Installation d'un routeur avec pfSense

PfSense est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD. Il utilise un parefeu, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il s'administre à distance depuis une interface web ce qui rend la prise en main plus agréable.

Dans ce tutoriel, nous allons voir comment installer le routeur et le configurer (NAT, relais DHCP, redirection de port). Le routeur ainsi que les sous-réseaux sont virtuels et il y a 5 interfaces dont l'interface « Pédagogique » qui sert d'interface WAN.

Configuration requise :

	Minimale	Recommandée
Processeur	500 MHz	1 GHz
Mémoire vive	256 Mo	1 Go
Stockage	> 1 Go	

Tout d'abord, il faut crée une nouvelle machine virtuel avec :

- l'image ISO de pfSense téléchargeable depuis le site officiel
- au moins 2 cartes réseau
- 1 Go de RAM
- 8 Go d'espace de stockage

Installation :

Démarrer la machine et l'installation va commencer :

Jelcome to pfSense!	Welcome-
<mark>Install</mark> Rescue Shell Recover config.xm	Install pfSense Launch a shell for rescue operations Recover config.xml from a previous install
C	<mark>]k > ⟨C</mark> ancel>
<u> </u>	D <mark>K > <c< mark="">ancel></c<></mark>

Choisir le partitionnement du disque automatique :



On peut maintenant redémarrer le système :

pfSense Installer	
	Complete Installation of pfSense complete! Would you like to reboot into the installed system now? KReboot> <shell></shell>
'	

On peut maintenant assigner les interfaces de notre machine virtuelle aux interfaces du routeur en tapant "1":

Starting syslogdone.	
Starting CRON done.	
pfSense 2.4.4-RELEASE amd64 Thu Sep 20	0 09:03:12 EDT 2018
Bootup complete	
FreeBSD/amd64 (pfSense.localdomain) (1	ttyv0)
UN	10. 0-1-10004400040160
VMWare Virtual Machine - Netgate Devic	ce ID: 2cac19884432240aee12
*** Walcome to ofSense 2 4 4-DELEASE	(amd64) on nfSonso ***
we we to be to be see 5.4.4 warming	analy on processe and
WAN (wan) -> емØ ->	
LAN (lan) -> em1 ->	
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
Reset to factory defaults	13) Update froм 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:	

Voulez vous configurer des interfaces VLAN ? Non, nous n'avons pas besoin de VLAN :



Entrer le nom des interfaces correspondant au WAN, au LAN et les interfaces restantes aux options en fonction des réseaux attribués dans les paramètres de la machine virtuelle, puis valider :

latériel Options Ressources Pr	ofils VServices		Version de machine virtuelle :
 Afficher tous les périphériques 	Ajouter Supprimer	Configuration	Taille
Matériel	Résumé	512 60	
Mémoire	512 Mo	012-00	Maximum recommandé pour ce SE invité : 1011 Go
CPU Carte vidéo Périphérique VMCI Contrôleur SCSI 0 Disque dur 1 Lecteur CD/DVD 1 Adaptateur réseau 1 Adaptateur réseau 2 Adaptateur réseau 3 Adaptateur réseau 4 Lecteur de disquettes 1 Adaptateur réseau 5	1 Carte vidéo Restreint Parallèle logique de LSI Disque virtuel [Datastore_VNX_12] I Pédagogique PPE2-Admin-Florent PPE2-OMZ-Florent PPE2-OMZ-Florent PPE2-Serveurs-Florent PÉ2-Prod-Florent	2255 G0 - 128 G0 - 32 G0 - 32 G0 - 4 G0 - 2 G0 - 1 G0 -	Maximum recommandé pour performance optimale : 32756 Mo. Recommandé par géfaut pour ce SE invité : 512 Mo. Minimum recommandé pour ce SE invité : 64 Mo.

Enter the WAN interface name or 'a' for auto-detection (em0 em1 em2 em3 em4 or a): em0 Enter the LAN interface name or 'a' for auto-detection NOTE: this enables full Firewalling/NAT mode. (em1 em2 em3 em4 a or nothing if finished): em1 Enter the Optional 1 interface name or 'a' for auto-detection (em2 em3 em4 a or nothing if finished): em2 Enter the Optional 2 interface name or 'a' for auto-detection (em3 em4 a or nothing if finished): em3 Enter the Optional 3 interface name or 'a' for auto-detection (em4 a or nothing if finished): em4 The interfaces will be assigned as follows: WAN -> em0 LAN -> em1 OPT1 -> ем2 ОРТ2 -> емЗ ОРТЗ -> ем4 Do you want to proceed [yin]? y

Appuyer ensuite sur "2" pour configurer les adresses IP sur chaque interfaces, puis sur "1" pour choisir l'interface WAN :

Enter an option: 2 Available interfaces: 1 — WAN (ем0 — dhcp, dhcp6) 2 — LAN (ем1 — static) 2 - LHN (EM1 3 - OPT1 (EM2) 4 - OPT2 (EM3) 5 - OPT3 (EM4) Enter the number of the interface you wish to configure: 1 Configure IPv4 address WAN interface via DHCP? (y/n) n Enter the new WAN IPv4 address. Press <ENTER> for none: > 172.16.20.108 Subnet masks are entered as bit counts (as in CIDR notation) in pfSense. e.g. 255.255.255.0 = 24 255.255.0.0 = 16 = 8 255.0.0.0 Enter the new WAN IPv4 subnet bit count (1 to 31): > 17 For a WAN, enter the new WAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none: > 172.16.127.254 Configure IPv6 address WAN interface via DHCP6? (y/n) n Enter the new WAN IPv6 address. Press <ENTER> for none: > Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y Please wait while the changes are saved to WAN... Reloading filter... Reloading routing configuration... DHCPD... Restarting webConfigurator... The IPv4 WAN address has been set to 172.16.20.108/17 Press <ENTER> to continue.

Recommencer ensuite pour chaque interfaces pour obtenir ceci :

```
The IPv4 OPT3 address has been set to 10.0.0.30/27
Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 49b344910cd909f2f6b0
*** Welcome to pfSense 2.4.4-RELEASE (amd64) on pfSense ***
 WAN (wan)
                  -> ем0
                                 -> v4: 172.16.20.108/17
                                 -> v4: 10.0.0.62/27
-> v4: 10.0.0.94/28
 LAN (lan)
                  -> ем1
 OPT1 (opt1)
OPT2 (opt2)
                  -> ем2
                                 -> v4: 10.0.0.78/28
                  -> емЗ
 OPT3 (opt3)
                                 -> v4: 10.0.0.30/27
                  -> ем4
 0) Logout (SSH only)
1) Assign Interfaces
                                          9) pfTop
                                         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
8) Shell
                                         16) Restart PHP-FPM
Enter an option: 📕
```

Vous pouvez ensuite redémarrer le routeur ("5"), pour être sur que tout les paramètres indiqués soient bien pris en compte.

Configuration avec l'interface Web :

Il faut maintenant à partir d'un sous réseau crée précédemment (Admin, DMZ, Serveur, Prod) créer une nouvelle machine virtuelle possédant une interface graphique. Dans votre navigateur web préféré, entrer l'adresse ip correspondant à l'interface WAN pour arriver sur la page de configuration. Par défaut : login – admin mot de passe – pfsense

🚮 Login				× +											X
€→	G	۵			i) 🔏 172.16.	20.108						⊘ ☆	lii V		Ξ
		p	S	e	1se								Login to pfS	ense	
									SIGN IN						
								admin		~					
								•••••	•						
									SIGN IN						
						pfSense	is develope	d and maintai	ined by Netgate	© ESF 2004	- 2019 View lic				
	C		1	0	6								FR 🔺 🍓 🔯 🕼	16:42	110

Entrer le nom du routeur ainsi que le nom de domaine. On peut aussi renseigner les adresses des serveurs DNS si vous en avez. (Possible de le faire plus tard)

of pfSense.localdomain - Wizard:	× +			- 6 🗙
← → ⊂ ŵ	① 172.16.	20.108/wizard.php?xml=setup_wizard.xml	<u></u>	
	NSC System -	Interfaces • Firewall • Services • VPN • Status • Diagnostics • Help •	•	<u>^</u>
WARN	VING: The 'admin' acco	unt password is set to the default value. Change the password in the User Manager.		
Wiz	ard / pfSense	Setup / General Information	Θ	
	Step 2 of 9			
Gene	eral Information			
		On this screen the general pfSense parameters will be set.		
	Hostname	routeur-pfSense		
	.	EXAMPLE: myserver		1
	Domain	local.scopti.tr EXAMPLE: mydomain.com		
		The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing	r. To use the g the wizard.	
Р	rimary DNS Server			
Sec	ondary DNS Server			
	Override DNS	I Allow DNS servers to be overridden by DHCP/PPP on WAN		
		» Next		
🕘 🙆 📋	0		FR 🔺 😼 🐿	16:45 20/03/2019

On peut ensuite configurer l'interface WAN. (qui est déjà fait normalement)

Tout en bas, il faut décocher les 2 cases si vous voulez que les adresses IP privée puissent se connecter par l'interface WAN :

of Sense.localdor	main - Wizard: 🗙 🕂			-	
(←) → ℃ 6	i 🔏 172.	16.20.108/wizard.php?xml=setup_wizard.xml 🗐 🚥 💟 🏠	I	ill 🗊) ≡
	PPTP configuration				^
	PPTP Username				
	PPTP Password				
	Show PPTP password	Reveal password characters			
	PPTP Local IP Address				
	pptplocalsubnet	32 *			
	PPTP Remote IP Address				
	PPTP Dial on demand	Enable Dial-On-Demand mode This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actua connection of the link is delayed until qualifying outgoing traffic is detected.	1		
	PPTP Idle timeout	If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disable this feature.	es		
	RFC1918 Networks				
	Block RFC1918 Private Networks	Block private networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172, 16/12, 192, 168/16) as well a loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.	98		Е
	Block bogon network	3			
	Block bogon networks	Block non-Internet routed networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.			
()	Image:	» Next	18 🖂 18	16:5 20/03/	51 /2019

Continuer ensuite l'installation jusqu'au redémarrage.

On peut ensuite renommer les interfaces pour plus de facilité dans le menu « Interfaces »:

outeur-pfSense.local.scopti.fr × +			
→ C û 🗿 🔏 172	.16.20.108/interfaces.php?if=lan 🚥 💀	1 合	
COMMUNITY EDITION	r Interfaces + Firewall + Services + VPN + Status + Diagnostics + Help +	۵	
Interfaces / Adm	in (em1)	≆ Ш 0	
The Admin configuration ha The changes must be appli Don't forget to adjust the D	is been changed. ad to take effect. HCP Server range if needed after applying.	oply Changes	
General Configuratio	n I Enable interface		
Description	Admin Enter a description (name) for the interface here.		
IPv4 Configuration Type	Static IPv4		
IPv6 Configuration Type	None		
MAC Address	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		
МТО	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.		
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will I	be in effect.	
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface.		
) 🙆 📋 🖸 🔞		FR 🔺 诸 🔁 🕯	20

Dans le menu « Firewall » -> « Rules , créer une nouvelle règle qui autorise tout et supprimer les règles existantes pour plus de facilité au début :

outeur-pfSense.loc	al.scopti.fr 🗙 🕂			-0	6	×
(←) → ℃ @	③ 172.16	20.108/firewall_rules_edit.php?ff=wan&after=-1	⊵ ☆	lii1\		≡
	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 ret whereas with block the packet is dropped silently. In either case, the original packet is discarded.	urned to the sender,			
	Disabled	Disable this rule Set this option to disable this rule without removing it from the list.				
	Interface	WAN				
		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	Any Choose which IP protocol this rule should match.				ш
	Source	any Source Address	/ *			
	Source					
	Destination					
	Destination	Invert match. Destination Address	/			
	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 r the Status: System Logs: Settings page).	emote syslog server (see			
	Description	A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and log.	displayed in the firewall			
👩 💋	🗎 🖸 🧕		FR 🔺 🔞	🐑 🍓 💡	17:06 0/03/201	9

Recommencer pour toutes les interfaces.

Aller maintenant dans « Firewall » -> « NAT »-> « Outbound » puis sélectionner « Manuel » et supprimer toutes les règles existantes :

P	ort Fr	orward	1:1 0	utbound N	IPt						
_			-								
0	utbo	ound NA	T Mode								
			Mode Ai (II in	© utomatic outbou le generation. Psec passthroug cluded)	und NAT gh	Hybrid Outbound I rule generation. (Automatic Outboo NAT + rules below	NAT N r und () C	Aanual Outbo Je generatio AON - Advan utbound NA	ound NAT on. iced T)	© Disable Outbound NAT rule generation. (No Outbound NAT rules)	
M	app	ings Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
	~	WAN	127.0.0.0/8	*	*	500	WAN addres	s *	~	Auto created rule for ISAKMP - localhost to WAN	✓☐☐
7	~	WAN	127.0.0.0/8	*	*	*	WAN addres	s *	x	Auto created rule - localhost to WAN	/0±
V	~	WAN	::1/128	*	*	500	WAN addres	s *	~	Auto created rule for ISAKMP - localhost to WAN	/0 0
7	~	WAN	:: <mark>1/12</mark> 8	*	*	*	WAN addres	s *	24	Auto created rule - localhost to WAN	/ () ()
V	~	WAN	10.0.0.32/2	7 *	*	500	WAN addres	s *	×	Auto created rule for ISAKMP - ADMIN to WAN	/0 0
V	~	WAN	10.0.0.32/2	7 *	*	*	WAN addres	s *	x ¢	Auto created rule - ADMIN to WAN	/0 t
J	~	WAN	10.0.0.80/2	8 *	*	500	WAN addres	s *	~	Auto created rule for ISAKMP - DMZ to WAN	✓☐ ☐
V	~	WAN	10.0.0.80/2	B *	*	*	WAN addres	s *	x ¢	Auto created rule - DMZ to WAN	Ø 🖸 🛍
	~	WAN	10.0.0.64/2	8 *	*	500	WAN addres	s *	~	Auto created rule for ISAKMP - SERVEUR to WAN	100
V	~	WAN	10.0.0.64/2	в *	*	*	WAN addres	s *	20	Auto created rule - SERVEUR to WAN	/ 🗇 🛍
V V		WAN	10.0.0/27	*	*	500	WAN addres	s *	*	Auto created rule for ISAKMP - PROD to WAN	/ () ()
V V V	*								116		

Créer une nouvelle règle en autorisant tout les protocoles et tout les sous réseaux :

of sense System		ces → VPN → Status → Diagnostics	- Help -			€	
COMMUNITY EDITION				_			
Firewall / NAT /	Outbound / Edit					0	
Edit Advanced Outbo	ound NAT Entry						
Disabled	🗐 Disable this rule						
Do not NAT	Enabling this option will disable NAT for the second se	traffic matching this rule and stop processing Outbo	ound NAT rules				
Interface	center Interface Interface Interface Interface Interface Interface Firewall / NAT / Outbound / Edit Edit Advanced Outbound NAT Entry Disabled Disable this rule Do not NAT Interface Interface Interface Interface Interface WAN Interface Interface Interface Interface Interface Interface Firewall / NAT / Outbound / Edit Edit Advanced Outbound NAT Entry Disabled Disable this rule Do not NAT Interface Interface Interface Interface Interface WAN Interface Interface Interface Interface Interface Interface Firewall / WAN Interface Interfa						
	The interface on which traffic is matched as	it exits the firewall. In most cases this is "WAN" or	another externally	connecte	···· ♥ ☆ ●		
Address Family	IPv4+IPv6 Select the Internet Protocol version this rule	applies to.					
Protocol	any Choose which protocol this rule should mate	▶. In most cases "any" is specified.					
Source	Any		/ 24	-			
	Туре	Source network for the outbound NAT mapping.			Port or Range		
Destination	Any		/ 24	Ŧ			
	Туре	Destination network for the outbound NAT mapp	ing.		Port or Range		
	Not Invert the sense of the destination match.						
Translation							

Configurer maintenant le relais DHCP dans le menu « Services »-> « DHCP Relay » en sélectionnant les sous réseaux voulu et l'adresse IP du serveur DHCP :

🗾 routeur-pfSense.local.scopti.fr 🗙 🕂		
← → C û 0 172	16.20.108/services_dhcp_relay.php … 🖂	☆ III\ 🗉 ≡
COMMUNITY EDITION	em ∙ Interfaces • Firewall • Services • VPN • Status • Diagnostics • Help •	۵
Services / DHC	CP Relay	E 🔟 🚍 😝
DHCP Relay Confi	guration	
Enab	e 🕼 Enable DHCP relay on interface	
<u>Interface(</u>	ADMIN DMZ SERVEUR PROD Interfaces without an IP address will not be shown.	
	Append circuit ID and agent ID to requests If this is checked, the DHCP relay will append the circuit ID (pfSense interface number) and the agent ID to the DHCP request.	
Destination serve	This is the IPv4 address of the server to which DHCP requests are relayed.	
	Add server	
	pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license.	
🚱 (ð) 🚞 🔍 🕹		FR 🍝 🍡 🖓 🌆 17:41 20/03/2019

Configuration de la redirection de port :

On va ensuite faire une redirection de port car il y a un site Web dans le sous-réseaux DMZ en commençant par changer le port d'accès à l'interface web qui est 80 par défaut :

			•
Admin Access Firew	all & NAT Networking Miscellaneou	us System Tunables Notifications	
webConfigurator			
Protocol	● HTTP	OHTTPS	
TCP port	8080		
	Enter a custom port number for the webCon	figurator above to override the default (80 for HTTP, 443 for HTTPS). Chang	ges will take effect immediatel
	after save.		
Max Processes	after save.		

On va maintenant faire en sorte que tout ce qui vient par l'interface WAN sur le port 80 soit rediriger vers le site web dans la DMZ :

lit Redirect Entry							
Disabled	Disable this rule						
No RDR (NOT)	Disable redirection for traffic matching this rule						
	This option is rarely needed. Don't use this without thorough knowledge of the implications.						
Interface	WAN						
	Choose which interface this rule applies to. In most cases "WAN" is specified.						
Protocol	ТСР						
	Choose which protocol this rule should match. In most cases "TCP" is specified.						
Source	Cisplay Advanced						
Destination	Invert match.	WAN address		~		1	
		Туре			Address/mask		
Destination port range	HTTP		HTTP	~			
	From port	Custom	To port		Custom		
	Specify the port or port ra	ange for the destination of the	packet for this mapping	. The 'to' field	may be left empty if only	mapping a single port.	
Redirect target IP	10.0.0.81						
	Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12						
Redirect target port	HTTP		~				
	Port			Custom			
	Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "from port" above.						
	This is usually identical to	o the "From port" above.					