Guastamacchia Livio

Tp pfSense :

SIO1

### Introduction :

Dans ce TP nous allons procéder a l'installation et aux paramétrage de règle du parefeu Pfsense.

#### TP:

Pour commencer ce TP, nous créons une VM pfSense en activant sur les deux cartes réseaux « l'usurpation d'adresse mac » dans les fonctionnalités de la carte



Maintenant, nous démarrons la VM et on procède à l'installation de pfSense

pfSense Installer 
Helcome to pfSense!
InstallInstall pfSenseRescueShellRecoverLaunch a shell for rescue operationsRecoverconfig.xmlRecoverconfig.xmlrom a previousinstall
Cancel>

Partitioning
How would you like to partition your disk?         Futo (ZFS)       Guided Root-on-ZFS         Auto (UFS)       Guided UFS Disk Setup         Manual       Manual Disk Setup (experts)         Shell       Open a shell and partition by hand
Cancel>

figure Options:	in iguración
>>> Install	Proceed with Installation
T Pool Type/Disks:	stripe: 0 disks
- Rescan Devices	*
– Disk Info	*
N Pool Name	pfSense
4 Force 4K Sectors?	YES
E Encrypt Disks?	NO
<b>P</b> Partition Scheme	GPT (BIOS)
S Swap Size	1g
M Mirror Swap?	NO
W Encrypt Swap?	NO

ptSense Installer
ZES_Configuration
Select Virtual Device type:
StripeNo RedundancymirrorMirror - n-Way Mirroringraid10RAID 1+0 - n x 2-Way Mirrorsraid21RAID-21 - Single Redundant RAIDraid22RAID-22 - Double Redundant RAIDraid23RAID-23 - Triple Redundant RAID
<mark>&lt; hvkvp0: detached</mark> el> hvkvp0: <hyper-v kvp=""> on vmbus0arrows, TAB or ENTER]</hyper-v>
Last Chancel Are you sure you want to destroy       the current contents of the following disks:       da0
LPress arrows, IHB or ENTERJ
efSeero Jostallar
Complete Installation of pfSense complete! Would you like to reboot into the installed system now?
[Reboot] [Shell ]

Après l'installation de faite, nous allons attribuer si il y a des cartes VLAN, dans notre cas nous n'en avons pas donc on va juste mettre "n"

```
Should VLANs be set up now [y|n]? 2024-03-01T08:22:56.725872+00:00 – php-fpm 395
– – /rc.linkup: Ignoring link event during boot sequence.
2024-03-01T08:22:56.725872+00:00 – php-fpm 394 – – /rc.linkup: Ignoring link eve
nt during boot sequence.
```

Puis nous allons paramétrer qui est notre carte LAN et WAN, notre LAN sera hn0 et notre WAN sera hn1.



Nous validons avec "y"

```
Do you want to proceed [yln]? y
```

Nous allons maintenant changer l'adresse IP du LAN



Nous choisirons bien l'interface LAN (2)

Available interfaces: 1 - WAN (hn1 - dhcp, dhcp6) 2 - LAN (hn0 - static) Enter the number of the interface you wish to configure: 2

On modifie l'adresse IP 192.168.1.1/24 par 192.168.20.1/24

Configure IPv6 address LAN interface via DHCP6? (y/n) n Enter the new LAN IPv6 address. Press <ENTER> for none: Do you want to enable the DHCP server on LAN? (y/n) n Disabling IPv4 DHCPD... Disabling IPv6 DHCPD... Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n Please wait while the changes are saved to LAN... Reloading filter... Reloading routing configuration... DHCPD... The IPv4 LAN address has been set to 192.168.10.1/24 You can now access the webConfigurator by opening the following URL in your web browser: https://192.168.10.1/

après avoir modifier l'adresse IP de notre LAN il nous reste plus qu'à aller sur le site ci-dessus sur une machine connecter au réseaux (de préférence client) pour pouvoir paramétrer notre parefeu

nous arrivons sur ce site, nous devrons se connecter avec l'identifiants « admin » et le mdp « pfsense » (il est conseiller de changer mdp de suite après la connexion)

<b>pf</b> sense		Login to pfSense
	SIGN IN	
	admin	
	•••••	
	SIGN IN	

Nous arrivons sur cette page qui est l'assistant de paramétrage pfsense.

	System - Interface	s 🕶 Firewall 👻		VPN -	Status 👻	Diagnostics 👻	Help 👻	G
WARNING: The 's	admin' account password is	s set to the default val	ue. Change the p	assword in th	e User Manage	r.		
Wizard / p	fSense Setup /							0
Stop								
pfSense Setu	P							
	Welcome t	o pfSense® soft	ware!					
	This wizard w	ill provide guidance th	rough the initial	configuration	of pfSense.			
	The wizard m	ay be stopped at any t	ime by clicking t	he logo image	e at the top of th	ie screen.		
	pfSense® sof	tware is developed an	nd maintained by	Netgate®				
	Learn more							
	>> Next							

General Information	
	On this screen the general pfSense parameters will be set.
Hostname	srv-v-pf1-LG
	Name of the firewall host, without domain part.
	Examples: pfsense, firewall, edgefw
Domain	liviog.local
	Domain name for the firewall.
	Examples: home.arpa, example.com
	Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.
	The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.
Primary DNS Server	192.168.10.\$
Secondary DNS Server	
Override DNS	
	Allow DNS servers to be overridden by DHCP/PPP on WAN

Nous allons continuer jusque cette page ou l'on va noté : le nom du parefeu, le nom du domaine ainsi que l'adresse IP de notre serveur DNS

il nous est maintenant demander de paramétrer l'heure pour nous on est en GMT+1

Time Server Information						
	Please enter the time, date and time zone.					
Time server hostname	2.pfsense.pool.ntp.org					
	Enter the hostname (FQDN) of the time server.					
Timezone	Etc/GMT+1	~				
	>> Next					

après cela on nous demandera de paramétrer le WAN que l'on ne changera pas car il est bien paramétrer par défaut et on nous demandera aussi si l'on veut modifier l'adresse IP du parefeu que l'on a déjà changer au préalable donc qui n'est pas nécessaire.

Après avoir passer les deux page de configuration, Nous arrivons a la modification du mdp du parefeu après il nous resteras plus qu'a accepter la demande de redémarrage

(j'ai oublier de prendre un screen et je ne peux plus aller en arrière)

On voit bien que le parefeu a bien été paramétrer

#### Status / Dashboard

System Inform	ation 🦻 🖨 😵	Netgate Services And Support 📃 🗢 🛠
Name	srv-v-pf1-LG.liviog.local	Contract type Community Support
User	admin@192.168.10.100 (Local Database)	Community Support Community Support Only
System	Microsoft Azure Netgate Device ID: <b>67d5d5ffc235d87ebbe8</b>	NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
BIOS	Vendor: 8 🔷 🔷 🔷 🖉 🖉 🖉 None Version: 838	If you purchased your of Sense gateway firewall appliance from Netgate and elected
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 19:10:00-01 2023 FreeBSD 14.0-CURRENT	Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.
	The system is on the latest version. Version information updated at Fri Mar 15 7:47:07 -01 2024 🔁	You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is
CPU Type	13th Gen Intel(R) Core(TM) i7-13620H 8 CPUs: 1 package(s) x 4 core(s) x 2 hardware threads AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No	more than competitive when compared to others in our space.         • Upgrade Your Support       • Community Support Resources         • Netgate Global Support FAQ       • Official pfSense Training by Netgate
Hardware crypto	Inactive	Netgate Professional Services     Visit Netgate.com
Kernel PTI	Disabled	
MDS Mitigation	Inactive	If you decide to purchase a Netgate Global TAC Support subscription, you MUST have your Netgate Device ID (NDI) from your firewall in order to
Uptime	00 Hour 29 Minutes 54 Seconds	validate support for this unit. Write down your NDI and store it in a safe place.
Current date/time	Fri Mar 15 8:16:01 -01 2024	You can purchase TAC supports nere.
DNS server(s)	<ul><li>127.0.0.1</li><li>172.25.0.1</li><li>192.168.10.5</li></ul>	Interfaces
Last config change	Fri Mar 15 8:12:56 -01 2024	
State table size	27 (21 (400000) 0	

+ 0

## maintenant nous allons passé aux règles de parefeu

# Nous irons dans l'onglet firewall puis sur rules

	Firewall 🗸	Services
	Aliases	
	NAT	_
	Rules	
	Schedules	۴
	Traffic Shape	r
oc	Virtual IPs	

on voit que tous est autorisé pour le LAN

Ru	Iles	(Drag to Chan	ge Order	)								
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	~	1/1.55 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	٥
	~	24/248.22 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	ᢤⅆⅅѺ菌×
	~	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	ᢤⅆŪѺ菌×

## on va premièrement modifier les paramètre IPV4 et IPV6 pour bloquer le passage

on clique sur le petit crayon



## puis on bloque les actions

Edit Firewall Rule	
Action	Block Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender,
Disabled	whereas with block the packet is dropped silently. In either case, the original packet is discarded.  Disable this rule Set this option to disable this rule without removing it from the list.
Interface	LAN  Choose the interface from which packets must come to match this rule.
<u>Address Family</u>	IPv4        Select the Internet Protocol version this rule applies to.
Protocol	Any  Choose which IP protocol this rule should match.

## deuxièmement nous créons un alias pour les port qui nous intéresse

pour cela nous allons sur firewall > aliases > port

Firewall +	Services							
Aliases								
NAT								
Rules								
Schedules	a	a						
Traffic Shaper	a 👘							
Virtual IPs								
Ports	URLs	All						
	Firewall - Aliases NAT Rules Schedules Traffic Shaper Virtual IPs	Firewall -ServicesAliases-NAT-Rules-Schedules-Traffic Shaper-Virtual IPs-PortsURLs						

et on add les port qui nous intéresse notamment les port internet donc le port 80 pour HTTP, le port 443 pour HTTPS et le port 53 pour DNS

Properties	
Name	base-internet The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	A description may be entered here for administrative reference (not parsed).
Туре	Port(s)
Port(s)	
Hint	Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.
Port	80 HTTP 🛅 Delete
	443 HTTPS 🛅 Delete
	53 DNS 🛅 Delete

Nous allons maintenant créer une règle de parefeu pour les alias créer

on ajoute une règle puis comme paramètre nous allons mettre

- Action : pass (autoriser les passages)
- Protocol : TCP/UDP
- Source : LAN subnets (autoriser tout ce qui vien du réseaux LAN)
- destination : ANY (pour n'importe quel destination)
- destination Port Range : base\_internet (alias créer au préalable)

et on coche les logs pour nous permettre d'avoir un historique des passages

Edit Firewall Rule	
Action	Pass
	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<ul> <li>Disable this rule</li> <li>Set this option to disable this rule without removing it from the list.</li> </ul>
Interface	LAN  Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	TCP/UDP       Choose which IP protocol this rule should match.

✓ := 0/0 B	IPv4 TCP/UDP LAN subnets * * Base_internet * none	
	Display Advanced	
	The <b>Source Port Range</b> for a connection is typically random and almost never equal to the destination port. In most cases this setting must its default value, <b>any</b> .	remain a
estination		
Destinatio	ion Invert match Any V Destination Address /	
Destination Port Rang	ige (other) V Base_internet (other) V	
	From Custom To Custom	
	Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.	
xtra Options		
Lo	.og 🔽 Log packets that are handled by this rule	
_	Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog ser	rver (se
	the Status: System Logs: Settings page).	
Descriptio	ion	
	A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the log.	firewall
Microsoft Bing	Q google Q 😥 🥑	
	Promu par Microsoft	
	ur un navigateur inte	erne
	G Google https://www.acoogle.fr	
	Google WEB Search the world's information, including webpages, images, videos and more. Google has many special features to help you find exactly what you're looking for.	
	Recherche Search the world's information, including webpages, images, v	
	Commencer Étape 2 : définissez Google comme page d'accueil Dans le me	

La recherche a bien fonctionné ce qui nous montre que nous avons réussis a avoir un accès internet

Sur pfsense nous pouvons bien voir qu'il y a eu du trafic qui est passer via cette règle

□ ✓	70/19.60	IPv4	LAN	*	*	Base_	*	none	む 🖉 🗋 🛇 🗰
ž≡	MiB	TCP/UDP	subnets			internet			×

pour finir on vas rajouter une règle pour les pings vers internet car il est impossible de faire un ping via internet



- action : pass

- protocole : IMCP (protocole pour les pings)
- source : LAN subnets

Action	Pass V
	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<ul> <li>Disable this rule</li> <li>Set this option to disable this rule without removing it from the list.</li> </ul>
Interface	LAN  Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	ICMP ~
ICMP Subtypes	any Alternate Host Datagram conversion error Echo reply

Source									
Source	Invert match	LAN subnets	~	Source Address	1	~			
Destination									
Destination	Invert match	Any	~	Destination Address	1	~			
Extra Options									
Log	Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).								
Description	A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.								
Advanced Options	Display Advanced								
	Save								

maintenant on voit bien que les ping sont possible vers internet

```
C:\Users\LG01>ping 9.9.9.9
Envoi d'une requête 'Ping' 9.9.9.9 avec 32 octets de données :
Réponse de 9.9.9.9 : octets=32 temps=175 ms TTL=49
Réponse de 9.9.9.9 : octets=32 temps=172 ms TTL=49
Réponse de 9.9.9.9 : octets=32 temps=300 ms TTL=49
Réponse de 9.9.9.9 : octets=32 temps=132 ms TTL=49
Statistiques Ping pour 9.9.9.9:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 132ms, Maximum = 300ms, Moyenne = 194ms
```

### conclusion :

SIO 1 : TP court et pas très compliquer a effectuer mis a part les problème d'accordement d IP qui reste un petit problème mais qui est réglable sans trop de soucis ou bien le fait d oublier de lancer la VM pfsense pour le paramétrer sur le site.

SIO 2 : TP rapide a effectué, problème de récupération d'ip pour le WAN du a des paramètres d'hyper V mal configuré mis a part ça aucun soucis.