Suivi des modifications

Version	Référence	Auteur	Date	Commentaires
Α	TP_Abo	Alexandre	29/01/2025	Création

Objet :

Mise en place d'un serveur Docker et Portainer sous Debian 12

Diffusion :

BTS SIO – Étudiants BTS SIO.

Développement :

Table des matières

Installation pfSense	2
Configuration du Pare-Feu pfSense	3
Configuration du proxy squid	4
Configuration VPN	6



.....

Installation pfSense

L'installation de pfSense ce fait assez simplement. Nous devons juste définir son adresse IP coté WAN, celle qui nous donnera internet, et son adresse IP coté LAN, ça sera notre passerelle pour notre réseau local. pfSense sera notre routeur mais également notre pare-feu (firewall) pour notre réseau LAN, il peut également faire office de proxy transparent, afin de bloquer certains site.

Starting syslogdone. Starting CRON done. pfSense 2.4.4-RELEASE amd64 Thu Sep 2 Bootup complete	0 09:03:12 EDT 2018
FreeBSD/amd64 (pfSense.localdomain) (ttyv0)
Hyper-V Virtual Machine - Netgate Dev	ice ID: 391ed73786ee43989c09
*** Welcome to pfSense 2.4.4-RELEASE	(amd64) on pfSense ***
WAN (wan) -> hn0 -> v4/ LAN (lan) -> hn1 -> v4:	DHCP4: 192.168.100.150/24 192.168.1.1/24
 O) Logout (SSH only) 1) Assign Interfaces 2) Set interface(s) IP address 3) Reset webConfigurator password 4) Reset to factory defaults 5) Reboot system 6) Halt system 7) Ping host 8) Shell 	 9) pfTop 10) Filter Logs 11) Restart webConfigurator 12) PHP shell + pfSense tools 13) Update from console 14) Enable Secure Shell (sshd) 15) Restore recent configuration 16) Restart PHP-FPM
Enter an option:	

Une fois l'installation faite tout ce passera sur l'interface web de pfSense.





[2SIO] _Abo

C 0 192 168 1						< 8 0	
Senne 👘	stern + Interfaces + Firewall + Services +	VIN + Status	e 1	legnostics •	Gold -	Help +	
Status / Dash	board						8+0
System Informat	ion /00	Interface					100
Name	pfsense kinto	4 MAN	*	1000baseT <t< td=""><td>vi-duplex-</td><td>83.</td><td>38</td></t<>	vi-duplex-	83.	38
System	pfSense	ALM.	÷	1000baseT +f	ul-duplex-	192	168.5.1
	Serial: 41dcded1-f581-11e5-8422-000db946799c Netgete Unique ID: 6985962a21ed1dd52962	Gateway	8				100
8105	Vendor coreboot	Name		RTT	RTTsd	Loss	Status
	Version: 4.0.7 Release Date: 02/28/2017	WAN_DHCP		7.0ms	2.0me	0.0%	Online
Version	2.3.4-RELEASE (wr/d-4) built on Wed May 03 15/13/29 (01 2017 Free850 10.3-RELEASE p19	Traffic G WAN	raphs	t		Creat (rs)	<i>200</i>
	Version 2.3.4.1 is available.					1	508
Platform	pfSense	10.2	٨	.1	/		1.
СРО Туре	AMD GX-412TC SOC 4 CPUs: 1 package(s) x 4 core(s)	h	WL	MAN	you	WW	MMA
Hardware crypto	AES-OBC.AES-XTS.AES-GCM.AES-ICM	V		N.	1		0.0
Uptime	2 Days 03 Hours 47 Minutes 05 Seconds	111	1.1		- his	M. L.	Color Market
Current date/time	Son Aug 13 21:27:53 UTC 2017	29.55		26.40		27:30	27:54
DNS server(x)	 127.0.0.1 83.255.255.2 83.255.255.1 	LAN					140 5005
Last config change	Son Aug 13 21:24:53 UTC 2017	1000-000	(bead)	Jane	and a state of the	MAGAAGIM	0.0
State table size	0% (194/188000) Show states			14.00	NYA.		11/10/-29
MBUF Usage	5% (8086/117464)	1	V		1	and the second second	- 1 - 438
Load average	0.26, 0.24, 0.12						000
CPU usage	35	-	* ****	a.e.		0.30	100
Memory usage		D.M.A.R.	r. orali				200

Configuration du Pare-Feu pfSense

Le pare-feu de pfSense permet de bloquer des ports, ou de faire des redirections de ports si nécessaire.

Exemple de règles de redirection de ports.

pf	Sei	nse	Syste	∙m + Ir	nterfaces -	Firewall -	Services -	VPN - Stat	us - Diagnos	tics 👻 Help 🗸		•
w	ARNI	NG: T	he 'admin' :	account pas	sword is set to th	e default value.	Change the pass	word in the User	Manager.			
F	irev	vall	/ NAT	/ Port F	Forward							0
P	ort Fo	orward	H 1:1	Outbo	ound NPt							
R	ules		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NATIP	NAT Ports	Description	Actions
	~	24	WAN	TCP/UDP	*	*	WAN address	3389 (MS RDP)	192.168.10.100	3389 (MS RDP)	win10	
0	~	24	WAN	TCP/UDP	*	*	WAN address	3390	192.168.10.250	3389 (MS RDP)	winserver	Ø0 0
	~	2\$	WAN	TCP/UDP	*	*	WAN address	2222	192.168.20.250	22 (SSH)	debiandatabases	Ø 🗋 💼
	~	*	WAN	TCP/UDP	*	*	WAN address	2022	192.168.50.250	22 (SSH)	debianweb	Ø 🗋 💼
	~	2\$	WAN	TCP	*	*	WAN address	4443	192.168.10.1	443 (HTTPS)	pfSense	Ø 🖸 💼
	~	2\$	WAN	TCP/UDP	*	*	WAN address	9443	192.168.20.250	9443	portainer_serverdatabases	e 🗋 🖉
	~	2\$	WAN	TCP/UDP	*	*	WAN address	8443	192.168.50.250	9443	portainer_serverweb	Ø 🗋 💼
	~	2\$	WAN	TCP/UDP	*	*	WAN address	81	192.168.50.250	81	nginx-admin	Ø 🗋 💼
	~	2\$	WAN	TCP/UDP	*	*	WAN address	443 (HTTPS)	192.168.50.250	443 (HTTPS)	nginx-proxy	e 🖓 🖓 🛅
	~	2\$	WAN	TCP/UDP	*	*	WAN address	80 (HTTP)	192.168.50.250	80 (HTTP)	nginx-proxy-80	
	~	24	WAN	TCP/UDP	*	*	WAN address	8180	192.168.50.250	8180	Wordpress sans proxy	Ø 🗋 💼
0	~	2\$	WAN	TCP/UDP	*	*	WAN address	8380	192.168.50.250	8380	prestashop	Ø 🗋 🖻
	~	2\$	WAN	TCP/UDP	*	*	WAN address	8280	192.168.50.250	8280	Nextcloud sans proxy	Ø 🗋 💼
	~	2\$	WAN	TCP/UDP	*	*	WAN address	7575	192.168.20.250	7575	homarr	<i>i</i> 🖓 🗇 💼
									1 Add	🕽 Add 🛅 Dele	te 🚫 Toggle 📑 Save	+ Separator

Règles de pare-feu.

				Travau pf	x Pratiques Sense	•				Versi	on : A	
FORMATION				[2SI	O] _Abo				Γ	Date : 29	/01/2025	
Firew	all / Rule	es / OPT	1								<u>.ul</u> 📰	0
Floatin	g WAN	LAN	OPT1 OPT	2 OPT3								
Rules	(Drag to Cl	hange Orde	er)									
Rules	(Drag to Cl States	hange Orde Protocol	er) Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	_
Rules	(Drag to Cl States 0/0 B	hange Orde Protocol IPv4 TCP	er) Source OPT2 address	Port 1514 - 1515	Destination 192.168.20.250	Port 1514 - 1515	Gateway *	Queue none	Schedule	Description	Actions	×
Rules	(Drag to Cl States 0/0 B 0/0 B	hange Orde Protocol IPv4 TCP IPv4 TCP	Source OPT2 address OPT3 address	Port 1514 - 1515 1514 - 1515	Destination 192.168.20.250 192.168.20.250	Port 1514 - 1515 1514 - 1515	Gateway * *	Queue none none	Schedule	Description	Actions ♣ ✔ 🗋 ◇ 🟛 ♣ ✔ 🗋 ◇ 💼	×
Rules	(Drag to Cl States 0/0 B 0/0 B 0/0 B	hange Orde Protocol IPv4 TCP IPv4 TCP IPv4 TCP	Source OPT2 address OPT3 address LAN address	Port 1514 - 1515 1514 - 1515 1514 - 1515	Destination 192.168.20.250 192.168.20.250 192.168.20.250	Port 1514 - 1515 1514 - 1515 1514 - 1515	Gateway * * *	Queue none none none	Schedule	Description	Actions $ \stackrel{\bullet}{\bullet} \stackrel{\bullet}{\bullet} \bigcirc \widehat{\square} $ $ \stackrel{\bullet}{\bullet} \stackrel{\bullet}{\bullet} \bigcirc \widehat{\square} $	×
Rules	(Drag to Cl States 0/0 B 0/0 B 0/0 B 2/2.95 GiB	Protocol IPv4 TCP IPv4 TCP IPv4 TCP IPv4 TCP	Pr) Source OPT2 address OPT3 address LAN address *	Port 1514-1515 1514-1515 1514-1515 1514-1515	Destination 192.168.20.250 192.168.20.250 192.168.20.250 192.168.20.250	Port 1514-1515 1514-1515 1514-1515 *	Gateway * * * *	Queue none none none	Schedule	Description	Actions \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	× × × ×

Ces règles permettent le bon fonctionnement de l'agent Wazuh, ainsi l'agent peut communiquer avec son serveur même si celui-ci est dans un VLAN différent que celui du serveur.

Configuration du proxy squid

Nous allons utiliser Squid en mode proxy transparent. Cela signifie que le trafic web des utilisateurs sera redirigé automatiquement vers le proxy, sans configuration manuelle sur les postes clients.

Dans ce mode, Squid ne déchiffre pas le contenu des paquets HTTPS, mais se limite à lire le nom de domaine (SNI - Server Name Indication) contenu dans la requête TLS. Grâce à cette information, Squid peut appliquer des règles de filtrage pour autoriser ou bloquer l'accès à certains sites en fonction de leur fiabilité ou de leur catégorie.

Ce fonctionnement permet de filtrer efficacement le trafic HTTPS sans inspection approfondie du contenu, ce qui évite des problèmes de certificats ou de confidentialité, mais limite aussi la finesse du contrôle (pas de filtrage par URL ou contenu précis en HTTPS).

2	- I		pfSense		Version : A
DE FORM	6 ATTON		[2SIO] _Abo	I	Date : 29/01/2025
DI COM	Sense Sys	tem • Interfaces	Firewall Services VPN	Status • Diagnostics • Help •	
2000	Package / Pro	xy Server: Gen	eral Settings / General		0 ≆ Ш =
	General Remote	Cache Local Cac	he Antivirus ACLs Traffic Mgmt	: Authentication Users Real Tin	ne Sync
	Squid General Se	ttings			
	Enable Squid Pro	xy Check to ena	able the Squid proxy. checked, ALL Squid services will be disabled and	d stopped.	
	Keep Settings/Da	ita 🗹 If enabled, th Important: If dis	e settings, logs, cache, AV defs and other data w sabled, all settings and data will be wiped on pac	II be preserved across package reinstalls. kage uninstall/reinstall/upgrade.	
	Listen IP Versi	on [IPv4 Select the IP ver	sion Squid will use to select addresses for accep	✓ ting client connections.	
	CARP Status \	/IP none Used to determi	ne the HA MASTER/BACKUP status. Squid will be	stopped when the chosen VIP is in BACKUP sta	itus, and started in MASTER statu
	Proxy Interface	(s) WAN PERIMETER	t forget to generate Local Cache on the secondar	y node and configure XMLRPC Sync for the set	ings syncronization.
	-	The interface(s)	the proxy server will bind to. Use CTRL + click to	* select multiple interfaces.	
(Proxy P	ort 3128 This is the port	the proxy server will listen on. Default: 3128		1
	[N	10 lines 🔹 Iax. lines to be displa	ved.		
	1				
	Ē	nter a grep-like string	/pattern to filter the log entries.		
	E	.g.: username, IP addr lse ! to invert the sens	ress, URL. e of matching (to select non-matching lines)		
Ta	ible				
			Squid - Access Logs		
	IP	Status	Address	User	De
14	192.168.100.100	TCP_DENIED/407	safebrowsing.googleapis.com:443		
:09	192,168,100,100	TCP_TUNNEL/200	site-cdn.onenote.net:443	rick.sanchez@JOURNEYOFTHEGEEK.LO	CAL 23
43	192,168,100,100	TCP_TUNNEL/200	www.amazon.com:443	rick.sanchez@JOURNEYOFTHEGEEK.LO	CAL 52
40	192.168.100.100	TCP_TUNNEL/200	images-na.ssl-images-amazon.com:443	rick.sanchez@JOURNEYOFTHEGEEK.LO	CAL 52
33	192.168.100.100	TCP_TUNNEL/200	b-ring.msedge.net:443	rick.sanchez@JOURNEYOFTHEGEEK.LO	CAL 13
32	192.168.100.100	TCP_TUNNEL/200	I-ring.msedge.net:443	rick.sanchez@JOURNEYOFTHEGEEK.LO	CAL 13
20	192,168,100,100	TCP_TUNNEL/200	a-ring.msedge.net:443 fn msedge.net:443	rick.sanchez@JOURNEYOFTHEGEEK.LO	CAL 20
49	192.168.100.100	TCP_TUNNEL/200	s.amazon-adsystem.com:443	rick.sanchez@JOURNEYOFTHEGEEK.LO	CAL 54
Tab	le				
			Sould - Cooke Loop		
	lessage		aquiu - cache Loga		
N	egotiate_kerberos_a ERomAEXtGu4X328	uth: DEBUG: AF oYGk 2TagvryJFayoyJbdQł	MIGhoAMKAQChCwYJKoZIgvcSAQICooGME 172s8cAILGouZGVR/HLysf2wxL5eJJ/eCa82X	81GJY1GGBgkqhkiG9x1BAgICAG93MHWgAwi 3d4RC41faHePJT9d1w34LSjxZNmQ5rC0Eu6	BBaEDAgEPo oohJyhakGCh9
N n 00gi		:nez@JOURNEYOFTF	IEGEEK.LUCAL		AAA
N n 00g ci	rp0dqKnE= rick.sano egotiate_kerberne_=	with: DEBLIG: Groups a	have the second second the manufacture of the second	Amonio della a con di anto contra contra della	2000.0
N 00gi 00n	rp0dqKnE= rick.san egotiate_kerberos_a egotiate_kerberos_a	uth: DEBUG: Groups ; uth: INFO: Read 492 c	of 496 bytes		
N 00gi ci 00n 00n	rp0dqKnE= rick.san egotiate_kerberos_a egotiate_kerberos_a egotiate_kerberos_a	with: DEBUG: Groups (with: INFO: Read 492 (with: INFO: Got ExtraS	of 496 bytes id S-1-18-1		
N 00gi 00n 00n 00n	rp0dqKnE= rick.sano egotiate_kerberos_a egotiate_kerberos_a egotiate_kerberos_a egotiate_kerberos_a	auth: DEBUG: Groups (auth: INFO: Read 492 (auth: INFO: Got ExtraS auth: INFO: Found 1 E	of 496 bytes id S-1-18-1 traSIDs		
N 00gi 00n 00n 00n	rpOdqKnE= rick.sano egotiate_kerberos_a egotiate_kerberos_a egotiate_kerberos_a egotiate_kerberos_a egotiate_kerberos_a	auth: DEBUG: Groups (auth: INFO: Read 492 (auth: INFO: Got ExtraS auth: INFO: Got ExtraS auth: INFO: Got Domai	of 496 bytes id S-1-18-1 «traSIDs nLogonId S-1-5-21-2573343550-445058083-	316878962	



[2SIO] _Abo

Configuration VPN

Nous allons utiliser pfSense pour mettre en place un VPN (réseau privé virtuel), ce qui permettra aux utilisateurs d'accéder à distance au réseau local de manière sécurisée, comme s'ils étaient physiquement connectés à celui-ci.

Le VPN créé avec pfSense établit un tunnel chiffré entre le poste client et le routeur pfSense, garantissant la confidentialité et l'intégrité des données qui transitent. Cela est particulièrement utile pour le télétravail, l'accès à des serveurs internes ou encore pour connecter plusieurs sites distants entre eux.

Avec pfSense, il est possible de configurer différents types de VPN, comme OpenVPN, IPSec ou WireGuard, chacun ayant ses avantages. OpenVPN est souvent privilégié pour sa compatibilité et sa simplicité de mise en œuvre. Une fois configuré, le VPN ne nécessite qu'un petit client sur l'ordinateur distant, et les règles de pare-feu permettent de contrôler précisément ce à quoi l'utilisateur a accès à travers le tunnel VPN.

								Captive	Portal				
Status	/ S	ervices						CARP (f	ailover)				
								Queues	,				
Services	S	Rovya						Services	5				
ervice		I	Descrip	tion				System	Logs	tus		Actions	
dhcpd			DHCP	Service						0		CO	新門
dpinger			Gatewa	ay Monit	oring Daemo	on				0		CO	記画
ipsec			IPsec \	/PN						۲		CO	新門
otoci			NTD al	ook ovno						0		CO	÷. Eladi
			NIPCI	JCK Sync						V			_
openvpn Tunnels	Mobile C	Clients Pre-Sha	OpenVI openVI	PN serve	er: Accès Def	fi Bois				0		C®	÷Ш
Depenypn Funnels M he IPsec tunne he changes m Psec Tunne	Mobile C el config nust be a el s	Clients Pre-Sha uration has been ch oplied for them to ta Preya	OpenVI red Keys anged ke effect.	PN serve Adva	er: Accès Def	fi Bois				0		C O :	y Change
Dopenvpn Tunnels M he IPsec tunne he changes m Psec Tunne	Mobile C el config nust be a el s IKE	Clients Pre-Sha puration has been ch pplied for them to ta Pavya Remote Gateway	OpenVI red Keys anged ke effect.	Adva Mode	er: Accès Def nced Settings P1 Protocol	fi Bois	P1 T	ransforms	P1 DH-0	Group	P1 Desc	C O :	y Change:
Depenypn Funnels Funnels Funnels Funnels Funnels Funnels Funnel Funnel Funnel Funnel Funnel	Mobile C el config ust be a els f IKE V2	Clients Pre-Sha uration has been ch pplied for them to ta Remote Gateway WAN 2.2.2.2	OpenVI red Keys anged ke effect.	Adva Mode	er: Accès Def nced Settings P1 Protocol AES256-GCM (fi Bois (128 bits)	P1 T SHA	ransforms 256	P1 DH-0 14 (204	Sroup 8 bit)	P1 Desc VPN ave	Apply ription ec site B	y Change Action
Depenypn	Mobile C el config ust be a els iKE V2	Clients Pre-Sha uration has been ch pplied for them to ta Remote Gateway WAN 2.2.2.2	Mode	Adva Mode	er: Accès Def nced Settings P1 Protocol AES256-GCM (bnet Remote S	fi Bois (128 bits) Subnet	P1 T SHA	ransforms 256 P2 Transfor	P1 DH-0 14 (204 ms	Sroup 8 bit) P2 Auth M	P1 Desc VPN ave Methods	ec site B P2 actions	y Change Action
Depenypn funnels M he IPsec tunne he changes m Psec Tunne	Mobile C el config nust be a el s IKE V2	Clients Pre-Sha puration has been ch polled for them to ta Remote Gateway WAN 2.2.2.2	Mode tunnel	Adva Adva Mode Local Sul	er: Accès Def need Settings P1 Protocol AES256-GCM (bnet Remote 192.168.	fi Bois (128 bits) Subnet 3.10.0/24	P1 T SHA P2 Protocol ESP	ransforms 256 P2 Transfor AES256 GC	P1 DH-(14 (204 ms M (128 bits)	Sroup 8 bit) P2 Auth M SHA256	P1 Desc VPN ave	ription ec site B P2 actions	y Change Action