PROJET PERSONNEL ENCADRÉE

7 avril 2024



NESUX 05 / 04 / 2024

CRAMPON Nicolas



BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

SESSION 2024

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (recto)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE N° réalisation :						
Nom, prénom : CRAMPON Nicolas N° candidat :						
Épreuve ponctuelle non Contrôle en cours de formation oui Date : 05 / 04 / 2024						
Organisation support de la réalisation professionnelle						
Intitulé de la réalisation professionnelle						
Période de réalisation : mars → 5 Avril 2024 Lieu : Senlis Modalité : oui Seul(e) non En équipe						
Compétences travaillées						
oui Concevoir une solution d'infrastructure réseau oui Installer tester et déployer une solution d'infrastructure réseau						
non Exploiter, dépanner et superviser une solution d'infrastructure ré	seau					
Conditions de réalisation ¹ (ressources fournies, résultats attendus)						
- 1 Windows Server 2022 \rightarrow Active Directory						
- 2 Windows $10 \rightarrow$ Clients						
- 1 Linux Server \rightarrow GLPI						
 PfSense → <u>CrowdSec</u> et Squid 						
- 1 Kali Linux						
- 1 téléphone : client VPN						
Description des ressources documentaires, matérielles et logicielles utilisé	es²					
Ressources Documentaires : Divers sites Internet comme IT-CONNECT						
Ressources Matérielles : Ordinateur portable avec 32 Go de ram, Core I7, RTX	4070					
Ressources Logiciels : Tout mon environnement est virtualisé sur VMware Worl	station	17 Pro				
Modalités d'accès aux productions ³ et à leur documentation ⁴		*				
Page 8 pour tous les mots de passes de mon environnement						

Introduction

NESUX considère la sécurisation de son infrastructure réseau comme une priorité essentielle pour assurer le bon fonctionnement de ses activités. Dans cet objectif, des mesures stratégiques sont prévues pour garantir une connectivité stable et sécurisée, répondant ainsi aux besoins fondamentaux de l'entreprise.



1) CANEVAS

<u> 1.1 - Mise en situation</u>

Dans le monde numérique en constante évolution, NESUX, une entreprise de développement logiciel en pleine croissance, se trouve à un tournant crucial dans son parcours. Consciente de l'importance capitale d'une infrastructure réseau fiable et sécurisée pour soutenir ses opérations, NESUX se lance dans un projet ambitieux visant à renforcer sa structure informatique.

Au cœur de cette initiative se trouve la création de deux zones distinctes : **la zone réseau local** et **la zone DMZ**. Dans la première, NESUX prévoit l'installation d'un **Active Directory central** pour gérer efficacement les identités et les accès des utilisateurs, ainsi que **deux clients Windows 10** pour faciliter l'accès aux ressources partagées. La zone DMZ va permettre de séparer les services critiques du réseau interne et de renforcer la sécurité contre les menaces externes. Un **serveur GLPI** sera déployé.

Pour protéger cette infrastructure contre les menaces en ligne croissantes, NESUX compte sur des solutions de sécurité avancées. **Un pare-feu pfSense** sera mis en place pour contrôler et surveiller le trafic réseau, tandis que **CrowdSec** sera utilisé pour détecter et bloquer les attaques par bruteforce provenant d'un **Kali Linux**, une machine dédiée aux tests de sécurité. De plus, l'intégration de **Squid** permettra de filtrer et de bloquer sélectivement l'accès à certains sites Web et communications c to c, renforçant ainsi la sécurité et la productivité des employés.

Afin de permettre un accès sécurisé aux ressources internes, même à distance, NESUX configurera **un client VPN**, permettant ainsi aux employés externes de se connecter en toute sécurité au réseau local de l'entreprise.

Ce projet représente un engagement fort de NESUX envers la sécurité et la fiabilité de son infrastructure réseau, assurant ainsi une connectivité stable et sécurisée pour ses employés, quel que soit leur emplacement. (*Le réseau sera réalisé avec VMWARE*)



1.2 - Cahier des charges

- ★ Ce que l'entreprise souhaite mettre en place réellement :
 - Zone locale : 1 Active Directory et 2 clients windows 10
 - Zone DMZ : Serveur GLPI
 - Un pare-feu pfSense : CrowdSec et Squid
 - Un kali linux afin de tester les attaques
 - Un client Vpn pour se connecter à la zone locale

1.3 - Solution

- ★ Zone locale, Installation et configuration
- ★ PFSENSE, Installation et configuration
- ★ PFSENSE, Création de l'interface DMZ
- ★ PFSENSE, Création des règles
- ★ Installation et configuration de la machine Kali
- ★ Installation de Hydra
- ★ Installation du dictionnaire
- ★ Cracker le mot de passe SSH
- ★ Crowdsec Installation et blocage
- ★ Enregistrement DNS
- ★ Création du certificat HTTPS
- ★ Installation de Squid
- ★ Blocage des C&C
- ★ Installation et configuration d'OpenVpn sur PFSENSE
- ★ Test OpenVPN
- ★ LDAP pour les utilisateurs de la zone locale (en cours)
- ★ Synthèse des règles (en cours)

<u>1.4 - Équipements et Logiciels nécéssaires</u>

- ★ 1 Windows Server 2022 \rightarrow Active Directory
- ★ 2 Windows $10 \rightarrow$ Clients
- ★ 1 Linux Server \rightarrow GLPI
- ★ PfSense → CrowdSec et Squid
- \star 1 Kali Linux
- ★ 1 téléphone : client VPN

1.5 - Schéma réseau



- LAN: 192.168.1.0/24
 - <u>Zone locale</u> : 192.168.1.0/29
- **DMZ** : 172.16.1.0/24
 - <u>Zone DMZ</u>: 172.16.1.0/29
- WAN : DHCP



<u> 1.6 - Tableau d'adressage</u>

LAN

	IP	MASQUE	BROADCAST	DNS	DNS2
AD	192.168.1.1	/29	192.168.1.6	Х	Х
CLIENT 1	192.168.1.2	/29	192.168.1.6	192.168.1.1	Х
CLIENT 2	192.168.1.3	/29	192.168.1.6	192.168.1.1	Х

DMZ

GLPI 172.16.1.1 /29	172.16.2.6	192.168.2.1	Х
---------------------	------------	-------------	---

WAN

CLIENT 3	DHCP	DHCP	DHCP	DHCP	DHCP
CLIENT 4	DHCP	DHCP	DHCP	DHCP	DHCP

PFSENSE

LAN	192.168.1.6	/29	Х	192.168.2.1	Х
DMZ	172.16.1.6	/29	Х	Х	Х
WAN	DHCP	DHCP	DHCP	DHCP	DHCP



<u> 1.7 - Tableau Mots de passe</u>

	Utilisateur	Mots de passe
AD	Administrateur	Admin00
GLPI	debian	root
PFSENSE	admin	Admin00
Client 1 (Thomas Shelby)	t.shelby	Admin00
Client 2 (Arthur Shelby)	a.shelby	Admin00
Client 3 (John Shelby)	j.shelby	Admin00
Client 4 (VPN)	vpn.pfsense.nesux	Admin00



2) SOLUTION

2.1 - Zone locale, Installation et configuration

Je commence par installer et configurer Windows Server, et créer mon domaine. En suivant la méthode AGDLP, j'ajoute des groupes, et je crée les utilisateurs nécessaires. Une fois cette étape terminée, j'intègre ces utilisateurs dans le domaine nouvellement créé. Client1 et Client2 avec leur adresse IP respective.



Utilisateurs et ordinateurs Active I	Directory		
Fichier Action Affichage ?			
🗢 🔿 🙍 🗊 📋 🔯 🖬	è 🖬 🕷 🔚	7 🗾 🐍	
 Utilisateurs et ordinateurs Active Requêtes enregistrées nesux.lan Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accoun Users Utilisateurs du domaine salariés 	Nom Constant Service Constant Service C	Type Groupe de séc Groupe de séc Groupe de séc Utilisateur Utilisateur Utilisateur	Description





2.2 - PFSENSE, Installation et configuration

J'ajoute une carte réseau avec un segment LAN destiné à mon réseau local.

Hardware			×
Device Memory Processors New CD/DVD (IDE) Network Adapter 3 USB Controller Sound Card Display	Summary 256 MB 1 Using file C:\Users\N Bridged (Automatic) NAT NAT Present Auto detect Auto detect Auto detect	lico\Desktop	Device status Connected Connected Connection Bridged: Connected directly to the physical network Replicate physical network connection state NAT: Used to share the host's IP address Host-only: A private network shared with the host Custom: Specific virtual network VMnet0 LAN segment: LAN Advanced
			Close Help

Je fais la même chose pour tous les appareils de mon réseau LAN.



Press <enter> to continue. WMware Virtual Machine - Netgate Device ID: 19253ebec0d106ea42ec **** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense *** WAN (wan) -> em0 -> v4/DHCP4: 10.101.32.99/16 LAN (lan) -> em1 -> v4: 192.168.1.6/29 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 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 16) Restart PHP-FPM 8) Shell Enter an option:</enter>	The IPv4 LAN address has been set to You can now access the webConfigurat browser: http://192.168.1.6/	о 192.168.1.6729 tor by opening the following URL in your web
<pre>*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense *** WAN (wan) -> em0 -> v4/DHCP4: 10.101.32.99/16 LAN (lan) -> em1 -> v4: 192.168.1.6/29 Ø) 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 13) Update from console 5) Reboot system 14) Enable Secure Shell (sshd) 6) Halt system 15) Restore recent configuration 7) Ping host 15) Restore recent configuration 16) Restart PHP-FPM 8) Shell</pre>	Press <enter> to continue. VMware Virtual Machine - Netgate Dev</enter>	vice ID: 19253ebec0d106ea42ec
WAN (wan) -> em0 -> v4/DHCP4: 10.101.32.99/16 LAN (lan) -> em1 -> v4: 192.168.1.6/29 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 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 16) Restart PHP-FPM 8) Shell Enter an option:	*** Welcome to pfSense 2.7.2-RELEAS	E (amd64) on pfSense ***
0) Logout (SSH only)9) pfTop1) Assign Interfaces10) Filter Logs2) Set interface(s) IP address11) Restart webConfigurator3) Reset webConfigurator password12) PHP shell + pfSense tools4) Reset to factory defaults13) Update from console5) Reboot system14) Enable Secure Shell (sshd)6) Halt system15) Restore recent configuration7) Ping host16) Restart PHP-FPM8) Shell14	WAN (wan) -> ем0 -> v4 LAN (lan) -> ем1 -> v4	4/DHCP4: 10.101.32.99/16 4: 192.168.1.6/29
Enter an option:	 Ø) 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:	

A Non sécurisé | 192.168.1.6

ofsense,

SIGN IN	
SIGN IN	

Je me connecte avec admin:pfsense

SIGN IN	
admin	
pfsense	Ŕ
	_

General Information	
	On this screen the general pfSense parameters will be set.
Hostname	pfSense
	Name of the firewall host, without domain part.
	Examples: pfsense, firewall, edgefw
Domain	home.arpa
	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	192.168.1.1
Secondary DNS Server	
Override DNS	
	Allow DNS servers to be overridden by DHCP/PPP on WAN
	>> Next

Je modifie le DNS.



Time Server Informa	on
Time server hostname	2.pfsense.pool.ntp.org Enter the hostname (FQDN) of the time server.
Timezone	Europe/Paris 🗸
	>> Next

Je sélectionne Europe/Paris.

Block RFC1918 Networks 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 as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.
Block bogon network	\$
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.
	>> Next

Je décoche ces deux cases pour ne pas bloquer le trafic entre le WAN et pfSense.

Set Admin WebGUI Password										
	On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.									
Admin Password	······									
Admin Password AGAIN										
	>> Next									

Je modifie le mot de passe avec Admin00.



Congratulations! pfSense is now configured. We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network. Check for updates
Remember, we're here to help.
Click here to learn about Netgate 24/7/365 support services.
User survey Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous) Anonymous User Survey
Useful resources.
Learn more about Netgate's product line, services, and pfSense software from our website To learn about Netgate appliances and other offers, visit our store Become part of the pfSense community. Visit our forum Subscribe to our newsletter for ongoing product information, software announcements and special offers. Finish



2.3 - PFSENSE, Création de l'interface DMZ

General Configuratio	n
Enable	Enable interface
Description	DMZ
	Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4 V
IPv6 Configuration Type	None 🗸
MAC Address	XXXXXXXXXXXX
	This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
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 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect)
	Explicitly set speed and duplex mode for this interface.
	WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configura	ation
IPv4 Address	172.16.1.6
IPv4 Upstream gateway	None Add a new gateway
	If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
	On local area network interfaces the upstream gateway should be "none".
	Gateways can be managed by clicking here.
Reserved Networks	
Block private networks	Π
and loopback addresses	Elocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per
	RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	
	Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet
	routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
	Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

The DMZ configuration has been changed. The changes must be applied to take effect. Don't forget to adjust the DHCP Server range if needed after applying.

Apply Changes



Interfaces / Interface Assignments												
Interface Assignments	Interface Groups	Wireless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges	LAGGs			
Interface	Network port	:										
WAN	em0 (00:0c	em0 (00:0c:29:f7:3d:31)										
LAN	em1 (00:0c	::29:f7:3d:3b)						~	Delete			
DMZ	em2 (00:0c	:29:f7:3d:45)	Delete									
Save												



2.4 - PFSENSE, Création des règles

Le but principal d'avoir une zone DMZ est de séparer le réseau local des serveurs comme glpi afin d'ajouter une couche de sécurité à mon réseau. Les utilisateurs du réseau local pourront se connecter aux différents services mis en place mais à l'inverse les appareils de la zone DMZ ne pourront pas communiquer avec les postes de mon réseau local.

Donc pour le moment j'ai créé qu'une seule règle qui va permettre que ma machine glpi puisse ping mon réseau local.

Flo	ating	WAN	I LAN	DMZ									
Ru	Rules (Drag to Change Order)												
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
	×	0/0 B	IPv4 *	172.16.1.1	*	192.168.1.0/29	*	*	none			ৼৢ৾ঀ৾৾৾৾৾৾৾৾৾৾৾৾৾৾৾	

Je n'ai pas besoin de créer de règle pour autoriser l'accès à glpi depuis un client du réseau local car après test ça fonctionne de base.





Mais si je mets en place cette règle je n'y ai plus accès.

FI	oating	g WAN	LAN	DMZ										
R	Rules (Drag to Change Order)													
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions		
	~	0/850 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	\$		
	×	0/0 B	IPv4 TCP	192.168.1.0/29	*	172.16.1.1	80 (HTTP)	*	none			ݨ∥□♡面		
	~	0/715 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	ᢤ聋▣⊘ā×		
	~	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	ᢤ᠕ᢆᢕᢩᢆ᠐᠅		

172.16.1.1	/install/insta	ll.php
------------	----------------	--------



Je l'enlève car ce n'est pas le but recherché.

Si jamais je veut bloquer mon réseau lan au wan je créer cette règle :



FI	oating	g WAN	LAN	DMZ										
R	Rules (Drag to Change Order)													
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions		
	~	0/1.10 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	\$		
	×	0/0 B	IPv4 *	192.168.1.0/29	*	192.168.110.140	*	*	none			ৼৢ৾ঀ৾৾৾৾৾৾৾৾৾৾৾৾৾৾		
	~	6/18.15 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	ϑ∥□⊘ā×		
	~	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	ϑ聋⊡⊘ā×		

Mais ce n'est pas le but recherché non plus.

Maintenant il faut que mon réseau local ait accès à mon réseau wan donc je supprime cette règle. A noter que dans la configuration ip de ma machine client sur mon réseau local il faut mettre l'ip qui permet de se connecter à internet en dns, dans mon cas quand je suis a Promeo, je vais mettre 192.168.110.140. Sur ma machine physique où est installé vmware j'ouvre mon terminal et je tape ipconfig /all et j'observe bien que l'ip est dans le même réseau.

```
Carte Ethernet VMware Network Adapter VMnet8 :

Suffixe DNS propre à la connexion. . . :

Description. . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet8

Adresse physique . . . . . . . . . : 00-50-56-C0-00-08

DHCP activé. . . . . . . . . . . : Non

Configuration automatique activée. . . : Oui

Adresse IPv6 de liaison locale. . . . : fe80::fd3d:117e:974d:25a8%16(préféré)

Adresse IPv4. . . . . . . . . . . : 192.168.110.1(préféré)

Masque de sous-réseau. . . . . . : 255.255.255.0

Passerelle par défaut. . . . . . : 704663638

DUID de client DHCPv6. . . . . . : 00-01-00-01-2D-50-E9-F2-74-5D-22-CF-33-1F

NetBIOS sur Tcpip. . . . . . : Activé
```

L'ip est aussi l'em0 sur mon pare-feu pour le réseau WAN.

Je veille à bien désactiver les pare-feux windows pour pouvoir autoriser la communication entre le wan et mon réseau local. Si jamais je veux que ma machine physique se connecte à mon lan je vais devoir créer 2 règles et désactiver la carte wifi par défaut pour laisser vmnet8 en priorité.



Ru	Rules (Drag to Change Order)												
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
	~	0/0 B	IPv4 *	192.168.110.0/24	*	192.168.1.0/29	*	*	none			҈∜₽́Ѻ ѽ ×	
	~	0/240 B	IPv4 *	192.168.110.0/24	*	192.168.110.0/24	*	*	none			ᢤ᠕ᢕᢆᢁ×	

R	ules (Drag to Change Order)													
		States Protocol Source Port		Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions			
	~	2/1.44 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	\$		
	~	1/37 KiB	IPv4 *	192.168.1.0/29	*	192.168.110.0/24	*	*	none			ᢤ᠕ᢕᢆᢁ		
	~	0/190.03 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	ϑ聋⊡⊘ā×		
	~	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	ϑ聋⊡⊘ <u>ڨ</u> ×		



2.5 - Installation et configuration de la machine Kali

Je sélectionne bien la bonne carte réseau lors de son installation.

\sim		
Network Adapter	NAT	Network connection
ビ USB Controller く Sound Card Display	Present Auto detect Auto detect	Bridged: Connected directly to the physical network Replicate physical network connection state
		 NAT: Used to share the host's IP address Host-only: A private network shared with the host Custom: Specific virtual network
		VMnet8 (NAT)

Ensuite j'ai ajouté 2 règles pour donner l'accès à la zone DMZ depuis le wan.

Rule	Rules (Drag to Change Order)											
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	 Image: A start of the start of	0/336 B	IPv4 *	192.168.110.0/24	*	172.16.1.0/29	*	*	none			ᢤ᠕ᢕᢆᢁ×
	~	0/8 KiB	IPv4 *	192.168.110.0/24	*	192.168.1.0/29	*	*	none			ϑ聋⊡⊘面×
	/	0/9 KiB	IPv4 *	192.168.110.0/24	*	192.168.110.0/24	*	*	none			ᢤᢧ∕°□⊘面×

Ru	Rules (Drag to Change Order)											
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	~	0/0 B	IPv4 *	192.168.110.0/24	*	172.16.1.0/29	*	*	none			ᢤ᠕ᢕᢆᢁ×
	×	0/89 KiB	IPv4 *	172.16.1.1	*	192.168.1.0/29	*	*	none			ᢤ∥□⊘亩

Et je modifie la configuration ip pour qu'elle soit sur le même réseau que mon wan.



2.6 - Installation de Hydra

Et j'ai installé hydra avec cette commande

```
—(admin⊕kali)-[/home/kali]
-$ sudo apt-get install hydra
```

2.7 - Installation du dictionnaire

https://github.com/LandGrey/pydictor/tree/master

J'accède à ce site pour téléchargerl la wordlist pydictor.

Sur kali je vais utiliser cette commande pour créer un répertoire nommé pydictor et y télécharger le contenu.

git clone https://github.com/LandGrey/pydictor.git

Ensuite je peux accéder au répertoire avec la commande cd

et je cherche le .txt qui m'intéresse



Le chemin est /home/kali/pydictor/wordlist/Web/CommonWebAdminPass.txt



2.8 - Cracker le mot de passe SSH

J'utilise la commande : hydra -t 50 -l debian -P /home/kali/pydictor/wordlist/Web/CommonWebAdminPass.txt -s 22 -f 172.16.1.1 ssh -l

hydra : parce que j'utilise Hydra

- -t 50 : 50 mdp seront testé simultanément
- -l root : j'hack le mot de passe avec l'utilisateur root
- -P /home/kali/pydictor/wordlist/Web/CommonWebAdminPass.txt : le chemin du dictionnaire
- -s 22 : pour spécifier le port 22 ssh
- -f: pour stopper le processus lorsque le mot de passe sera trouvé
- 172.16.1.1 : l'adresse ip de mon serveur ssh

ssh : le protocole utilisé

-I: pour hydra lorsque le mot de passe sera trouvé

Et j'attends une bonne trentaine de minutes.



Et voilà le mot de passe à été trouvé.



2.9 - Crowdsec Installation et blocage

Maintenant je vais installer Crowdsec pour pouvoir détecter l'attaque et la bloquer.

Je commence par me connecter en ssh à mon pare-feu pfsense.

Pour ça j'active le ssh de pfsense.

Secure Shell	
Secure Shell Server	Enable Secure Shell
SSHd Key Only	Password or Public Key
	When set to Public Key Only, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to Require Both Password and Public Key, the SSH daemon requires both authorized keys and valid passwords to gain access. The default Password or Public Key setting allows either a valid password or a valid authorized key to login.
Allow Agent Forwarding	Enables ssh-agent forwarding support.
SSH port	22
	Note: Leave this blank for the default of 22.

et j'utilise putty pour y accéder.

8	PuTTY Configuration		? ×
	PuTTY Configuration tegony: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Colours Seteral Proxy SSH Serial Tenet	Basic options for your PuTTY sessi Specify the destination you want to connect the thost Name (or IP address) P192.168.1.6 Connection type: SSH Segial Other: Telnet Load, save or delete a stored session Saved Sessions Default Settings	? × on to on ti 22 · V <u>Load</u> Sa <u>ve</u> <u>Delete</u>
		Close window on exit: Always Never Only on clear	n exit

Et je me connecte avec admin:Admin00





Et je saisis 8 pour ouvrir le Shell.

Et je tape les commande de l'installation :

setenv IGNORE_OSVERSION yes

pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/abseil-20230125.3.pkg

pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/re2-20231101.pkg

pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/crowdsec-1.6.0.pkg

pkg add -f

https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/crowdsec-firewall-bouncer-0.0.28_3.pkg

pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/pfSense-pkg-crowdsec-0.1.3.pkg



Et puis je redémarre pfsense afin que Crowdsec démarre.

Maintenant je vais sur l'interface web et je vérifie que crowdsec est activé.

Package / Services: CrowdSec 🔁 🛄							
Documentation	Documentation						
IMPORTANT	It is recommended that you read the documentation before taking any action.						
Remediation compor	nent (firewall bouncer)						
Enable							
	Feed the blocklists to the pfSense firewall. Always required, even if you use your own firewall rules.						
Log processor (Crow	dSec agent)						
Enable							
	Read logs from pfSense and its packages to detect threats. Recommended.						

Si je lance une attaque bruteforce depuis ma machine kali

9	lp:192.168.110.141	crowdsecurity/ssh-bf	ban:1	a few seconds ago
10	lp:192.168.110.141	crowdsecurity/ssh-slow-bf	ban:1	a few seconds ago
11	lp:192.168.110.140	firewallservices/pf-scan-multi_ports	ban:1	a few seconds ago

Je vois bien que l'attaque à été bloquée parce que maintenant, si j'essaie de ping mon pare-feu ça ne fonctionne plus.



Et dans le SLI du pare-feu on peut voir que l'ip de ma machine kali à été ban mais aussi celle de mon wan.

[2.7.2-R	.7.2-RELEASE][admin@pfSense.home.arpa]/root: cscli decisions list								
ID	Source	Scope:Value	Reason	Action	Country	AS	Events	expiration	Alert ID
45009 45007	crowdsec crowdsec	Ip:192.168.110.140 Ip:192.168.110.141	firewallservices/pf-scan-multi_ports crowdsecurity/ssh-slow-bf	ban ban			18 11	3h58m24.183734406s 3h57m19.04865639s	12 10

Pour les débloquer je peux faire : cscli decisions delete -ip x.x.x.x

2.7.2-RELEASE][admin@pfSense.home.arpa]/root: cscli decisions deleteip 192.168.110.141 NFO[2024-03-22T09:47:11+01:00] 2 decision(s) deleted 2.7.2-RELEASE][admin@pfSense.home.arpa]/root: cscli decisions list									
ID	Source	Scope:Value	Reason	Action	Country	AS	Events	expiration	Alert ID
45009	crowdsec	Ip:192.168.110.140	firewallservices/pf-scan-multi_ports	ban			18	3h56m4.168231551s	12
duplica [2.7.2-RF [NFO[2024 [2.7.2-RF To active	duplicated entries skipped 2.7.2-RELEASE][admin@pfSense.home.arpa]/root: cscli decisions deleteip 192.168.110.140 IFO[2024-03-22T09:47:25401:00] 2 decision(s) deleted 2.7.2-RELEASE][admin@pfSense.home.arpa]/root: cscli decisions list o active decisions								



2.10 - Enregistrement DNS

🍰 Gestionnaire DNS			
Fichier Action Affichage ?			
◆ ● 2 🖬 🗙 🖻 🗟	? 🖬 📲 🖬		Propriétés de : pfsense ? X
 DNS AD Cones de recherche direction rnsdcs.nesux.lan Tones de recherche invertion Points d'approbation Redirecteurs conditionne 	Nom msdcs sites tcp udp DomainDnsZones ForestDnsZones (identique au dossier parent) (identique au dossier parent) (identique au dossier parent) (identique au dossier parent) Identique au dossier	Type Source de nom (SOA) Serveur de noms (NS) Hôte (A) Hôte (A) Hôte (A) Hôte (A)	Hôte local (A) Sécurité Hôte (utilise le domaine parent si ce champ est vide) : pfsense pfsense Nom de domaine pleinement qualifié (FQDN) : pfsense.nesux.lan Adresse IP : 192.168.1.6 ØMettre à jour l'enregistrement de pointeur (PTR) associé

Et été dans SYSTEM \rightarrow ADVANCED \rightarrow ADMIN ACCESS sur mon pare-feu et j'ai entré le fqdn.

Alternate Hostnames	pfsense.nesux.lan					
	Alternate Hostnames for DNS Rebinding and HTTP_REFERER Checks. Specify alternate hostnames by which the router may be queried, to bypass DNS Rebinding Attack checks. Separate hostnames with spaces.					
of pfSense.hom	e.arpa - Status: Dast 🗙 🕂					
\leftarrow \rightarrow (Non sécurisé https://pfsense.nesux.lan					
	Sense System - Interfaces - Firewall - Services -					



2.11 - Création du certificat HTTPS

Authorities Certificat	es Revocation
Create / Edit CA	
Descriptive name	HTTPS PFSENSE CERTIFICAT
	The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, ", "
Method	Create an internal Certificate Authority
Trust Store	Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.
Randomize Serial	Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.
Internal Certificate A	uthority
Key type	RSA
	2048 The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	sha256 The digest method used when the CA is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.
Lifetime (days)	3650
Common Name	nesux-internal-ca
	The following certificate authority subject components are optional and may be left blank.
Country Code	None
State or Province	FRANCE
City	SENLIS
Organization	NESUX
Organizational Unit	e.g. My Department Name (optional)

Ensuite je copie certificate data et private key



Existing Certificate Au	thority	
<u>Certificate data</u>	BEGIN CERTIFICATE MIID2zCCAsOgAwIBAgIIdhhSWflAN3kwDQYJKoZIhvcNAQELBQAwTj EaMBgGA1UE AxMRbmVzdXgtaW50ZXJuYWwtY2ExDzANBgNVBAgTBkZSQU5DRTEPMA 0GA1UEBxMG	•
	Paste a certificate in X.509 PEM format here.	
Certificate Private Key (optional)	BEGIN PRIVATE KEY MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCfma iFyfFU3KoS NecpW2pR/Q1Ab+BcclYrJeNId/4nefqQIPfI11cpgAg7ZMVjkP9bp6 gqtyNikzgx	•

Et j'importe le certificat

Authorities Certific	ates Certificate Revocation	
Add/Sign a New Ce	rtificate	
Method	Import an existing Certificate	
Descriptive name	HTTPS PFSENSE CERTIFICAT The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: $?, >, <, &, /, \setminus$ ", '	
Import Certificate		
Certificate Type		
<u>Certificate data</u>	BEGIN CERTIFICATE MIID2zCCAsOgAwIBAgIIdhhSwflAN3kwDQYJKoZIhvcNAQELBQAwTj EaMBgGA1UE AxMRbmVzdXgtaWS0ZXJuYWwtY2ExDzANBgNVBAgTBkZSQU5DRTEPMA GGA1UEBxMG Paste a certificate in X.509 PEM format here.	
<u>Private key data</u>	BEGIN PRIVATE KEY MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCfma iFyfFU3KoS NecpW2pR/Q1Ab+BcclYrJeNId/4nefqQIPfI11cpgAg7ZMVjkP9bp6 gqtyNikzgx Paste a private key in X.509 PEM format here. This field may remain empty in certain cases, such as when the private key is stored on a PKCS: token.	#11
	Save	



2.12 - Installation de Squid

Squid est un proxy qui va me permettre de bloquer des sites internet et des c to c.

Je commence par l'installer sur mon pare-feu.

System	I / Pac	kage Manager / Available Packages	0
Installed P	ackages	Available Packages	
Search			Ð
Search ter	m	squid Both - Q Search Clear	
		Enter a search string or *nix regular expression to search package names and descriptions.	
Package	S		
Name	Version	Description	
Lightsquid	3.0.7_3	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	+ Install
		Package Dependencies: Ø lighttpd-1.4.72 Ø lightsquid-1.8_5	
squid	0.4.46	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.	+ Install
		Package Dependencies:	
		squidclamav-7.2	
squidGuard	1.16.19	High performance web proxy URL filter.	+ Install
		Package Dependencies: Ø squidguard-1.4_15 Ø pfSense-pkg-squid-0.4.46	

Et dans Service \rightarrow Squid Proxy Server je save local cache et general en activant le proxy.

Package / Proxy Server: General Settings / General								?• 💷 🗉 (
General	Remote Cache	Local Cache	Antivirus	ACLs	Traffic Mgmt	Authentication	Users	Real Time	Status	Sync	
Squid Gei	neral Settings										
Enable	Squid Proxy	Check to enable the mportant: If uncheck	ne Squid proxy. ced, ALL Squid s	services wil	be disabled and st	opped.					



J'active le proxy transparent http.



Et j'active Access Logging pour permettre de savoir qui fait quoi sur Internet

Logging Settings	
Enable Access Logging	 This will enable the access log. Warning: Do NOT enable if available disk space is low.
Log Store Directory	/var/squid/logs The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs Important: Do NOT include the trailing / when setting a custom location.
Rotate Logs	365 Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Et je décoche ça afin de masquer les informations sur Squid, comme la version.

Suppress Squid Version 🛛 Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

Maintenant le certificat HTTPS que j'ai créé juste avant va me servir à bloquer des sites web, il faut que je fasse 2 choses pour que cela fonctionne.

Dans PROXY SERVER \rightarrow GENERAL

SSL Man In the Midd	le Filtering
HTTPS/SSL Interception	Enable SSL [Itering.
SSL/MITM Mode	Splice Whitelest, Bump Otherwise The SSL/MITM mode determines how SSL interception is treated when 'SSL Man in the Middle Filtering' is enabled. Details: Selve Middle Filtering is enabled. Details: Selve Middle Filtering in the Middle Filtering is enabled.
SSL Intercept Interface(s)	With With DMZ The interface(i) the proxy server will intercept SSL requests on. Use CTEL + click to select multiple interfaces.
SSL Proxy Port	This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129
SSL Proxy Compatibility Mode	Modern The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. Click Info for details.
DHParams Key Size	2048 (default) v DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.
CA	Select Certificate Authority to use when SSL interception is enabled.



Et ensuite dans SYSTEM \rightarrow ADVANCED j'active HTTPS(SSL/TLS)

System / Advanced / Admin Access							
Admin Access	Firewall	& NAT	Networking	Miscellaneous	System Tunables	Notifications	
webConfigu	rator						
	Protocol	O HTT	ΓP			HTTPS (SSL/TLS)	

je vais faire le test avec francetvinfo.fr :

Avant blacklist :

\leftarrow	С	×) Noi	n sécurise	é h i	ttps://w	ww.francet	tvinfo	.fr/interne	t/amaz	zon/													
						fre	ancein	fo		fra	ince.tv	1	re	adiofra	nce								Con	fidentia
						f	ranc	:ei	nfo	:						vi	idéos	ra	dio	jt	émi	ssions		Q
						습	politique	• v	rai ou fau	x so	ociété	faits-div	vers	santé	éco/conso	monde	culture	sport	env	ironnement	météo	l'actu po	ur les j	jeunes

Amazon



Le youtuber MrBeas dans la téléréalité a Amazon

La superstar de YouTube se prépare à org compétition de téléréalité la plus lucrativ



Après blacklist :



The following error was encountered while trying to retrieve the URL: https://www.francetvinfo.fr/

Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect. Your cache administrator is <u>admin@localhost</u>.

Package / Proxy Server: Access Control / ACLs

Blacklist

francetvinfo.fr

Destination domains that will be blocked for the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.

Voilà comment bloquer des sites avec Squid !



2.13 - Blocage des C&C

Je me rends sur ce site pour voir quelques adresses IP C&C :

https://exchange.xforce.ibmcloud.com/statshistory/botnetcommandandcontrolserver

Adresse IP 160.121.122.130	Botnet Command and Control Server	South Africa	Consigné le 5 avr. 2024 10:14:34
Adresse IP 122.51.59.18	Botnet Command and Control Server	China	Consigné le 5 avr. 2024 10:14:30
Adresse IP 168.206.214.183	Botnet Command and Control Server	Hong Kong S.A.R. of China	Consigné le 5 avr. 2024 10:14:22
Adresse IP 43.139.48.143	Botnet Command and Control Server		Consigné le 5 avr. 2024 10:14:16
Adresse IP 160.121.120.154	Botnet Command and Control Server	South Africa	Consigné le 5 avr. 2024 10:14:12
Adresse IP 160.121.120.133	Botnet Command and Control Server	South Africa	Consigné le 5 avr. 2024 10:13:58
Adresse IP 160.121.124.154	Botnet Command and Control Server	South Africa	Consigné le 5 avr. 2024 10:13:56
Adresse IP 168.206.215.173	Botnet Command and Control Server	Hong Kong S.A.R. of China	Consigné le 5 avr. 2024 10:13:54

Et ensuite je les mets dans la blacklist.

Blacklist



Destination domains that will be blocked for the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.



<u>2.14 - Installation et Configuration d'OpenVPN sur Pfsense</u>

je commence par créer mon autorité de certification.

Create / Edit CA	
Descriptive name	CA-NESUX
	The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \backslash_i , '
Method	Create an internal Certificate Authority
Trust Store	Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.
Randomize Serial	Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.
Internal Certificate A	uthority
Key type	RSA
	2048 The length to use when generating a new RSA key, in bits.
	The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	sha256 The digest method used when the CA is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.
Lifetime (days)	3650
Common Name	pfsense.nesux
	The following certificate authority subject components are optional and may be left blank.

	The following certificate authority subject components are optional and may be left blank.
Country Code	FR v
State or Province	Picardie
City	Senlis
Organization	Nesux
Organizational Unit	e.g. My Department Name (optional)
	B Save



CA-NESUX

 \checkmark



Et je créer mon certificat en sélectionnant l'autorité créée juste avant.

Add/Sign a New Cert	ificate
Method	Create an internal Certificate
Descriptive name	Certificat-OpenVPN
	The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, ", '
Internal Certificate	
Certificate authority	CA-NESUX ~
Key type	RSA ~
	2048 🗸
	The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	sha256 🗸
	The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.
<u>Lifetime (days)</u>	3650
	The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.
Common Name	pfsense-nesux-firewall

	The following certificate subject components are optional and may be left blank.
Country Code	FR v
State or Province	Picardie
City	Senlis
Organization	Nesux
Organizational Unit	e.g. My Department Name (optional)
Certificate Attributes	
Attribute Notes	The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode. For internal Certificates, these attributes are added directly to the certificate as shown.
Certificate Type	Server Certificate Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.
Alternative Names	FQDN or Hostname Value Type Value Enter additional identifiers for the cert in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.
Add SAN Row	+ Add SAN Row
	Save



Certificat-OpenVPN Server Certificate CA: **No** Server: **Yes** CA-NESUX ST=Picardie, O=Nesux, L=Senlis, CN=pfsense-nesux-firewall, C=FR Valid From: Wed, 03 Apr 2024 10:33:31 +0200 Valid Until: Sat, 01 Apr 2034 10:33:31 +0200

OpenVPN Server 🖉 🏶 🗖 🖬 😋

Maintenant je crée l'utilisateur PFSENSE.

User Properties		
Defined by	USER	
Disabled	This user cannot login	
Username	vpn.pfsense.nesux	
Password	[••••••	[••••••
Full name	User's full name, for administrative information only	
Expiration date	Leave blank if the account shouldn't expire, otherwise enter the expiration da	ite as MM/DD/YYYY
Custom Settings	Use individual customized GUI options and dashboard layout for this use	r.
Group membership	admins	Î
	Not member of	Member of
	>> Move to "Member of" list	K Move to "Not member of" list
	Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.	
Certificate	Click to create a user certificate	
Create Certificate for	r User	
Descriptive name	Certificat-VPN-pfsense.nesux	
Certificate authority	CA-NESUX ~	
Key type	RSA v	
	2048 🗸	

Leven vpn.pfsense.nesux

✓ Ø m

Ensuite je configure le serveur.

Ici j'ai modifié plusieurs choses :

- **DESCRIPTION :** description au choix
- **SERVER MODE :** Remote access (SSL/TLS + User Auth)
- **PEER CERTIFICAT AUTHORITY :** (Authorité de certification créé précédemment)
- SERVER CERTIFICATE : (Certificat créé précédemment)
- IPV4 TUNNEL NETWORK : (le tunnel va permettre plus de sécurité grâce à des protocoles de chiffrement et d'authentification afin de protéger la communication. Je lui ai mis le réseau 10.10.10.0/24)
- IPV4 LOCAL NETWORK : (Ici je déclare les réseaux qui seront accessible depuis le VPN)
- **CONCURRENT CONNECTION :** (J'ai mis 10 connection maximum)
- DYNAMIC IP et TOPOLOGY : (Je l'ai activé pour le maintien des connexions et j'ai sélectionner la topologie en /30)
- **DNS DEFAULT DOMAIN :** (j'ai mis le nom de mon domaine)
- **DNS SERVER :** (J'ai mis l'ip de mon Serveur)
- **CUSTOM OPTION :** (protection supplémentaire contre le vol des identifiants en refusant la mise en cache)

General Information	
Description	Accès distant OpenVPN A description of this VPN for administrative reference.
Disabled	 Disable this server Set this option to disable this server without removing it from the list.
Unique VPN ID	Server 1 (ovpns1)
Mode Configuration	
Server mode	Remote Access (SSL/TLS + User Auth)
Backend for authentication	Local Database
Device mode	tun - Layer 3 Tunnel Mode "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Endpoint Configuration	n
Protocol	UDP on IPv4 only V
Interface	WAN
Local port	1194 The port used by OpenVPN to receive client connections.

Cryptographic Settin	gs
TLS Configuration	Ise a TLS Key A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.
<u>TLS Key</u>	# # 2048 bit OpenVPN static key #BEGIN OpenVPN Static key V1 3f68674d68a44a1d7f3e3c64b2c62c55 Paste the TLS key here.
	This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.
TLS Key Usage Mode	TLS Authentication ~
	In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.
TLS keydir direction	Use default direction
	The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.
Peer Certificate Authority	CA-NESUX ~
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check	Check client certificates with OCSP
Server certificate	Certificate-OpenVPN (Server: Yes, CA: CA-NESUX, In Use) Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.
DH Parameter Length	2048 bit ~
	Diffie-Hellman (DH) parameter set used for key exchange. 🕕



ECDH Curve	Lice Default		
Lobirourio	The Elliptic Curve to use for key evolutions		
	The curve from the server certificate is used by default when the server	uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.	
Data Encryption Algorithms	AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-CFB8 (128 bit key, 128 bit block) AES-128-CFB8 (128 bit key, 128 bit block)	AES-256-GCM AES-128-GCM CHACHA20-POLY1305	
	AES-128-05W (122 bit key, 128 bit block) AES-128-06B (128 bit key, 128 bit block) AES-192-05B (192 bit key, 128 bit block)		
	Available Data Encryption Algorithms Click to add or remove an algorithm from the list	Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list	
	The order of the selected Data Encryption Algorithms is respected by O	penVPN. This list is ignored in Shared Key mode. 🟮	
Fallback Data Encryption	AES-256-CBC (256 bit key, 128 bit block)	×	
Algorithm	The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.		
Auth digest algorithm	SHA256 (256-bit)		
	The algorithm used to authenticate data channel packets, and control of When an AEAD Encryption Algorithm mode is used, such as AES-GCM, The server and all clients must have the same setting. While SHA1 is th	hannel packets if a TLS Key is present. his digest is used for the control channel only, not the data channel. e default for OpenVPN, this algorithm is insecure.	
Hardware Crypto	No Hardware Crypto Acceleration		
Certificate Depth	One (Client+Server)		
	When a certificate-based client logs in, do not accept certificates below generated from the same CA as the server.	this depth. Useful for denying certificates made with intermediate CAs	
Strict User-CN Matching	Enforce match		
	When authenticating users, enforce a match between the common name	e of the client certificate and the username given at login.	
Client Certificate Key	Enforce key usage		
Usage Validation	Verify that only hosts with a client certificate can connect (EKU: "TLS W	eb Client Authentication").	

General Information	
Description	Accès distant Open/UN
Description	
	A description of this VPN for administrative reference.
Disabled	Disable this server
	Set this option to disable this server without removing it from the list.
Unique VPN ID	Server 1 (ovpns1)
Modo Configuration	
woue configuration	
Server mode	Remote Access (SSL/TLS + User Auth)
Backend for	Local Database
authentication	
Device mode	tun - Layer 3 Tunnel Mode 🗸 🗸
	"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
	"tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Endpoint Configuration	nn
Enapoint configuration	
Protocol	UDP on IPv4 only 🗸
Interface	WAN
	The interface or Virtual IP address where OpenVPN will receive client connections.
Local port	1194
	The port used by OpenVPN to receive client connections.



Cryptographic Settings		
TLS Configuration	Use a TLS Key A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.	
<u>TLS Key</u>	# # 2048 bit OpenVPN static key #BEGIN OpenVPN Static key V1 3F68674d68a4Aa1d7F3=3c6db2c62c55 Paste the TLS key here. This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.	
TLS Key Usage Mode	TLS Authentication In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.	
TLS keydir direction	Use default direction The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.	
Peer Certificate Authority	CA-NESUX 🗸	
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager	
OCSP Check	Check client certificates with OCSP	
Server certificate	Certificat-OpenVPN (Server: Yes, CA: CA-NESUX, In Use) Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.	
DH Parameter Length	2048 bit ~	

Diffie-Hellman (DH) parameter set used for key exchange.

ECDH Curve	Use Default	
	The Elliptic Curve to use for key exchange.	
	The curve from the server certificate is used by default when the server	uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
Data Encryption Algorithms	AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-GFB (128 bit key, 128 bit block) AES-128-GCM (128 bit key, 128 bit block) AES-128-GCM (128 bit key, 128 bit block) AES-128-GE (192 bit key, 128 bit block) AES-192-CFB (192 bit key, 128 bit block)	AES-256-GCM AES-128-GCM CHACHA20-POLY1305
	Available Data Encryption Algorithms	Allowed Data Encryption Algorithms. Click an algorithm name to remove
	Click to add or remove an algorithm norm the list	
	The order of the selected Data Encryption Algorithms is respected by Op	eenVPN. This list is ignored in Shared Key mode. 📵
Fallback Data Encryption Algorithm	AES-256-CBC (256 bit key, 128 bit block)	0
5	The Fallback Data Encryption Algorithm used for data channel packets in negotiation (e.g. Shared Key). This algorithm is automatically included in	when communicating with clients that do not support data encryption algorithm n the Data Encryption Algorithms list.
		,, , ,
Auth digest algorithm	SHA256 (256-bit)	•
	The algorithm used to authenticate data channel packets, and control cl When an AEAD Encryption Algorithm mode is used, such as AES-GCM, t The server and all clients must have the same setting. While SHA1 is the	nannel packets if a TLS Key is present. his digest is used for the control channel only, not the data channel. e default for OpenVPN, this algorithm is insecure.
Hardware Crypto	No Hardware Crypto Acceleration	3
Certificate Depth	One (Client+Server)	
	When a certificate-based client logs in, do not accept certificates below	
	generated from the same CA as the server.	
Strict User-CN Matching	Enforce match	
	When authenticating users, enforce a match between the common name	e of the client certificate and the username given at login.
Client Certificate Key		
Usage Validation	Verify that only hosts with a client certificate can connect (FKU: "TLS W	eb Client Authentication").
	,	



Tunnel Settings	
IPv4 Tunnel Network	10.10.10.0/24 This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients. A tunnel network of /30 or smaller puts Open/VPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.
IPv6 Tunnel Network	This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Redirect IPv4 Gateway	Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	192.168.1.0/29 IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
IPv6 Local network(s)	IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent connections	10 Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression	Refuse any non-stub compression (Most secure) Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack. Asymmetric compression allows an easier transition when connecting with older peers.

Type-of-Service	Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-client communication	Allow communication between clients connected to this server
Duplicate Connection	Allow multiple concurrent connections from the same user When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session. Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.
Client Settings	
Dynamic IP	Allow connected clients to retain their connections if their IP address changes.
Topology	net30 – Isolated /30 network per client Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".
Ping settings	
Inactive	300 Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device. Activity is based on the last incoming or outgoing tunnel packet. A value of 0 disables this feature. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.
Ping method	keepalive – Use keepalive helper to define ping configuration keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows: ping = interval ping-restart = timeout*2 push ping = interval push ping-restart = timeout
Interval	10



Timeout	60	
Advanced Client Se	ttings	
DNS Default Domain	Provide a default domain name to clients	
DNS Default Domain	nesux.lan	
DNS Server enable	Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.	
DNS Server 1	192.168.1.1	
DNS Server 2		
DNS Server 3		
DNS Server 4		
Block Outside DNS	☐ Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VP Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore th not affected.	N DNS servers. e option as they are
Force DNS cache update	Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.	
NTP Server enable	Provide an NTP server list to clients	
NetBIOS enable	Enable NetBIOS over TCP/IP If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.	
Advanced Configura	ation	
Username as Common Name	Use the authenticated client username instead of the certificate common name (CN). When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes such as determining Client Specific Overrides.	
UDP Fast I/O	Use fast I/O operations with UDP writes to tun/tap. Experimental. Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.	
Exit Notify	teconnect to this server / Retry once v a an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting a a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. This option is ignored in Peer-to-Peer Shared Key ode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.	
Send/Receive Buffer	Default Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.	
Gateway creation	Both OIPv4 only OIPv6 only	
	If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.	
Verbosity level	default v Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output. None: Only fatal errors Default through 4: Normal usage range 5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.	
	e-11: Debug info range	



Maintenant j'exporte la configuration de mon utilisateur. Avant il faut installer "openvpn-client-export" dans System -> Package Manager -> Available Packages

System / Pac	kage N	Ianager / Available Packages
Installed Packages	Availa	ble Packages
Search		•
Search term		openvpn Both 🔻 🖓 Clear
	E	inter a search string or *nix regular expression to search package names and descriptions.
Packages		
Name	Version	Description
openvpn-client-export	1.4.23	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.
		Package Dependencies:

Et je vais dans OpenVPN \rightarrow Client Export

Voici les choses que j'ai modifié ici :

- **REMOTE ACCESS SERVER :** J'ai bien sélectionner le bon Serveur VPN créé juste avant
- ADDITIONAL CONFIGURATION OPTIONS : Je remets auth-nocache



OpenVPN / Client Export Utility

Server	Client	Client Specific Overrides Wizards Client Export		
OpenVP	N Server			
Remote Access Server		Accès distant OpenVPN UDP4:1194		
Client Co	onnection	Behavior		
Host Nar	ne Resolutior	Interface IP Address v		
Ve	rify Server CN	Automatic - Use verify-x509-name where possible		
Block	c Outside DNS	NS DIBlock access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.		
	Legacy Clien	t Do not include OpenVPN 2.5 and later settings in the client configuration. When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.		
S	Silent Installe	Create Windows installer for unattended deploy. Create a silent Windows installer for unattended deploy; installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.		
	Bind Mode	Do not bind to the local port If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.		

Certificate Export Options					
PKCS#11 Certificate Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files. Storage					
Microsoft Certificate Storage	Use Microsoft Certificate Storage instead of local files.				
Password Protect Certificate	□ Use a password to protect the PKCS#12 file contents or key in Viscosity bundle.				
PKCS#12 Encryption	High: AES-256 + SHA256 (pfSense Software, FreeBSD, Linux, Windo 💉 Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program				
Proxy Options					
Use A Proxy	Use proxy to communicate with the OpenVPN server.				
Advanced					
Additional configuration options	auth-nocache				
	Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.				
	EXAMPLE: remote-random;				
	Save as default				
Search	•				
Search term	Q. Search 5 Clear				
	Enter a search string or *nix regular expression to search.				



0

Et dans Bundled Configuration je télécharge l'archive.

Et dans Current Windows Installers (2.6.7-lx001) je télécharge OpenVPN.

OpenVPN Clients					
User	Certificate Name	Export			
vpn.pfsense.nesux	Certificat-VPN-pfsense.nesux	 Inline Configurations: Bundled Configurations: Bundled Configurations: Archive			
Only OpenVPN-compatible user of If a client is missing from the I firewall, or a user certificate is Clients using OpenSSL 3.0 ma OpenVPN 2.4.8+ requires Win	certificates are shown ist it is likely due to a CA mismatch between the OpenVPN s not associated with a user when local database authenticat y not work with older or weaker ciphers and hashes, such as dows 7 or later	erver instance and the client certificate, the client certificate does not exist on this ion is enabled. SHA1, including when those were used to sign CA and certificate entries.			
Links to OpenVPN clients for vari OpenVPN Community Client - Bir OpenVPN For Android - Recomm OpenVPN Connect: Android (Goo Viscosity - Recommended comm Tunnelblick - Free client for OS X	ious platforms: naries for Windows, Source for other platforms. Packaged ab ended client for Android ygle Play) or iOS (App Store) - Recommended client for iOS lercial client for Mac OS X and Windows	ove in the Windows Installers			







2.15 - Test OpenVPN



Je me connecte avec l'utilisateur créer sur pfsense.

🔁 Connexion OpenVPN (pfSense-UDP4-1194-vpn.pfsense.nesux-config) — 🗆 🗙						
Etat actuel: En cours de connexion						
Wed Apr 3 15:48:37 2024 OpenVPN 2.6.7 [git:v2.6.7/53c9033317b3b8fd] Windows [SSL (OpenSSL)] [LZO] [l Wed Apr 3 15:48:37 2024 Windows version 10.0 (Windows 10 or greater), amd64 executable Wed Apr 3 15:48:37 2024 library versions: OpenSSL 3.1.4 24 Oct 2023, LZO 2.10 Wed Apr 3 15:48:37 2024 DCO version: 1.0.0						
	Utilisateur: vpn.pfsense.nesux Mot de passe:					
	Enregistrer mot de passe					
<	OK Annuler					
	OpenVPN GUI 11.45.0.0/2.6.7					
Déconnecter Reprendre	Fermer					





2.16 - LDAP pour les utilisateurs de la zone locale (en cours)



2.17 - Synthèse des règles (en cours)



3) CONCLUSION

L'entreprise de développement logiciels NESUX possède désormais un réseau fonctionnel avec une zone locale, une zone DMZ, un VPN et un pare-feu PFSENSE qui comporte les fonctionnalités CROWDSEC et SQUID.