BTS SERVICES INFORMATIQUES AUX ORGANISATIONS SESSION 2025

<u>Épreuve E5 - Administration des systèmes et des</u> <u>réseaux (Option SISR)</u>

Projet 2 : Mise en place d'une infrastructure <u>réseau avancée</u>

Contexte :

Nous souhaitons renforcer la sécurité et la résilience de l'infrastructure réseau de l'étude Moreau & Associés en intégrant une solution de redondance Active Directory et DNS, un VPN pour les accès distants, un système de détection/prévention d'intrusions (IDS/IPS), un serveur de messagerie ainsi que des stratégies de groupe avancées pour la protection des postes clients.

Objectifs du projet :

- Assurer la haute disponibilité des services grâce à un contrôleur de domaine secondaire en cas de panne du principal.
- Proposer une solution VPN sécurisée pour permettre aux employés d'accéder aux ressources à distance.
- Surveiller les intrusions via un système IPS avec Snort et une analyse Complémentaire avec Wireshark.
- Mettre en place un serveur de sauvegarde performant
- Proposer un mail dédié a l'étude notarial

L'infrastructure ainsi que les outils déployés

Redondance Active Directory et DNS

- Mise en place d'un contrôleur de domaine principal sous Windows Server 2019.
- Déploiement d'un serveur secondaire assurant la redondance d'Active Directory et du DNS.
- Réplication automatique des objets Active Directory et des enregistrements DNS pour garantir une continuité de service en cas de panne.

VPN sécurisé avec OpenVPN

- Mise en place de OpenVPN pour sécuriser les connexions distantes des collaborateurs.
- Authentification via les comptes Active Directory pour garantir un accès sécurisé aux ressources internes.
- Chiffrement des communications pour empêcher toute interception des données.

Surveillance réseau avec Snort, et Wireshark

- **Snort** : Déploiement d'un système de détection d'intrusion (IDS) et de prévention (IPS) pour analyser le trafic réseau et bloquer les menaces en temps réel.
- Wireshark : Utilisé pour l'analyse détaillée du trafic et le diagnostic des incidents réseau.

Stockage et partage de fichiers avec un NAS

- Mise en place d'un serveur de stockage NAS pour centraliser les données.
- Configuration des droits d'accès basés sur les groupes Active Directory.
- Sauvegarde automatique des fichiers critiques avec une solution de réplication en réseau.

Messagerie d'entreprise avec Zimbra

- Mise en place de Zimbra comme solution de messagerie collaborative.
- Création d'un **webmail interne accessible via un navigateur**, adapté aux besoins des collaborateurs.
- Configuration des certificats et du chiffrement SSL/TLS pour garantir la confidentialité des échanges.

Table des matières

- 1. Infrastructure réseau
- 1.1. Redondance Active Directory et DNS
 - 1.1.1. Serveur principal sous Windows Server 2019
 - 1.1.2. Serveur de secours pour la continuité de service
- 1.2. VPN sécurisé avec OpenVPN
 - 1.3.1. Authentification et gestion des accès distants
 - 1.3.2. Chiffrement et sécurité des connexions
- 2. Surveillance et sécurité du réseau
- 2.1. Système de détection d'intrusion (IDS/IPS)
 - 2.1.1. Déploiement de Snort pour l'analyse du trafic
- 2.2. Analyse du trafic avec Wireshark
 - 2.2.1. Surveillance des échanges réseau
 - 2.2.2. Détection et diagnostic des anomalies
- 3. Stockage et partage des données
- 3.1. Infrastructure NAS
 - 3.1.1 Configuration nas via TrueNAS

- 3.1.2. Sauvegarde automatique et réplication des fichiers via bucket AWS
- 4. Messagerie d'entreprise
 - 4.1. Déploiement d'un webmail interne avec Zimbra
 - 4.2. Intégration aux comptes Active Directory
 - 4.3. Sécurisation des échanges et accès externes

Conclusion

Cette infrastructure offre une solution robuste et sécurisée pour TechNovalis. La redondance de l'Active Directory assure une continuité de service en cas de panne d'un serveur. Le VPN permet un accès distant sécurisé pour les employés, tandis que l'IPS et l'analyse réseau renforcent la détection des menaces. Enfin, la messagerie interne Zimbra et l'application des GPO garantissent une gestion optimisée des postes utilisateurs.

Avec ces solutions, TechNovalis dispose d'une infrastructure résiliente et adaptée aux besoins actuels en matière de sécurité et de connectivité.

1. Infrastructure réseau

1.1. Redondance Active Directory et DNS

Pour mettre en place la redondance, nous commençons par déployer une seconde machine virtuelle sous Windows Server afin d'assurer la continuité de service.

Nous installons Windows Server sur une nouvelle machine virtuelle afin d'assurer la redondance de notre infrastructure. Cette étape consiste à copier les fichiers nécessaires et préparer l'installation avant d'ajouter les rôles et fonctionnalités requis pour l'intégration du serveur dans notre domaine existant.



Nous configurons l'adresse IP statique de notre serveur de secours afin d'assurer sa disponibilité sur le réseau. L'adresse 192.168.2.6 est attribuée à la machine, avec comme DNS principal le contrôleur de domaine principal (192.168.2.4).



Nous intégrons le serveur de secours SRVBACKUP au domaine technovalis.local.

BERRADA Ilyes		
		1
Modification du nom ou du domaine de l'ordinateur	tance	
Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.	r votre	r les propriétés de connexion
Nom de l'ordinateur : SRVBACKUP	S" ou	les réseaux disponibles
Nom complet de l'ordinateur : SRVBACKUP		fier vos paramètres réseau
Autres Membre d'un (Domaine :	di <u>f</u> ier	lodifier les options d'adaptateur fichez les cartes réseau et modifiez les par
technovalis.local	Modification	du nom ou du domaine de l'ordinateur 🛛 🗙
O Groupe de travail : WORKGROUP	İ Bie	nvenue dans le domaine technovalis.local.
OK Annuler		ОК
OK Annuler	Appliquer	vos propriétés réseau
	Pare-fe	u Windows

On redémarre la VM

Arrêt des services

Nous installons les rôles AD DS et DNS sur le serveur backup pour assurer la redondance du domaine.



Nous configurons notre nouveau serveur en tant que contrôleur de domaine supplémentaire dans la forêt existante du domaine principal technovalis.local. Cette étape permet d'assurer la redondance d'Active

Directory et du DNS, garantissant ainsi une continuité de service en cas de défaillance du serveur principal.

Assistant Configuration des se	rvices de domaine Active Directory	- 🗆 X]
Configuration de	déploiement	SERVEUR CIBLE WIN-OM09ODE5AHR	🚡 Sélectionner un domaine dans la forêt 🛛 — 🗌 🗙
Configuration de déploie Options du contrôleur de Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Sélectionner l'opération de déploiement Ajouter un contrôleur de domaine à un domaine existant Ajouter un nouveau domaine à une forêt existante Ajouter une nouvelle forêt Spécifiez les informations de domaine pour cette opération Domaine : technovalis.local Fournir les informations d'identification pour effectuer cette opération WIN-OM09ODE5AHR\administrateur	Sélectionner Modifier	Sélectionnez un domaine dans la forêt où le nouveau contrôleur de domaine résidera. technovalis.local OK Annuler 1 OK Facilité de gestion

Nous avons effectué la vérification de la configuration requise avant l'installation d'Active Directory sur notre serveur secondaire. Toutes les vérifications ont été validées avec succès, nous pouvons maintenant lancer l'installation sans problème.

Vérification de la	SERVEUR CIBLE
Toutes les vérifications de l	a configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer l'installation. Afficher plus 🗴
Configuration de déploie Options du contrôleur de Options DNS	La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur Réexécuter la vérification de la configuration requise
Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Pésuitats	Voir les résultats Voir les résultats Les contrôleurs de domaine Windows Server 2019 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 40 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles loss de l'établissement de tessions sur canal accurise. Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (http://go.microsoft.com//winkl/TLinkld=104751). I est impossible de créer une délégation pour ce serveur DNS car la zone paremé faisant autorité est introvable ou elle méxecure para se serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez manauléement créer une délégation pour ce serveur DNS dans la care paremet pour ce terme refolution de nome in technovails.cola ». Sinon, aucune action n'est requise.
	Verification de la configuration requise terminée Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer l'installation.

Nous pouvons à présent redémarrer le second serveur.



Le serveur SRVBACKUP a été intégré en tant que contrôleur de domaine secondaire dans Active Directory, assurant la redondance et la continuité des services d'authentification en cas de défaillance du contrôleur principal SRV22-BTS.

Utilisateurs et ordinateurs Active I	Directory				
Fichier Action Affichage ?					
← 🔶 🖄 📰 📋 🖼 🖬	è 🛛 🖬 🐍	🐮 🛅 🍸 🗾 🕯	8		
Utilisateurs et ordinateurs Active	Nom	Туре	Type de contrô	Site	Description
> interpretes enregistrees	🔝 SRV22-BTS	Ordinateur	GC	Default-First-Si	
Builtin	NRVBACKUP	Ordinateur	GC	Default-First-Si	
> 🧮 Computers					
Domain Controllers					
> PoreignSecurityPrincipal:					
> Managed Service Accour					
> 📓 Tehnovalis users Etude N					
> 🚞 Users					

Nous avons configuré le serveur DNS sur SRVBACKUP, où nous retrouvons les enregistrements des hôtes et des services du domaine technovalis.local. Les enregistrements SOA (Start of Authority) et NS (Name Server) confirment que ce serveur est bien un serveur DNS secondaire, assurant la redondance avec SRV22-BTS.

	Nom	Туре	Données	Horodateur
 DNS SRVBACKUP Zones de recherche direc msdcs.technovalis.lc Tones de recherche inver Points d'approbation Redirecteurs conditionne 	Nom	Type Source de nom (SOA) Serveur de noms (NS) Serveur de noms (NS) Hôte (A) Hôte (A)	Données [535], srvbackup.technova srvbackup.technovalis.local. srv22-bts.technovalis.local. 192.168.2.4 192.168.2.6 192.5 5.0	Horodateur statique statique 13/03/2025 23:00:00 14/03/2025 08:00:00
	Collaborateur2	Hôte (A)	192.168.2.51	27/11/2024 09:00:00
	DESKTOP-C2GOORM	Hôte (A)	192.168.2.51	21/11/2024 01:00:00
	PFSENSE	Alias (CNAME)	routeur.technovalis.local.	statique
	routeur	Hôte (A)	192.168.2.1	statique
	SERVEUR	Hôte (A)	192.168.2.4	statique
	Srv	Alias (CNAME)	srv22-bts.technovalis.local.	statique
	srv22-bts	Hôte (A)	192.168.2.4	statique
	SRV_BACKUP	Hôte (A)	192.168.2.6	14/03/2025 06:00:00
	srvbackup	Hôte (A)	192.168.2.6	statique

Nous avons effectué une résolution de nom avec NSLOOKUP en interrogeant SRVBACKUP (192.168.2.6). Celui-ci renvoie bien les adresses IP des deux contrôleurs de domaine (SRV22-BTS et SRVBACKUP), confirmant ainsi que la redondance DNS est opérationnelle.

```
C:\Users\Administrateur.TECHNOVALIS>nslookup technovalis.local 192.168.2.6
Serveur : SRVBACKUP.technovalis.local
Address: 192.168.2.6
Nom : technovalis.local
Addresses: 192.168.2.4
192.168.2.6
```

Nous allons ensuite passer à la configuration d'openVPN pour les clients de l'étude

1.2. VPN sécurisé avec OpenVPN

Nous avons installé le package openvpn-client-export sur pfSense. Ce package nous permet d'exporter facilement des configurations OpenVPN préconfigurées pour les clients.

In	stalled Packa	iges				
	Name	Category	Version	escription		Actions
~	openvpn- client-export	security	1.9.2	exports pre-configured OpenVPN Client configurations directly fro	m pfSense software.	ina 1
				Package Dependencies: Ø openvpn-client-export-2.6.7 Ø openvpn-2.6.8_1 Ø zip-3	.0_1 🕜 7-zip-23.01	•
	Services 🗸	VPN 🗸	Status	Diagnosti		
_	_	IPsec				
		L2TP				
		OpenVPN	I			
	ئ 🗢 🔍		vetgate	ervices And		
			C	tract type C C		

Nous accédons à l'interface de configuration d'OpenVPN sur pfSense via **VPN > OpenVPN > Servers**. À cette étape, aucun serveur VPN n'est encore configuré.

Servers	Clients	Client Specific Overrides	Wizards	Client Export		
OpenVPI	N Servers					

Nous configurons le serveur OpenVPN en mode Remote Access (SSL/TLS), permettant aux clients de se connecter de manière sécurisée. Nous définissons l'interface d'écoute sur WAN et utilisons le port standard 1194/UDP. Une clé TLS est activée pour renforcer la sécurité du tunnel VPN

Servers	Clients	Client Specific Overrides Wizards Client Export
General In	formation	
	Description	OpenVPN Remote Access 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.
Uni	ique VPN ID	Server 1 (ovpns1)
Mode Con	figuration	
S	erver mode	Remote Access (SSL/TLS)
D	evice mode	tun - Layer 3 Tunnel Mode *un' 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 (Configurat	ion
	Protocol	UDP on IPv4 only
	Interface	WAN The Interface or Virtual IP address where OperVPN will receive client connections.
	Local port	1194 The port used by OpenVPN to receive client connections.
Cryptogra	phic Settir	ngs
TLS Co	onfiguration	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>	# # 2848 bit OpenVPN static key # # # # # # # # # # # # # # # # # # #

Nous mettons en place les paramètres de sécurisation du tunnel OpenVPN en activant l'authentification TLS et en utilisant un certificat serveur OpenVPN-CA. L'algorithme de chiffrement choisi est AES-256-GCM, et nous appliquons un échange de clés Diffie-Hellman en 2048 bits pour garantir un niveau de sécurité optimal.

TLS Key Usage Mode	TLS Authentication	*
	In Authentication mode the TLS key is used only as HMAC a Encryption and Authentication mode also encrypts control of	uthentication for the control channel, protecting the peers from unauthorized connections. 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 value: Both may be set to omit the direction, in which case the TLS	s on the client and server. For example, if the server is set to 0, the client must be set to 1. 3 Key will be used bidirectionally.
eer Certificate Authority	OpenVPN-CA	v
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created	d here: System > Cert. Manager
OCSP Check	Check client certificates with OCSP	
Server certificate	OpenVPN-Server (Server: Yes, CA: OpenVPN-CA, In Use)	~
	Certificates known to be incompatible with use for OpenVPI digest algorithms.	N are not included in this list, such as certificates using incompatible ECDSA curves or we
DH Parameter Length	2048 bit	v
	Diffie-Hellman (DH) parameter set used for key exchange.	0
ECDH Curve	Use Default	~
	The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default whe	n 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-CFBB (128 bit key, 128 bit block) AES-129-CFB (128 bit key, 128 bit block) AES-129-CFC (128 bit key, 128 bit block) AES-129-CFC (129 bit key, 128 bit block) AES-129-CFC (192 bit key, 128 bit block)	CHACHA20-POLY1305 AES-256-0CM
	Available Data Encryption Algorithms Click to add or remove an algorithm from the list The order of the selected Data Encryption Algorithms is res	Allowed Data Encryption Algorithms. Click an algorithm name to remov it from the list pected by OpenVPN. This list is ignored in Shared Key mode.
allback Data Encryption	AES-256_CBC (256 hit key 128 hit block)	
Algorithm	The Fallback Data Encryption Algorithm used for data chan negotiation (e.g. Shared Key). This algorithm is automatical	
Auth digest algorithm	SHA256 (256-bit)	v
	The algorithm used to authenticate data channel packets a	ind control channel packets if a TLS Key is present

Nous configurons le réseau du tunnel VPN en attribuant une plage d'adresses IP privée 10.0.2.0/24 pour la communication entre le serveur et les clients OpenVPN. Nous activons également l'option de redirection de la passerelle IPv4, afin que tout le trafic des clients passe par le tunnel sécurisé. Le nombre maximal de connexions simultanées est défini à 10.

Tunnel Settings	
IPv4 Tunnel Network	10.0.2.0/24
	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::/f64). 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.
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/PREFX 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 VPM (e.g. HTP). 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.

Nous configurons les paramètres avancés des clients OpenVPN pour assurer une connectivité fluide et sécurisée. Nous définissons la topologie du VPN en mode subnet, attribuant une adresse IP distincte à chaque client connecté. Pour améliorer la stabilité, nous utilisons le mode de ping keepalive avec un intervalle de 10 secondes et un timeout de 60 secondes afin de détecter les connexions inactives.

Nous configurons également le serveur DNS interne (192.168.2.4) pour que les clients du VPN puissent résoudre les noms internes du domaine.

Dynamic IP	Allow connected clients to retain their connections if their IP address changes.
Topology	Subnet One IP address per client in a common subnet
	Specifies are inertical used to supply a mixed adapter in adapter adapter with a suppression of the suppression of the suppression of the suppression of the superson of the s
Ping settings	
Inactive	300
	Causes Open/VPN 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 giored 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-restart = timeout*2 pung-ing = interval push ping-interval push ping-restart = timeout
Interval	10
Timeout	60
Advanced Client Sett	ings
DNS Default Domain	Provide a default domain name to clients
DNS Server enable	Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	192.168.2.4
DNS Server 2	
DNS Server 3	
DNS Server 4	
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 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.
DNS Server 4 Block Outside DNS Force DNS cache update	 Make Windows 10 Clients Block 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. 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.
DNS Server 4 Block Outside DNS Force DNS cache update NTP Server enable	Make Windows 10 Clients Block 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. 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. Provide an NTP server list to clients

On sauvegarde, et le serveur vpn est configuré.

OpenVP	N Servers				
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.0.2.0/24	Mode: Remote Access (SSL/TLS) Data Ciphers: CHACHA20-POLY1305, AES-256-GCM, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	OpenVPN Remote Access	d 🗋 🧳

Nous créons une Autorité de Certification OpenVPN qui servira à signer les certificats nécessaires à l'authentification des clients et du serveur.

a								
Search					_	2		
Search term	nter a search string or "nix regular express	sion to search certificate names	Both ~	Q Search	llear			
Certificate Authorities								
Name Internal	Issuer Certificates	Distinguished Name		In Use	Actions			
		Valid From: Fri, 08 Nov 2024 03 Valid Until: Mon, 06 Nov 2034 0	1:13:48 +0100 13:13:48 +0100					
					+	bbA		
/ 5-1: - 0.								
ate / Edit CA								
Descriptive name	OpenVPN-CA							
	The name of this entry as	s displayed in the GUI	for reference.					
	This name can contain s	paces but it cannot co	ontain any of the fo	llowing chara	cters: ?, >, <, &, /			
Method	Import an existing Cert	ificate Authority		~				
Trust Store			na System Trust St	tore				
Thus otore	Add this Certificate A	uthority to the Operati				d booth and a second second		
Thus otore	Add this Certificate A When enabled, the content	nts of the CA will be a	dded to the trust st	tore so that th	ey will be truste	ed by the operating	system.	
Randomize Serial	Add this Certificate Av When enabled, the conte Use random serial num	nts of the CA will be a mbers when signing c	dded to the trust st ertificates	tore so that th	ey will be truste	ed by the operating	system.	
Randomize Serial	Add this Certificate Ad When enabled, the conter Use random serial num When enabled, if this CA	mbers when signing c	dded to the trust st ertificates certificates then se	tore so that th	for certificates	ed by the operating signed by this CA w	system. /ill be automatically rai	ndomized and
Randomize Serial	Add this Certificate Ar When enabled, the conter Use random serial nur When enabled, if this CA checked for uniqueness i	mbers when signing c is capable of signing the signing	dded to the trust st ertificates certificates then se equential value fror	tore so that th erial numbers m Next Certifi	for certificates a cate Serial.	ed by the operating signed by this CA w	system. vill be automatically rai	ndomized and
Randomize Serial	Add this Certificate A When enabled, the conte Use random serial nu When enabled, if this CA checked for uniqueness i Authority	nts of the CA will be a mbers when signing c is capable of signing instead of using the s	dded to the trust st ertificates certificates then se equential value fror	tore so that th erial numbers m Next Certifi	for certificates cate Serial.	ed by the operating signed by this CA w	system. vill be automatically rai	ndomized and
Randomize Serial	Add this Certificate A When enabled, the conte Use random serial nu When enabled, if this CA checked for uniqueness i Authority	nts of the CA will be a mbers when signing c is capable of signing instead of using the s	dded to the trust si ertificates certificates then se equential value fror	tore so that th erial numbers m Next Certifi	for certificates (cate Serial.	ed by the operating signed by this CA w	system. /ill be automatically rai	ndomized and
Randomize Serial sting Certificate a	Add this Certificate A When enabled, the conter Use random serial nur When enabled, if this CA checked for uniqueness in Authority BEGIN CERTIFIC	unonly to the Operation ints of the CA will be a mbers when signing c is capable of signing instead of using the se	dded to the trust st ertificates certificates then se equential value fror	tore so that th erial numbers m Next Certifi	ey will be truste for certificates : cate Serial.	ed by the operating	system. /ill be automatically rai	ndomized and
Randomize Serial sting Certificate a	Add this Certificate A When enabled, the conte Use random serial nu When enabled, if this CA checked for uniqueness i Authority BEGIN CERTIFIC MIIOyTCCArGgAWIBAGI EEMAGGAUE	unonly to the Operation ints of the CA will be a mbers when signing c is capable of signing instead of using the signing ATE IFYG4gsjVBIYWDQYJJ	dded to the trust st ertificates certificates then se equential value fror coZIhvcNAQELBQAN	tore so that the erial numbers m Next Certifi	for certificates a cate Serial.	ed by the operating	system. vill be automatically rai	ndomized and
Randomize Serial	Add this Certificate A When enabled, the conte Use random serial nu When enabled, if this CA checked for uniqueness i Authority BEGIN CERTIFIC MIIDyTCCArGgAwIBAgI EPMA@GAIUE AXM6V1B0LUNBMQSwCQYI	unonly to the Operation ints of the CA will be a mbers when signing c is capable of signing instead of using the signing ATE IFYG4gsjVBIYWDQYJJ DVQQGEWJGUJESMBAG/	dded to the trust st ertificates certificates then se equential value fror coZIhvcNAQELBQAN	erial numbers m Next Certifi	for certificates : cate Serial.	ed by the operating	system.	ndomized and
Randomize Serial	Add this Certificate A When enabled, the conter Use random serial nut When enabled, if this CA checked for uniqueness i Authority BEGIN CERTIFIC MIIDyTCCArGgAWIBAGI EPMA@GAIUE AXM6V1B0LUNBMQSwCQYI 11MRQwEgYD	unony to the Operation nts of the CA will be a mbers when signing c is capable of signing instead of using the signing ATE IFYG4gsjVBIYWDQYJI DVQQGEwJGUJESMBAG/	dded to the trust st ertificates certificates then se equential value fror cozIhvcNAQELBQAN	tore so that the erial numbers m Next Certifi wSD	for certificates : cate Serial.	ed by the operating	system.	ndomized and
Randomize Serial sting Certificate a	Add this Certificate A When enabled, the conter Use random serial nur When enabled, if this CA checked for uniqueness i Authority BEGIN CERTIFIC MIDOYTCCArGgAwIBAGI EPMAGGAUE AXMGVIBOLUNBMQSwCQY 11MRQwEgYD Paste a certificate in X.50	unony to the Operation nts of the CA will be a mbers when signing c is capable of signing instead of using the signing ATE IFYG4gsjVBIYWDQYJI DVQQGEWJGUJESMBAG D9 PEM format here.	dded to the trust st ertificates certificates then se equential value fror COZINYCNAQELBQAI	tore so that the erial numbers m Next Certifi wSD	ey will be truste for certificates : cate Serial.	ed by the operating	system.	ndomized and
Randomize Serial sting Certificate a Certificate data	Add this Certificate A When enabled, the conter Use random serial nur When enabled, if this CA checked for uniqueness in Authority BEGIN CERTIFIC MIDyTCCArGgAwIBAgI EPMAGGAIUE AXMGVIBOLUNBMQSwCQYI 11MRQWEgYD Paste a certificate in X.50 BEGIN PRIVATE	unonty to the Operation ints of the CA will be a mbers when signing c is capable of signing instead of using the se ATE IFYG4gsjVBIYWDQYJJ DVQQGEWJGUJESMBAG/ D9 PEM format here. KEY	dded to the trust st ertificates certificates then se equential value fror COZINVCNAQELBQAN	tore so that the erial numbers m Next Certifi wSD	ey will be truste for certificates : cate Serial.	ed by the operating	system.	ndomized and
Randomize Serial sting Certificate a Certificate data ertificate Private Key (optional)	Add this Certificate A When enabled, the conter Use random serial nur When enabled, if this CA checked for uniqueness i Authority BEGIN CERTIFIC MIIOYTCCArGgAwIBAgI EPMA0GAIUE AXMGVIB0LUNBMQSwCQY 11MRQwEgYD Paste a certificate in X.50 BEGIN PRIVATE MIIE vQIBADANBgkqhki	unony to the Operation ints of the CA will be a mbers when signing c is capable of signing instead of using the signing ATE IFYG4gsjVBIYWDQYJI DVQQGEWJGUJESMBAG D9 PEM format here. KEY G9WBBAQEFAASCBKcW	dded to the trust si ertificates certificates then se equential value fror coZIhvcNAQELBQAi AlUECBMJT2NjaXRI	erial numbers m Next Certifi wSD	ey will be truste for certificates : cate Serial.	ed by the operating	system.	ndomized and
Randomize Serial sting Certificate ata <u>Certificate data</u> rtificate Private Key (optional)	Add this Certificate A When enabled, the conter Use random serial nur When enabled, if this CA checked for uniqueness in Authority BEGIN CERTIFIC MIIDyTCCArGgAwIBAgI EPMA0GAIUE AXMGVIB0LUNBMQSwCQYI 11MRQWEgYD Paste a certificate in X.500 BEGIN PRIVATE MIIEvQIBADANBgkqhkin X/i0ph/Hh0	unony to the Operation nts of the CA will be a mbers when signing c is capable of signing instead of using the su ATE IFYG4gsjVBIYWDQYJH DVQQGEWJGUJESMBAG/ D9 PEM format here. KEY G9wBBAQEFAASCBKcwg	dded to the trust si ertificates certificates then se equential value fror coZIhvcNAQELBQAi AlUECBMJT2NJaXRI	erial numbers m Next Certifi wSD 0 hbm v	ey will be truste for certificates : cate Serial.	ed by the operating signed by this CA w	system.	ndomized and
Randomize Serial sting Certificate A Certificate data rtificate Private Key (optional)	Add this Certificate A When enabled, the conte Use random serial nut When enabled, if this CA checked for uniqueness i Authority BEGIN CERTIFIC MIIDyTCArGgAwIBAgI EPMA@GAUE AXMGVIBOLUNBMQSwCQYI 11MRQwEgYD Paste a certificate in X.50 BEGIN PRIVATE MIIEvQIBADANBgkqhki X/i@ph/Hh@ 1wxtL1PH46IgneGzeY2 51ut-2020	unonty to the operation of the CA will be a mbers when signing c is capable of signing instead of using the signing c is capable of signing instead of using the signing c is capable of signing the signification of the sis the signification of the signification of the signification	dded to the trust st ertificates certificates then se equential value fror coZIhvcNAQELBQAI ALUECBMJT2NJaXRI ggSJAgEAA0IBAQCS tcq1+pB8093uK/yG	tore so that the erial numbers m Next Certifi wSD bbm v pp7 c cos	ey will be truste for certificates : cate Serial.	ed by the operating signed by this CA w	system.	ndomized and
Randomize Serial sting Certificate ata <u>Certificate data</u> rtificate Private Key (optional)	Add this Certificate A When enabled, the conter Use random serial nur When enabled, if this CA checked for uniqueness i Authority BEGIN CERTIFIC MIIOyTCCArGgAwIBAgI EPMA0GAIUE AXMGVIB0LUNBMQSwCQY 11MRQwEgYD Paste a certificate in X.50 BEGIN PRIVATE MIIEvQIBADANBgkqhkii X/iaph/Hhb 1wtL1PH46IgneGzeYZ' FjU+t2PaQP Paste the private key for:	unony to the Operation ints of the CA will be a mbers when signing c is capable of signing instead of using the signing ATE IFYG4gsjVBIYWDQYJI DVQQGEWJGUJESMBAG D9 PEM format here. KEY G9W0BAQEFAASCBKCWI YdPA2X4QLJ1uqGRq+1 the above certificate h	dded to the trust si ertificates certificates then se equential value fror cozIhvcNAQELBQAi AlUECBMJT2NJaXRI ggSJAgEAAOIBAQCS tcq1+pB8093uK/yd ere. This is option	tore so that the erial numbers m Next Certifi wSD 0 hbm v 9p7 0 603 v al in most cast	ey will be truste for certificates i cate Serial.	ed by the operating signed by this CA w	ystem. vill be automatically rai	indomized and
Randomize Serial sting Certificate a Certificate data rtificate Private Key (optional)	Add this Certificate Ai When enabled, the conter Use random serial nui When enabled, if this CA checked for uniqueness i Authority BEGIN CERTIFIC MIIDyTCCArGgAwIBAgI EPMA06AIUE AXMGVIBOLUNBMQswCQYI llMRQwEgYD Paste a certificate in X.50 BEGIN PRIVATE MIIEVQIBADANBgknkii X/iaph/Hh0 lwxtL1PH46IgneGzeYz FJU+t2PaQP Paste the private key for	unony to the Operation ints of the CA will be a mbers when signing c is capable of signing instead of using the signing ATE IFYG4gsjVBIYWDQYJJ DVQQGEWJGUJESMBAG D9 PEM format here. KEY G9w0BAQEFAASCBKCwg YdPA2X4QLJ1uqGRq+1 the above certificate h	dded to the trust si ertificates certificates then se equential value fror coZIhvCNAQELBQAI AUUECBMJT2NjaXRI ggSjAgEAAOIBAQCS tcql+pB8093uK/yc here. This is option	srial numbers m Next Certifi wSD 0 hbm v 9p7 0 603 v al in most cas	es, but is requir	ed by the operating signed by this CA w	ystem. vill be automatically rai	ndomized and
Randomize Serial sting Certificate ata Certificate data rtificate Private Key (optional)	Add this Certificate A When enabled, the conter Use random serial nui When enabled, if this CA checked for uniqueness i checked for uniqueness i Checked for uniqueness i EMAGANUE CHECKERSENCERTIFICE MIDVTCCAFGGAWIBAGI EPMA@GANUE AXMGVIBOLUNBMQSwCQYI 11MRQWEgYD Paste a certificate in X.50 CHECKERSENCERTIFICE MIIEVQIBADANBGkhki X/iaph/HhB 1wxtL1PH46IgneGzeYz FJU+t2PaQP Paste the private key for 3	unony to the Operation ints of the CA will be a mbers when signing c is capable of signing instead of using the se ATE IFYG4gsjVBIYWDQYJJ DVQQGEWJGUJESMBAG D9 PEM format here. KEY G9W0BAQEFAASCBKCwy YdPA2X4QLJ1uqGRq+1 the above certificate h	dded to the trust si ertificates certificates then se equential value fror cozIhvcNAQELBQAN AUUECBMJT2NJaXRI 2gSJAgEAAOIBAQCS tcql+pB8093uK/yd here. This is option.	srial numbers m Next Certifi wSD 0 hbm 7 9p7 0 603 7 al in most cas	for certificates i cate Serial.	ed by the operating signed by this CA w	ystem. vill be automatically rai	indomized and
Randomize Serial sting Certificate A Certificate data rtificate Private Key (optional)	Add this Certificate A When enabled, the conte Use random serial nui When enabled, if this CA checked for uniqueness i Authority BEGIN CERTIFIC MIIDYTCARGAWIBAgI EFMA@GAIUE AXMGV1BOLUNBMQSwCQYI 11MRQwEgYD Paste a certificate in X.50 BEGIN PRIVATE MIIEVQIBADANBgkqhki X/iaph/Hab 1wxtL1PH46IgneGzeY2 FJU+t2PaQP Paste the private key for: 3 Enter a decimal number t Serial is checked.	unony to the Operation ints of the CA will be a mbers when signing c is capable of signing instead of using the signing ATE DVQQGEwJGUJESMBAG/ D9 PEM format here. KEY G9w0BAQEFAASCBKcwl YdPA2X4QLJ1uqGRq+1 the above certificate h to be used as a seque	dded to the trust si ertificates certificates then se equential value fror cozIhvcNAQELBQAA ALUECBMJT2NJAXRA gg5JAgEAAOIBAQCS tcq1+pB8093uK/yo here. This is option ntial serial number	tore so that the erial numbers m Next Certifi wSD 0 hbm 9 p7 0 6 03 2 2 al in most cas for the next of	es, but is requir ertificate to be a	ed by the operating signed by this CA w ed when generating signed by this CA. 1	ystem. vill be automatically rai	ndomized and

Notre Autorité de Certification OpenVPN a été générée et auto-signée. Elle est valide jusqu'en 2035 et servira à authentifier les connexions VPN en signant les certificats des serveurs et des clients

Nous avons généré un certificat serveur OpenVPN, signé par notre Autorité de Certification.

OpenVPN-Server (OpenVPN-CA	ST=Occitanie, L=Montpellier, CN=vpn-server, C=FR	0	OpenVPN Server	∥‡₽ ≣C
Server Certificate CA: No Server: Yes		Valid From: Sun, 02 Feb 2025 20:31:15 +0100 Valid Until: Wed, 31 Jan 2035 20:31:15 +0100			

Nous avons généré un certificat utilisateur pour vpnuser1, signé par notre Autorité de Certification

vpnuser1	OpenVPN-CA	ST=Occitanie, L=Montpellier, CN=vpnuser1, C=FR	0	⇙兼ᄵबᢗ面
User Certificate CA: No Server: No		Valid From: Sun, 02 Feb 2025 20:54:47 +0100 Valid Until: Wed, 31 Jan 2035 20:54:47 +0100		

Nous allons exporter le fichier de configuration OpenVPN (.ovpn) pour l'utilisateur vpnuser1. Ce fichier contient toutes les informations nécessaires pour établir une connexion sécurisée au serveur VPN.

lser	Certificate Name	Export
Certificate (SSL/TLS, no Auth)	vpnuser1	- Inline Configurations:
		📩 Most Clients 🛛 📩 Android 🔂 OpenVPN Connect (iOS/Android)
		- Bundled Configurations:
		📩 Archive 🛛 📩 Config File Only
		- Current Windows Installer (2.6.7-Ix001):
		📩 64-bit 🛃 32-bit
		- Previous Windows Installer (2.5.9-Ix601):
		📩 64-bit 🛃 32-bit
		- Legacy Windows Installers (2.4.12-Ix601):
		📩 10/2016/2019 📩 7/8/8.1/2012r2
		- Viscosity (Mac OS X and Windows):
		📩 Viscosity Bundle 🛛 📩 Viscosity Inline Config
		- Yealink SIP Handsets:
		📩 T28 🛃 T38G (1) 🛃 T38G (2) / V83
		- Snom SIP Handsets:
		snom

On installe ensuite openVPN sur un poste client pour y intégrer le fichier de configuration précédemment téléchargé.

UPLOAD FILE Type Server Address or Cloud ID	<u></u> Ge	t connected	
⑦ What's my URL?	Type Server Address o	UPLOAD FIL	E
	What's my UPI		7
			C.

On importe le profile vpnuser1



Nous avons importé le fichier de configuration OpenVPN sur le client. Une fois le profil vpnuser1 chargé dans OpenVPN Connect, nous avons initié la connexion au serveur VPN. L'état CONNECTED ainsi que les statistiques de trafic confirment que l'utilisateur est bien connecté et que la communication chiffrée est active.

2. Surveillance et sécurité du réseau

2.1. Système de détection d'intrusion (IDS/IPS)

- 2.1.1. Déploiement de Snort pour l'analyse du trafic

Nous avons installé Snort sur pfSense avec succès. Cette installation nous permet de mettre en place un système de détection et de prévention d'intrusion (IDS/IPS) afin d'analyser le trafic réseau et de détecter d'éventuelles menaces.

Installed Packages Ava	allable Packages Package Installer		
Package Installation			
Please note that, by defa default snaplen of 15158 Stream5 target-based reas your card supports it.	ault, snort will truncate packets larger than the bytes. Additionally, LRO may cause issues with ssembly. It is recommended to disable LRO, if	•	
This can be done by apper	nding '-lro' to your ifconfig_ line in rc.conf.		
Message from pfSense-pkg	-snort-4.1.6_17:		
 Please visit Services - S Global tab. Afterwards vi >>> Cleaning up cache Success	Snort - Interfaces tab first to add an interface, then select your desired rules packages at the Services - Snort - isit the Updates tab to download your configured rulesets. done.		
✓ snort securit	4.1.6_17 Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the b protocol, and anomaly-based inspection.	enefits of signature	, 面口 i
	Package Dependencies: Ø snort-2.9.20_8		
General Settings			
Enable	Enable interface		
Interface	WAN (em0)		
	Choose the interface where this Snort instance will inspect traffic.		
Description	Block IP wan		
	Enter a meaningful description here for your reference.		
Snap Length	1518		
	Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.		

Nous avons activé Snort sur l'interface WAN (em0) et configuré l'envoi d'alertes dans le journal système du pare-feu. Les paquets générant une alerte seront automatiquement capturés et stockés dans un fichier pour analyse.

Enable	Enable interface
Interface	WAN (em0)
	Choose the interface where this Snort instance will inspect traffic.
Description	Block IP wan
	Enter a meaningful description here for your reference.
Snap Length	1518
	Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.
Alert Settings	
Send Alerts to System Log	Snort will send Alerts to the firewall's system log. Default is Not Checked.
System Log Facility	LOG_AUTH
	Select system log Facility to use for reporting. Default is LOG_AUTH.
System Log Priority	LOG_ALERT
	Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.
Enable Packet Captures	Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Packet Capture File Size	128
	Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_em046856 is rotated and a new file opened.
Enable Unified2 Logging	Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.
	Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Nous avons activé le mode **IPS en "Legacy Mode"**, permettant à **Snort** d'inspecter les paquets et de bloquer automatiquement les adresses IP malveillantes. Nous avons également activé la suppression des sessions associées aux IP bloquées pour une meilleure réactivité.

Block Settings	
Block Offenders	Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode	Legacy Mode
	Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.
Kill States	Checking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block	BOTH Select which IP extracted from the packet you wish to block. Default is BOTH.
Detection Performan	ce Settings
Search Method	AC-BNFA Choose a fast pattern matcher algorithm. Default is AC-BNFA.
Split ANY-ANY	Enable splitting of ANY-ANY port group. Default is Not Checked.
Search Optimize	Enable search optimization. Default is Not Checked.
Stream Inserts	Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.
Checksum Check Disable	Disable checksum checking within Snort to improve performance. Default is Not Checked.

Nous avons mis à jour les règles de détection de Snort, incluant des signatures provenant de plusieurs sources telles que Snort Subscriber Ruleset, Emerging Threats Open Rules et Feodo Tracker Botnet C2 IP Rules. Ces mises à jour permettent d'améliorer la détection des menaces en temps réel et d'optimiser la protection du réseau.

Installed Rule Set MD5 Signature							
Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date					
Snort Subscriber Ruleset	ef356004644a1f6df8a52573776ef0e4	Thursday, 13-Mar-25 23:01:02 CET					
Snort GPLv2 Community Rules	b0c300c5610bb3793c46cdd7655916b5	Thursday, 13-Mar-25 23:01:02 CET					
Emerging Threats Open Rules	4c24342a857178cd120dd16e009a6af0	Saturday, 15-Mar-25 23:00:10 CET					
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Wednesday, 19-Feb-25 14:07:03 CET					
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Wednesday, 19-Feb-25 14:07:03 CET					
Feodo Tracker Botnet C2 IP Rules	b61779a7fa2b715e88b0cc4e4ab4d326	Saturday, 15-Mar-25 23:21:06 CET					

Nous configurons la mise à jour automatique des règles de Snort afin de garantir une protection continue contre les menaces. L'intervalle est fixé à 24 heures avec une mise à jour programmée à 23h00.

Rules Update Setting	S
Update Interval	□ DAY Please select the interval for rule updates. Choosing NEVER disables auto-updates.
Update Start Time	23:00 Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of
Hide Deprecated Rules Categories	simultaneous requests.
Disable SSL Peer Verification	Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

Nous accédons à l'onglet des alertes de Snort pour surveiller les événements détectés sur l'interface WAN (em0). Nous activons l'actualisation automatique pour afficher en temps réel les alertes générées. Cette interface nous permettra de télécharger ou de purger les journaux d'alerte selon les besoins.

Services / Snort / Alerts								0	
Snort Interfaces G	lobal Settings	Updates	Alerts Bloc	ked Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
Alert Log View Set	tings								
Interface to Inspect	t WAN (em Choose inte	0) 🗸	Auto-refresh	view 250 Alert	lines to display.	B Sa	ve		
Alert Log Actions	Downlos	ad <u> </u> Clear							
Alert Log View Filt	er								÷
0 Entries in Active	Log								
Date Action	Pri Pro	oto Class	Source IP	SPort	Destination I	P DI	Port GIE	D:SID De	scription

Snort est maintenant configuré avec toutes les règles nécessaires à la surveillance.

2.2. Analyse du trafic avec Wireshark

Nous téléchargeons la dernière version stable de Wireshark (4.4.5) pour l'installer sur notre machine d'analyse réseau.



Nous avons installé avec succès Wireshark 4.4.5 sur notre machine, prêt à capturer et analyser le trafic réseau.



Nous lançons Wireshark et accédons à l'interface principale, où nous pouvons sélectionner une interface réseau pour commencer la capture des paquets.

🚄 L'analyseur de réseau Wireshark	
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outil	s Aide
◢ ■ ∅ ◎ 📙 🗈 🕱 🖬 ९ ⇔ 🕾 🖗 🖢 🧮 🗮 🤤 ९ ९ ९ 🦉 🔠	
Appliquer un filtre d'affichage < Ctrl-/>	
Bienvenue dans Wireshark	
Cantura	
Capture	
en utilisant ce filtre : 📙 Entrer un filtre de capture	
Ethernet	
Adapter for loopback traffic capture	
Connexion au réseau local* 9	
Connexion au réseau local* 8	
Connexion au réseau local* 7	
Event Tracing for Windows (ETW) reader	

Nous lançons une capture de trafic sur l'interface Ethernet avec Wireshark. Nous observons les paquets échangés, incluant des requêtes DNS, des connexions TCP, ainsi qu'un message ICMP

4.0					
<u>a</u> 0	pture en cours de Eth	iernet			- U X
Fichi	er Editer Vue A	Iller Capture Analyser	Statistiques Telephoni	e Wireless C	Jutils Aide
	l 🔬 💿 📃 🛅	🖹 🛱 🔍 🗢 🖻 🖺	🗿 👲 📃 📃 🔍 ሮ	L Q. 🎹 🗄	
A	opliquer un filtre d'aff	ichage <ctrl-></ctrl->			🖘 v +
No.	Time	Source	Destination	Protocol	Lengtl Info
_	1 0.000000	192.168.2.50	192.168.2.4	DNS	78 Standard query 0xd9a6 A edge.microsoft.com
	2 0.000192	192.168.2.4	192.168.2.1	DNS	101 Standard query 0x7aee A edge-domain.trafficmanager.net OPT
	3 0.000417	192.168.2.50	192.168.2.4	DNS	78 Standard query 0xf7d4 HTTPS edge.microsoft.com
	4 0.000520	192.168.2.4	192.168.2.1	DNS	101 Standard query 0x4bfa HTTPS edge-domain.trafficmanager.net OPT
	5 0.020439	192.168.2.1	192.168.2.4	DNS	198 Standard query response 0x7aee A edge-domain.trafficmanager.net CNAME edge-microsoft-com.ax-0002.ax-msedge.net CNAME a
L.	6 0.020578	192.168.2.4	192.168.2.50	DNS	219 Standard query response 0xd9a6 A edge.microsoft.com CNAME edge-domain.trafficmanager.net CNAME edge-microsoft-com.ax-0
	7 0.038526	192.168.2.1	192.168.2.4	DNS	226 Standard query response 0x4bfa HTTPS edge-domain.trafficmanager.net CNAME edge-microsoft-com.ax-0002.ax-msedge.net CNA-
	8 0.038732	192.168.2.4	192.168.2.1	DNS	92 Standard query 0xdb3c HTTPS ax-0002.ax-msedge.net OPT
	9 0.039171	192.168.2.1	192.168.2.4	DNS	152 Standard query response 0xdb3c HTTPS ax-0002.ax-msedge.net SOA ns1.ax-msedge.net OPT
	10 0.039249	192.168.2.4	192.168.2.50	DNS	187 Standard query response 0xf7d4 HTTPS edge.microsoft.com CNAME edge-domain.trafficmanager.net CNAME edge-microsoft.com
	11 0.039450	192.168.2.50	192.168.2.4	ICMP	215 Destination unreachable (Port unreachable)
	12 2.242052	192.168.2.50	192.168.2.4	TCP	60 50714 → 135 [FIN, ACK] Seg=1 Ack=1 Win=8211 Len=0
	13 2.242087	192.168.2.4	192.168.2.50	TCP	54 135 → 50714 [ACK] Seq=1 Ack=2 Win=8211 Len=0
	14 2.242163	192.168.2.4	192.168.2.50	TCP	54 135 → 50714 [FIN, ACK] Seq=1 Ack=2 Win=8211 Len=0
	15 2.242188	192.168.2.50	192.168.2.4	TCP	60 50715 → 49667 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
	16 2.242200	192.168.2.4	192.168.2.50	TCP	54 49667 → 50715 [ACK] Seq=1 Ack=2 Win=8209 Len=0
	17 2.242241	192.168.2.4	192.168.2.50	TCP	54 49667 → 50715 [FIN, ACK] Seq=1 Ack=2 Win=8209 Len=0
	18 2.242370	192.168.2.50	192.168.2.4	TCP	60 50714 → 135 [ACK] Seq=2 Ack=2 Win=8211 Len=0
	19 2.242539	192.168.2.50	192.168.2.4	TCP	60 50715 → 49667 [ACK] Seq=2 Ack=2 Win=1024 Len=0
> Fr > E1 > Ir > U: > Do	ame 1: 78 bytes chernet II, Src: sternet Protocol ser Datagram Prot omain Name System	on wire (624 bits), : PCSSystemtec_3a:5b:11 Version 4, Src: 192. cocol, Src Port: 6534: a (query)	78 bytes captured (6 8 (08:00:27:3a:5b:18 168.2.50, Dst: 192.1 1, Dst Port: 53	24 bits) on :), Dst: PCS5 68.2.4	interface \Device\NPF_[14D] 0000 08 00 27 21 bd c1 08 00 27 3a 5b 18 08 00 45 00't't[t] ystemtec_21:bd:c1 (08:0012 0010 00 40 ff 3f 00 00 81 1b 56 c5 ca 80 23 22 cd s8 0; 0020 02 04 ff 3d 00 35 00 2c dd f3 d3 m6 01 00 00 01

Nous avons capturé et analysé le trafic réseau en temps réel avec Wireshark, cet outil permet d'identifier d'éventuels problèmes de communication et d'analyser les flux réseau en détail.

3.1. Infrastructure NAS

- 4.1.1 Configuration nas via TrueNAS

Nous commençons tout d'abord par monter une vm NAS en utilisant pour ce faire TrueNAS

Général
Nom : Projet BTS blanc VM TrueNas Système d'exploitation : FreeBSD (64-bit)
🚺 System
Mémoire vive : 8192 Mo Processeurs : 4 Ordre d'amorçage : Disquette, Optique, Disque dur Accélération : Pagination imbriquée
Affichage
5tockage
Contrôleur : IDE Maître primaire IDE : Projet BTS blanc VM TrueNas.vdi (Normal, 8,00 Gio) IDE Primary Device 1: Projet BTS blanc VM TrueNas_1.vdi (Normal, 30,00 Gio)
խ Audio
Pilote hôte : Par défaut Contrôleur : ICH AC97
🗗 Réseau
Interface 1: Intel PRO/1000 MT Desktop (Réseau interne, 'intnet')
🤌 USB
Contrôleur USB : OHCI, EHCI Filtres de périphérique : 0 (0 actif)
Dossiers partagés
Aucun
Description

Nous avons démarré l'ISO de TrueNAS sur notre machine virtuelle. L'écran d'installation s'affiche et on sélectionne "Install/Upgrade".

TrueNAS 13.0-U6.7 Console Setup
1 [Install/Upgrade 2 Shell 3 Reboot System 4 Shutdown System
Cancel>

Nous sélectionnons le disque sur lequel TrueNAS sera installé. Nous avons choisi le disque ada0 (8 GiB) afin de réserver le second disque ada1 (30 GiB) pour le stockage des données.

Select one installed for instal	or more drives (use arrow keys llation; select a	where TrueNAS should be to navigate to the drive(drive with the spacebar)	(s)).
	[*] ada0 VBOX H [] ada1 VBOX H	ARDDISK 8.0 GiB ARDDISK 30.0 GiB]
	< <mark>0</mark> K >	<cancel></cancel>	

Nous avons sélectionné le mode de démarrage de TrueNAS. Nous avons choisi Boot via BIOS, ce qui est recommandé pour les infrastructures d'entreprise et les environnements legacy. L'option UEFI aurait été préférable pour un matériel plus récent.

TrueNAS can be booted in either BIOS or UEFI mode.	
BIOS mode is recommended for legacy and enterprise hardware, whereas UEFI may be required for newer consumer motherboards.	
<pre></pre>]

L'installation de **TrueNAS** s'est terminée avec succès. On redémarre la VM et on enlève l'ISO d'installation.

The TrueNAS installation on ada0 succeeded! Please reboot and remove the installation media.

TrueNAS est bien installé et nous avons accès au menu de configuration. L'interface web est disponible à l'adresse 192.168.2.63 fournit grâce au DHCP.

FreeBSD/amd64 (truenas.local) (ttyv0)
Console setup
 Configure Network Interfaces Configure Link Aggregation Configure VLAN Interface Configure Default Route Configure Static Routes Configure DNS Reset Root Password Reset Configuration to Defaults Shell Reboot Shut Down
The web user interface is at:
http://192.168.2.63 https://192.168.2.63
Enter an option from 1-11:

Nous arrivons sur la page de connexion de TrueNAS. Nous allons nous connecter avec l'utilisateur root et le mot de passe défini lors de l'installation.

Norm d'utilisateur * ▲	
Mot de passe *	
TrueNAS CORE ® © 2025 🌾 systems	

TrueNAS () systems ≡ < 🕸 单 😫 🎕 ባ TrueNAS CORE® © 2025 - iXsystems, I root truenas.local System Information TrueNAS Dashboard Overview Accounts Platform: Generic **__** System Version: TrueNAS-13.0-U6.7 📩 Tasks stName: truenas.local X Network Uptime: 4 minutes as of 18:58 Storage CHECK FOR UPDATES Directory Services • Sharing CPU ıĿ 글는 Services Plugins

Nous sommes maintenant sur le tableau de bord de TrueNAS.

Nous sommes dans la section Pools du stockage. Nous allons créer un nouveau pool pour utiliser notre disque dur disponible.

	truenas.local				
8	Dashboard	Create or import pool	Decrypt pool	Gelect pool to import	🕢 Confirm Options
#	Accounts				
▫	System	Create a pool: Create new pool 			
		O Import an existing pool ③			
x	Network				
≡		CANCEL CREATE POOL			
	VMware-Snapshots				
	Import Disk				

Nous avons sélectionné notre disque de 30 Go (ada1) pour créer un pool de stockage en mode Stripe.

Name* Disk 1 ⑦	Encryption						
RESET LAYOUT SUGGEST L	LAYOUT ⑦ ADD VD						
Avai	ilable Disks			Data VDe	evs		
🗌 Disk	Type Capacity		~	Disk	Туре	Capacity	
		→ ←	~	ada1	UNKNOW	30 GiB	
0 selected / 0 total			1 selected	/ 1 total			
Filter disks by name	Filter disks by capacity		Stripe Estimated raw	r capacity: 28 GiB Ø			▼ X
Estimated total raw data capacity: 2	28 GiB						
✓ Force							
CREATE							

Notre pool Disk 1 est maintenant créé et opérationnel.

Pools									
Disk 1 (System Dataset Pool) ONLINE 🌍 6.85 MB (0%) Used 26.63 GB Free								\$ ^	
Name ©	Туре Ф	Used 🕈	Available 🌻	Compression @	Compression Ratio	Readonly 🕈	Dedup 🕈	Comments 🗢	
Disk 1	FILESYSTEM	6.86 MiB	26.63 GiB			false			

Le service SMB est maintenant activé et configuré pour démarrer automatiquement au boot. Cela nous permettra de partager des fichiers sur le réseau en utilisant le protocole Samba.

Filter Service Q, smb			
Name	Running	Start Automatically	Actions
SMB	••		1

Nous avons créé un partage réseau SMB nommé Étude, pointant vers le disque Disk 1. Ce partage est activé et utilisera les paramètres par défaut.

Basic			
Path* /mnt/Disk 1		Ø	
▼ ■ /mnt		¥	
Disk 1			
Name Etude			0
- Purpose Default share parameters	- @ De	escription	
			_~
Access		Other Options	
Inable ACL 🕜		Use as Home Share 🕜	
Export Read Only 🕜		Time Machine	
✓ Browsable to Network Clients ⊘		Enable Shadow Copies 🕢	
✓ Allow Guest Access ⑦		Export Recycle Bin 🕜	
Access Based Share Enumeration 🧭		Use Apple-style Character Encoding 🕜	
Hosts Allow	0	Enable Alternate Data Streams 🔞	
Hosts Domy	ര	Enable SMB2/3 Durable Handles 🕜	
nosis Deny		Enable FSRVP 🕜	
			0
		Auxiliary Parameters	
			<i>"</i> @
SUBMIT CANCEL BASIC OPTIONS			

Nous avons configuré les permissions du dataset **Rédacteurs**, en attribuant tous les droits (lecture, écriture, exécution) aux utilisateurs, groupes et autres.

Dataset Path						
Path /mnt/Disk 1/Redacteurs						
Owner		Access				
User root	• @	Access I	Node)		
			Read	Write	Execute	
		User		\checkmark		
wheel	• 🔊	Group				
Apply Group (?)		Other				
Advanced						
Apply Permissions Recursively 🕥						
Traverse ⊘						
SAVE CANCEL USE ACL	MANAGER					

Nous avons ajouté le dataset Rédacteurs au pool Disk 1, permettant d'organiser le stockage en sousvolumes distincts. Ce dataset hérite de la compression lz4 et est opérationnel.



Maintenant que tout est en place, les collaborateurs pourront accéder au stockage via l'explorateur de fichier en tapant \\192.168.2.63

- 3.1.2. Sauvegarde automatique et réplication des fichiers via bucket AWS

Maintenant nous accédons à Cloud Credentials pour configurer notre sauvegarde sur AWS

	•	
General		
NTP Servers		
Boot		
Advanced		
Email		
System Dataset		
Reporting		
Alert Services		
Alert Settings		
Cloud Credentials		

Nous avons ajouté nos identifiants AWS dans la section Cloud Credentials de TrueNAS. Cela nous permettra de configurer la sauvegarde vers Amazon S3.

Name and Provider Name* Nas AWS Backup		Authentication Access Key ID *		0
Provider * Amazon S3	•0	Secret Access Key *	& 0	
		Maximum Upload Parts		_0
Authentication Advanced Options				
Advanced Settings				
SUBMIT CANCEL VERIFY CREDENTIAL				

Nos identifiants AWS ont été validés avec succès. Nous pouvons maintenant configurer la sauvegarde automatique de notre NAS vers Amazon S3.

1 Valid	
The Credential is valid.	
	CLOSE

Tout d'abord nous allons nous rendre sur la console administrateur AWS et créer un **compartiment S3** nommé **"truenasbackup".**

Ce compartiment servira à stocker les sauvegardes de notre TrueNAS.

Configuration générale	
Région AWS	
Europe (Paris) eu-west-3	
Nom du compartiment Info	
truenasbakcup	
Les noms de compartiment doivent comporter de 3 à 63 caractères et être uniques da et se terminer par une lettre ou un chiffre. Les caractères valides sont les suivants : a-2	ns l'espace de noms global. Les noms des compartiments doivent également commence z, 0-9, points (.) et tirets (-). <u>En savoir plus [7</u>
Copier les paramètres depuis un compartiment existant - facultatif	
Sélectionner un compartiment	
Secure and the share for the	

Nous avons configuré une tâche de synchronisation Cloud Sync pour envoyer (PUSH) les fichiers de /mnt/Disk 1 vers notre compartiment S3 "truenasbackup". La synchronisation se fera quotidiennement à minuit en mode COPY, ce qui garantit que les fichiers du NAS seront copiés sur AWS sans suppression des données existantes. Les sauvegardes s'effectueront tous les soir à minuit.

Transfer		Remote		
Description * Nas AWS Backup	0	Credential* Nas AWS Backup (S3)		• ?
Direction * PUSH	•0	_{Bucket} * truenasbakcup		• @
Transfer Mode * COPY	• ?	Folder		
COPY : Files from the source are <u>copied</u> to the		► /	0	
destination. If files with the same names are pres the destination, they are <u>overwritten</u> .	ent on	-		
Directory/Files* /mrt/Disk 1				
▶ 🛅 Disk 1				
Control				
Schedule* Daily (0 0 * * *) at 00:00 (12:00 AM)	• 🕐			
Fnabled ?				
Advanced Options				
Take Snapshot (?)				
Follow Symlinks (?)				
Pre-script	Po	ist-script		
			?C)
Exclude	0			
Advanced Remote Options				
Server Side Encryption None	<u>*</u> @_	rage Class	• @)
Use -fast-list (?)				
Remote Encryption ⑦				
Transfers	@ Ba	indwidth Limit	0)
SUBMIT CANCEL DRY RUN				

Nous avons effectué un Dry Run pour vérifier la synchronisation des fichiers vers AWS S3. Le test montre qu'un fichier testnas.txt a bien été identifié pour transfert, confirmant que la configuration est correcte.

Dry Run Clou	ıd Sync Task
2025/03/15 19:43	::30 NOTICE:
Transferred:	0 B / 0 B, -, 0 B/s, ETA -
Elapsed time:	4.1s
2025/03/15 19:43	::31 NOTICE:
Transferred:	0 B / 0 B, -, 0 B/s, ETA -
Elapsed time:	5.0s
2025/03/15 19:43	:31 NOTICE: Redacteurs/Piece/testnas.txt: Skipped copy as –dry
2025/03/15 19:43	:31 NOTICE:
Transferred:	9 B / 9 B, 100%, 0 B/s, ETA -
Transferred:	1 / 1, 100%

CLOSE

Elapsed time:

5.2s

Le fichier **testnas.txt** est bien présent dans le compartiment configuré, confirmant que la synchronisation entre **TrueNAS et AWS** fonctionne correctement.

Objets (1)						
C Copier l'URI S	53	Copier l'URL	Télécharger	Ouvrir		
Supprimer Act	ions 🔻	Créer un dossier	↑ Charger			
Les objets sont les entités <u>S3</u> 2 pour obtenir une lis accéder à vos objets, vous	fondamentale te de tous les devez leur acc	es stockées dans Amaz objets de votre compa corder explicitement d	on S3. Vous pouv artiment. Pour que es autorisations. E	ez utiliser l' d'autres p in savoir pl	'inventaire Am ersonnes puis us [2]	sent
□ Nom ▲	Туре		o ▼ Taille	▼	Classe de stockage	⊽
E testnas.txt	txt	16 Mar 202 03:44:38 A CET	25 M	9.0 o	Standard	

5/ Messagerie d'entreprise avec Zimbra

Je possède le nom de domaine moreaunotaires.fr

Ajouter des options à vos noms de domaine	
Ajouter des comptes e-mail liés au domaine Vous pouvez ajouter d'autres comptes e-mail si nécessaire. La pré-installation s'effectue via votre espace client OVHcloud.	Votre sélection Noms de domaine moreaunotaires.fr
moreaunotaires.fr 1 compte e-mail Zimbra Starter inclus	Durée 1 an Renouvellement en mars 2026 pour 7,79 Option DNSSEC (DNS sécurisé) ①

Activation d'un compte Zimbra lié au domaine moreaunotaires.fr via OVH.

Nous allons ajouter un enregistrement DNS CNAME pour valider le domaine moreaunotaires.fr auprès de Zimbra.

Zimbra



Nous avons validé l'installation de la zone DNS du domaine moreaunotaires.fr via OVHcloud.

	alay al				
OVH	Cloud				Suivant →
Bon de co	mmande			(🛱 Version imprimable
luméro :	225026579				Contact de facturation : ILYES BERRADA
ate:	10 mars 2025 21:17:15		3	35 Avenue Frédéric Sabatier	d'Espeyran, Bat B Apt 5
xpiration :	24 mars 2025 23:29:59				34090 MONTPELLIER FR
tat :	En cours de validation				
	INSTALLATION	Domaine	Prix unitaire	Quantité	Prix HT
moreaunotaires	.fr - Zone DNS - Installation	*001	-	1	0,00 PTS
DNS zone		*001	-	1	0,00 PTS
				SOUS-TOTAL	0,00 PTS
	SPÉCIAL		Domaine	Prix unitaire Quant	ité Prix HT
Exécution immé	diate de la commande en renonçant au droit de rétractation			- 1	0,00 PTS
				SOUS-TO	DTAL 0,00 PTS
	ABONNEMENT	Domaine	Prix unitaire	Quantité	Prix HT
moreaunotaires	.fr - Zone DNS - Installation	*001	-	1	0,00 PTS
				SOUS-TOTAL	0,00 PTS
				Total HT	0,00 PTS

Nous utilisons les serveurs DNS d'OVH (dns20.ovh.net et ns20.ovh.net) pour la gestion du domaine moreaunotaires.fr.

Nons de domaine / moreaunotaires.fr / Serveurs DNS										
moreaunotaires.fr O Roadmap & Changelog Actions V										
Informations générales	Zone DNS	Serveurs DNS	Redirection	GLUE	DS Records	Tâches récentes	Gérer les co	intacts		
(i) Pour vous assurer du bon f	onctionnement de vo	tre configuration, vou	ıs pouvez utiliser cet outi	l de vérification D	NS. 🗗			Commander DNS Anycast Modifier les serveurs DNS		
Serveur DNS	IP associ	ée	Statut	Type de	es serveurs DNS					
dns20.ovh.net			Actif	Stand	ard 🕜			Guides		
ns20.ovh.net	-		Actif	Stand	ard 🕜			Serviceurs DNS		
							< >	Serveus Dra		

Nous avons activé la zone DNS du domaine pour une durée de 12 mois, avec validation des conditions d'utilisation.

RRADA Ilyes								
Informations générales	Zone DNS	Serveurs DNS	Redirection	GLUE	DS Records	Tâches récentes	Gérer les contacts	
← Retour à la page précédente								
Activer votre zone	DNS							
Pour répondre aux requêtes DNS souhaitez l'activer, validez les éta	votre nom de doma pes suivantes.	aine doit être relié à une z	one DNS. Vous pourre	z y configurer ver	s quelle adresse IP se	ra redirigé votre domaine et :	ses sous domaines. La zone l	DNS de votre domaine est désactivé. Si
 Choisissez votre du 12 mois : Inclus 	rée							
Activation Afin de confirmer votre	demande, veuillez a	ccepter les conditions d'u	tilisation.					
 J'ai pris connaissar Data_Protection_ CONDITIONS PAR Conditions Gener 	ice et j'accepte les f Agreement 🖄 FICULIERES D'ENRE ales de Services 🖄	termes des contrats suiv	ants : VELLEMENT ET DE TR	ANSFERT DE NO	MS DE DOMAINE 🖉			

Nous avons configuré les enregistrements DNS nécessaires (A, MX, SPF, TXT, CNAME) pour assurer le bon fonctionnement du domaine moreaunotaires.fr avec la messagerie et le site.

Domaine	TTL	Туре	Cible		e
moreaunotaires.fr.	0	NS	dns20.ovh.net.		
moreaunotaires.fr.	0	NS	ns20.ovh.net.		
moreaunotaires.fr.	0	А	213.186.33.5		
www.moreaunotaires.fr.	0	А	213.186.33.5		\odot
ftp.moreaunotaires.fr.	0	CNAME	moreaunotaires.fr.		\bigcirc
moreaunotaires.fr.	0	SPF	v=spf1 include:mx.ovh.com -all		
moreaunotaires.fr.	0	TXT	"1 www.moreaunotaires.fr"		
www.moreaunotaires.fr.	0	TXT	"3 welcome"		
moreaunotaires.fr.	0	MX	1 mx1.mail.ovh.net.		
moreaunotaires.fr.	0	MX	5 mx2.mail.ovh.net.		
« < 1 2 > »				10 V Page 1 / 2	ок

Nous avons associé le domaine moreaunotaires.fr à l'organisation "Étude" et confirmé que le statut du service Zimbra est "READY".

Informations générales Domaine Compte emai				
+ Ajouter un domaine				
Domaine	Organisation	Nombre de comptes	Statut	
moreaunotaires.fr	Etude	1	READY	:

Nous avons créé le compte mail isabelle.moreau@moreaunotaires.fr pour une collaboratrice de l'étude, rattaché à l'organisation "Étude".

Etude Etude X			
← Retour vers mes comptes emails			
Modifier le compte isabelle.moreau@moreaunotaires	.fr		
Paramètres du compte			
Les champs mentionnés avec un astérisque * sont obligatoires.			
Compte email *			
isabelle.moreau	@	moreaunotaires.fr	~
La partie locale de votre adresse (le texte précédant le « © ») doit suivre les lignes directrices suivantes : - Elle doit se terminer par une lettre ou un numéro - Les caractères spéciaux autorisés sont "", "+", "et ", " et ", " - Les caractères spéciaux ne pavvent pas être plaés côte à côte			
O Votre compte fera partie de l'organisation Etude			
Nom		Prénom	
MOREAU		Isabelle	
Nom à afficher			
MOREAU Isabelle			
Mot de passe			
	25		
Votre mot de passe doit contenir au minimum : - 10 caractères - 1 define et L'acaractère spécial (\$,1,8,) - 1 lettre majuncule Enregistrer Annuler			

Le compte de la cliente a bien été créé, en se rendant sur le webmail elle pourra travailler sans soucis de manière sécurisée

zimbra	
Connexion	
Utilisateur	
isabelle.moreau@moreaunotaires.fr	
Mot de passe	
	Afficher
Connexion Mémoriser mes v d'accès	aleurs
Version	
Défaut	~

Je créé aussi un raccourci sur le bureau pour que la cliente se rende sur son mail plus facilement.



Fiche de tests

Nous allons maintenant vérifier si toutes les configurations faites précédemment fonctionnent. Nous procèderons comme ceci :

- 1. Redondance Active Directory et DNS
- 2. VPN Sécurisé avec OpenVPN
- 3. Surveillance et Sécurité du Réseau
- 3.1. Système de Détection d'Intrusion (IDS/IPS)
- 3.2. Analyse du Trafic avec Wireshark
- 4. Stockage et Partage des Données
- 4.1. Infrastructure NAS avec TrueNAS

1. Redondance Active Directory et DNS

En premier lieu nous allons éteindre le serveur principal et voir si le serveur secondaire prend le relais.



Il prend bien le relai, maintenant nous allons tenter la modification des identifiant d'un utilisateur.

Réinitialiser le mot de pass	e	?	×
Nouveau mot de passe :	•••••		
Confirmer le mot de passe :	•••••		
L'utilisateur doit changer session	le mot de passe à la procha	ine ouverture	e de
L'utilisateur doit fermer puis modifications prennent effe État de verrouillage du comp	s ouvrir à nouveau sa sessio st. te sur ce contrôleur de dom	n afin que le aine : Déver	es rouillé
Déverrouiller le compte	de l'utilisateur		
	ОК	Annu	uler

2. VPN Sécurisé avec OpenVPN

Les identifications utilisateur ont bien été modifiés





2. VPN Sécurisé avec OpenVPN

OpenVPN C	onnect – ×
≡	Profiles 🔁
CONNEG	CTED
	OpenVPN Profile 10.0.2.15 [pfSense-UDP4- 1194-vpnuser1-config (7)]
CONNE	CTION STATS
6.2KB/s	
0B/s	
BYTES IN 40 B/S	BYTES OUT 1.14 KB/S
DURATIO 00:00:1	N PACKET RECEIVED 2 1 sec ago
YOU	+

On arrive bien à se connecter à notre server VPN.

3. Système de Détection d'Intrusion (IDS/IPS)

2017-07-22 2 06:15:49	UDP	Potentially Bad Traffic	163.172.17.76 Q ⊞	54465	Q 🕀	5060	140:26 🕀 🗙	(spp_sip) Method is unknown
2017-07-21 2 09:26:30	UDP	Potentially Bad Traffic	163.172.22.169 Q ⊞	52428	Q 🕀	5060	140:26	(spp_sip) Method is unknown
2017-07-21 2 01:03:28	UDP	Potentially Bad Traffic	163.172.17.76 Q ⊞	46834	Q 🕀	5060	140:26 🕀 🗙	(spp_sip) Method is unknown
2017-07-20 2 20:36:37	UDP	Potentially Bad Traffic	163.172.22.169 Q ⊞	54788	Q 🕀	5060	140:26	(spp_sip) Method is unknown

Notre système de détection d'intrusion fonctionne correctement, des alertes commencent à remonter Analyse du Trafic avec Wireshark

ICMP

101 Destination unreachable (Port unreachable)

Je lance wireshark sur l'interface Ethernet puis je tente de faire un ping depuis une autre machine.

La trame icmp du ping remonte bien.

3. Infrastructure NAS avec TrueNAS

Je test sur un poste client l'accès au nas depuis l'explorateur de fichier

On a bien accès au server depuis un poste

L 68 8.190140 192.168.2.50 192.168.2.4



De plus la sauvegarde cloud du serveur de stockage se fait bien comme le montre la console AWS

Objets (1)									
C Copier l'URI S3 Copier l'URL 🛨 Télécharger Ouvrir [2]									
Supprimer Actions Créer un dossier Créer Supprimer									
Les objets sont les entités fondamentales stockées dans Amazon S3. Vous pouvez utiliser l' <u>inventaire Amazon</u> <u>S3</u> 2 pour obtenir une liste de tous les objets de votre compartiment. Pour que d'autres personnes puissent accéder à vos objets, vous devez leur accorder explicitement des autorisations. En savoir plus [2]									
Q Rechercher des objets en fonction du préfixe < 1 > 🔞									
Nom▲Type▼Dernière modificatioTaille▼Classe de stockagen									
□ Lestnas.txt txt 03:44:38 AM 9.0 o Standard CET									

4. Messagerie d'entreprise

La cliente se rendre sus zimbra pour pouvoir s'y connecter

zimpr	a
Connexion	
Utilisateur	
isabelle.moreau@	moreaunotaires.fr
Mot de passe	
•••••	Afficher
Connexion	Mémoriser mes valeurs d'accès
Version	
Défaut	•

Une fois ici on va se connecter et simplement faire un test d'envoi réception vers une adresse gmail, plus précisément la mienne

lest	bolle de l'écepti	ion x
A moi	AU Isabelle	
test	De:	MOREAU Isabelle <isabelle.moreau@moreaunotaires.fr></isabelle.moreau@moreaunotaires.fr>
	à:	"ilyes.berrada" <ilyes.berrada@gmail.com></ilyes.berrada@gmail.com>
	Date:	19 mars 2025 23:13
(Objet:	test
	Envoyé par:	moreaunotaires.fr
	signé par:	moreaunotaires.fr
	sécurité:	Chiffrement standard (TLS) En savoir plus
	>:	Ce message a été classé dans les messages importants par Goog

Nous pouvons voir que l'envoi de mail fonctionne bien.

Ainsi que la réception.

zimbra			Q. Rechercher dans boite aux lettres	- ¢
messagerie				
NOUVEAU E-MAIL	•	Date 🗸	🔶 🦛 🌩 🖀 Archiver 😭 Déplacer 🗸 🥫 Supprimer 🦁 Spam 🚥 Plus 📑	Afficher 🗸 🧴
Boite de réception Brouillons Envoyés	Nyes 2 test test	12:26	 test tiyes «lyes.berrada@gmail.com» 	* 12:26
Spam Corbeille + Ajouter un dossier			À tsabelle moreau test ♠ Répondre ≪ Répondre à tous ♣ Faire suivre ••• Suite	
✓ Mots clés				
Aujourd'hui < >				
+ Ajouter un évènement				ļ