

Début du TP1 : 17/04/2025

Mise en place de GNS3 en client local sur macOS avec l'utilisation du serveur GNS3 du lab via WireGuard.

1. Setup des VPC et réseau :

- Mise en place de 3 VPC avec un switch Ethernet.
- Attribution des adresses IP et test de ping entre les différentes machines pour vérifier la connectivité.

Début du TP2 : 17/04/2025

Lancement du TP2.

1. Installation de pfSense sur GNS3 :

- J'ai fait le premier root avec l'installation de pfSense dans l'émulation de GNS3.
- Installation de VNC Viewer pour avoir un accès graphique.
- Configuration de pfSense avec le DHCP.
- Vérification des IPs attribuées aux VPC et test de ping pour m'assurer que tout fonctionne.

Question : La passerelle est définie à 0.0.0.0. Quelles conséquences cela a-t-il sur la connectivité de cette machine ?

Réponse : La passerelle définie à 0.0.0.0 veut dire que les PC ne savent pas comment atteindre d'autres réseaux. Ils peuvent communiquer entre eux dans le même réseau, mais ils ne peuvent pas accéder à Internet ou à d'autres réseaux externes.

Téléchargement et configuration des systèmes :

1. MicroCore Linux :

- J'ai tenté avec la version V4 clean, mais les commandes ne marchaient pas (beaucoup plus rapide à télécharger, 15 min pour le V6 avec la Wi-Fi).
- J'ai donc pris la version V6, récupéré l'image, préparé le template et vérifié l'IP avec **ip a**. Tout est bien configuré depuis le serveur DHCP.

2. WebTerms :

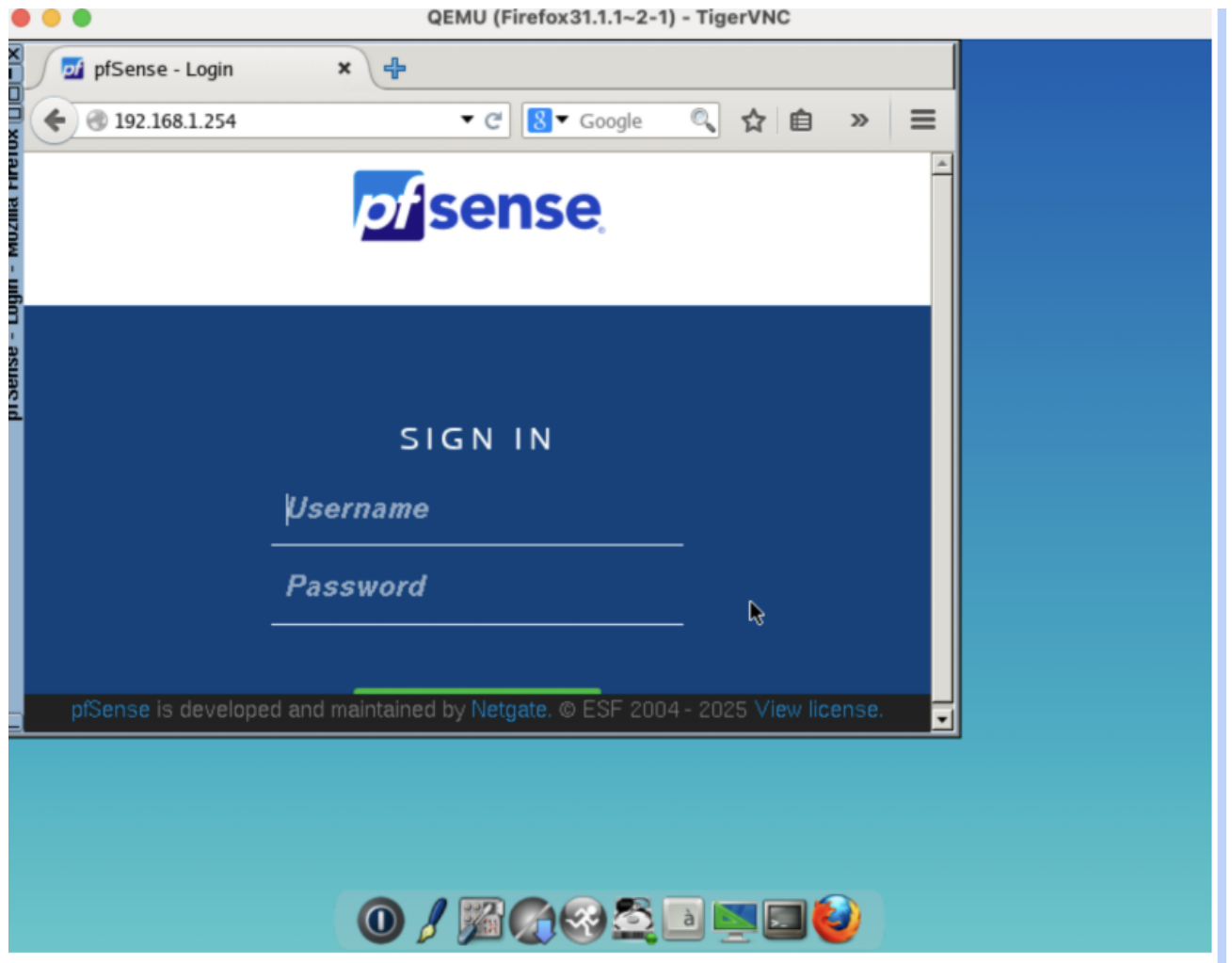
- Tentatives d'ajout de la configuration et de la bonne adresse IP.
- Vérification de la connexion, tout est ok.
- Tentative de connexion à pfSense, mais erreur. J'ai aussi tenté via VNC, mais ça a échoué. Le redémarrage de pfSense a été nécessaire, car j'avais mis la machine en pause pendant la pause déjeuner.

3. Connexion réussie à pfSense via Firefox :

- Une fois l'IP bien configurée, la connexion à pfSense via Firefox s'est bien passée. Test de ping effectué et tout est ok.

4. Setup de FirefoxGuest :

- Cette fois, c'était plus simple grâce au DHCP, connexion à pfSense directement avec l'IP vérifiée.



Gestion de l'administration de pfSense :

1. Changement de mot de passe :

- J'ai changé le mot de passe par défaut sur pfSense.

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

[» Next](#)

2. Lecture des règles de pare-feu :

Firewall / Rules / WAN

Floating WAN LAN

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	×	0/0 B	*	RFC 1918 networks	*	*	*	*	*	Block private networks	
<input checked="" type="checkbox"/>	×	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	Block bogon networks	

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	5/1.54 MiB	*	*	*	LAN Address	80	*	*		Anti-Logout Rule	
<input checked="" type="checkbox"/>	0/152 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

Question : Sur quelle interface se fait l'administration du pare-feu ? **Réponse :** L'administration du pare-feu se fait via l'interface LAN, avec le port 80, comme on peut le voir dans les règles, où ce port est toujours accessible pour ne pas bloquer l'accès à l'interface admin.

Question : Quelles remarques sur la sécurisation de l'accès à l'interface d'administration ? **Réponse :** La sécurité est assez faible car l'interface est en HTTP. Il serait préférable de limiter l'accès à des IPs spécifiques et d'ajouter une authentification multi-facteurs (MFA) pour renforcer la sécurité.

Configuration des règles supplémentaires :

1. Mapping statique de FirefoxGuest :

- Je n'oublie pas de faire un mapping statique pour FirefoxGuest depuis le serveur DHCP.

DHCP Static Mappings				
Static ARP	MAC address	IP address	Hostname	Description
	0c:b4:d1:d4:00:00	192.168.1.3		

2. Application de la configuration :

- Ne pas oublier d'appliquer la configuration sinon ça sert à rien de faire plein de restart ça corrigera pas le problème....

3. Ajout des règles pour limiter l'accès à pfSense :

- J'ai bloqué l'accès à l'adresse LAN pour toutes les personnes qui ne sont pas dans l'alias par 192.168.1.2 et 192.168.1.3.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input type="checkbox"/>	✓ 0/276 KiB	IPv4 *	AdminPc	LAN address	*	*	none		Webterm	<div>Alias details</div> <div><div>Value</div><div>Description</div><div>192.168.1.2</div><div>Webterm</div><div>192.168.1.3</div><div>Firefox</div></div> <div> </div>	
<input type="checkbox"/>	✗ 0/14 KiB	IPv4 *	*	LAN address	*	*	none		Firefox	<div> </div>	
<input type="checkbox"/>	✓ 0/310 KiB	IPv4 *	LAN subnets	*	*	*	none		Default allow LAN to any rule	<div> </div>	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	none		Default allow LAN IPv6 to any rule	<div> </div>	

Add

Add

Delete

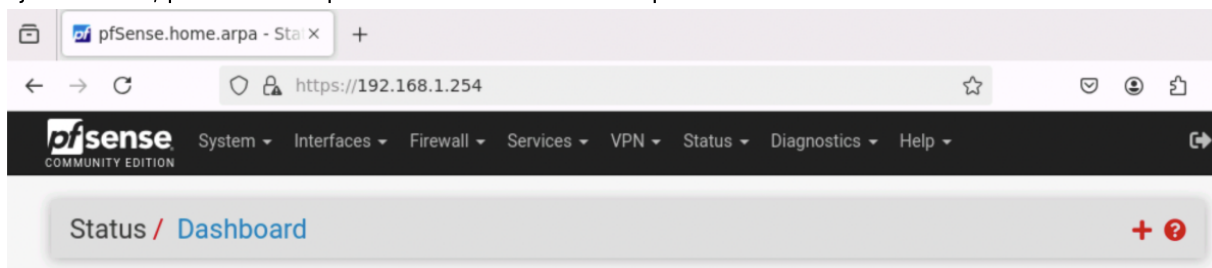
Toggle

Copy

Save

Separator

- Ajout du TLS, puis une exception car le certificat n'était pas reconnu.



4. Règles HTTPS pour plus de sécurité :

- J'ai configuré des règles pour ne permettre l'accès qu'en HTTPS, ce qui renforce la sécurité.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 7/221 KiB	IPv4 TCP	AdminPc	*	LAN address	443 (HTTPS)	*	none			
<input type="checkbox"/>	✗ 0/23 KiB	IPv4 *	*	*	LAN address	*	*	none			
<input type="checkbox"/>	✓ 0/310 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	
<div> Add Add Delete Toggle Copy Save Separator </div>											

Question : Pourquoi le navigateur signale-t-il un risque de sécurité ? **Réponse :** Le navigateur montre un risque car le certificat est auto-signé. Il n'est pas reconnu par les autorités de certification, d'où l'avertissement.

Oublie de la configuration de l'IP : Ajout de l'ip administrateur 192.168.1.1 donc ajouter a l'alias.

Objectifs de sécurité adressés :

- **Sécurisation de l'accès à l'interface pfSense :** J'ai restreint l'accès à l'interface d'administration à seulement les IPs 192.168.1.2 et 192.168.1.3 pour limiter l'accès à des machines connues.
- **Passage de HTTP à HTTPS :** J'ai renforcé la sécurité en passant à HTTPS pour chiffrer les communications.
- **Gestion des certificats SSL :** J'ai ajouté une exception pour le certificat auto-signé pour éviter les erreurs de connexion tout en maintenant une sécurité acceptable.
- **Règles d'accès au pare-feu :** J'ai mis en place des règles pour limiter l'accès à pfSense uniquement aux IPs autorisées.

Voici la reprise de ton texte avec une mise en forme claire, incluant les tableaux et les étapes que tu as mentionnées :

Début du TP3 : 18/04/2025

1. **Ajout de l'interface en mode IP statique** avec l'adresse 192.168.2.254/24.

2. Vérification au niveau du DHCP pour s'assurer qu'il est bien désactivé.

LAN **SRV**

General DHCP Options

DHCP Backend	ISC DHCP
Enable	<input type="checkbox"/> Enable DHCP server on SRV interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries

Connexion SSH au pfSense

Ajout de la règle SSH dans le firewall pour autoriser les accès SSH depuis les PC admin.

 sylvainrougie — webterm2-1 — telnet 192.168.32.104 5011 — 80x24

```
ED25519 key fingerprint is SHA256:2//tT6JnzAyo25QzXd33gFDH1kCBoo4rUL0A1nAiFYw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.254' (ED25519) to the list of known hosts.
(admin@192.168.1.254) Password for admin@pfSense.home.arpa:
QEMU Guest - Netgate Device ID: b17b738917b3d84765f2
```

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

Création de la clé privée/public

Ajout de la clé publique sur l'interface web de pfSense pour le user **admin**. Ensuite, aller dans le système de configuration avancée et sélectionner l'utilisation obligatoire de la clé publique.

```
[/ # cat /root/.ssh/id_ecdsa.pub
ecdsa-sha2-nistp521 AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBAFiezVu
vJtT33eZ1ukRpSk9aYYdgft/gIRrTQlZUcM85YrKnLhgCgFxApxgVfqZ2TfzP+00yJpzOk5PVC3yxS66
1gEFbBvKF09EBktUwahaVMc1yM2+6QXZj3chIPJqdvbG2g8/cs8UhNzPoXwBBmVePH+0Vzcy5TPAhY0Z
4KLD1hEyeg== root@webterm2-1]
```

Secure Shell

Secure Shell Server

☒ Enable Secure Shell

SSHD Key Only

Public Key Only

When set to *Public Key Only*, SSH access requires authorized keys been granted secure shell access. If set to *Require Both Password keys and valid passwords* to gain access. The default *Password o valid authorized key* to login.

```
[/ # ssh admin@192.168.1.254
admin@192.168.1.254: Permission denied (publickey).
[/ # ssh admin@192.168.1.254
QEMU Guest – Netgate Device ID: b17b738917b3d84765f2
```

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

Matrice de test

Voici la matrice de test de connectivité entre les différentes machines :

To/From	Firefox	Webterm	Admin	PC1	PC2	App Server	DB Server	LAN Address	SRV Address
Firefox	-	OK	OK	OK	OK	n.u.	n.u.	t.o.	n.u.
Webterm	OK	-	OK	OK	OK	t.o.	t.o.	t.o.	t.o.
Admin	OK	OK	-	OK	OK	n.u.	n.u.	t.o.	n.u.
PC1	OK	OK	OK	-	OK	n.u.	n.u.	t.o.	n.u.
PC2	OK	OK	OK	OK	-	n.u.	n.u.	t.o.	n.u.
App Server	n.u.	n.u.	n.u.	n.u.	n.u.	-	OK	n.u.	t.o.
DB Server	n.u.	n.u.	n.u.	n.u.	n.u.	OK	-	n.u.	t.o.
FW	OK	OK	OK	OK	OK	OK	OK	OK	OK

Seul le webterm ici peut pinger le serveur de base de données et l'application, parce qu'il a une gateway de setup.

Utilisation de tcpdump

Voici les détails des captures réseau avec leurs interprétations et commentaires associés :

Source	Destination	Traces em1 (o/n)	Traces em2 (o/n)	Interprétation et commentaires
MicroCoreAdmin	Webterm	n	n	Ping OK, aucun flux capturé car le trafic passe uniquement par le switch.
MicroCoreAdmin	fw LAN Address	o	n	Ping OK, flux aller/retour. 09:58:52.713773 IP 192.168.1.1 > 192.168.1.254: ICMP echo request
MicroCoreAdmin	MicroCore-server	n	n	Ping échoué : ping: sendto: Network is unreachable.
Webterm	MicroCore-server	n	n	Ping échoué mais flux capturé.

Source	Destination	Traces em1 (o/n)	Traces em2 (o/n)	Interprétation et commentaires
MicroCore- Server	fw SRV address	n	o	Timeout PING, mais ARP capturé. 10:07:12.783039 ARP, Request who-has 192.168.2.254
fw SRV address	MicroCoreServer	n	o	PING OK. Captures ARP et ICMP, flux aller/retour.

Résolution du problème de ping

Afin de résoudre le problème de l'absence de réponse au ping (capture sans réponse), on va autoriser les pings depuis n'importe où vers pfSense en ajoutant une règle dans le firewall.

L'ajout de la règle permet au protocole ICMP, peu importe sa provenance, de permettre le ping.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B IPv4 ICMP any	*	*	*	*	*	none		Autoriser les pings sortant vers toutes les destinations	

Problème de la passerelle (gateway)

Lors du test de ping entre le LAN et le SRV, le ping ne peut pas s'effectuer car les machines n'ont pas de gateway sur laquelle aller pour après chercher le bon réseau.

Gateway

192.168.1.254

The default is to use the IP address of this firewall interface as the correct gateway for the network. Enter "none" for no gateway

Pour les machines qui ne sont pas sous DHCP (comme celles du sous-réseau SRV), on doit ajouter la passerelle manuellement dans le fichier de démarrage :

```
sudo route add default gw 192.168.2.254
```

Observation

On remarque que ce soit dans le sous réseau SRV ou dans le LAN, on a bien le ping qui passe entre les deux réseaux parce que l'on a bien mis la gateway et qu'il y a la règle dans le firewall pour autoriser le ping.

gns3@box:~\$ ping 192.168.1.103
PING 192.168.1.103 (192.168.1.103): 56 data bytes
64 bytes from 192.168.1.103: seq=0 ttl=63 time=7.185 ms
64 bytes from 192.168.1.103: seq=1 ttl=63 time=6.204 ms
64 bytes from 192.168.1.103: seq=2 ttl=63 time=7.698 ms
64 bytes from 192.168.1.103: seq=3 ttl=63 time=7.698 ms
64 bytes from 192.168.1.103: seq=4 ttl=63 time=8.735 ms
64 bytes from 192.168.1.103: seq=5 ttl=63 time=7.556 ms
64 bytes from 192.168.1.103: seq=6 ttl=63 time=8.082 ms
64 bytes from 192.168.1.103: seq=7 ttl=63 time=33.027 ms
64 bytes from 192.168.1.103: seq=8 ttl=63 time=8.008 ms
64 bytes from 192.168.1.103: seq=9 ttl=63 time=7.597 ms
64 bytes from 192.168.1.103: seq=10 ttl=63 time=7.314 ms

PC3> show ip

NAME : PC3[1]
IP/MASK : 192.168.1.103/24
GATEWAY : 192.168.1.254
DNS : 192.168.1.254
DHCP SERVER : 192.168.1.254
DHCP LEASE : 7079, 7200/3600/6300
DOMAIN NAME : home.arpa
MAC : 00:50:79:66:68:02
LPORT : 20036
RHOST:PORT : 127.0.0.1:20037
MTU : 1500

PC3> ping 192.168.2.1

84 bytes from 192.168.2.1 icmp_seq=1 ttl=63 time=9.260
84 bytes from 192.168.2.1 icmp_seq=2 ttl=63 time=6.227
84 bytes from 192.168.2.1 icmp_seq=3 ttl=63 time=8.168
84 bytes from 192.168.2.1 icmp_seq=4 ttl=63 time=6.080
84 bytes from 192.168.2.1 icmp_seq=5 ttl=63 time=13.733

4, length 64
12:31:41.853898 IP 192.168.1.103 > 192.168.2.1: ICMP echo reply, id 15107, seq 4, length 64
12:31:42.851073 IP 192.168.2.1 > 192.168.1.103: ICMP echo request, id 15107, seq 5, length 64
12:31:42.854396 IP 192.168.1.103 > 192.168.2.1: ICMP echo reply, id 15107, seq 5, length 64
12:31:43.853185 IP 192.168.2.1 > 192.168.1.103: ICMP echo request, id 15107, seq 6, length 64
12:31:43.856716 IP 192.168.1.103 > 192.168.2.1: ICMP echo reply, id 15107, seq 6, length 64
12:31:44.871736 IP 192.168.2.1 > 192.168.1.103: ICMP echo request, id 15107, seq 7, length 64
12:31:44.884006 IP 192.168.1.103 > 192.168.2.1: ICMP echo reply, id 15107, seq 7, length 64
12:31:45.857383 IP 192.168.2.1 > 192.168.1.103: ICMP echo request, id 15107, seq 8, length 64
12:31:45.861137 IP 192.168.1.103 > 192.168.2.1: ICMP echo reply, id 15107, seq 8, length 64
12:31:46.858261 IP 192.168.2.1 > 192.168.1.103: ICMP echo request, id 15107, seq 9, length 64
12:31:46.861637 IP 192.168.1.103 > 192.168.2.1: ICMP echo reply, id 15107, seq 9, length 64

Début du TP4 : 05/05/2025

Regle de pare-feu actuelle :

LAN:

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>		0/0 B	IPv4 TCP	AdminPc	*	LAN address	22 (SSH)	*	none		
<input type="checkbox"/>		1/98 KiB	IPv4 TCP	AdminPc	*	LAN address	443 (HTTPS)	*	none		
<input type="checkbox"/>		0/0 B	IPv4 ICMP	any	*	*	*	*	none	Autoriser les pings sortant vers toutes les destinations	

SRV:

Floating

WAN

LAN

SRV

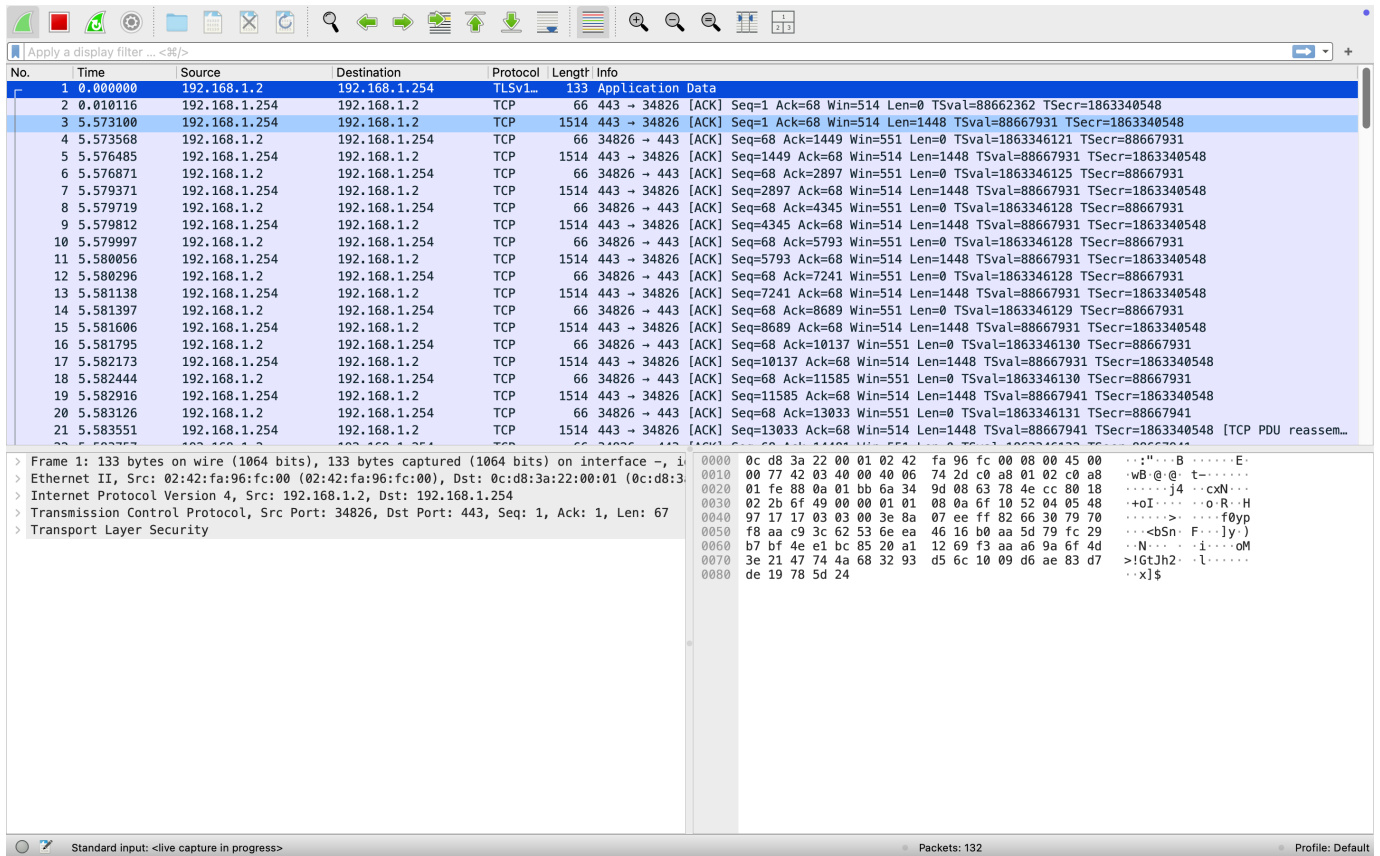
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>		0/0 B	IPv4 ICMP	any	*	*	*	*	none	Autoriser les pings sortant vers toutes les destinations	

Matrice de flux:

Source - Name	Source - IP	Firewall Incoming Interface	Firewall Outgoing Interface	Destination - Name	Destination - IP	Protocol (L3-L4)	Port / Service (L5-L7)	Action
All internal	*	All internal interfaces	any	*	*	IMCP		Allow
PCAdmin	192.168.1.1-3	em1		FW	192.168.1.254	TCP	HTTPS / SSH	Allow

WireShark

Connexion a l'interface de pfSense via le webterm resultat dans le Wireshark:



◆ 1. Décomposition OSI de la trame 1

Couche OSI	Protocole/Donnée dans cette trame
Couche 2 - Liaison	Ethernet II : adresses MAC source/destination
Couche 3 - Réseau	IPv4 : IP source 192.168.1.2 → IP destination 192.168.1.254
Couche 4 - Transport	TCP : port source 34826 → port destination 443
Couche 5 à 7 - Session / Présentation / Application	TLSv1.2

◆ 2. Evidence du handshake TCP

Dans cette capture Wireshark, le handshake TCP initial (SYN, SYN-ACK, ACK) n'apparaît pas dans les paquets visibles. L'échange commence à partir du paquet numéro 2, où le client (192.168.1.2) envoie déjà un paquet **ACK** au serveur (192.168.1.254) sur le port 443, ce qui indique que la connexion TCP a **déjà été établie**. Les paquets suivants montrent les échanges TLS, qui reposent sur cette connexion préexistante.

Configuration des VLANs

Après avoir configuré les VLANs sur pfSense, il faut modifier le VLAN user pour ajouter le DHCP.

Enable



Enable DHCP server on VLAN10USER interface

Primary Address Pool

Subnet 192.168.10.0/24

Subnet Range 192.168.10.1 - 192.168.10.254

Address Pool Range

192.168.10.1

From

192.168.10.254

To

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools

[+ Add Address Pool](#)

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

La configuration au niveau du switch pour le vlan user:

Node properties

Switch1 configuration

General

Name: Switch1

Console type: none

Settings

Port: 8

VLAN: 1

Type: access

QinQ EtherType: 0x8100

AddDelete

Ports

Port	VLAN	Type	EtherType
0	10	access	
1	10	access	
2	10	access	
3	1	dot1q	
4	1	access	
5	1	access	
6	1	access	
7	1	access	

ResetApplyCancelOK

Test de ping entre PC1 et PC2:

```
sylvainrougie — PC1 — telnet 192.168.32.104 500...
NAME      : PC1[1]
IP/MASK    : 192.168.10.1/24
GATEWAY    : 0.0.0.0
DNS        : 192.168.10.254
DHCP SERVER : 192.168.10.254
DHCP LEASE  : 7191, 7200/3600/6300
DOMAIN NAME : home.arpa
MAC        : 00:50:79:66:68:01
LPORT      : 20020
RHOST:PORT  : 127.0.0.1:20021
MTU        : 1500

PC1> dhcp
DORA
PC1> ping 192.168.10.2 IP 192.168.10.1/24

84 bytes from 192.168.10.2 icmp_seq=1 ttl=64 time=1.593 ms
84 bytes from 192.168.10.2 icmp_seq=2 ttl=64 time=1.519 ms
84 bytes from 192.168.10.2 icmp_seq=3 ttl=64 time=1.325 ms
84 bytes from 192.168.10.2 icmp_seq=4 ttl=64 time=1.177 ms
84 bytes from 192.168.10.2 icmp_seq=5 ttl=64 time=1.448 ms

PC1> ]

sylvainrougie — PC2 — telnet 192.168.32.104 5002...
PC2> dhcp
DDORA
PC2> dhcp IP 192.168.10.2/24
DORA
PC2> j IP 192.168.10.2/24
Bad command: "j". Use ? for help.

PC2> ping 192.168.10.2

192.168.10.2 icmp_seq=1 ttl=64 time=0.001 ms
192.168.10.2 icmp_seq=2 ttl=64 time=0.001 ms
192.168.10.2 icmp_seq=3 ttl=64 time=0.001 ms
192.168.10.2 icmp_seq=4 ttl=64 time=0.001 ms
192.168.10.2 icmp_seq=5 ttl=64 time=0.001 ms

PC2> ping 192.168.10.1

84 bytes from 192.168.10.1 icmp_seq=1 ttl=64 time=1.180 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=64 time=1.181 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=64 time=1.478 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=64 time=1.102 ms
84 bytes from 192.168.10.1 icmp_seq=5 ttl=64 time=1.458 ms

PC2> ]
```