

Procédure Windows 10

CRÉATION D'UN PARE-FEU (PFSENSE)

Stcherbinine Mattéo | Windows 10 | 28/02/23 Attention : à regarder en mode Web !

Introduction

Dans cette procédure nous allons voir comment installer un pare-feu sur une machine virtuelle HyperV

Prérequis :

- Avoir télécharger l'iso de pfSense
- Avoir créer une machine virtuelle (4Go de RAM, 20Go de stockage)

ETAPES :

Tout d'abord il faut créer un port WAN et un port LAN. Pour se faire il faut ouvrir le gestionnaire des commutateurs virtuels :



Pour le LAN il faut cocher réseau Interne.

Commutateurs virtuels	🚜 Propriétés du commutateur virtuel —
👫 Nouveau commutateur réseau virtuel	
🚜 Default Switch	Nom :
Réseau par défaut	LAN
Intel(R) Wireless-AC 9462	Notes :
LAN Interne uniquement	
Paramètres du réseau global	
Plage d'adresses MAC 00-15-5D-51-C0-00 à 00-15-5D-51	Type de connexion À quoi voulez-vous connecter ce commutateur virtuel ? O Réseau externe :
	Intel(R) Wireless-AC 9462
	Autoriser le système d'exploitation de gestion à partager cette carte réseau
	Réseau interne Réseau privé
	ID du réseau local virtuel
	 Activer l'identification LAN virtuelle pour le système d'exploitation de gestion
	L'identificateur VLAN spécifie le réseau local virtuel utilisé par le système d'exploitation de gestion pour toutes les communications réseau par le biais de cette carte réseau. Ce paramètre n'affecte pas la mise en réseau d'ordinateurs virtuels. 2
	Supprimer

Pour le WAN il faut cocher réseau Externe.

commutateurs virtuen	Propriétés du c	commutateur virtuel
Nouveau commutateur	seau virtuel	
Réseau par défaut	WANI	
wan		
Intel(R) Wireless-AC 9	2 Notes :	
LAN		^ ^
Paramètres du réseau	obal	
00-15-5D-51-C0-00 à	-15-5D-51 À quoi voulez-vo Réseau exte	n us connecter ce commutateur virtuel ? rme :
	Intel(R) Wire	eless-AC 9462 v
	Autoriser réseau	le système d'exploitation de gestion à partager cette carte
	O Réseau inter	ne
	Réseau prive	
	ID du réseau loca	lvirtuel
	Activer lider	tification LAN virtuelle pour le système d'exploitation de gestion
	L'identificateur V d'exploitation de cette carte rése virtuels. 2	LAN spécifie le réseau local virtuel utilisé par le système gestion pour toutes les communications réseau par le biais de au. Ce paramètre n'affecte pas la mise en réseau d'ordinateurs
		Supprimer

Ensuite il faut les ajouter à notre machine virtuelle :

Il faut cliquer sur « Ajouter un matériel » et ensuite choisir notre commutateur. Ensuite il faut activer l'usurpation d'adresse MAC :





Ensuite on peut démarrer la machine virtuelle :

Une fois démarrée il faut faire accepter puis vous arriverez sur cette fenêtre où il faut faire « OK » :

pfSense Installer	
Welcome	
Welcome to pfSense!	
Install Install pfSense	
Rescue Shell Launch a shell for rescue operations	
L Recover config.xml Recover config.xml from a previous filscall	
<pre>Cancel></pre>	

Ensuite on sélectionne la langue qui nous convient puis vous pouvez faire « Continue » tout en haut :



Ensuite on choisit auto $2fs \rightarrow install \rightarrow stripe \rightarrow on choisit bien dao puis on confirme.$

Sur pfsense :

System - Interfaces -	Firewall - Services	- VPN -	Status -	Diagnostics 🗸	Help 👻	•
'admin' account password is set to t	the default value. Change t	the password in th	e User Manage	r.		
ofSense Setup /						0
up						
Welcome to pfSe	ense® software!					
This wizard will provid The wizard may be sto	le guidance through the ini	itial configuration	of pfSense.	e screen		
pfSense® software is	developed and maintaine	d by Netgate®				
Learn more						
>> Next						
F	System • Interfaces • • admini account password is set to pfSense Setup / tup Welcome to pfSe This wizard will provid The wizard may be st pfSense® software is Learn more	System • Interfaces • Firewall • Services • admini account password is set to the default value. Change • pfSense Setup / tup Welcome to pfSense® software! This wizard will provide guidance through the in The wizard may be stopped at any time by click pfSense® software is developed and maintaine Learn more Next	System • Interfaces • Firewall • Services • VPN • *admini account password is set to the default value. Change the password in the pfSense Setup / Image: Change the password in the password in the password in the physical set to the default value. Change the password in the pfSense Setup / tup Welcome to pfSense® software! This wizard will provide guidance through the initial configuration The wizard may be stopped at any time by clicking the logo image pfSense® software is developed and maintained by Netgate® Learn more >> Next	System • Interfaces • Firewall • Services • VPN • Status • *admini account password is set to the default value. Change the password in the User Manage pfSense Setup / tup Welcome to pfSense® software! This wizard will provide guidance through the initial configuration of pfSense. The wizard may be stopped at any time by clicking the logo image at the top of the pfSense® software is developed and maintained by Netgate® Learn more >> Next	System • Interfaces • Firewall • Services • VPN • Status • Diagnostics • • admini account password is set to the default value. Change the password in the User Manager. pfSense Setup / tup Welcome to pfSense® software! This wizard will provide guidance through the initial configuration of pfSense. The wizard may be stopped at any time by clicking the logo image at the top of the screen. pfSense® software is developed and maintained by Netgate® Learn more >> Next	System • Interfaces • Firewall • Services • VPN • Status • Diagnostics • Help • •*admini account password is set to the default value. Change the password in the User Manager. pfSense Setup / tup Welcome to pfSense® software! This wizard will provide guidance through the initial configuration of pfSense. The wizard may be stopped at any time by clicking the logo image at the top of the screen. pfSense® software is developed and maintained by Netgate® Learn more > Next

Une fois sur pfSense on peut faire next puis suivre la configuration :

General Information	
	On this screen the general pfSense parameters will be set.
Hostname	srv-MS-pfSense
	EXAMPLE: myserver
Domain	ms.local
	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. 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	192.168.1.2
Secondary DNS Server	8.8.8.8
Override DNS	
	Allow DNS servers to be overridden by DHCP/PPP on WAN

COMMUNITY EDITION		Services - VPN		Diagnostics 🗸	Help 🗸	C)
WARNING: The 'admin' acc	ount password is set to the default v	alue. Change the password	in the User Manag	er.		
Wizard / pfSense	e Setup / Time Server Ir	nformation				Ø
Step	13 of 9					
	Please enter the time, date and tir	ne zone.				
Time server hostname	2.pfsense.pool.ntp.org Enter the hostname (FQDN) of the	time server.				
Timezone	Etc/GMT+1		~			
	>> Next					

Pour l'étape 4 on peut juste faire next

		✓ Services ✓ VPN ✓	Status - Diagnostics -	Help 🗸	G
WARNING: The 'admin' acco	ount password is set to the defaul	It value. Change the password in the	e User Manager.		
Wizard / pfSense	Setup / Configure LA	AN Interface			0
	Step 5 of 9		-		
Configure LAN Interf	ace				
	On this screen the Local Area N	letwork information will be configur	red.		
LAN IP Address	192.168.1.254				
	Type dhcp if this interface uses	DHCP to obtain its IP address.			
Subnet Mask	24		~		

Pour l'étape 7 il faut mettre un mot de passe sécurisé mais pour l'exemple j'ai utilisé un mot de passe banal.

Wizard /	pfSense Setup / Reload configuration			0
	Step 7 of 9			
Reload con	figuration			
	Click Reload to reload ptSense with new changes.			
	>> Reload			
alsense	Oustava Istanfaasa Fiinaural - Daavisaa - V	/DN Ctatua _	Disgractica - Llala -	
	System • Interfaces • Firewall • Services • V	′PN ▼ Status ▼	Diagnostics 🕶 Help 🕶	
	System → Interfaces → Firewall → Services → V	′PN → Status →	Diagnostics + Help +	
	System • Interfaces • Firewall • Services • V Dashboard	′PN + Status +	Diagnostics + Help +	+ €
Status /	System → Interfaces → Firewall → Services → V Dashboard ormation	/PN - Status - Netgate Serv	Diagnostics + Help +	+ €
Status / System Inf Name	System + Interfaces + Firewall + Services + V Dashboard ormation F	/PN - Status - Netgate Serv	Diagnostics • Help • vices And Support	+ e • e
Status / System Inf Name User	System → Interfaces → Firewall → Services → V Dashboard ormation srv-MS-pfSense.ms.local admin@192.168.1.1 (Local Database)	/PN - Status - Netgate Serv Contra	Diagnostics + Help + vices And Support act type Community Support Community Support O	+ € ● €
Status / System Inf Name User System	System → Interfaces → Firewall → Services → V Dashboard ormation	/PN - Status - Netgate Ser Contra	Diagnostics • Help • vices And Support het type Community Support Community Support O	+ € • &
Status / System Inf Name User System BIOS	System + Interfaces + Firewall + Services + V Dashboard ormation From Contemporation Srv-MS-pfSense.ms.local admin@192.168.1.1 (Local Database) Microsoft Azure Netgate Device ID: f51243c9a3f65828a28b Relaese Data: Wed Des 31.1869	/PN - Status - Netgate Serv Contra	Diagnostics Help vices And Support act type Community Support Community Support Community Support Community Support O	+ @
Status / System Inf Name User System BIOS	System + Interfaces + Firewall + Services + V Dashboard ormation	/PN - Status - Netgate Serv Contra NETG/	Diagnostics Help vices And Support vices And Support Community Support Community Support Community Support Community Support Unour pfSense cateway freward	+ @
Status / System Inf Name User System BIOS Version	System → Interfaces → Firewall → Services → V Dashboard ormation	/PN - Status - Netgate Serv Contra NETG/ If you purchased Community Su	Diagnostics Help	+ € o & o support resources
Status / System Inf Name User System BIOS Version	System → Interfaces → Firewall → Services → V Dashboard	PN - Status - Netgate Serv Contra If you purchase Community Su hardware, you h	Diagnostics Help	+ € INV
Status / System Inf Name User System BIOS Version	System ◆ Interfaces ◆ Firewall ◆ Services ◆ V Dashboard ormation	PN - Status - Netgate Serv Contra If you purchaser Community Su hardware, you h the NETGATE F	Diagnostics Help	+ € NIY SUPPORT RESOURCES ppliance from Netgate and elected led pfSense on your own support resources. This includes ical Assistance Center (TAC)
Status / System Inf Name User System BIOS Version	System ◆ Interfaces ◆ Firewall ◆ Services ◆ V Dashboard ormation	PN - Status - Netgate Serv Contra If you purchased Community Su hardware, you h the NETGATE F You also may up Support subscri	Diagnostics Help	+ €
Status / System Inf Name User System BIOS Version	System + Interfaces + Firewall + Services + V Dashboard ormation	PN - Status - Netgate Serv Contra If you purchased Community Su hardware, you h the NETGATE You also may up Support subscri Support subscri	Diagnostics Help	+ € Inly SUPPORT RESOURCES ppliance from Netgate and elected led pfSense on your own r support resources. This includes ical Assistance Center (TAC) is staffed 24x7x365 and de support at a price point that is no uncome
Status / System Inf Name User System BIOS Version	System ◆ Interfaces ◆ Firewall ◆ Services ◆ V Dashboard ormation	PN - Status - Netgate Serv Contra NETG/ If you purchased Community Su hardware, you h the NETGATE F You also may up Support subscrip committed to de more than comp	Diagnostics Help Vices And Support Vices And Support Community Support Community Support O ATE AND pfSense COMMUNITY d your pfSense gateway firewall a port at the point of sale or insta ave access to various community RESOURCE LIBRARY. Dygrade to a Netgate Global Techn plon. We're always on! Our team livering enterprise-class, worldwive tetlitve when compared to others	e e e e e e e e e e e e e e e e e e e
Status / System Inf Name User System BIOS Version	System ◆ Interfaces ◆ Firewall ◆ Services ◆ V Dashboard ormation	PN - Status - Netgate Serv Contra NETG/ If you purchased Community Su hardware, you h the NETGATE F You also may up Support subsort committed to de more than comp • Upgrade Yo	Diagnostics Help	+ @
System Inf System Inf Name User System BIOS Version CPU Type Hardware crypt	System ◆ Interfaces ◆ Firewall ◆ Services ◆ V Dashboard ormation	PN - Status - Netgate Serv Contra NETG/ If you purchased Community Su hardware, you h the NETGATE You also may up Support subscri committed to de more than comp • Upgrade You • Netgate Glo	Diagnostics Help Vices And Support Vices And Support Community Support Community Support Community Support ONTE AND pfSense COMMUNITY d your pfSense gateway firewall a port at the point of sale or insta ave access to various community RESOURCE LIBRARY. Dograde to a Netgate Global Techn pion. We're always on! Our team livering enterprise-class, worldwi vetiftive when compared to others ur Support • Commu bal Support FAQ • Official g	+ @

Création et modification des règles :

F	irew	all / Rules	/ LAN									≢ Ш 🗏 😯
FI	oating	WAN	LAN									
R	ules	(Drag to Chan	ge Order)	Dort	Destination	Port	Cataway	00000	Sabadula	Description	Actions
0	~	19 /2.32 MiB	*	*	*	LAN Address	443	*	*	Scheuule	Anti-Lockout Rule	
							80					
	~	2 /98.64 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	ৼ৵৻ৢ৾৾৾৾৾৾৾৾৾৾৾৾৾৾৾৾৾
	~	0 /0 B	IPv6 *	I AN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	ৼ৵ঢ়৹ঢ়
				Es artifict							,	

On modifie la règle IPv4 pour changer « Pass » sur « Block ». On va faire de même sur la règle IPv6.

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, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Ensuite il ne faut pas oublier d'appliquer les changements :

The firewall rule configuration has been changed. The changes must be applied for them to take effect.	✓ Apply Changes
---	-----------------

On se rend maintenant dans Firewall \rightarrow Aliases \rightarrow Ports

COMMUNITY EDITION	ystem - Interface	es 🔹 🛛 Firewall 👻	Services -	VPN 🕶	Status 🕶	Diagnostics -	Help 👻	¢
Firewall / Alia	iases / Ports							幸 🔟 😯
IP Ports	URLs All							
Firewall Aliases	s Ports							
Name	Value	s	Des	cription			Actions	
								+ Add 1mport

Puis on va ajouter 3 ports :

COMMUNITY EDITION Sys	tem -	Interfaces 🗸	Firewall 🗸	Services 🗸	VPN 🗸	Status 🗸	Diagnostics 🗸	Help 🕶	•
Firewall / Alia	ses /	' Edit							Ø
Properties									
Nar	ne	Base-Internet							
		The name of the ali	as may only con	sist of the charac	ters "a-z, A-Z	, 0-9 and _".			
Descripti	on								
		A description may b	e entered here f	or administrative	reference (n	ot parsed).			
<u>Ty</u>	pe	Port(s)				~			
Port(s)									
н	int	Enter ports as desir	ed, with a single	port or port rang	e per entry. F	Port ranges car	be expressed by sep	parating with a co	olon.
P	ort	80			Н	TTP			Delete
		443			Η	TTPS			Delete
		53			D	NS			Delete
		Save + Add	d Port						

Il ne faut pas oublier d'appliquer :

The alias list has been change The changes must be applied	d. for them to take effect.		✓ Apply Changes
IP Ports URLs	All		
Name	Values	Description	Actions
Base_Internet	80, 443, 53		✓ □ 面
			+ Add 🔝 impo

Ensuite on va ajouter une règle de pare-feu en cliquant sur le premier Add :



Dans la configuration on va mettre Pass pour laisser passer le flux, LAN car on est en local, IPv4 car c'est ce que l'on a configuré, protocole TCP/UDP, destination port range on choisit l'Alias qu'on a créer plutôt. On va enfin cocher les logs.

Action	Pass		~				
	Choose what to do with packe	ts that match the criteria sp	ecified below.				
	Hint: the difference between b	lock and reject is that with r	eject, a packet (TCP	RST or ICMP p	oort unreachable for UDP) is re	eturned to the se	ender,
	whereas with block the packet	t is dropped silently. In eithe	r case, the original p	acket is discar	ded.		
Dischlad	Dischle this rule						
Disabled							
	Set this option to disable this	rule without removing it from	n the list.				
Interface	LAN						
interrute			· · · · · · ·				
	Choose the interface from wh	ich packets must come to m	latch this rule.				
Address Family	IDv/		~				
<u></u>	Calent the Internet Distance	raion this rule applies to					
	Select the internet Protocol ve	i sion this fulle applies to.					
Protocol	TCP/UDP		~				
	Choose which IP protocol this	rule should match					
	choose which if protocol this	rule should match.					
Source							
		onv			Source Address	1	
Source	Invert match	any		•	Source Address	1	~
	Display Advanced						
	The Source Port Range for a c	connection is typically rando	m and almost never	equal to the d	estination port. In most cases	this setting mu	st remain at
	its default value, any .						
	its default value, any .						
Destination	its default value, any .						
Destination	its default value, any .	any		~	Destination Address	1	~
Destination Destination	its default value, any.	any		~	Destination Address	/	~

OMM	Sens	C System	n 👻 Interface	es 🔹 🕴	irewall	l → Service	is → VPN →	Statu	IS ¥	Diagnostic	s • Help •				
F	irewal	I / Rules	/ LAN										-	<u>≢ Iui</u>	• •
Tł	ne change	es have been a	pplied successfu	lly. The fire	wall rul	es are now relo	ading in the back	ground.							×
FI	loating	WAN	LAN												
F	loating	WAN	LAN												
FI RI	loating ules (Di	WAN rag to Char States	LAN nge Order) Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description			Actions	
FI RI	loating ules (Di	WAN rag to Char States 4 /2.71 MiB	LAN nge Order) Protocol	Source *	Port *	Destination LAN Address	Port 443 80	Gateway *	Queue *	Schedule	Description Anti-Lockout Rul	e		Actions	
FI RI	loating ules (Di	WAN rag to Char States 4/2.71 MiB	LAN Protocol * IPv4 TCP/UDP	Source * *	Port * *	Destination LAN Address *	Port 443 80 Base_Internet	Gateway * *	Queue * none	Schedule	Description Anti-Lockout Ruk	e		Actions	QQT
FI RI D	loating ules (D X	WAN rag to Char States 4/2.71 MiB 0/0 B 0/28 KiB	LAN Protocol * IPv4 TCP/UDP IPv4 *	Source * * LAN net	Port * * *	Destination LAN Address *	Port 443 80 Base_Internet *	Gateway * *	Queue * none none	Schedule	Description Anti-Lockout Rul Default allow LAI	e N to any rule		Actions C C C C C C C C C C C C C C C C C C C	90i

Même si maintenant on a internet, on ne peut pas ping avec l'invite de commande, pour y remédier on va ajouter une règle :

Disabled	Disable this rule						
	Set this option to disabl	e this rule without removing it fro	om the list.				
Interface	LAN		~				
	Choose the interface fro	om which packets must come to	match this rule.				
Address Family	IPv4 ~						
	Select the Internet Proto	col version this rule applies to.					
Protocol	ICMP		~				
	Choose which IP protoc	ol this rule should match.					
ICMP Subtypes	any		<u>~</u>				
	Datagram conversion e	error					
	For ICMP rules on IPv4,	one or more of these ICMP subty	ypes may be specified.				
Source							
Source	Invert match	LAN net		~	Source Address	17	Ŷ
Destination							
Destination	Invert match	any		~	Destination Address	1	Ý
Extra Options							
Log	Log packets that are	handled by this rule					
	Lint: the firewall has lim	aited local log enges. Don't turn o	a leasing for monthing. If	daina a	lat of logging consider using a res	ante evelo e como	lana

Après avoir paramétrer la règle, la sauvegarder et appliquer les changements on peut ping :

	- 🗆 ×	
- Microsoft Windows [version 10.0.19045.2251] (c) Microsoft Corporation. Tous droits réservés.	^	≢ ਘ 🗉 😯
C:\Users\Service Info>ping 9.9.9.9		
ThEnvoi d'une requête 'Ping' 9.9.9.9 avec 32 octets de données : Miképonse de 9.9.9.9 : octets=32 temps=30 ms TH=51 Réponse de 9.9.9.9 : octets=32 temps=32 ms TH=51 Réponse de 9.9.9 : octets=32 temps=32 ms TH=51 Réponse de 9.9.9.9 : octets=32 temps=32 ms TH=51		×
F Statistiques Ping pour 9.9.9.9: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 6%), Ourée approximative des boucles en millisecondes : R Minimum = 30ms, Maximum = 38ms, Moyenne = 33ms		
C:\Users\Service Info>_		Actions
		\$
		ৢঀ৻৻৻
		₺₡₽०ĭ
	to envirole	₺∥₽©ĩ
	to any rule	

Et voilà le pare-feu est maintenant installé, configuré et prêt pour l'utilisation !