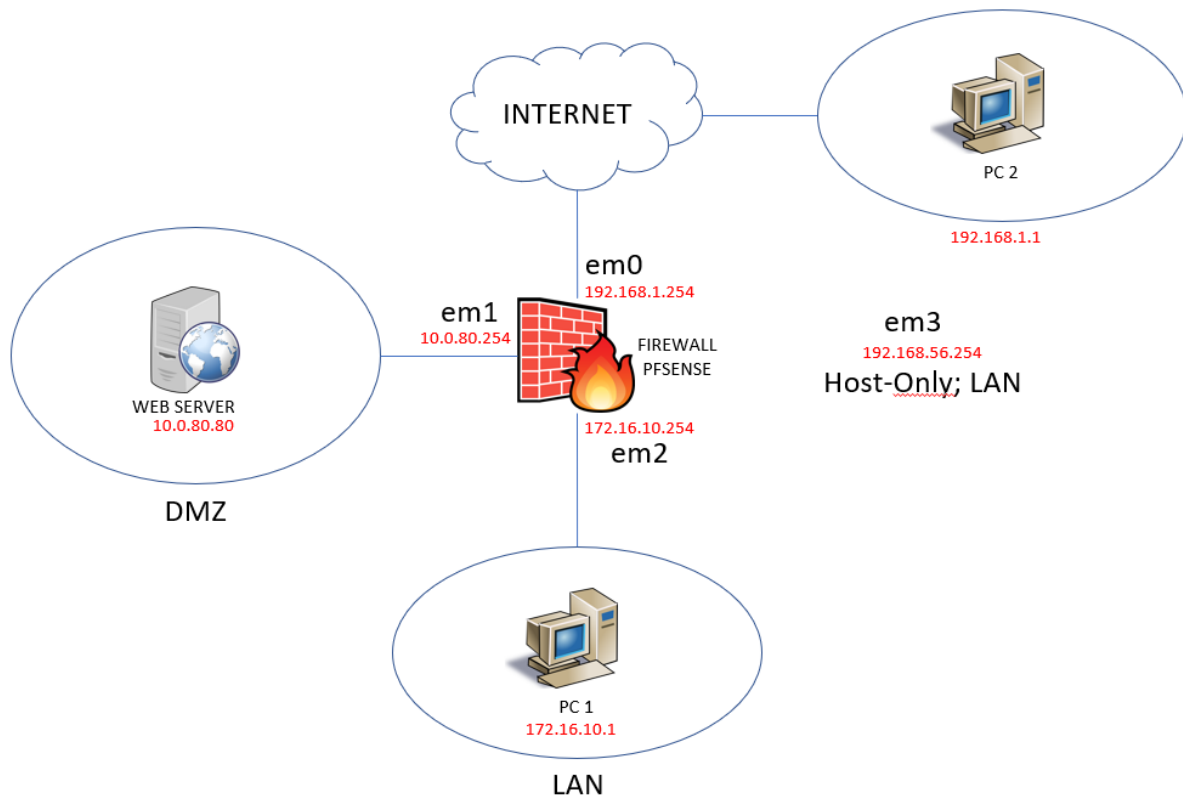


TP2 - Pare-Feu



1. Monter la maquette de la figure 1 en proposant un plan d'adressage de votre choix.



2. Ecrire les règles du parefeu pour satisfaire les contraintes suivantes :
 - a. Il doit permettre l'accès à Internet des utilisateurs, mais uniquement vers un serveur http ou https (n'oublier pas d'autoriser DNS).

Ajout des 3 règles autorisant l'accès aux serveurs HTTP, HTTPS et aux DNS

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			allow, log
0/0 B	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none			allow, log
0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			allow, log

test d'une communication HTTP

```

PC1 [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
root@debian:~# curl -I www.google.fr
HTTP/1.1 200 OK
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3pl
Date: Wed, 09 Feb 2022 10:55:10 GMT
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Transfer-Encoding: chunked
Expires: Wed, 09 Feb 2022 10:55:10 GMT
Cache-Control: private
Set-Cookie: NID=511=LkSrkgM4PQ7DE_ifS5V4Kjqu6RUg
P_0olzQrEfmvVEiKeATWvGrNBTvhgakaGWPR0ga5a7sQ2A4l
=Thu, 11-Aug-2022 10:55:10 GMT; path=/; domain=
root@debian:~# _

```

- b. Il doit permettre le ping d'une machine interne vers un serveur sur Internet. L'inverse est interdit.

Nous avons ajouté 2 règles, une interdisant tous ping en destination du réseau LAN, et une autre, autorisant tous ping vers un serveur internet.

Floating WAN LAN DMZ **PC1**

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗	0/0 B	IPv4 ICMP	*	*	PC1 address	*	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 ICMP	*	*	*	*	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		

Add
 Add
 Delete
 Save
 Separator

essaye de ping vers le DNS de Google

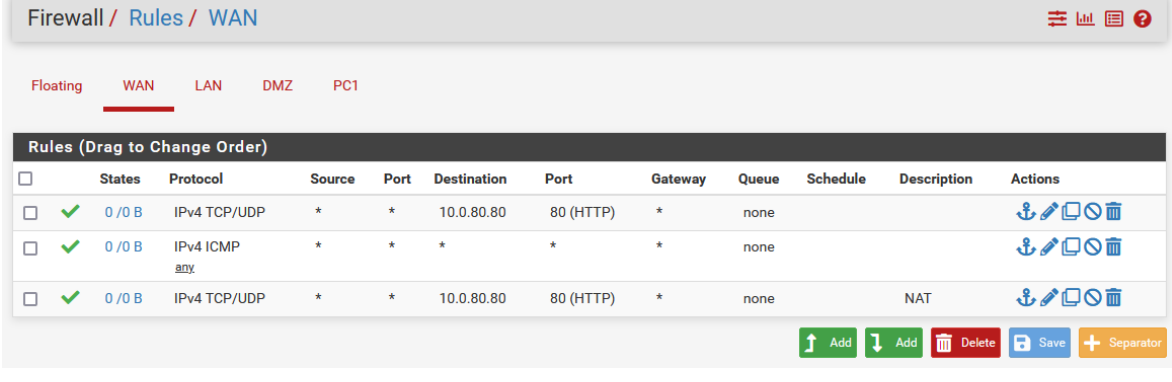
```

PC1 [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide

root@debian:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=7.62 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=9.49 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=9.25 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 7.615/8.786/9.490/0.833 ms
root@debian:~# _
  
```

- c. Les machines du réseau LAN ne doivent pas être visible d'Internet (SNAT)

Par défaut sur pfSense les machines du réseau LAN ne sont pas visible d'internet



Firewall / Rules / WAN

Floating **WAN** LAN DMZ PC1

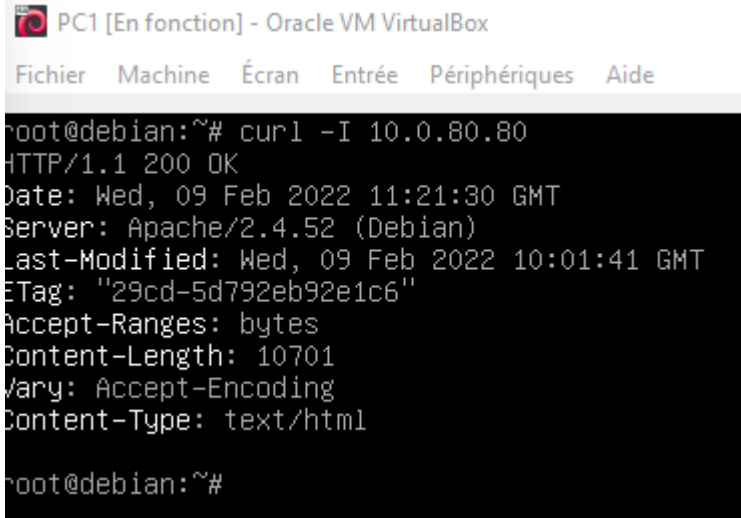
Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	*	*	10.0.80.80	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 ICMP any	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	*	*	10.0.80.80	80 (HTTP)	*	none		NAT	

↑ Add ↓ Add Delete Save + Separator

- d. Le serveur WEB dans la DMZ est accessible depuis le réseau LAN.

La règle permettant les communications de type HTTP vers n'importe quelle destination a été ajoutée à la question 2.a



PC1 [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

```

root@debian:~# curl -I 10.0.80.80
HTTP/1.1 200 OK
Date: Wed, 09 Feb 2022 11:21:30 GMT
Server: Apache/2.4.52 (Debian)
Last-Modified: Wed, 09 Feb 2022 10:01:41 GMT
ETag: "29cd-5d792eb92e1c6"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Content-Type: text/html

root@debian:~#

```

- e. Le serveur WEB dans la DMZ n'est pas accessible directement depuis Internet (Utiliser le port forwarding).

Dans un premier, nous autorisons les accès TCP/UDP en destination du serveur Web

Floating **WAN** LAN DMZ PC1

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4	TCP/UDP	*	*	10.0.80.80	80 (HTTP)	*	none	
<input type="checkbox"/>	✓	0/0 B	IPv4	ICMP	*	*	*	*	*	any	

Add Add Delete Save Separator

Ensuite on configure l'accès au serveur Web en indiquant qu'il faut passer par l'interface du WAN

Port Forward **1:1** Outbound NPt

Rules

<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	✓	TCP/UDP	*	*	*	80 (HTTP)	10.0.80.80	80 (HTTP)		


Add Add Delete Save Separator

Maintenant nous pouvons accéder à notre serveur en passant par l'adresse
192.168.56.80

pfSense.home.arpa - Firewall: N XTP2-PareFeu.pdfApache2 Debian Default Page: It wo X

192.168.56.80

ADD-ONSYouTubeNetflixLingueeCrédit MutuelinformatiqueEcole - JobShopiptvAutres marque-pages



Apache2 Debian Default Page

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.

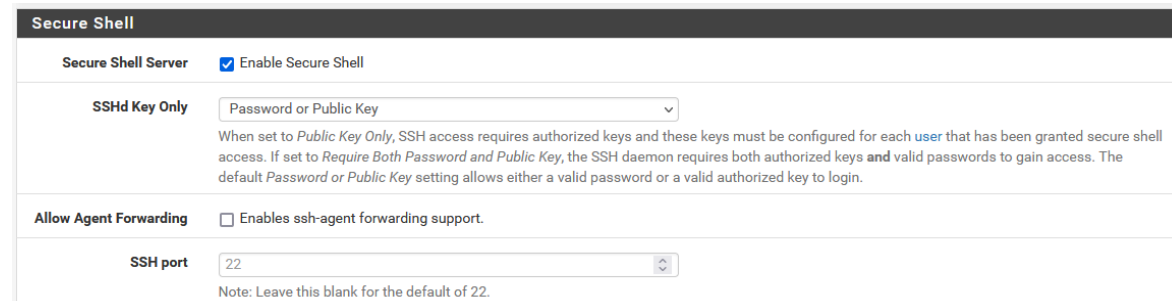
The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/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

f. Le pare-feu est accessible en utilisant SSH.

Nous devons activer la Secure Shell sur pfsense et nous avons laissé le port 22 par défaut pour les connexions en SSH



Secure Shell

Secure Shell Server ☒ Enable Secure Shell

SSHd Key Only Password or Public Key

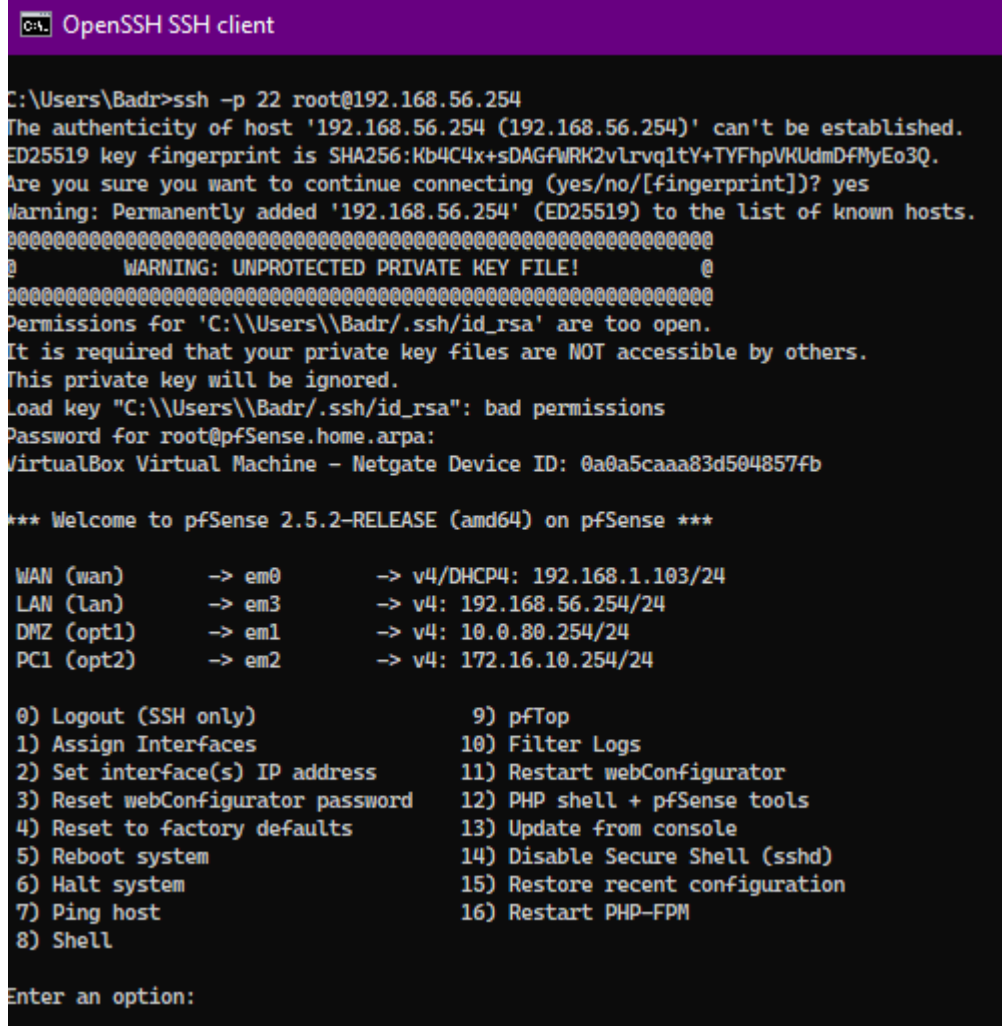
When set to *Public Key Only*, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to *Require Both Password and Public Key*, the SSH daemon requires both authorized keys and valid passwords to gain access. The default *Password or Public Key* setting allows either a valid password or a valid authorized key to login.

Allow Agent Forwarding ☐ Enables ssh-agent forwarding support.

SSH port 22

Note: Leave this blank for the default of 22.

Nous testons si la connexion SSH est possible en tapant sur l'invite de commande Windows, la commande : **ssh -p 22 root@192.168.56.254**



```
C:\Users\Badr>ssh -p 22 root@192.168.56.254
The authenticity of host '192.168.56.254 (192.168.56.254)' can't be established.
ED25519 key fingerprint is SHA256:Kb4C4x+sDAGfWRK2vLrvq1tY+TYFhpVKUdmDfMyEo3Q.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.254' (ED25519) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@          WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions for 'C:\\Users\\Badr\\.ssh\\id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "C:\\Users\\Badr\\.ssh\\id_rsa": bad permissions
Password for root@pfSense.home.arpa:
VirtualBox Virtual Machine - Netgate Device ID: 0a0a5caaa83d504857fb

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

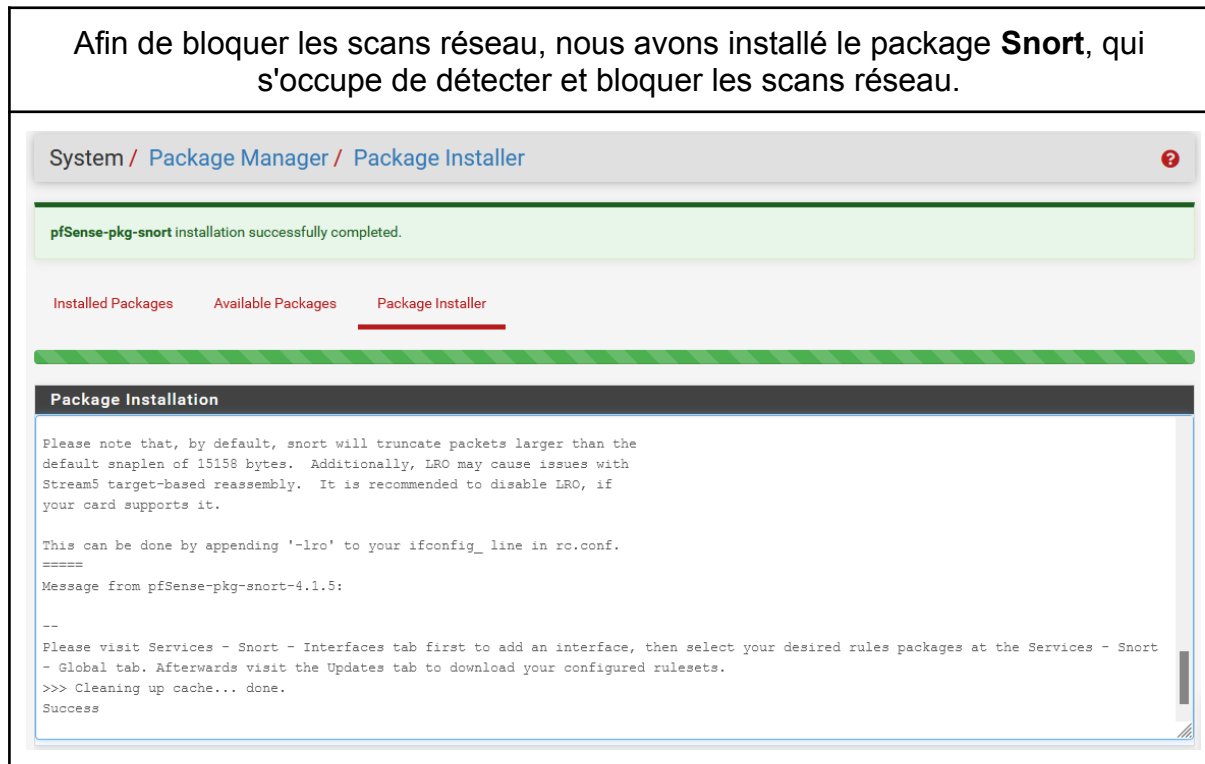
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.103/24
LAN (lan)      -> em3      -> v4: 192.168.56.254/24
DMZ (opt1)     -> em1      -> v4: 10.0.80.254/24
PC1 (opt2)     -> em2      -> v4: 172.16.10.254/24

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) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option:
```


3. Configurer le pare-feu pour qu'il puisse détecter et bloquer les scans réseau (nmap)

Afin de bloquer les scans réseau, nous avons installé le package **Snort**, qui s'occupe de détecter et bloquer les scans réseau.



Nous avons ensuite configuré les paramètres sur service **Snort** et bloqué tous les hosts qui génère une alerte.

Services / Snort / WAN - Interface Settings

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

WAN Settings

General Settings

Enable

☒ Enable interface

Interface

WAN (em0)

Choose the interface where this Snort instance will inspect traffic.

Description

WAN

Enter a meaningful description here for your reference.

Snap Length

1518

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

Send Alerts to System Log

☒ Snort will send Alerts to the firewall's system log. Default is Not Checked.

System Log Facility

LOG_AUTH

Select system log Facility to use for reporting. Default is LOG_AUTH.

System Log Priority

LOG_ALERT

Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.

Enable Packet Captures

☒ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Packet Capture File Size

128

Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_em035053 is rotated and a new file opened.

Enable Unified2 Logging

☒ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Log U2 VLAN Events

☐ Checking this option will cause Snort to log VLAN events to the unified2 binary format log for this interface. Default is Not Checked.

Log U2 MPLS Events

☐ Checking this option will cause Snort to log MPLS events to the unified2 binary format log for this interface. Default is Not Checked.

Block Settings

Block Offenders

☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode

Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, ems, ice, igb, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States

☒ Checking this option will kill firewall established states for the blocked IP. Default is checked.

Which IP to Block

BOTH

Select which IP extracted from the packet you wish to block. Default is BOTH.

4. Ajouter les règles qui permettent de protéger le pare-feu et les services internes des attaques DoS. Plusieurs solutions sont possibles. Faites une recherche et implémenter celle qui vous paraît la plus pertinente.

Afin de se prémunir des attaques DoS, nous avons ajouté les règles suivantes dans Snort :

emerging-dos.rules
snort_ddos.rules
snort_dos.rules

Snort Subscriber IPS Policy Selection

Use IPS Policy ☐ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.

Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

Select the rulesets (Categories) Snort will load at startup

- Category is auto-enabled by SID Mgmt conf files

- Category is auto-disabled by SID Mgmt conf files

Select All

Unselect All

Save

Enable	Ruleset: Snort GPLv2 Community Rules					
<input type="checkbox"/>	Snort GPLv2 Community Rules (Talos certified)					
Enable	Ruleset: ET Open Rules	Enable	Ruleset: Snort Text Rules	Enable	Ruleset: Snort SO Rules	Snort OPENAPPID rules are not enabled.
<input type="checkbox"/>	emerging-activex.rules	<input type="checkbox"/>	snort_app-detect.rules	<input type="checkbox"/>	snort_browser-chrome.so.rules	
<input type="checkbox"/>	emerging-attack_response.rules	<input type="checkbox"/>	snort_attack-responses.rules	<input type="checkbox"/>	snort_browser-ie.so.rules	
<input type="checkbox"/>	emerging-botoc.portgrouped.rules	<input type="checkbox"/>	snort_backdoor.rules	<input type="checkbox"/>	snort_browser-other.so.rules	
<input type="checkbox"/>	emerging-botoc.rules	<input type="checkbox"/>	snort_bad-traffic.rules	<input type="checkbox"/>	snort_browser-webkit.so.rules	
<input type="checkbox"/>	emerging-chat.rules	<input type="checkbox"/>	snort_blacklist.rules	<input type="checkbox"/>	snort_exploit-kit.so.rules	
<input type="checkbox"/>	emerging-ciarmy.rules	<input type="checkbox"/>	snort_botnet-cnc.rules	<input type="checkbox"/>	snort_file-executable.so.rules	
<input type="checkbox"/>	emerging-compromised.rules	<input type="checkbox"/>	snort_browser-chrome.rules	<input type="checkbox"/>	snort_file-flash.so.rules	
<input type="checkbox"/>	emerging-current_events.rules	<input type="checkbox"/>	snort_browser-firefox.rules	<input type="checkbox"/>	snort_file-image.so.rules	
<input type="checkbox"/>	emerging-deleted.rules	<input type="checkbox"/>	snort_browser-ie.rules	<input type="checkbox"/>	snort_file-java.so.rules	
<input type="checkbox"/>	emerging-dns.rules	<input type="checkbox"/>	snort_browser-other.rules	<input type="checkbox"/>	snort_file-multimedia.so.rules	
<input checked="" type="checkbox"/>	emerging-dos.rules	<input type="checkbox"/>	snort_browser-plugins.rules	<input type="checkbox"/>	snort_file-office.so.rules	
<input type="checkbox"/>	emerging-drop.rules	<input type="checkbox"/>	snort_browser-webkit.rules	<input type="checkbox"/>	snort_file-other.so.rules	
<input type="checkbox"/>	emerging-dshield.rules	<input type="checkbox"/>	snort_chat.rules	<input type="checkbox"/>	snort_file-pdf.so.rules	
<input type="checkbox"/>	emerging-exploit.rules	<input type="checkbox"/>	snort_content-replace.rules	<input type="checkbox"/>	snort_indicator-shellcode.so.rules	
<input type="checkbox"/>	emerging-ftp.rules	<input checked="" type="checkbox"/>	snort_ddos.rules	<input type="checkbox"/>	snort_malware-cnc.so.rules	
<input type="checkbox"/>	emerging-games.rules	<input type="checkbox"/>	snort_deleted.rules	<input type="checkbox"/>	snort_malware-other.so.rules	
<input type="checkbox"/>	emerging-icmp.rules	<input type="checkbox"/>	snort_dns.rules	<input type="checkbox"/>	snort_netbios.so.rules	
<input type="checkbox"/>	emerging-icmp_info.rules	<input checked="" type="checkbox"/>	snort_dos.rules	<input type="checkbox"/>	snort_os-linux.so.rules	
<input type="checkbox"/>	emerging-imap.rules	<input type="checkbox"/>	snort_experimental.rules	<input type="checkbox"/>	snort_os-other.so.rules	
<input type="checkbox"/>	emerging-inappropriate.rules	<input type="checkbox"/>	snort_exploit-kit.rules	<input type="checkbox"/>	snort_os-windows.so.rules	

5. Écrire des règles de protection contre les attaques par usurpation (spoofing).

Par défaut pfSense block les attaques par usurpation

Prevent IP Spoofing

This is a commonly cited reason for employing egress filtering, but pfSense automatically blocks spoofed traffic via pf's *antispoof* functionality, so it isn't applicable here. Preventing IP Spoofing means that malicious clients cannot send traffic with obviously falsified source addresses.

6. Le pare-feu est accessible par SSH. Faites le nécessaire afin de bloquer une adresse IP pour une heure après 5 tentatives de connexions SSH échouées.

Nous indiquons ici, qu'après 5 tentatives de connexion, l'adresse IP sera bloquée pendant 3600 secondes.

Login Protection	
Threshold	<input type="text" value="5"/> <small>Block attackers when their cumulative attack score exceeds threshold. Most attacks have a score of 10.</small>
Blocktime	<input type="text" value="3600"/> <small>Block attackers for initially blocktime seconds after exceeding threshold. Subsequent blocks increase by a factor of 1.5. Attacks are unblocked at random intervals, so actual block times will be longer.</small>
Detection time	<input type="text" value="1800"/> <small>Remember potential attackers for up to detection_time seconds before resetting their score.</small>
Pass list	<input type="text" value="Address"/> / 128 <small>Addresses added to the pass list will bypass login protection.</small>
Add address	<input type="button" value="+ Add address"/>