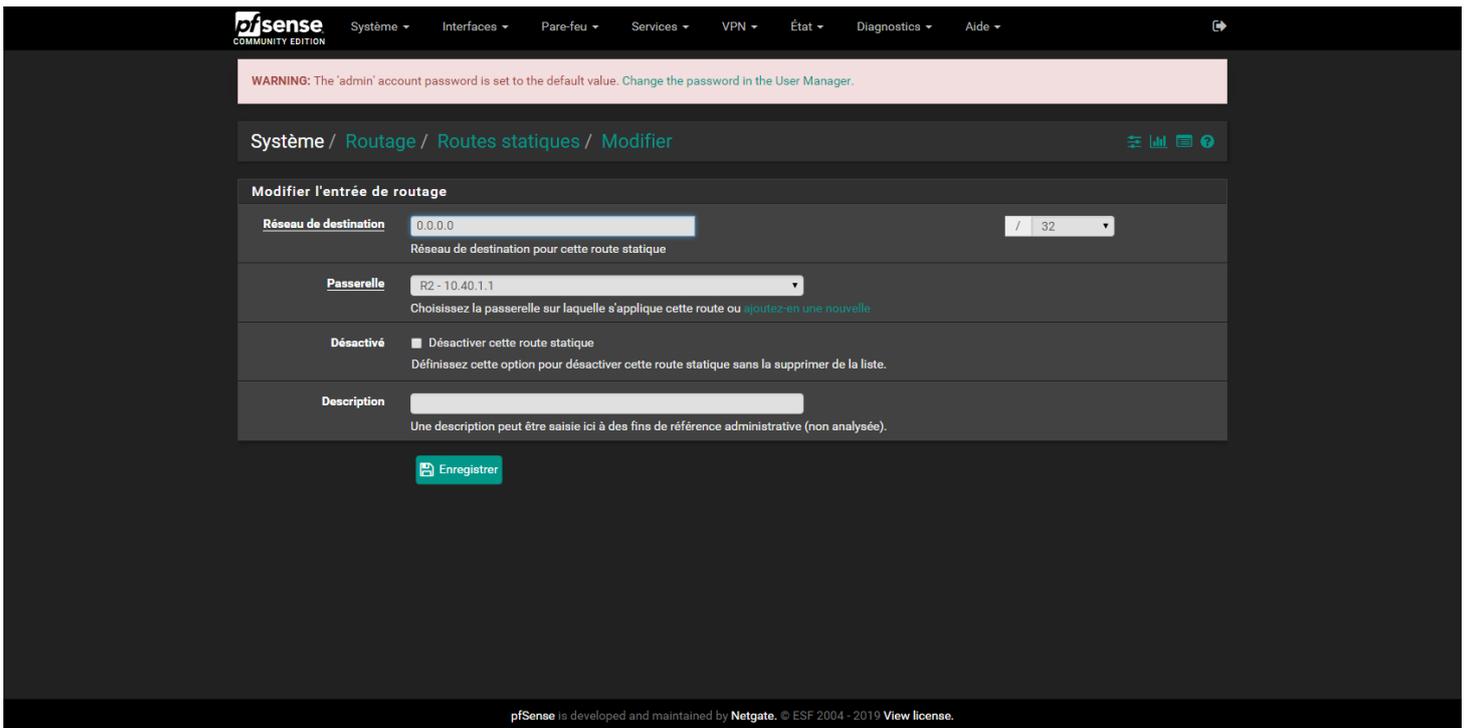


SISR5 – FIREWALL

I. Accès web depuis le LAN (ICMP + http)

Pour commencer, nous avons besoin de créer une route par défaut afin de diriger les requêtes du LAN d'accéder au WAN (et donc internet).

Voici la configuration :



The screenshot shows the pfSense web interface for configuring a static route. The breadcrumb navigation is "Système / Routage / Routes statiques / Modifier". A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The configuration form is titled "Modifier l'entrée de routage" and contains the following fields:

- Réseau de destination:** Input field containing "0.0.0.0" and a dropdown menu showing "/ 32". Below the input is the text "Réseau de destination pour cette route statique".
- Passerelle:** A dropdown menu showing "R2-10.40.1.1". Below the dropdown is the text "Choisissez la passerelle sur laquelle s'applique cette route ou [ajoutez-en une nouvelle](#)".
- Désactivé:** A checkbox labeled "Désactiver cette route statique". Below the checkbox is the text "Définissez cette option pour désactiver cette route statique sans la supprimer de la liste."
- Description:** An empty input field. Below the input is the text "Une description peut être saisie ici à des fins de référence administrative (non analysée)".

At the bottom of the form is a blue button labeled "Enregistrer". The footer of the interface reads: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license."

Nous indiquons donc dans « Réseau de destination » l'adresse IP : **0.0.0.0** avec le masque **/32** (CIDR). Afin nous indiquons que la passerelle est la routeur R2, donc **10.40.1.1**.

Une fois cela fait passons à présent à la translation d'adresse. Pour se faire direction le NAT dans les réglages du pare-feu. Ensuite dans l'onglet « Sortant », ajouter une nouvelle règle comme ceci :

The screenshot shows the 'Modifier l'entrée NAT sortant avancée' configuration page. The 'Désactivé' checkbox is checked. The 'Ne pas faire de NAT' checkbox is unchecked. The 'Interface' is set to 'WAN'. The 'Famille d'adresse' is set to 'IPv4'. The 'Protocole' is set to 'tout'. The 'Source' and 'Destination' are both set to 'Tous'. The 'Traduction' section has 'Adresse' set to 'Adresse de l'interface' and 'Port ou plage' is empty. The 'Port statique' checkbox is checked.

Choisir l'interface WAN, indiquer vouloir autoriser tous les protocoles. De même sur la source et la destination, on laisse vide les champs des adresses IP afin de tout autoriser.

Au niveau des règles du pare-feu, onglet LAN, voici ce qu'il faut ajouter ensuite :

The screenshot shows the 'Règles (Faire glisser pour changer l'ordre)' table for the LAN interface. Two rules are highlighted with a red box: 'IPv4 ICMP any' and 'IPv4 TCP'. The table has columns for 'États', 'Protocole', 'Source', 'Port', 'Destination', 'Port', 'Passerelle', 'File d'attente', 'Ordonnement', 'Description', and 'Actions'.

États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
✓ 0 / 5,20 MIB	*	*	*	LAN Address	443	*	*	*	Règle anti-blocage	⚙️
✓ 0 / 2 KiB	IPv4 ICMP	*	*	*	*	*	aucun	*		📌 🔄 🗑️
✓ 0 / 0 B	IPv4 TCP	*	*	*	*	*	aucun	*		📌 🔄 🗑️
✓ 1 / 7 KiB	IPv4 *	LAN net	*	*	*	*	aucun	*	Default allow LAN to any rule	📌 🔄 🗑️
✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	aucun	*	Default allow LAN IPv6 to any rule	📌 🔄 🗑️

Il s'agit de deux règles permettant de lui indiquer qu'il doit laisser passer les trames ICMP et TCP provenant de n'importe quelle source en direction de n'importe quelle destination et de

Afin de justifier que le PC n'a plus accès à internet voici quelques trames d'avant et après le FireWall :

AVANT LE PARE-FEU

No.	Time	Source	Destination	Protocol	Length	Info
9053	1371.633508	10.40.1.1	10.40.1.10	ICMP	60	Echo (ping) reply id=0x3f1d, seq=2806/62986, ttl=255 (request in 9052)
9054	1372.131534	PcsCompu_e9:bc:bd	PcsCompu_32:0c:0a	ARP	42	Who has 10.40.1.10? Tell 10.40.1.20
9055	1372.131588	10.40.1.20	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=128 (no response found!)
9056	1372.131697	PcsCompu_32:0c:0a	PcsCompu_e9:bc:bd	ARP	42	10.40.1.10 is at 08:00:27:32:0c:0a
9057	1372.174043	aa:bb:cc:00:02:00	Spanning-tree-(for...	STP	60	RST. Root = 32768/1/aa:bb:cc:00:02:00 Cost = 0 Port = 0x8001

APRES LE PARE-FEU

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::5837:ae5e:830...	ff02::1:2	DHCPv6	156	Solicit XID: 0x76d905 CID: 000100011d97288d08002757a867
2	0.998390	fe80::5837:ae5e:830...	ff02::1:2	DHCPv6	156	Solicit XID: 0x76d905 CID: 000100011d97288d08002757a867
3	2.998854	fe80::5837:ae5e:830...	ff02::1:2	DHCPv6	156	Solicit XID: 0x76d905 CID: 000100011d97288d08002757a867
4	4.969873	192.168.1.10	192.168.1.255	BRONSER	243	Local Master Announcement VM-WINDOWS7-PC, Workstation, Server, NT Workstation, Potential Browser, Master Browser
5	6.998456	fe80::5837:ae5e:830...	ff02::1:2	DHCPv6	156	Solicit XID: 0x76d905 CID: 000100011d97288d08002757a867
6	14.998637	fe80::5837:ae5e:830...	ff02::1:2	DHCPv6	156	Solicit XID: 0x76d905 CID: 000100011d97288d08002757a867
7	30.998252	fe80::5837:ae5e:830...	ff02::1:2	DHCPv6	156	Solicit XID: 0x76d905 CID: 000100011d97288d08002757a867

On peut voir que la trame à destination de 192.168.1.1 ne passe pas à travers le FireWall. Sur la capture d'écran d'après le FireWall, on ne voit donc aucune trace de la trame.

III. Accès DMZ depuis l'intérieur (LAN)

Afin que le réseau LAN puisse avoir accès à la DMZ nous devons créer de nouvelles règles afin de lui permettre d'y accéder. Nous indiquons en source LAN address afin d'inclure toutes les adresses du réseau LAN et au niveau des ports et de la destination, nous laissons passer partout. Grâce à ces règles, le réseau LAN aura donc forcément accès à la DMZ.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Pare-feu / Règles / LAN

Flottante) WAN LAN OPT1

Règles (Faire glisser pour changer l'ordre)

États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
2/1.21 MIB	*	*	*	LAN Address	443 80	*	*	*	Règle anti-blocage	🔄
0/0 B	IPV4 TCP/UDP	10.40.1.20	*	10.40.1.10	443 (HTTPS)	*	aucun	*		📄 🔄 🗑️
0/0 B	IPV4 TCP/UDP	10.40.1.20	*	10.40.1.10	80 (HTTP)	*	aucun	*		📄 🔄 🗑️
0/8 KIB	IPV4 *	10.40.1.20	*	*	*	*	aucun	*		📄 🔄 🗑️
0/0 B	IPV4 *	10.30.0.0/16	*	*	*	*	aucun	*		📄 🔄 🗑️
0/0 B	IPV4 ICMP any	LAN address	*	*	*	*	aucun	*		📄 🔄 🗑️
0/0 B	IPV4 TCP LAN address	LAN address	*	*	*	*	aucun	*		📄 🔄 🗑️
0/0 B	IPV4 *	LAN net	*	*	*	*	aucun	*	Default allow LAN to any rule	📄 🔄 🗑️
0/0 B	IPV6 *	LAN net	*	*	*	*	aucun	*	Default allow LAN IPv6 to any rule	📄 🔄 🗑️

📄 Ajouter 📄 Ajouter 🗑️ Supprimer 📄 Enregistrer ➕ Séparer

IV. Masquage des adresses IP

Voici les tests concluant sur le masquage de l'adresse IP :

7977	1808.820089	10.40.1.10	10.40.1.1	ICMP	42	Echo (ping) request	id=0x4059, seq...
7978	1808.820590	10.40.1.1	10.40.1.10	ICMP	60	Echo (ping) reply	id=0x4059, seq...
7979	1809.163811	10.30.1.10	192.168.1.10	ICMP	74	Echo (ping) request	id=0x0001, seq...
7980	1809.164360	192.168.1.10	10.30.1.10	ICMP	74	Echo (ping) reply	id=0x0001, seq...
7981	1809.362336	10.40.1.10	10.40.1.1	ICMP	42	Echo (ping) request	id=0x4059, seq...
7982	1809.371865	10.40.1.1	10.40.1.10	ICMP	60	Echo (ping) reply	id=0x4059, seq...
7983	1809.900841	10.40.1.10	10.40.1.1	ICMP	42	Echo (ping) request	id=0x4059, seq...
244	1665.425350	192.168.1.1	192.168.1.10	ICMP	74	Echo (ping) request	id=0x60c5, seq...
245	1665.426253	192.168.1.10	192.168.1.1	ICMP	74	Echo (ping) reply	id=0x60c5, seq...
246	1666.425931	192.168.1.1	192.168.1.10	ICMP	74	Echo (ping) request	id=0x60c5, seq...
247	1666.426140	192.168.1.10	192.168.1.1	ICMP	74	Echo (ping) reply	id=0x60c5, seq...
248	1667.426869	192.168.1.1	192.168.1.10	ICMP	74	Echo (ping) request	id=0x60c5, seq...

V. Accès DMZ depuis l'extérieur

Pour pouvoir accéder à Internet depuis l'extérieur, nous avons besoin de faire un transfert de port (PAT). Pour se faire il faut ajouter deux règles sur le port OPT1.

La première permet de rediriger le port 80 et la deuxième permet de laisser passer toutes les trames pour ping un utilisateur.

The screenshot shows the piSense firewall configuration interface. At the top, there is a navigation menu with options like 'Système', 'Interfaces', 'Pare-feu', 'Services', 'VPN', 'État', 'Diagnostics', and 'Aide'. A warning message is displayed: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this, the current configuration is for 'Pare-feu / Règles / OPT1'. There are tabs for 'Flottant(e)', 'WAN', 'LAN', and 'OPT1'. The main area shows a table of rules with the following columns: 'Règles (Faire glisser pour changer l'ordre)', 'États', 'Protocole', 'Source', 'Port', 'Destination', 'Port', 'Passerelle', 'File d'attente', 'Ordonnement', 'Description', and 'Actions'. Two rules are listed:

Règles (Faire glisser pour changer l'ordre)	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
■	✓	0/0 B	IPV4 TCP/UDP	*	*	80 (HTTP)	*	aucun			↓ ↗ ↘ ↻ 🗑️
■	✓	0/0 B	IPV4 ICMP	any	*	*	*	aucun			↓ ↗ ↘ ↻ 🗑️

At the bottom of the table, there are buttons for 'Ajouter', 'Ajouter', 'Supprimer', 'Enregistrer', and 'Séparateur'. The footer of the interface states: 'piSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license.'

Afin de justifier tout cela, voici une preuve via la commande *tracert* dans l'invite de commande Windows.

```
C:\Users\UM-Windows7>ping 192.168.1.10
Envoi d'une requête 'Ping' 192.168.1.10 avec 32 octets de données :
Réponse de 192.168.1.10 : octets=32 temps=1 ms TTL=125

Statistiques Ping pour 192.168.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

C:\Users\UM-Windows7>tracert 192.168.1.10

Détermination de l'itinéraire vers 192.168.1.10 avec un maximum de 30 sauts.

  1  <1 ms    <1 ms    <1 ms    10.30.1.1
  2  <1 ms    <1 ms    <1 ms    10.2.2.2
  3   1 ms    <1 ms    <1 ms    10.40.1.10
  4   1 ms    <1 ms    <1 ms    192.168.1.10

Itinéraire déterminé.
```