

Compte Rendu de TP - GNS3 et pfSense

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.
-

TP2

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 :

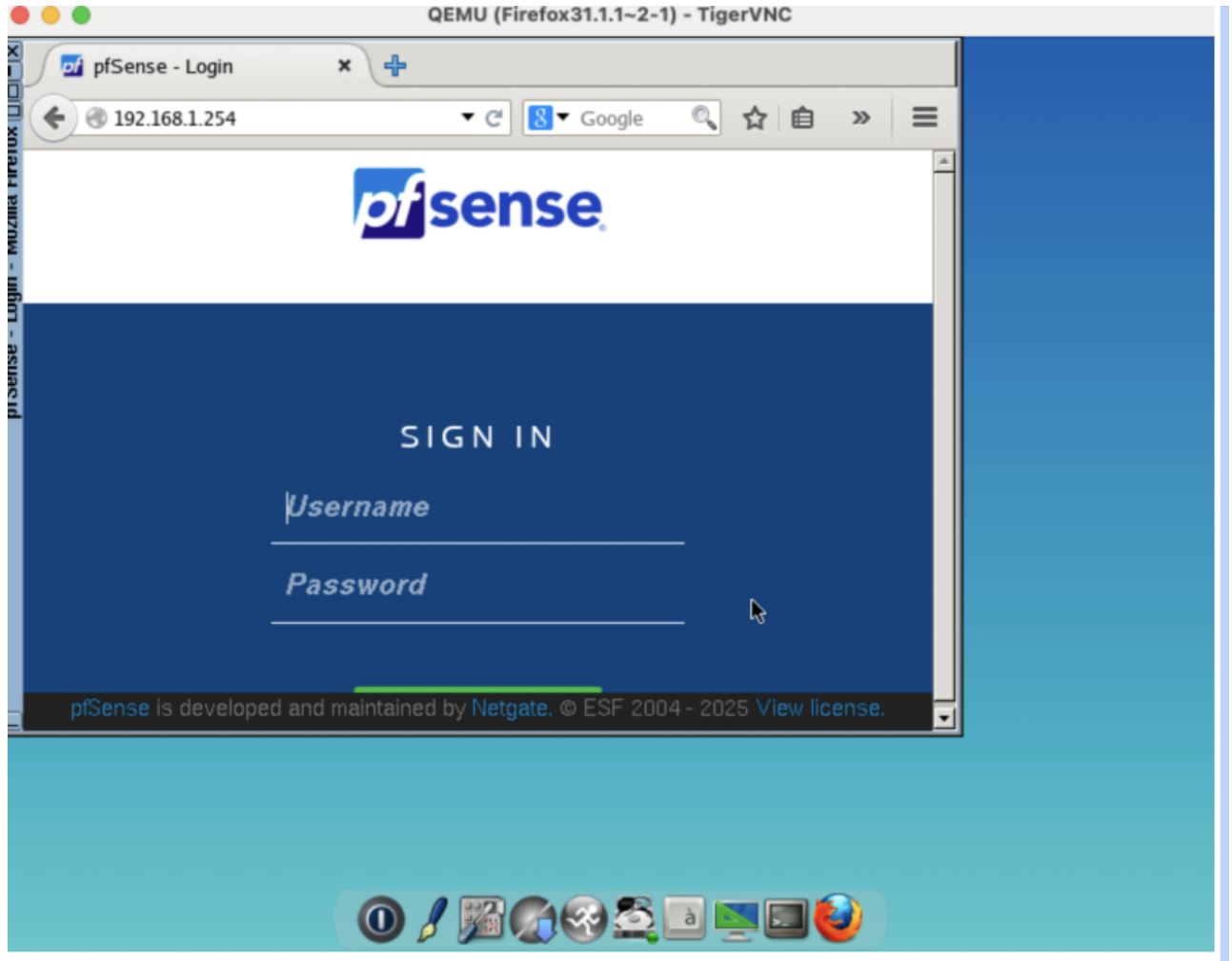
- Tentatives d'ajout de la configuration et de la bonne adresse IP.
- Vérification de la connexion, tout est ok.
- Tentative de connexion à pfSense, mais erreur. J'ai aussi tenté via VNC, mais ça a échoué. Le redémarrage de pfSense a été nécessaire, car j'avais mis la machine en pause pendant la pause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

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 5/1.54 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✓ 0/152 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	🔗 🖋️ 📄 ⏏️ 🗑️ ✖️

⬆️ 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	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions						
<input type="checkbox"/>	✓ 0/276 KiB	IPv4 *	AdminPc					none			<div><div>Alias details</div><table><tr><th>Value</th><th>Description</th></tr><tr><td>192.168.1.2</td><td>Webterm</td></tr><tr><td>192.168.1.3</td><td>Firefox</td></tr></table></div> <div><div><div><div><div><div></div></div></div><div><div><div></div></div></div></div><div><div><div></div></div></div><div><div><div></div></div></div></div><div><div><div></div></div></div><div><div><div></div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div>	Value	Description	192.168.1.2	Webterm	192.168.1.3	Firefox
Value	Description																
192.168.1.2	Webterm																
192.168.1.3	Firefox																
<input type="checkbox"/>	✗ 0/14 KiB	IPv4 *	*		LAN address	*	*	none			<div><div><div><div><div></div></div></div><div><div><div></div></div></div></div><div><div><div></div></div></div><div><div><div></div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div>						
<input type="checkbox"/>	✓ 0/310 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	<div><div><div><div><div></div></div></div><div><div><div></div></div></div></div><div><div><div></div></div></div><div><div><div></div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div>						
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	<div><div><div><div><div></div></div></div><div><div><div></div></div></div></div><div><div><div></div></div></div><div><div><div></div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div> <div><div><div></div></div></div>						

↑ Add

↓ Add

🗑 Delete

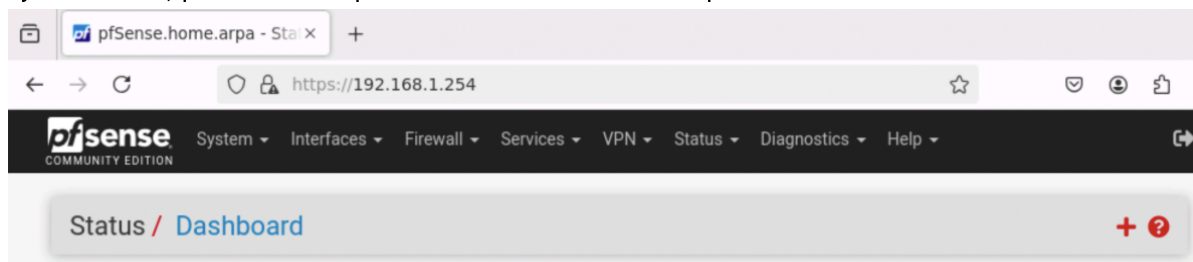
🔄 Toggle

📄 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	

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.



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/gIRrTQ1ZUcM85YrKnLhgCgFxAPxgVfqZ2TfzP+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.
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

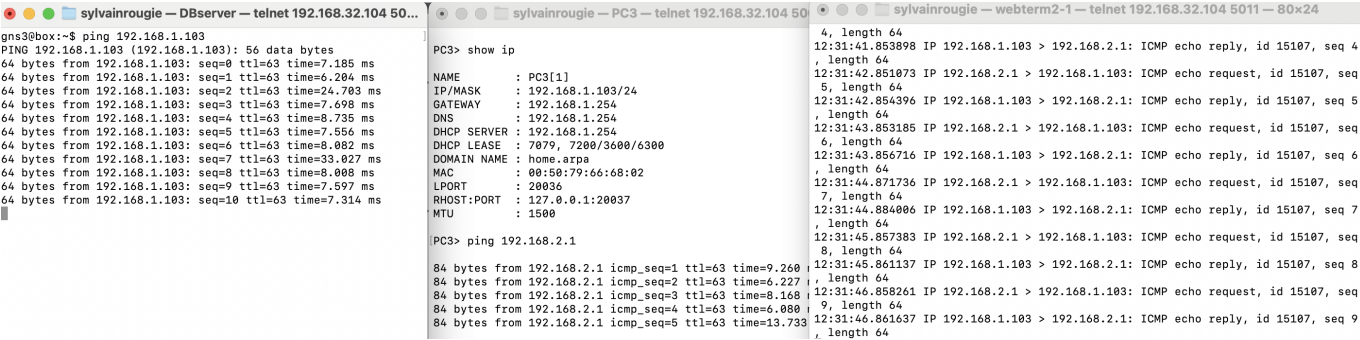
The default is to use the IP address of this firewall interface as the correct gateway for the network. Enter "none" for no gateway

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 reseau 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.



Début du TP3 : 05/05/2025

Regle de pare-feu actuelle :

LAN:

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 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	*	*	*	*	*	none		Autoriser les pings sortant vers toutes les destinations	

SRV:

FloatingWANLANSRV

Rules (Drag to Change Order)

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

Matrice de flux:

Source Name	Source IP	FW Incoming IF	FW Outgoing IF	Destination Name	Destination IP	Protocol (Layer 3-4)
PCAdmin	192.168.1.1-3	em1	em2	Server & DB	192.168.2.1-2	ICMP

Source Name	Source IP	FW Incoming IF	FW Outgoing IF	Destination Name	Destination IP	Protocol (Layer 3-4)
Server	192.168.2.1-2	em2	em1	Admin	192.168.1.1-3	ICMP
PCAdmin	192.168.1.1-3	em1	em2	Server & DB	192.168.2.1-2	TCP
Server	192.168.2.1-2	em2	em1	Admin	192.168.1.1-3	TCP
PCAdmin	192.168.1.1-3	em1		FW	192.168.1.254	TCP
Server	192.168.2.1-2	em2		FW	192.168.2.254	TCP

WireShark

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

Apply a display filter ... <[?/>>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.2	192.168.1.254	TLSv1	133	Application Data
2	0.010116	192.168.1.254	192.168.1.2	TCP	66	443 → 34826 [ACK] Seq=1 Ack=68 Win=514 Len=0 TSval=88662362 TSecr=1863340548
3	5.573100	192.168.1.254	192.168.1.2	TCP	1514	443 → 34826 [ACK] Seq=1 Ack=68 Win=514 Len=1448 TSval=88667931 TSecr=1863340548
4	5.573568	192.168.1.2	192.168.1.254	TCP	66	34826 → 443 [ACK] Seq=68 Ack=1449 Win=551 Len=0 TSval=1863346121 TSecr=88667931
5	5.576485	192.168.1.254	192.168.1.2	TCP	1514	443 → 34826 [ACK] Seq=1449 Ack=68 Win=514 Len=1448 TSval=88667931 TSecr=1863340548
6	5.576871	192.168.1.2	192.168.1.254	TCP	66	34826 → 443 [ACK] Seq=68 Ack=2897 Win=551 Len=0 TSval=1863346125 TSecr=88667931
7	5.579371	192.168.1.254	192.168.1.2	TCP	1514	443 → 34826 [ACK] Seq=2897 Ack=68 Win=514 Len=1448 TSval=88667931 TSecr=1863340548
8	5.579719	192.168.1.2	192.168.1.254	TCP	66	34826 → 443 [ACK] Seq=68 Ack=4345 Win=551 Len=0 TSval=1863346128 TSecr=88667931
9	5.579812	192.168.1.254	192.168.1.2	TCP	1514	443 → 34826 [ACK] Seq=4345 Ack=68 Win=514 Len=1448 TSval=88667931 TSecr=1863340548
10	5.579997	192.168.1.2	192.168.1.254	TCP	66	34826 → 443 [ACK] Seq=68 Ack=5793 Win=551 Len=0 TSval=1863346128 TSecr=88667931
11	5.580056	192.168.1.254	192.168.1.2	TCP	1514	443 → 34826 [ACK] Seq=5793 Ack=68 Win=514 Len=1448 TSval=88667931 TSecr=1863340548
12	5.580296	192.168.1.2	192.168.1.254	TCP	66	34826 → 443 [ACK] Seq=68 Ack=7241 Win=551 Len=0 TSval=1863346128 TSecr=88667931
13	5.581138	192.168.1.254	192.168.1.2	TCP	1514	443 → 34826 [ACK] Seq=7241 Ack=68 Win=514 Len=1448 TSval=88667931 TSecr=1863340548
14	5.581397	192.168.1.2	192.168.1.254	TCP	66	34826 → 443 [ACK] Seq=68 Ack=8689 Win=551 Len=0 TSval=1863346129 TSecr=88667931
15	5.581606	192.168.1.254	192.168.1.2	TCP	1514	443 → 34826 [ACK] Seq=8689 Ack=68 Win=514 Len=1448 TSval=88667931 TSecr=1863340548
16	5.581795	192.168.1.2	192.168.1.254	TCP	66	34826 → 443 [ACK] Seq=68 Ack=10137 Win=551 Len=0 TSval=1863346130 TSecr=88667931
17	5.582173	192.168.1.254	192.168.1.2	TCP	1514	443 → 34826 [ACK] Seq=10137 Ack=68 Win=514 Len=1448 TSval=88667931 TSecr=1863340548
18	5.582444	192.168.1.2	192.168.1.254	TCP	66	34826 → 443 [ACK] Seq=68 Ack=11585 Win=551 Len=0 TSval=1863346130 TSecr=88667931
19	5.582916	192.168.1.254	192.168.1.2	TCP	1514	443 → 34826 [ACK] Seq=11585 Ack=68 Win=514 Len=1448 TSval=88667941 TSecr=1863340548
20	5.583126	192.168.1.2	192.168.1.254	TCP	66	34826 → 443 [ACK] Seq=68 Ack=13033 Win=551 Len=0 TSval=1863346131 TSecr=88667941
21	5.583551	192.168.1.254	192.168.1.2	TCP	1514	443 → 34826 [ACK] Seq=13033 Ack=68 Win=514 Len=1448 TSval=88667941 TSecr=1863340548 [TCP PDU reassem...

> Frame 1: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on interface ..., i

> Ethernet II, Src: 02:42:fa:96:fc:00 (02:42:fa:96:fc:00), Dst: 0c:d8:3a:22:00:01 (0c:d8:3

> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.254

> Transmission Control Protocol, Src Port: 34826, Dst Port: 443, Seq: 1, Ack: 1, Len: 67

> Transport Layer Security

0000 0c d8 3a 22 00 01 02 42 fa 96 fc 00 08 00 45 00 ...:..B.....E

0010 00 77 42 03 40 00 40 06 74 2d c0 a8 01 02 c0 a8 ...wB.@.t.....

0020 01 fe 88 0a 01 bb 6a 34 9d 08 63 78 4e cc 08 18j4...cxN...

0030 02 2b 6f 49 00 00 01 01 08 0a 6f 10 52 04 05 48 ...+oI.....o:R..H

0040 97 17 17 03 03 00 3e 8a 07 ee ff 82 66 30 79 70>...f0yp

0050 f8 aa c9 3c 62 53 6e ea 46 16 b0 aa 5d 79 fc 29 ...-c5n..F...ly.)

0060 b7 bf 4e e1 bc 85 20 a1 12 69 f3 aa a6 9a 6f 4d ...N.....i...oM

0070 3e 21 47 74 4a 68 32 93 d5 6c 10 09 d6 ae 83 d7 ...!GtJh2-.l.....

0080 de 19 78 5d 24 ...x)\$

Standard input: <live capture in progress>

Packets: 132

Profile: Default