

PPE N°3 PfSense -CrowdSec

DOCUMENTATION TECHNIQUE





Nolian Botelho PROMEO

SOMMAIRE

۱.	Présentation du projet
1.1	Introduction

II.	Contexte
2.1.	Scénario
2.2	Cahier des charges
2.3	Besoin logiciels
2.4	Schéma réseaux

III. Déroulement de l'installation et des configurations

I. Présentation du Projet

3.1 Introduction

Dans un monde où la cybercriminalité est en constante évolution, la sécurisation des réseaux informatiques est devenue une préoccupation majeure pour les entreprises.

Afin de protéger efficacement les données sensibles et d'assurer la continuité des opérations, il est essentiel de mettre en place des solutions de sécurité robustes et adaptées aux besoins spécifiques de chaque organisation. Dans ce contexte, la mise en œuvre d'un pare-feu performant tel que pfSense, associé à des outils de filtrage web comme Squid et à des mécanismes de détection d'intrusion tels que CrowdSec, représente une stratégie essentielle pour renforcer la sécurité du réseau.

2.1 Scénario

SecureNet Solutions spécialisée dans les services informatiques et la sécurité des réseaux. Forte de son expertise, l'entreprise s'est vu confier la mission de concevoir et de déployer une infrastructure réseau sécurisée pour un client stratégique, une grande entreprise internationale opérant dans le secteur financier.

Pour répondre aux besoins spécifiques de ce client, SecureNet Solutions a décidé de mettre en place une architecture réseau comprenant un pare-feu pfSense configuré avec plusieurs zones distinctes, notamment un LAN (Local Area Network), un WAN (Wide Area Network) et une DMZ (Zone Démilitarisée). Cette architecture permettra de segmenter le réseau et de limiter l'exposition aux menaces potentielles.

De plus, afin de renforcer la sécurité du réseau, SecureNet Solutions prévoit d'installer Squid, un proxy/cache web, pour filtrer le trafic web et limiter l'accès à certains sites jugés non sécurisés ou non conformes aux politiques de l'entreprise. Parallèlement, l'entreprise envisage d'intégrer CrowdSec, un système de détection d'intrusion collaboratif, pour détecter et bloquer automatiquement les comportements malveillants sur le réseau.

2.2 Cahier des Charges

Configuration du réseau :

- Installation d'un pare-feu pfSense pour assurer la sécurité du réseau.
- Configuration d'un réseau local (LAN) pour les utilisateurs internes de TechCorp.
- Configuration d'un réseau étendu (WAN) pour la connexion à Internet.
- Mise en place d'une zone démilitarisée (DMZ) pour héberger les serveurs accessibles depuis l'extérieur tout en isolant le réseau interne.

<u>Sécurité du réseau :</u>

• Mise en œuvre de règles de pare-feu strictes pour contrôler le trafic entrant et sortant.

• Configuration de listes de contrôle d'accès (ACL) pour restreindre l'accès aux ressources sensibles.

• Utilisation de VLANs pour segmenter le réseau et limiter la propagation des menaces potentielles.

Filtrage web :

• Installation et configuration de Squid comme proxy pour le filtrage du contenu web.

• Paramétrage de règles de filtrage pour bloquer l'accès à des sites web malveillants ou non autorisés.

• Mise en place de rapports de journalisation pour suivre l'activité web des utilisateurs et détecter les comportements suspects.

Protection contre les menaces :

• Intégration de CrowdSec pour détecter et bloquer automatiquement les tentatives d'attaques sur le réseau.

• Configuration de règles de détection pour identifier les comportements anormaux et les activités malveillantes.

• Mise en place de mécanismes de réponse automatisée pour neutraliser les attaques et protéger l'intégrité du réseau.

Test d'intrusion :

• Configuration d'une machine Kali Linux pour simuler une attaque depuis l'extérieur du réseau.

• Réalisation de tests d'intrusion réguliers pour évaluer l'efficacité des mesures de sécurité mises en place.

• Analyse des résultats des tests d'intrusion pour identifier les failles potentielles et renforcer la sécurité du réseau.

2.3 Besoins Logiciels

- Machine Kali Linux
- Serveur Active Directory
- Serveur Contrôleur de domaine
- Serveur WEB
- Machine PfSense
- 1 client Windows 10
- 1 client Windows 10

2.4 Schéma Reseaux



III. Déroulement de l'Installation de PFSENSE

Pour commencer nous allons commencer par l'installation de PfSense. Lancer la VM précédemment télécharger sur le site de PfSense.

pcib28: <ACPI PCI-PCI bridge> at device 24.1 on pci8 pcib29: <ACPI PCI-PCI bridge> at device 24.2 on pci8 pcib38: <ACPI PCI-PCI bridge> at device 24.3 on pci8 pcib31: <ACPI PCI-PCI bridge> at device 24.4 on pci8 pcib32: <ACPI PCI-PCI bridge> at device 24.5 on pci8 pcib33: <ACPI PCI-PCI bridge> at device 24.6 on pci8 pcib34: <ACPI PCI-PCI bridge> at device 24.7 on pci8 acpi_acad0: <AC Adapte> on acpi8 atkbdc8: <Keyboard controller (18042)> port 0x60,0x64 irq 1 on acpi0 atkbd0: <AT Keyboard> irq 1 on atkbdc0 kbd0 at atkbd8 atkbd0: (GIANT-LOCKED] psM0: (PS/2 Mouse> irq 12 on atkbdc8 psM0: [GIANT-LOCKED] HARNING: Device "psM" is Giant locked and May be deleted before FreeBSD 14.0. psM0: <ISA Option ROMs> at ioHem 0xc0000-0xc7fff,0xc80000-0xc9fff,0xca000-0xcafff ,0xcb0000-0xcbfff,0xcc0000-0xccfff,0xdc000-0xdffff,0xc80000-0xc9fff,0xca000-0xcafff ,0xcb0000-0xcbfff,0xcc0000-0xccfff,0xdc0000-0xdffff,0xc80000-0xc0fff pnpid DRM0000 o n isa0 vga0: 'Generic ISA UGA> at port 0x3c0-0x3df ioHem 0xa0000-0xbffff pnpid PNP0900 on isa0 Timecounter "TSC-low" frequency 1896440000 Hz quality 1000 Timecounter tick every 10.000 Msec

Une fois fait appuyé sur entrée :

pfSense Installer Copyright and distribution notice Copyright and Trademark Notices. Copyright(c) 2004-2016. Electric Sheep Fencing, LLC ("ESF"). All Rights Reserved. Copyright(c) 2014-2023. Rubicon Communications, LLC d/b/a Netgate ("Netgate"). All Rights Reserved. All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate. "pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are 26%-[Accept]

pfSense Installer	
Welcome to pfSense!	
Install Install pfSense	
Rescue Shell Launch a shell for rescue operations Recover config.xml Recover config.xml from a previous install	
Cancel>	
pfSense Installer	
Partitioning- How would you like to partition your disk?	
luto (ZFS) Guided Root-on-ZFS	
Huto (UFS) Guided UFS Disk Setup Manual Manual Disk Setup (experts)	Veuillez donc suivre
Shell Upen a Shell and partition by hand	les encadrement.
Cancel>	
To use ZFS with less than 8GB RAM, see https://wiki.freebsd.org/2FSTuningGuide	
pfSense Installer	
ZFS Configuration	
T Pool Type/Disks: Stripe: 0 disks	
– Disk Info * N Pool Name nfSense	
4 Force 4K Sectors? YES E Encrypt Disks? NO	
P Partition Scheme GPT (BIOS) S Swap Size 1g	
M Mirror Swap? NÖ W Encrypt Swap? NO	
KSelect> <cancel> [Use alnum, arrows, punctuation, TAB or ENTER]</cancel>	
Create ZFS boot pool with displayed options	

pfSense Installer	
ZFS ConfigurationSelect Virtual Device type:Stripe Stripe - No RedundancyMirror Mirror - n-Way Mirroringraid10 RAID 1+0 - n x 2-Way Mirrorsraid21 RAID-21 - Single Redundant RAIDraid22 RAID-22 - Double Redundant RAIDraid23 RAID-23 - Triple Redundant RAID	
Cancel> [Press arrows, TAB or ENTER]	

Ici, il faut séléctionner le disque virtuel, on appuye donc sur Espace puis Entrée.

ZFS Configuration	Last Chance! Are you sure you want to destroy the current contents of the following disks:
[*] 1a0 VMware, VMware Virtual S	da0
✓ DK > < Back >	<pre></pre>

Une fois l'installation terminer relancer le système et l'installation est terminer.

Une fois PfSense lancer on se retrouvre donc sur cette page.

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VMware Virtual Machine - Netgate Device ID: d4f7d4fa69d64052c10b
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***
WAN (wan)
                   -> ем0
                                   -> v4/DHCP4: 192.168.0.193/24
                                   -> v4: 192.168.1.1/24
LAN (lan)
                   -> ем1
0) Logout (SSH only)
                                            9) pfTop
 1) Assign Interfaces
                                           10) Filter Logs
2) Set interface(s) IP address
                                           11) Restart webConfigurator
                                           12) PHP shell + pfSense tools
13) Update from console

    Reset webConfigurator password
    Reset to factory defaults

5) Reboot system
                                           14) Enable Secure Shell (sshd)
6) Halt system
7) Ping host
                                           15) Restore recent configuration
                                           16) Restart PHP-FPM
8) Shell
Enter an option: 📕
```

Nous allons configurer l'IP WAN de notre PfSense, pour ce faire nous suivons les encadrés orange.

*** Welcome to pfSense 2.7.0-RELEAS	SE (amd64) on pfSense ***
WAN (wan) -> ем0 -> ч	v4/DHCP4: 192.168.0.193/24
LAN (lan) -> em1 -> v	v4: 192.168.1.1/24
0) Logout (SSH only)	9) pfTop
1) Assign Interfaces	10) Filter Logs
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 systeм	15) Restore recent configuration
7) Ping host	16) Restart PHP-FPM
8) Shell	
Enter an option: <mark>2</mark>	



Détails de notre configuration :

Adresse IP LAN : 192.168.100.1 Masque de sous-réseau : 24 = 255.255.255.0 Pas de passerelle Pas de configuration IPv6 Pas de server DHCP

> Enter the new LAN IPv4 address. Press <ENTER> for none: > 192.168.100.1 Subnet Masks are entered as bit counts (as in CIDR notation) in pfSense. e.g. 255.255.255.0 = 24 255.255.0.0 = 16 255.0.0.0 = 16 255.0.0.0 = 8 Enter the new LAN IPv4 subnet bit count (1 to 32): > 24 For a WAN, enter the new LAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none > 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

Il faut désormais se conecter a l'interface web de PfSense grace a l'ip <u>https://192.168.100.1</u>

Les identifiants sont :

Id : admin Mdp : pfsense

IV. Installation de Crowdsec

COMMUNITY EDITION Sys	stem +	Interfaces +	Firewall +	Services +	VPN •	Status +	Diagnostics -
Diagnostics /	Comn	nand Promp	ot				
Advanced Users The capabilities offerer	Only d here can	be dangerous. No s	upport is availab	le. Use them at you	ur own risk!		
Execute Shell Co	mmand						
Command							
Secure Shell Secure Shell Sec	rver E	Enable Secure :	Shell 🔫	_			
SSHd Key 0	Only	Password or Pub	lic Key			~	
	v a d	Vhen set to Public ccess. If set to Re lefault Password c	Key Only, SSH a quire Both Pass or Public Key set	ccess requires a word and Public i ting allows either	uthorized key Key, the SSH r a valid pass	is and these ke daemon requir word or a valid	ays must be con res both authoria authorized key
Allow Agent Forward	ding (_ Enables ssh-ag	ent forwarding	support.			
SSH	port	9922 🔶					
	N	lote: Leave this bi	ank for the defa	ult of 22			
ssh admin@192	.168.1	00.1 -p 99	22				

```
Windows PowerShell
                        ×
PS C:\> ssh admin@192.168.100.1 -p 9922 *
The authenticity of host '[192.168.100.1]:9922 ([192.168.100.1]:9922)' can't be established.
ED25519 key fingerprint is SHA256:NyjF3X1psKbziThEGAsGF7BUYFZGXlQH66R2hw7KHdU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.100.1]:9922' (ED25519) to the list of known hosts.
(admin@192.168.100.1) Password for admin@pfSense.home.arpa:
VMware Virtual Machine - Netgate Device ID: d78dc7fa6e70ecde9511
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
                                -> v4/DHCP4: 192.168.1.60/24
WAN (wan)
                -> em0
LAN (lan)
                 -> em1
                                -> v4: 192.168.100.1/24
DMZ (opt1)
                 -> em2
                                -> v4: 192.168.200.1/24
B) Logout (SSH only)
                                        9) pfTop
1) Assign Interfaces
                                       10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator

3) Reset webConfigurator password
4) Reset to factory defaults
12) PHP shell + pfSense tools
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: 8 <
```

Ensuite nous rentrons cette commande :

```
setenv IGNORE_OSVERSION yes
```

Puis :

pkg	add	-f	https://github.com/crowdsecurity/pfSense-pkg-
crowdse	ec/releas	ses/downlo	ad/v0.1.3/abseil-20230125.3.pkg
pkg	add	-f	https://github.com/crowdsecurity/pfSense-pkg-
crowdse	ec/releas	ses/downlo	ad/v0.1.3/re2-20231101.pkg
pkg	add	-f	https://github.com/crowdsecurity/pfSense-pkg-
crowdse	ec/releas	ses/downlo	ad/v0.1.3/crowdsec-1.6.0.pkg
pkg	add	-f	https://github.com/crowdsecurity/pfSense-pkg-
crowdse	ec/releas	ses/downlo	ad/v0.1.3/crowdsec-firewall-bouncer-
0.0.28	_3.pkg		
pkg	add	-f	https://github.com/crowdsecurity/pfSense-pkg-
crowdse	ec/releas	ses/downlo	ad/v0.1.3/pfSense-pkg-crowdsec-0.1.3.pkg



Ensuite nous retournons sur notre interface PfSense et dans « Services » -> CrowdSec

COMMUNITY EDITION System -	Interfaces +	Firewall 👻	Services +	VPN +	Status 🕶	Diagnostic
Diagnostics / Com	mand Promp	ot	Acme Certific Auto Config B Captive Porta	ates ackup I		
Advanced Users Only The capabilities offered here car	n be dangerous. No s	upport is availabl	CrowdSec DHCP Relay			
Package / Services	s: CrowdSec					
Documentation IMPORTANT	It is recommended tha	t you read the docu	mentation before ta	king any actio	n.	
Remediation componer	nt (firewall bounc	er)				
Enable						

Feed the blocklists to the pfSense firewall. Always required, even if you use your own firewall rules.

Log processor	(CrowdSec	agent

Enable 🗾

Read logs from pfSense and its packages to detect threats. Recommended.

Veuillez rentrez donc cette configuration :

Enable	
	Enable a local API on the pfSense box. Used by log processor and remediation components.
	Recommended unless:
	 you have a pre-existing main installation, maybe running on linux you want more control over the configuration, backup/restore, need a bigger machine or a postgres database you want more control over the running versions or want to run them on docker, kBs If disabled, use a remote LAPI on an external machine.
LAPI host	127.0.0.1
	Host name or IP. Change this to expose the LAPI to the LAN. For example you can have other servers running only the report to the LAPI in this pfSense machine. Otherwise, leave the default value (127.0.0.1).
LAPI port	Host name or IP. Change this to expose the LAPI to the LAN. For example you can have other servers running only the report to the LAPI in this pfSense machine. Otherwise, leave the default value (127.0.0.1).

CrowdSec rules setting	ngs
-	Poules will be hidden in the pfSense UI. If you have special needs, you can disable the rules here and provide your own.
Apply to all interfaces	a
Direction	In (inbound)
Log	
Tag	
	The actual rules may be slightly different according to the above options. Check /var/log/system.log
Enable CrowdSec IPv4 blocklist rule	block drop (direction) dog) quick on (interfaces) inet from crowdsec_blacklists to any label "CrowdSec iPv4" tag (tag)
Enable CrowdSec IPv6 blocklist rule	Z block drop (direction) (log) quick on (interfaces) inet6 from crowdsec6_blacklists to any label "CrowdSec iPv6" tag (tag)
	Save

CrowdSec rules settin	ngs
	Rules will be hidden in the pfSense UI. If you have special needs, you can disable the rules here and provide your own.
Apply to all interfaces	2
Direction	In (inbound)
Log	
Tag	
	The actual rules may be slightly different according to the above options. Check /var/log/system.log
Enable CrowdSec IPv4 blocklist rule	Dlock drop {direction} {log} quick on {interfaces} inet from crowdsec_blacklists to any label "CrowdSec IPv4" tag {tag}
Enable CrowdSec IPv6 blocklist rule	Diock drop (direction) {log) quick on {interfaces} inet6 from crowdsec6_blacklists to any label "CrowdSec IPv6" tag {tag}
	Saving settings, please wait

Community earlier System - Interfaces - Firewall - Services - VPN -	Status - Diagnos	tics + 🦂 🕴
Status / CrowdSec	Captive Portal CARP (failover)	黄星 國
Running services: security engine ✓ - finewall remediation ✓ Matchives Bouncers Collections Scenarios Parsers Postoverflows Last refresh: a few seconds ago Name * IP Address Last Update	CrowdSec Status Dashboard DHCP Leases DHCPv6 Leases DNS Resolver Filter Reload Gateways	Q. Search 2 50 • H •
pfsense 127.0.0.1 a few seconds ago	HAProxy Stats Interfaces IPsec Monitoring NTP	v1.5.5-freebsd-d2d788c5 Showing 1 to 1 of 1 entries

Last refresh: a few seconds ago			Q. Search 2 50 - 1				
Collection	* Status	Version	Description				
orowdsecurity/base-http-scenarios	enabled	0.8	http common : scanners detection				
crowdsecurity/freebsd	enabled	0.1	core freebad support : syslog+geoip+ssh				
crowdsecurity/http-cve	enabled	2.5	Detect CVE exploitation in http logs				
crowdeecurity/nginx	enabled	0.2	nginx support : parser and generic http scenarios				
crowdsecurity/pfsense	enabled	0.2	core pfsense support				
crowdsecurity/pfsense-gui	enabled	0.1	pfSense web authentication support				
crowdeecurity/sehd	enabled	0.3	sahd support : parser and brute-force detection				
firewallservices/pf	enabled	0.2	Parser and scenario for Packet Filter logs				

Une fois ceci fait, nous pouvons lancer un nmap comme ceci :

nmap -sv 192.1	68.1.60				
Status / CrowdSec					(a)
nning services: security engine 🛩 - fire	ewall remediation 🗸				
Machines Bouncers Alerts	Decisions Hub *				
Machines Bouncers Alerts Note: the decisions coming from th	e CAPI (signals collected by the CrowdSec users) do n	tot appear here. To show th	iem, use csc	li decisions lis	st 🦂 in a shell.
Machines Bouncers Alerts Note: the decisions coming from th Last refresh: a few seconds ago	e CAPI (signale collected by the CrowdSec users) do n	iot appear here. To show th	iem, use csc	li decisions lis Search	st -a in a shell.
Machines Bouncers Alerts Note: the decisions coming from th Last refresh: a few seconds ago Scope:Value	Pecisions Hub * e CAPI (signals collected by the CrowdSec users) do n	tot appear here. To show th Country	em, use csc Q AS	li decisions lin Search Events	at 🔹 in a shell.

Par la suite nous vérifions si l'ip a bien était bannie en consultant la liste des décision :

cscli decisions list

On peut constater que l'ip a bien été banni.

<pre>[2.7.2-RELEASE][admin pfSense.home.arpa]/root: cscli decisions list</pre>									
ID	Source	Scope:Value	Reason	Action	Country	AS	Events	expiration	Alert ID
15001	crowdsec	Ip:192.168.1.96	firewallservices/pf-scan-multi_ports	ban			16	3h52m22.15208364s	2
[2:7-2-RELEASE][admin:pfSense.home.arpa]/root:									