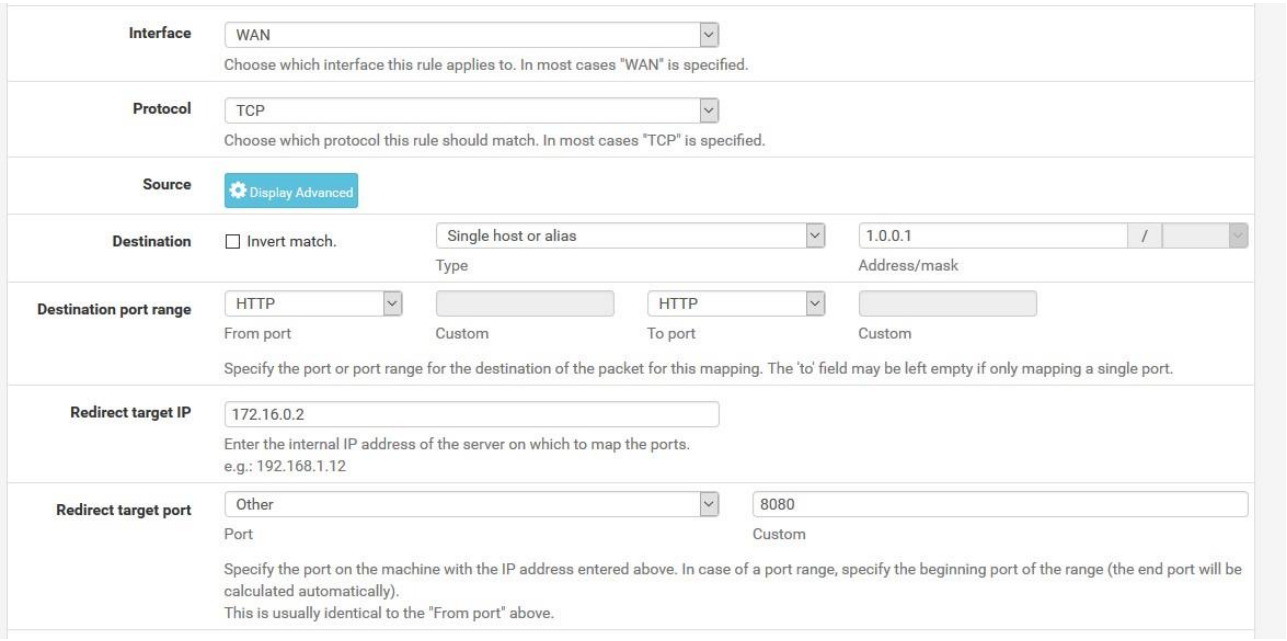
On veut maintenant masquer l'adresse IP interne du serveur web. L'utilisateur tape dans son navigateur l'adresse WAN du pfSense (1.0.0.1 port 80) et consulte le site sur le serveur Web (172.16.0.101 port 8080)

Question

Modifier la règle de port forwarding pour obtenir le résultat souhaité.

D.



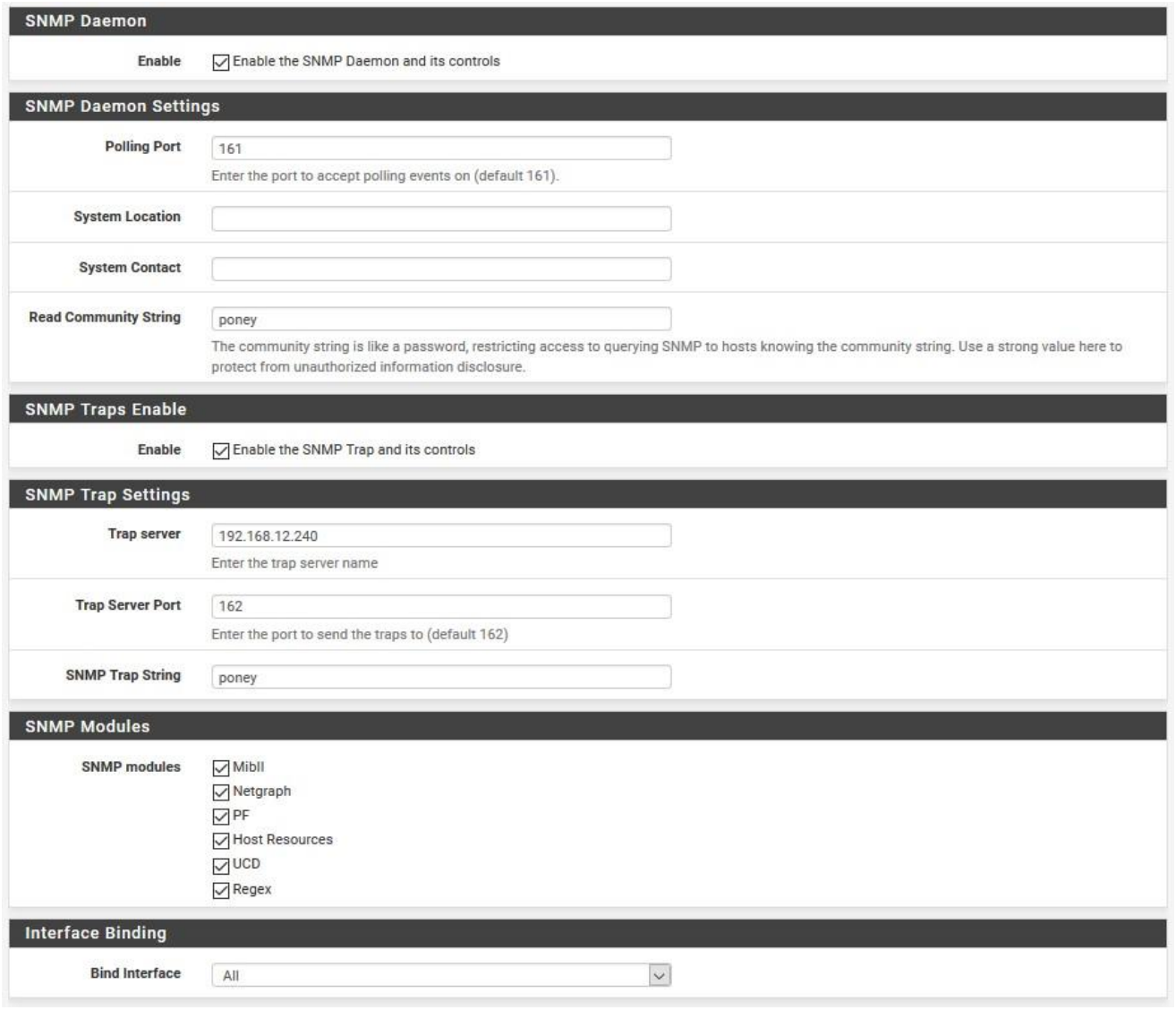


Supervision

Question

Intégrer votre pfSense au système de supervision (disponibilité et capacité) Centreon via SNMP : surveillance de la mémoire, du CPU et du débit sur les interfaces réseau.

E.


SNMP Daemon
Enable
Enable the SNMP Daemon and its controls
SNMP Daemon Settings
Polling Port
161
Enter the port to accept polling events on (default 161).
System Location
System Contact
Read Community String
poney
The community string is like a password, restricting access to querying SNMP to hosts knowing the community string. Use a strong value here to protect from unauthorized information disclosure.
SNMP Traps Enable
Enable
Enable the SNMP Trap and its controls
SNMP Trap Settings
Trap server
192.168.12.240
Enter the trap server name
Trap Server Port
162
Enter the port to send the traps to (default 162)
SNMP Trap String
poney
SNMP Modules
SNMP modules
MibII
Netgraph
PF
Host Resources
UCD
Regex
Interface Binding
Bind Interface
All