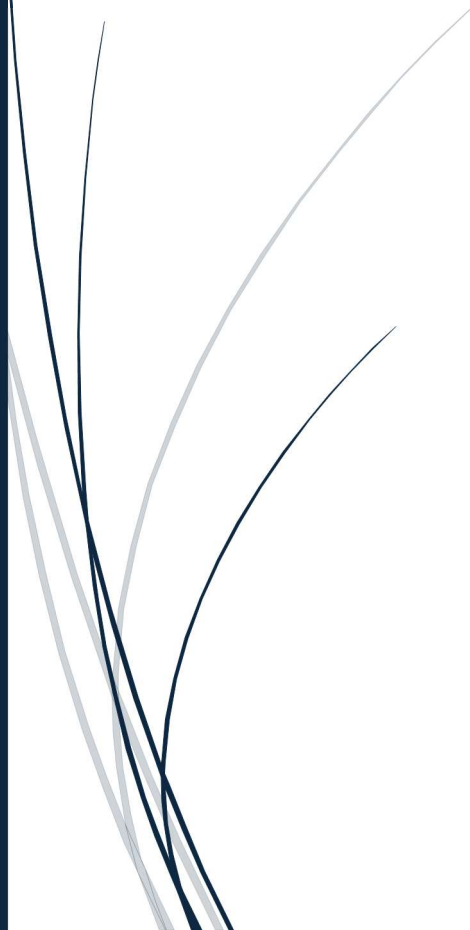


05/04/2024

PFSENSE



Alexis PENET
TECHVISTA

Page 0 sur 30

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE		N° réalisation :
Nom, prénom : Alexis PENET		N° candidat :
Épreuve ponctuelle ☐	Contrôle en cours de formation ☒	Date : 05/04/2023
Organisation support de la réalisation professionnelle		
Intitulé de la réalisation professionnelle Mise en d'un pare-feu sous PFSENSE.		
Période de réalisation : 15/11/2023 – 15/12/2023 Lieu : Senlis		
Modalité : ☒ Seul(e) ☐ En équipe		
Compétences travaillées ☒ Concevoir une solution d'infrastructure réseau ☒ Installer, tester et déployer une solution d'infrastructure réseau ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau		
Conditions de réalisation* (ressources fournies, résultats attendus)		
Serveur LINUX Serveur AD Client W10 Serveur AD Serveur PFSENSE Kali linux Les résultats attendus du PPE sont : SQUID Crowdsec VPN LDAP DMZ (un serveur linux avec service web) Lan (active directory et 2 clients windows)		
Description des ressources documentaires, matérielles et logicielles utilisées*		
https://www.it-connect.fr/tuto-installation-crowdsec-pare-feu-pfsense/?utm_content=cmp-true https://www.it-connect.fr/mise-en-place-et-configuration-dun-proxy-avec-squid/ VMware Workstation 17 Pfsense Windows 11 22h2 Debian 11 Windows server 2022 Word, bloc note		
Modalités d'accès aux productions* et à leur documentation*		
Windows 11 → 1er mdp Azerty1* 2ème Azerty1, Azerty12, alexis → Azerty12		

Sommaire

Introduction.....	3
Contexte.....	3
Architecture réseau	4
Configuration PFSENSE	6
HTTPS	8
SQUID.....	10
Règles pare-feu	13
Mise en place du VPN.....	15
Connexion LDAP	21
Installation Crowdsec.....	25
Attaque NMAP	28
Conclusion	30

Introduction

Cette mission consiste à installer 6 VM sous PFSense, LINUX, Windows, Windows Server, Kali linux afin de créer un réseau avec un pare-feu.

Le but est de construire un réseau avec 3 sites (WAN ,LAN,DMZ) pour mettre en place

- SQUID
- Crownsec
- VPN
- LDAP
- DMZ (un serveur linux avec service web)
- Lan (active directory et 2 clients windows)

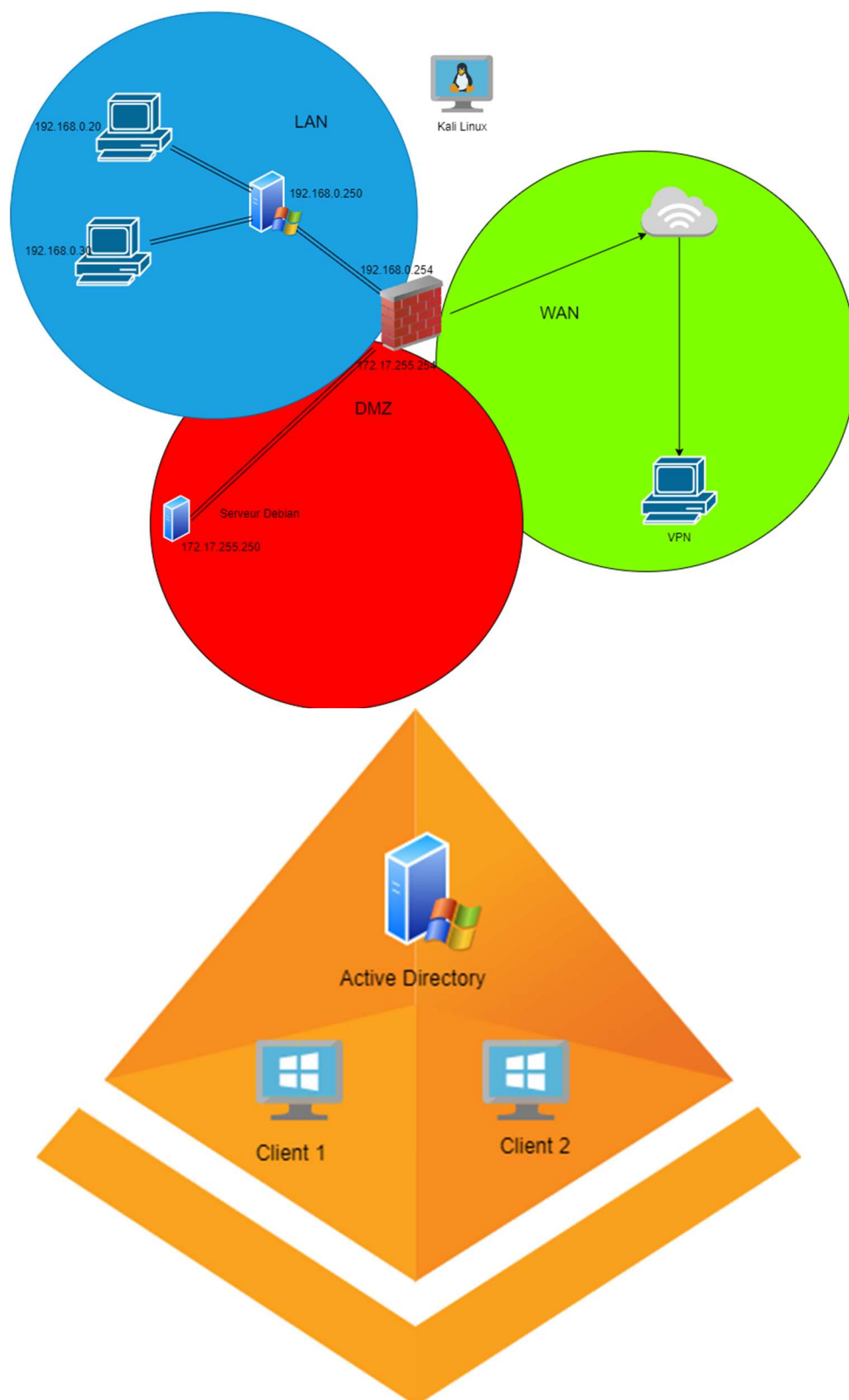
Contexte

Dans le cadre d'un déploiement réseau pour une entreprise, l'équipe informatique utilise pfSense pour mettre en place une infrastructure sécurisée.

Trois zones principales sont définies : le WAN pour l'accès à Internet, le LAN pour les ressources internes, et la DMZ pour les serveurs accessibles depuis Internet.

Avec pfSense, des règles de pare-feu précises sont configurées pour contrôler le flux de trafic entre ces zones, assurant ainsi une sécurité renforcée et des performances optimales.

Architecture réseau



WAN = DHCP

LAN = 192.168.0.254 /24

DMZ = 172.17.255.254 /16

Serveur Debian (DMZ) = 172.17.255.250 /16

AD (LAN) = 192.168.0.250 /24

Client 1 (LAN) = 192.168.0.20 /24

Client 2 (LAN) = 192.168.0.30 /24

Kali linux = ?

Configuration PFSENSE

PFsense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD.

1. Configuration des cartes WAN, LAN, DMZ.

Un WAN (Wide Area Network, ou réseau étendu) est un réseau couvrant une zone géographique de grande envergure. Votre modem envoie et reçoit des informations depuis et vers Internet via son port WAN.

Le LAN (Local Area Network, ou réseau local) désigne les appareils connectés, par Wi-Fi ou connexion filaire, dans votre domicile ou bureau. Il s'agit d'un réseau personnel.

Une zone démilitarisée (DMZ, Demilitarized Zone) est un sous-réseau physique ou logique qui sépare un réseau local interne (LAN, Local Area Network) d'autres réseaux non sécurisés tels qu'Internet.

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.99/24
LAN (lan)      -> em2      -> v4: 192.168.0.254/24
DMZ (opt1)     -> em1      -> v4: 172.17.255.254/16

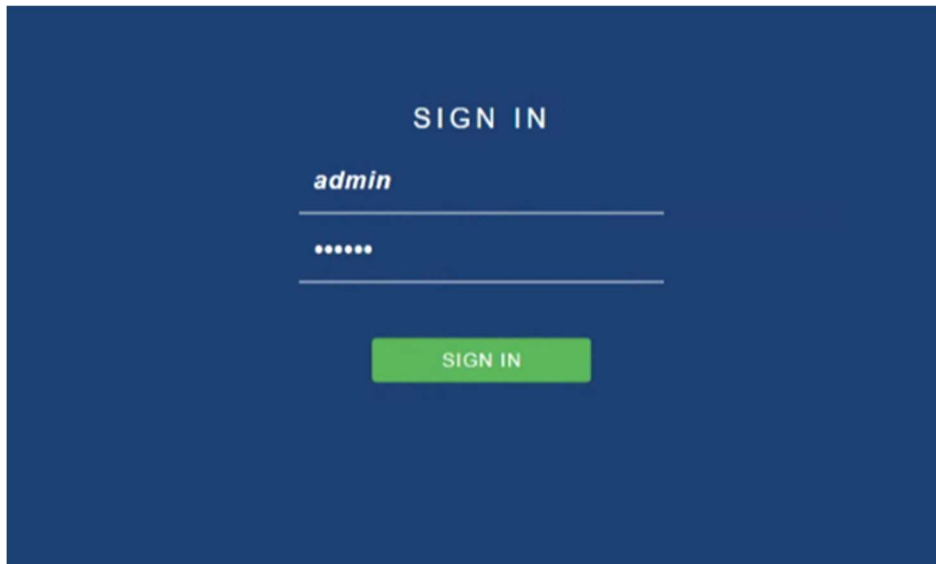
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
```

Pour configurer les cartes il faut ajouter des cartes virtuelles dans la vm PFSENSE, clic droit → settings → on ajoute 2 LAN SEGMENT qu'on appellera LAN et DMZ puis on ajoute une vmet en bridge pour le WAN.

Ensuite on appuie sur "Assign Interfaces" puis on suit les étapes pour ajouter les cartes virtuelles en faisant attention aux configurations précédentes.

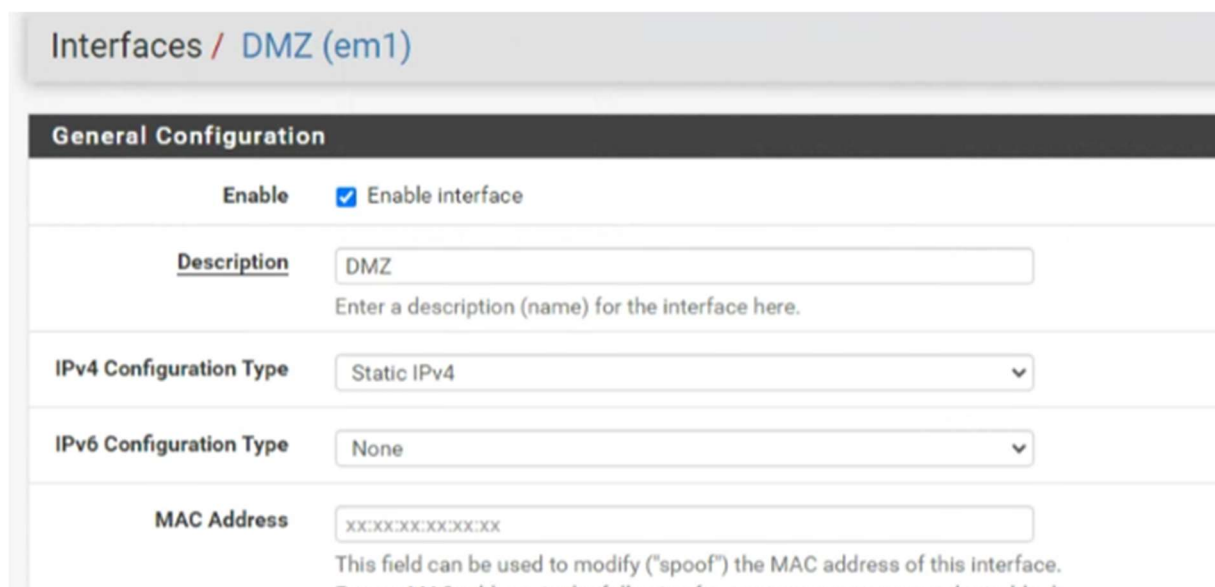
On tape 2 pour ajouter des adresses au WAN, LAN et DMZ.

Une fois fait on prends un pc connecté au lan puis on se rend sur l'interfaces WEB du pfsense. "<http://192.168.0.254> ou <https://192.168.0.254>"



User=admin

Password=pfsense

A screenshot of the PfSense web interface showing the configuration for the DMZ interface (em1). The page title is "Interfaces / DMZ (em1)". Below the title is a "General Configuration" section. It contains several fields: "Enable" with a checked checkbox "Enable interface"; "Description" with a text box containing "DMZ" and a hint "Enter a description (name) for the interface here."; "IPv4 Configuration Type" with a dropdown menu set to "Static IPv4"; "IPv6 Configuration Type" with a dropdown menu set to "None"; and "MAC Address" with a text box containing "xx:xx:xx:xx:xx:xx" and a hint "This field can be used to modify ('spoof') the MAC address of this interface.".

Une fois dans l'interface WEB on renomme la carte par DMZ puis on l'active.
Pour ce qui est des cartes tout est fait.

HTTPS

Le protocole HTTPS (hyper text transfert protocol secure) c'est une extension du protocole http mais grâce à l'https les données entre le navigateur et l'internaute sont chiffrés, ils ne peuvent pas être espionnés. Une attaque MitmHTTP permet d'intercepter des communications pour pouvoir le lire le https offrent une option de cryptage ce qui nous permettra de ne pas être lu.

Nous allons voir comment le mettre en place.

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA Techvista	✓	self-signed	2	ST=Hauts-de-France, O=techvista, L=Senlis, CN=internal-ca Valid From: Wed, 20 Mar 2024 16:26:39 +0100 Valid Until: Sat, 18 Mar 2024 16:26:39 +0100	Squid (2)	   
VPN	✓	self-signed	2	ST=Hauts-de-France, O=techvista, L=Senlis, CN=internal-ca, C=FR Valid From: Fri, 22 Mar 2024 11:23:44 +0100 Valid Until: Mon, 20 Mar 2024 11:23:44 +0100	OpenVPN Client	   

 Add

On appuie sur ADD puis on remplit les cases correspondantes pour créer l'autorité de certification.

CA techvista Server Certificate CA: No Server: Yes	CA Techvista	ST=Hauts-de-France, O=techvista, L=Senlis, CN=https://pfsense/ Valid From: Wed, 20 Mar 2024 16:31:00 +0100 Valid Until: Sat, 18 Mar 2024 16:31:00 +0100	   
CA Techvista User Certificate CA: No Server: No	CA Techvista	ST=Hauts-de-France, O=techvista, L=Senlis, CN=https://pfsense/ Valid From: Wed, 20 Mar 2024 16:36:55 +0100 Valid Until: Sat, 18 Mar 2024 16:36:55 +0100	   

On appuie sur ADD puis on remplit toutes les cases. (exemple si dessous)
Pour le deuxième certificat on change le "Certificate type" par server certificate.

Add/Sign a New Certificate

Method

Create an internal Certificate

Descriptive name

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 Techvista

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.

Lifetime (days)

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

techvista.lan

The following certificate subject components are optional and may be left blank.

Country Code

None

State or Province

Hauts-de-France

City

Senlis

Organization

techvista

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 selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type

User Certificate

Add type-specific usage attributes to the signed certificate. Used for placing the certificate in a specific location, or granting abilities to, the signed certificate.

Alternative Names

FQDN or Hostname

techvista.lan

Microsoft Store

webConfigurator

Protocol

HTTP

HTTPS (SSL/TLS)

Non sécurisé

https://192.168.0.254/system

Ensuite on va dans système → Advanced → Admin Access puis on active le protocole HTTPS.

SQUID

Squid est un serveur proxy spécialisé, basé sur Unix, qui agit comme un proxy de mise en cache pour les objets web accessibles par HTTP, HTTPS, FTP, etc. Il est couramment utilisé à plusieurs fins, notamment pour la mise en cache, l'équilibrage de la charge, le filtrage du trafic des sites web et la sécurité.

Pour commencer nous allons dans services → Squid Proxy Server → General.

The screenshot shows the 'Squid General Settings' page. It includes several configuration options:

- Enable Squid Proxy:** A checkbox that is checked. Below it, a note states: 'Important: If unchecked, ALL Squid services will be disabled and stopped.'
- Keep Settings/Data:** A checkbox that is checked. Below it, a note states: 'Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.'
- Listen IP Version:** A dropdown menu set to 'IPv4'. Below it, a note says: 'Select the IP version Squid will use to select addresses for accepting client connections.'
- CARP Status VIP:** A dropdown menu set to 'none'. Below it, a note says: 'Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status. Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization.'
- Proxy Interface(s):** A multi-select dropdown menu with 'WAN', 'LAN', 'DMZ', and 'loopback' options. Below it, a note says: 'The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.'

On coche les cases au-dessus.

The screenshot shows the 'General DNS Forwarder Options' page. It includes several configuration options:

- Enable:** A checkbox that is checked, labeled 'Enable DNS forwarder'.
- DNS Query Forwarding:** A section with three options:
 - ☐ Query DNS servers sequentially: If this option is set pfSense DNS Forwarder (dnsmasq) will query the DNS servers sequentially in the order specified (System - General Setup - DNS Servers), rather than all at once in parallel.
 - ☒ Require domain: If this option is set pfSense DNS Forwarder (dnsmasq) will not forward A or AAAA queries for plain names, without dots or domain parts, to upstream name servers. If the name is not known from /etc/hosts or DHCP then a 'not found' answer is returned.
 - ☐ Do not forward private reverse lookups: If this option is set pfSense DNS Forwarder (dnsmasq) will not forward reverse DNS lookups (PTR) for private addresses (RFC 1918) to upstream name servers. Any entries in the Domain Overrides section forwarding private 'n.n.n.in-addr.arpa' names to a specific server are still forwarded. If the IP to name is not known from /etc/hosts, DHCP or a specific domain override then a 'not found' answer is immediately returned.
- Listen Port:** A text input field containing '53'. Below it, a note says: 'The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.'
- Interfaces:** A multi-select dropdown menu with 'All', 'WAN', 'LAN', and 'DMZ' options. Below it, a note says: 'Interface IPs used by the DNS Forwarder for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected above are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.'
- Strict binding:** A checkbox that is unchecked, labeled 'Strict interface binding'.

This is the port the proxy server will send and receive ICP queries to and from neighbor caches.
Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

Allow Users on Interface	☒ If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.
Patch Captive Portal	This feature was removed - see Bug #5594 for details!
Resolve DNS IPv4 First	☒ Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites.

Dans service → DNS Forwarder on coche les cases suivantes pour pouvoir bloquer les sites en HTTPS.

Puis dans services → Squid Proxy Server → General on remplis/coche toutes les cases ci-dessous.

Logging Settings

Enable Access Logging ☒ This will enable the access log.
Warning: Do NOT enable if available disk space is low.

Log Store Directory
The directory where the logs will be stored; also used for logs other than the Access
Important: Do NOT include the trailing / when setting a custom location.

Rotate Logs

SSL Man In the Middle Filtering

HTTPS/SSL Interception ☒ Enable SSL filtering.

Headers Handling, Language and Other Customizations

Visible Hostname
This is the hostname to be displayed in proxy server error messages.

Administrator's Email
This is the email address displayed in error messages to the users.

Error Language
Select the language in which the proxy server will display error messages to users.

X-Forwarded Header Mode
Choose how to handle X-Forwarded-For headers. Default: on ⓘ

Disable VIA Header ☐ If not set, Squid will include a Via header in requests and replies as required by RFC2616.

URI Whitespace Characters Handling
Choose how to handle whitespace characters in URL. Default: strip ⓘ

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

Une fois faits-nous pouvons faire un essai dans blacklist pour voir si le site bloque le HTTPS.

Squid Access Control Lists

Allowed Subnets

Enter subnets that are allowed to use the proxy in CIDR format. All the other subnets won't be able to use the proxy. Put each entry on a separate line.

When 'Allow Users on Interface' is checked on 'General' tab, there is no need to add the 'Proxy Interface(s)' subnet(s) to this list.

Unrestricted IPs

Enter unrestricted IP address(es) / network(s) in CIDR format. Configured entries will NOT be filtered out by the other access control dir this page.

Put each entry on a separate line. 

Banned Hosts Addresses

Enter IP address(es) / network(s) in CIDR format. Configured entries will NOT be allowed to use the proxy. Put each entry on a separate line.

Whitelist

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

Blacklist

w3.uqo.ca
developer.mozilla.org
youtube.com
amazon.fr



Connexion bloquée : problème de sécurité potentiel

Firefox a détecté une menace potentielle de sécurité et a interrompu le chargement de www.facebook.com, car ce site web nécessite une connexion sécurisée.

Que pouvez-vous faire ?

www.facebook.com a recours à une stratégie de sécurité HTTP Strict Transport Security (HSTS), une connexion sécurisée est obligatoire pour y accéder. Vous ne pouvez pas ajouter d'exception pour visiter ce site.

Le problème vient probablement du site web, donc vous ne pouvez pas y remédier.

Si vous naviguez sur un réseau d'entreprise ou si vous utilisez un antivirus, vous pouvez contacter les équipes d'assistance pour obtenir de l'aide. Vous pouvez également signaler le problème aux personnes qui administrent le site web.

[En savoir plus...](#)

[Retour](#)[Avancé...](#)

Nous pouvons voir que ça a fonctionner.

Règles pare-feu

Nous allons ajouter des règles pour pouvoir autoriser des communications et interdire des communications en réseau.

Nous allons en appliquer sur le WAN, LAN et DMZ.

WAN :

Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0/0 B	IPv4 *	172.16.255.0/24 *	192.168.0.0/24 *	*	*	none			
☐	✓	0/0 B	IPv4 *	172.16.255.0/24 *	172.17.255.0/16 *	*	*	none			
☐	✓	0/0 B	IPv4 *	172.16.255.0/24 *	172.16.255.0/24 *	*	*	none			
☐	✓	0/0 B	IPv4 UDP *	*	1194 (OpenVPN)	172.16.255.0/24	1194 (OpenVPN) *	none		Autoriser le VPN SSL	
Add Add Delete Toggle Copy Save Separator											

La première règle sert à autoriser le WAN à communiquer avec la LAN.

La deuxième sert à autoriser la communication entre la Wan et la DMZ.

La troisième sert à autoriser les communications du entre WAN.

La dernière sert à autoriser le flux VPN.

LAN :

Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	7/943 KiB	*	*	*	LAN Address	443 80 9922	*	*		Anti-Lockout Rule	
☐	✓ 0/0 B	IPv4 *	192.168.0.0/24 *	*	172.16.255.0/24 *	*	*	none			
☐	✓ 0/0 B	IPv4 *	172.16.255.0/24 *	*	192.168.0.0/24 *	*	*	none			
☐	✓ 111/60 KiB	IPv4 *	LAN subnets *	*	*	*	*	none		Default allow LAN to any rule	
☐	✓ 0/0 B	IPv6 *	LAN subnets *	*	*	*	*	none		Default allow LAN IPv6 to any rule	
Add Add Delete Toggle Copy Save Separator											

La deuxième réglé sert à autoriser la connexion entre le Lan et le WAN.

La troisième sert à autoriser la communication en sens inverse du Wan au LAN.

DMZ :

Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	 0/0 B	IPv4 *	172.17.255.0/16	*	192.168.0.0/24	*	*	none			   
☐	 0/0 B	IPv4 *	172.16.255.0/24	*	172.17.255.0/16	*	*	none			    

 Add  Add  Delete  Toggle  Copy  Save  Separator



La première règle permet d’interdire la communication entre la DMZ et la LAN.

La deuxième règle permet d’autoriser la communication entre le WAN et la DMZ.

Toutes c’est règles sont utiles à notre réseau.

Mise en place du VPN

Les VPN servent à transmettre des données de manière sûre et anonyme sur des réseaux publics.

Le VPN créer un tunnel sécurisé d'un point A à un Point B.

Pour l'installation du VPN nous devons créer 2 certificats 1 pour le serveur et 1 pour le user.

VPN server -1 Server Certificate CA: No Server: Yes	VPN	ST=Hauts-de-France, O=techvista, L=Senlis, CN=techvista.lan, C=FR Valid From: Fri, 22 Mar 2024 11:26:08 +0100 Valid Until: Mon, 20 Mar 2034 11:26:08 +0100	OpenVPN Server
VPN-client -1 User Certificate CA: No Server: No	VPN	ST=Hauts-de-France, O=techvista, L=Senlis, CN=techvista.lan, C=FR Valid From: Fri, 22 Mar 2024 11:26:25 +0100 Valid Until: Mon, 20 Mar 2034 11:26:25 +0100	OpenVPN Client

+ Add/Sign

Une fois faits-nous allons dans VPN → OPENVPN → Servers pour configurer l'accès VPN.

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.10.10.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	VPN-SSL	  

+ Add

Ensuite il faudra remplir les cases comme en-dessous, attention il ne faut pas se tromper entre le certificat serveur et utilisateurs.

Mode Configuration

Server mode

Remote Access (SSL/TLS + User Auth)

Backend for authentication

LDAP Active Directory

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

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.

TLS Key

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
772799e4321c46bfe72f851dcd82ba3f
```

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

VPN

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

VPN server -1 (Server: Yes, CA: VPN, 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. [i](#)

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-CFB1 (128 bit key, 128 bit block)

AES-128-CFB8 (128 bit key, 128 bit block)

AES-128-GCM (128 bit key, 128 bit block)

AES-128-OFB (128 bit key, 128 bit block)

AES-192-CBC (192 bit key, 128 bit block)

AES-192-CFB (192 bit key, 128 bit block)

AES-192-CFB1 (192 bit key, 128 bit block)

AES-192-CFB8 (192 bit key, 128 bit block)

AES-256-GCM

AES-128-GCM

CHACHA20-POLY1305

Available Data Encryption Algorithms

Click to add or remove an algorithm from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. [i](#)

Page 16 sur 30

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 OpenVPN 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)	192.168.0.0/24
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.	

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 Settings	
DNS Default Domain	☒ Provide a default domain name to clients
DNS Default Domain	techvista.lan
DNS Server enable	☒ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	192.168.0.250
DNS Server 2	8.8.8.8

Advanced Configuration

Custom options

auth-nocache

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.

EXAMPLE: push "route 10.0.0.0 255.255.255.0"

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

Reconnect to this server / Retry once

Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for 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 mode 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
 ☐ IPv4 only
 ☐ IPv6 only

User :

OpenVPN Clients					
Interface	Protocol	Server	Mode / Crypto	Description	Actions
WAN	UDP4 (TUN)	172.16.255.51:1194	Mode: Peer to Peer (SSL/TLS) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256	VPN-SSL	  

+

Add

Server mode

Peer to Peer (SSL/TLS)

Device mode

tun - Layer 3 Tunnel Mode

"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mo
 "tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol

UDP on IPv4 only

Interface

WAN

The interface used by the firewall to originate this OpenVPN client connection

Local port

Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic p

Server host or address

172.16.255.51

The IP address or hostname of the OpenVPN server.

Server port

1194

The port used by the server to receive client connections.

Proxy host or address

The address for an HTTP Proxy this client can use to connect to a remote server.
TCP must be used for the client and server protocol.

Proxy port

Proxy Authentication

none

The type of authentication used by the proxy server.

User Authentication Settings

Username

alexis

Leave empty when no user name is needed

Password

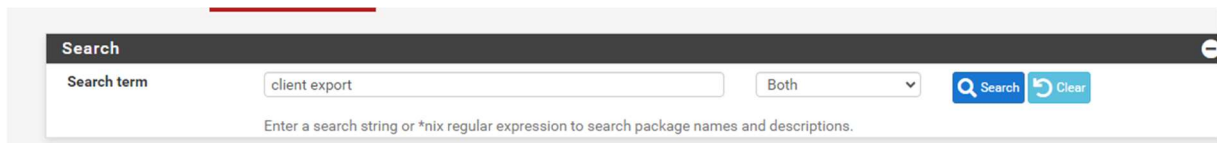
TLS Configuration	☒ Use a TLS Key A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.
TLS Key	<pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 16f45f704303e69d5b0381d391e97b58</pre> 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	Both directions 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	VPN
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation
Client Certificate	VPN-client-1 (CA: VPN, 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

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.
TLS Key	<pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 16f45f704303e69d5b0381d391e97b58</pre> 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	Both directions 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	VPN
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation
Client Certificate	VPN-client-1 (CA: VPN, 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

Ensuite nous allons dans Firewall → Rules → Wan puis on rentre cette règle.
Elle permet d'autoriser le flux VPN

☐	☒	0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none	Autoriser le VPN SSL	    
--------------------------	-------------------------------------	-------	----------	---	---	-------------	----------------	---	------	----------------------	---

On installe client export pour exporter la configuration VPN.

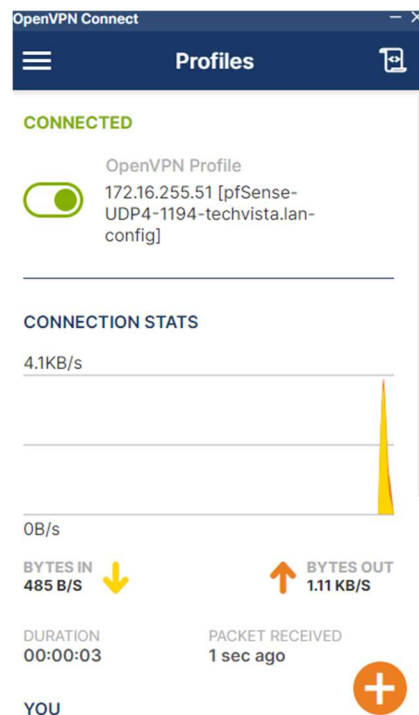


The screenshot shows a search bar with the text "client export" entered. Below the search bar, there is a dropdown menu set to "Both" and two buttons: "Search" and "Clear". A small text hint below the search bar reads: "Enter a search string or *nix regular expression to search package names and descriptions."

On clique sur **Archive et Config File Only**.

OpenVPN Clients		
User	Certificate Name	Export
Certificate with External Auth	VPN-client -1	- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installer (2.6.7-1x001): 64-bit 32-bit - Previous Windows Installer (2.5.9-1x601): 64-bit 32-bit - Legacy Windows Installers (2.4.12-1x601): 10/2016/2019 7/8/8.1/2012r2 - Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config

On importe les fichiers OpenVPN puis on se connecte avec l'utilisateurs LDAP.



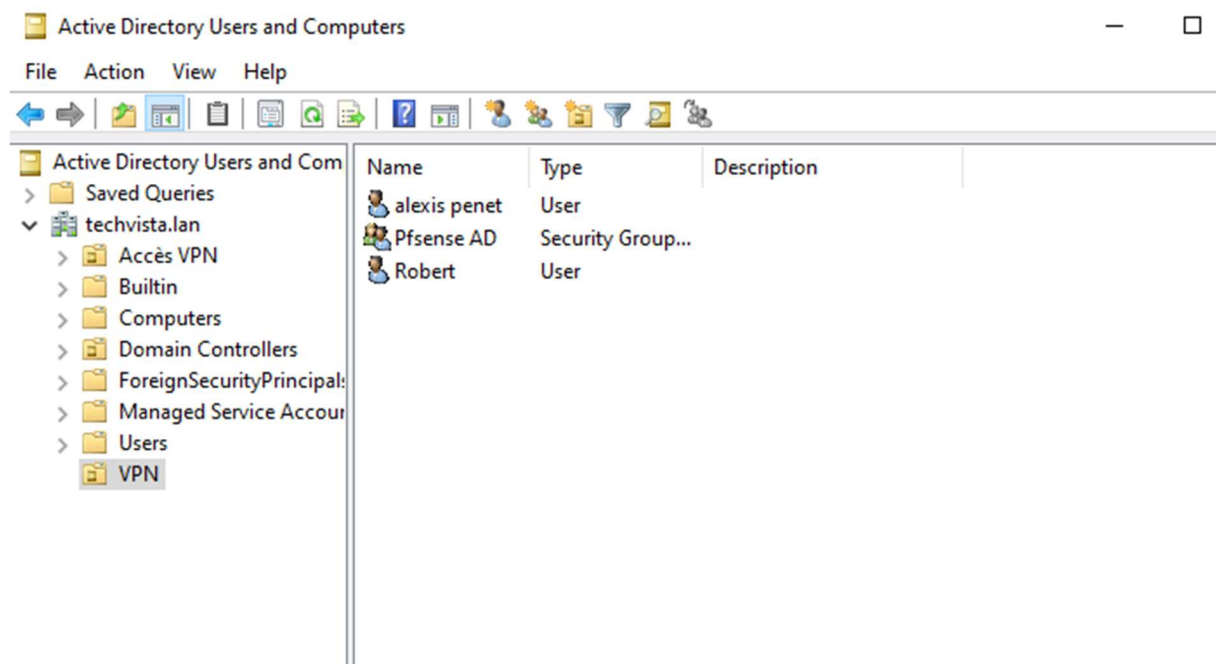
Connexion LDAP

Le LDAP est un protocole d'authentification pour les services d'annuaire. Ils stockent des informations telles que :

- Les utilisateurs
- Les caractéristiques de ces utilisateurs
- Le privilège d'appartenance à un groupe
- Et plus encore ...

Nous allons voir comment le mettre en place sur PFSense.

Pour commencer nous allons a créer un OU et un groupe d'utilisateurs. On mets les droits administrateurs à l'utilisateurs Alexis PENET.



Ensuite nous allons dans le PFSense dans système → User Manager puis on clique sur ADD pour créer un groupe. (Il faut qu'il soit écrit de la même manière)

Group Properties

Group name

Pfsense AD

Scope

Remote

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description

VPN Accès AD

Group description, for administrative information only

Group membership

admin

Not members

Members

Move to "Members"

Move to "Not members"

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Une fois fait on ajoute tous les droits captive portal et on ajoute All Pages.

WebCfg - Services: Captive Portal: Allowed IPs	Allow access to the 'Services: Captive Portal: Allowed IPs' page.	
WebCfg - Services: Captive Portal: Edit Allowed Hostnames	Allow access to the 'Services: Captive Portal: Edit Allowed Hostnames' page.	
WebCfg - Services: Captive Portal: Edit Allowed IPs	Allow access to the 'Services: Captive Portal: Edit Allowed IPs' page.	
WebCfg - Services: Captive Portal: Edit MAC Addresses	Allow access to the 'Services: Captive Portal: Edit MAC Addresses' page.	
WebCfg - Services: Captive Portal: Edit Zones	Allow access to the 'Services: Captive Portal: Edit Zones' page.	
WebCfg - Services: Captive Portal: File Manager	Allow access to the 'Services: Captive Portal: File Manager' page.	
WebCfg - Services: Captive Portal: Mac Addresses	Allow access to the 'Services: Captive Portal: Mac Addresses' page.	
WebCfg - Status: Captive Portal	Allow access to the 'Status: Captive Portal' page.	
WebCfg - Status: Captive Portal Voucher Rolls	Allow access to the 'Status: Captive Portal Voucher Rolls' page.	
WebCfg - Status: Captive Portal Vouchers	Allow access to the 'Status: Captive Portal Vouchers' page.	
WebCfg - Status: Captive Portal: Expire Vouchers	Allow access to the 'Status: Captive Portal: Expire Vouchers' page.	
WebCfg - Status: Captive Portal: Test Vouchers	Allow access to the 'Status: Captive Portal: Test Vouchers' page.	
WebCfg - System: User Manager: Add Privileges	Allow access to the 'System: User Manager: Add Privileges' page. (admin privilege)	
WebCfg - All pages	Allow access to all pages (admin privilege)	
Security notice: Users in this group effectively have administrator-level access		

Après on vas dans authentication servers puis on configure le LDAP sur PFSsense.

Pour récupérer le distinguished name pour la base DN, l'ou et l'utilisateurs il

suffit d'afficher les details puis on regarde les paramètres dans éditeurs d'attributs.

LDAP Server Settings

Hostname or IP address

192.168.0.250

NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.

Port value

389

Transport

Standard TCP

Peer Certificate Authority

CA Techvista

This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.

Protocol version

3

Server Timeout

25

Timeout for LDAP operations (seconds)

Search scope

Level

Entire Subtree

Base DN

DC=techvista,DC=lan

Authentication containers

OU=VPN,DC=techvista,DC=lan

Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component.
Example: CN=Users,DC=example,DC=com or OU=Staff,OU=Freelancers

Select a container

Extended query

☐ Enable extended query

Bind anonymous

☐ Use anonymous binds to resolve distinguished names

Bind credentials

CN=alexis penet,OU=VPN,DC=techvista,DC=lan

User naming attribute

samAccountName

Group naming attribute

cn

Group member attribute

memberOf

RFC 2307 Groups

☐ LDAP Server uses RFC 2307 style group membership

RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

Group Object Class

posixGroup

Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

Shell Authentication Group DN

If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login.
Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com

UTF8 Encode

☐ UTF8 encode LDAP parameters before sending them to the server.

Required to support international characters, but may not be supported by every LDAP server.

Username Alterations

☐ Do not strip away parts of the username after the @ symbol

e.g. user@host becomes user when unchecked.

Allow unauthenticated bind

☐ Allow unauthenticated bind

Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers allow this type of bind without any possibility to disable it.

Network Connections

Ensuite on tente une connexion on va dans diagnostics → Authentification puis on fais le test.

User alexis authenticated successfully. This user is a member of groups:

- Pfsense AD

Authentication Test

Authentication Server

LDAP Active Directory

Select the authentication server to test against.

Username

alexis

Password

.....

Debug

☐ Set debug flag

Sets the debug flag when performing authentication, which may trigger additional d



On voit que c'est fonctionnel on peut donc se connecter avec un utilisateur de l'AD sur Pfsense.

Installation Crowdsec

Crowdsec sert à bloquer les adresses IP malveillantes, notamment à l'origine d'attaques brute force, de scans de port et de recherche de vulnérabilités web (HTTP).

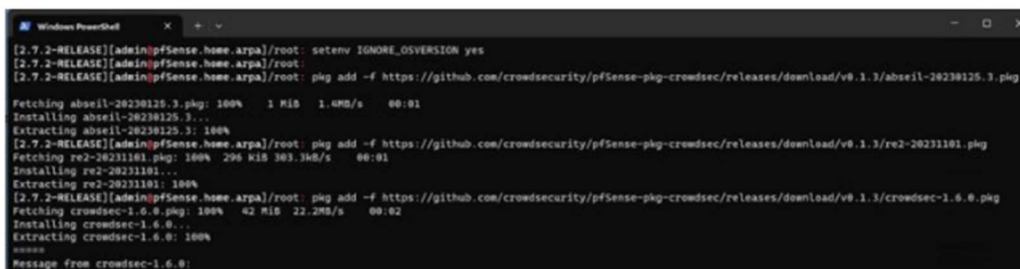
Nous allons voir comment le mettre en place.

Dans la console, saisissez cette commande :

```
setenv IGNORE_OSVERSION yes
```

Puis exécutez les commandes suivantes pour télécharger et installer les paquets :

```
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
```



```
Windows PowerShell
[2.7.2-RELEASE][admin@pfSense.home.arpa]:root: setenv IGNORE_OSVERSION yes
[2.7.2-RELEASE][admin@pfSense.home.arpa]:root: pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/abseil-20230125.3.pkg
[2.7.2-RELEASE][admin@pfSense.home.arpa]:root: Fetching abseil-20230125.3.pkg: 100% 1 MiB 1.4MB/s 00:01
Installing abseil-20230125.3...
Extracting abseil-20230125.3: 100%
[2.7.2-RELEASE][admin@pfSense.home.arpa]:root: pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/re2-20231101.pkg
[2.7.2-RELEASE][admin@pfSense.home.arpa]:root: Fetching re2-20231101.pkg: 100% 296 KiB 383.3KB/s 00:01
Installing re2-20231101...
Extracting re2-20231101: 100%
[2.7.2-RELEASE][admin@pfSense.home.arpa]:root: pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/crowdsec-1.6.0.pkg
[2.7.2-RELEASE][admin@pfSense.home.arpa]:root: Fetching crowdsec-1.6.0.pkg: 100% 42 MiB 22.2MB/s 00:02
Installing crowdsec-1.6.0...
Extracting crowdsec-1.6.0: 100%
Message from crowdsec-1.6.0:
```

L'installation de CrowdSec est effectuée à l'emplacement suivant :

```
/usr/local/etc/crowdsec/
```

Par la suite, si vous avez besoin de redémarrer CrowdSec, utilisez cette commande (adaptez également pour l'arrêter / le démarrer) :

```
service crowdsec.sh restart
```

Une fois faits-nous allons dans service → Crowdsec.

On coche toutes les cases ci-dessous pour que crowdsec soit actif est opérationnel.

Documentation

IMPORTANT It is recommended that you [read the documentation](#) before taking any action.

Remediation component (firewall bouncer)

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.

Local API

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, k8s

If disabled, use a remote LAPI on an external machine.

LAPI host

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

Port number for the LAPI endpoint. Change in case of conflict with other services.

CrowdSec rules settings

 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 ☒

Direction

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) (log) quick on (interfaces) inet from crowdsec_blacklists to any label "CrowdSec IPv4" tag (tag)

Enable CrowdSec IPv6 blocklist rule ☒ block drop (direction) (log) quick on (interfaces) inet6 from crowdsec6_blacklists to any label "CrowdSec IPv6" tag (tag)

 Save

CrowdSec rules settings

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

☒

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} {log} quick on {interfaces} inet from crowdsec_blacklists to any label "CrowdSec IPv4" tag {tag}

Enable CrowdSec IPv6 blocklist rule

☒ block drop {direction} {log} quick on {interfaces} inet6 from crowdsec6_blacklists to any label "CrowdSec IPv6" tag {tag}

Saving settings, please wait..

Cette fois le crowdsec est opérationnel est fonctionnel.

Attaque NMAP

NMAP (Network Mapper), il s'agit d'un des outils de découverte qui permet de fournir des informations sur les services et les systèmes d'exploitation qu'ils exécutent.

Nous allons voir comment le mettre en place.

On prend un Kali linux est on se mets sur le réseau WAN du PFSENSE.

On tape la commande “sudo nmap 172.16.255.51 -Sv -v -Pn”, ça permet de récupérer les ports.

```
(root@kali)-[~]
# sudo nmap 172.16.255.51 -sV -v -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-04 10:10 CEST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 10:10
Scanning 172.16.255.51 [1 port]
Completed ARP Ping Scan at 10:10, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:10
Completed Parallel DNS resolution of 1 host. at 10:10, 0.01s elapsed
Initiating SYN Stealth Scan at 10:10
Scanning 172.16.255.51 [1000 ports]
Discovered open port 53/tcp on 172.16.255.51
Discovered open port 80/tcp on 172.16.255.51
Discovered open port 443/tcp on 172.16.255.51
Completed SYN Stealth Scan at 10:10, 4.97s elapsed (1000 total ports)
Initiating Service scan at 10:10
Scanning 3 services on 172.16.255.51
Completed Service scan at 10:10, 12.04s elapsed (3 services on 1 host)
NSE: Script scanning 172.16.255.51.
Initiating NSE at 10:10
Completed NSE at 10:10, 0.02s elapsed
Initiating NSE at 10:10
Completed NSE at 10:10, 0.02s elapsed
Nmap scan report for 172.16.255.51
Host is up (0.00050s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  dnsmasq 2.89
80/tcp    open  http    nginx
443/tcp   open  ssl/http nginx
MAC Address: 00:0C:29:A9:A5:46 (VMware)

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.34 seconds
Raw packets sent: 2000 (87.984KB) | Rcvd: 6 (248B)

(root@kali)-[~]
#
```

Nous voyons que la commande est bien passé, maintenant nous devons voir si crowdsec à ban l'ip du Kali.

Pour ça nous allons dans → Status → Crowdsec Status.

MachinesBouncersAlertsDecisionsHub

Note: the decisions coming from the CAPI (signals collected by the CrowdSec users) do not appear here. To show them, use `csccli decisions list -a` in a shell.

Last refresh: a few seconds ago

Q

Search

↺

50

≡

	Scope:Value	Reason	Country	AS	Events	Expiration
	Ip:172.16.255.45	crowdsecurity/http-bad-user-agent			2	4 hours

Nous pouvons voir qu'à la suite de la commande le firewall a ban l'adresse ip du Kali linux.

Crowdsec est donc fonctionnel pour cette attaque.

Conclusion

Pour conclure, j'ai réalisé cette mission sous Vmare contenant Un pfsense avec WAN,LAN,DMZ, 1 Windows server (AD), 2 Windows 11, un Serveur Linux.
Ce réseau répondra au mieux aux besoins de l'entreprise TechVista.

L'entreprise d'un nouveau Pare-Feu sécurisé en HTTPS.
Des règles ont été fait pour sécuriser un maximum les différents réseaux, Squid est Crowdsec ont été installé , Une connexion LDAP a été configurés ainsi qu'un tunnel OPENVPN avec accès LAN et DMZ.

Ce nouveau site répondra aux mieux au besoin du réseau et à sa disponibilité.