

CONFIGURATION DU PARE-FEU IPFIRE ET D'UN ACCES SSH

TABLE DES MATIERES

Contexte du projet	1
Installation et configuration du Pare-Feu IPFIRE	1
Configuration d'un accès SSH sur une machine Linux	12

CONTEXTE DU PROJET

Dans le cadre de la sécurisation des infrastructures réseau d'une organisation, il est essentiel de contrôler et de protéger les accès aux différentes machines du système d'information. Dans ce projet réalisé en cours de formation un Pare-Feu ainsi qu'un accès SSH est mis en place.

INSTALLATION ET CONFIGURATION DU PARE-FEU IPFIRE

Lors du démarrage sur un disque contenant l'image ISO du logiciel IPFIRE voici le menu qui s'affiche. Dans le cadre de l'installation on choisit la première option.



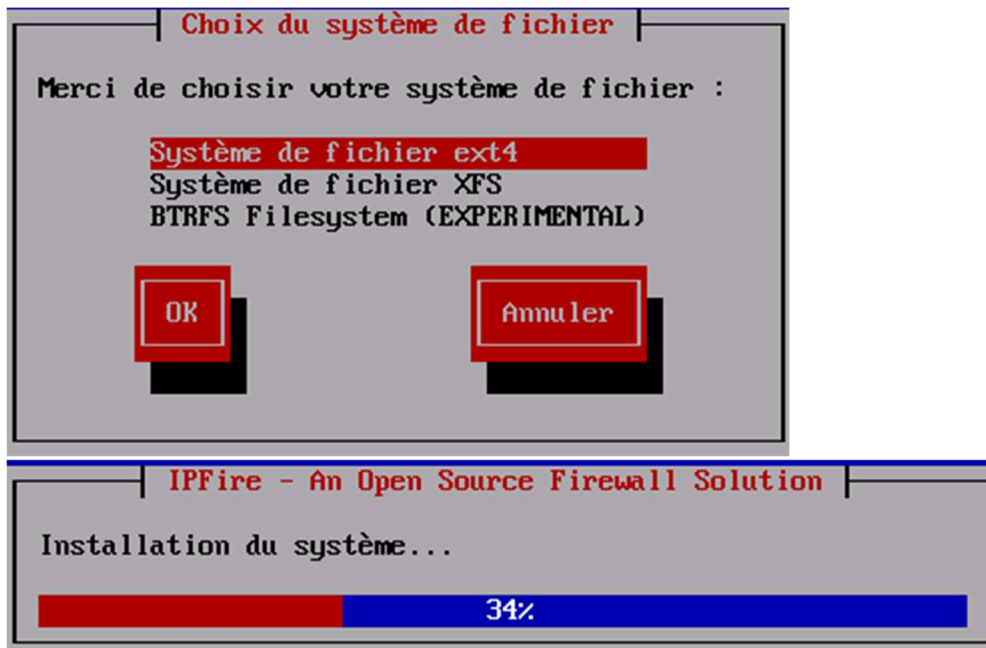
Puis nous devons choisir la langue de l'installation. Une fois sélectionner nous pouvons commencer l'installation : « **Démarrer l'installation** »



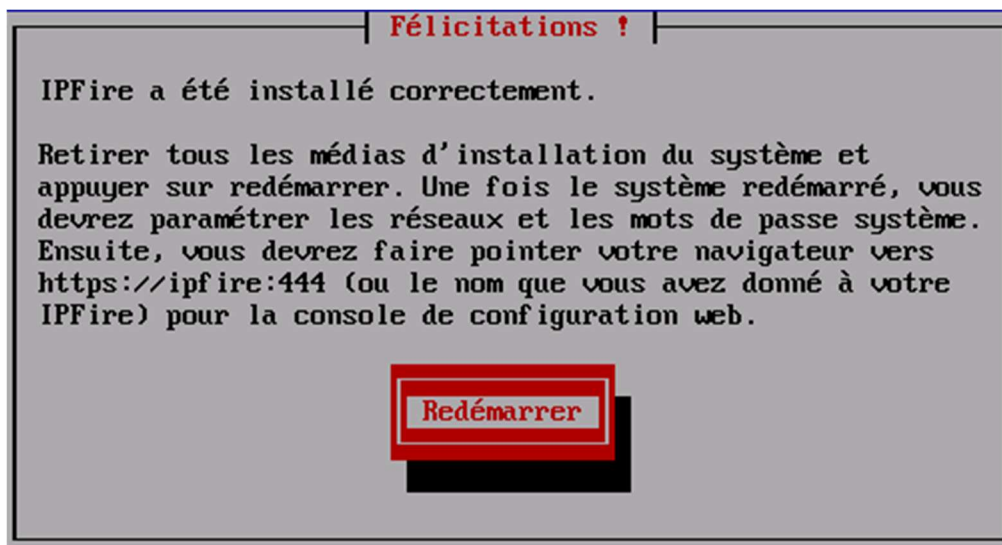
La première étape de l'installation consiste au choix du disque sur lequel nous souhaitons installer IPFIRE



Nous choisissons ensuite le système de fichiers qui nous convient pour l'installation puis nous cliquons sur « **OK** ». L'installation se lance.



Au terme d'une installation réussite du logiciel IPFIRE voici le message que nous obtenons. Nous sommes invités à redémarrer la machine.



Après le redémarrage nous sommes invités à choisir la disposition de claviers et le fuseau horaire qui nous correspondent



Nous devons ensuite configurer le nom d'hôte de la machine ainsi qu'un domaine.





Après ces étapes nous devons configurer les mots de passe de l'utilisateur **root** et **admin**



Nous arrivons au choix du type de configuration réseau. Dans notre cas nous choisissons une configuration de type **GREEN + RED**

Menu de configuration Réseau

Configuration actuelle : GREEN + RED

Type de configuration réseau
Affectation des Pilotes et des Cartes
Configuration d'adresse

OK Terminé

Type de configuration réseau

Choisir la configuration réseau pour IPFire.
Les types suivants correspondent aux interfaces Ethernet connectées. Tout changement dans le paramétrage nécessite une reconfiguration de la couche réseau et des pilotes associés.

GREEN + RED
GREEN + RED + ORANGE
GREEN + RED + BLUE
GREEN + RED + ORANGE + BLUE

OK Annuler

Nous devons ensuite attribuer les deux cartes réseau de notre machine soit au réseau **GREEN** soit au réseau **RED**. Dans le cas d'une installation du logiciel IPFIRE sur une machine virtuelle, au moins une carte réseau doit être en mode bridge.

Menu de configuration Réseau

Configuration actuelle : GREEN + RED

A l'issue de la configuration, un redémarrage de la couche réseau est nécessaire.

Type de configuration réseau
Affectation des Pilotes et des Cartes
Configuration d'adresse

OK **Terminé**

Cartes attribuées

Veuillez choisir l'interface que vous souhaitez changer.

GREEN : Non défini
RED : Non défini

GREEN
RED

Sélectionner **Enlever** **Terminé**

Étendre le Menu Réseau

Veuillez choisir un adaptateur réseau pour l'interface - GREEN.

pci: Intel Corporation 82545EM Gigabit Ethernet Co... (00:0c:29:65:f3:0f)
pci: Intel Corporation 82545EM Gigabit Ethernet Co... (00:0c:29:65:f3:19)

Sélectionner **Identifier** **Annuler**

Cartes attribuées	
Veuillez choisir l'interface que vous souhaitez changer.	
GREEN : "pci: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) (rev 01)"	
GREEN : (00:0c:29:65:f3:19)	
RED : Non défini	
<div>GREEN</div> <div>RED</div>	
Sélectionner	Enlever
Terminé	

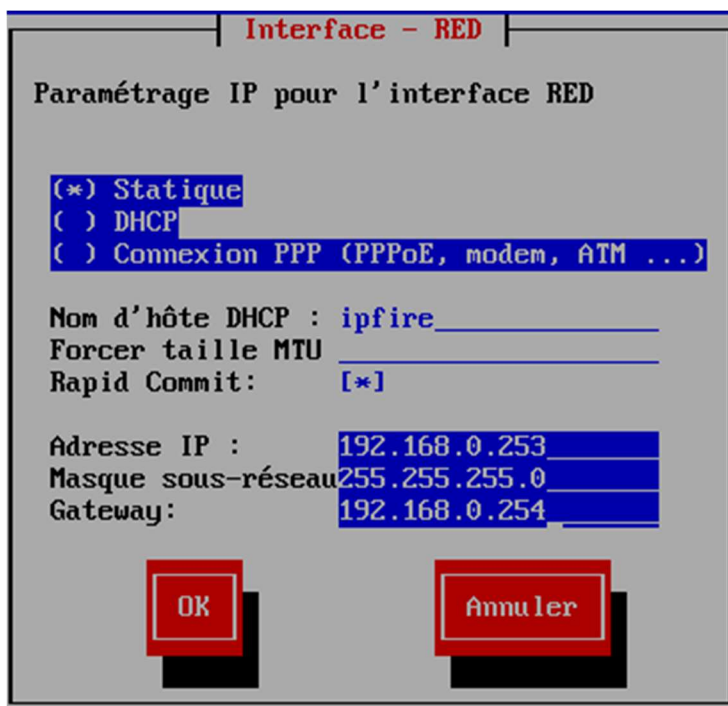
Etendre le Menu Réseau	
Veuillez choisir un adaptateur réseau pour l'interface - RED.	
pci: Intel Corporation 82545EM Gigabit Ethernet Co... (00:0c:29:65:f3:0f)	
Sélectionner	Identifier
Annuler	

Désormais nous devons configurer les adresses IP sur nos deux cartes réseau

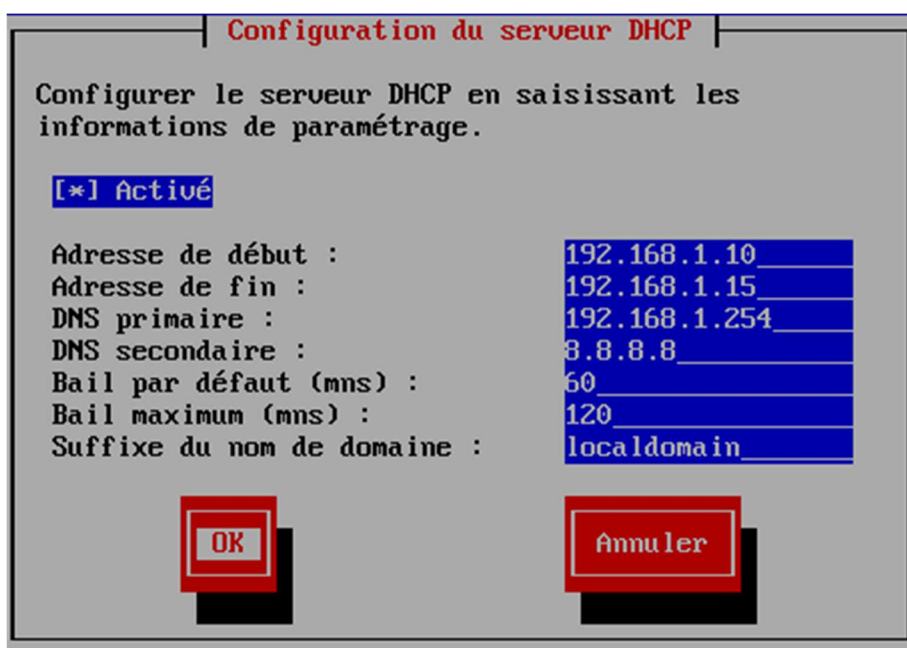
Menu de configuration Réseau	
Configuration actuelle : GREEN + RED	
A l'issue de la configuration, un redémarrage de la couche réseau est nécessaire.	
Type de configuration réseau	
Affectation des Pilotes et des Cartes	
Configuration d'adresse	
OK	Terminé



L'adresse IP qui sera affectée à l'interface **RED** doit être une adresse IP non utilisée sur le réseau dans le cas d'une installation du logiciel **IPFIRE** dans une machine virtuelle.



IPFIRE propose aussi un service DHCP



Configuration du serveur DHCP

Configurer le serveur DHCP en saisissant les informations de paramétrage.

[*] Activé

Adresse de début :	192.168.1.10
Adresse de fin :	192.168.1.15
DNS primaire :	192.168.1.254
DNS secondaire :	8.8.8.8
Bail par défaut (mns) :	60
Bail maximum (mns) :	120
Suffixe du nom de domaine :	localdomain

OK **Annuler**

Après la configuration des paramètres du DHCP, IPFIRE est prêt.



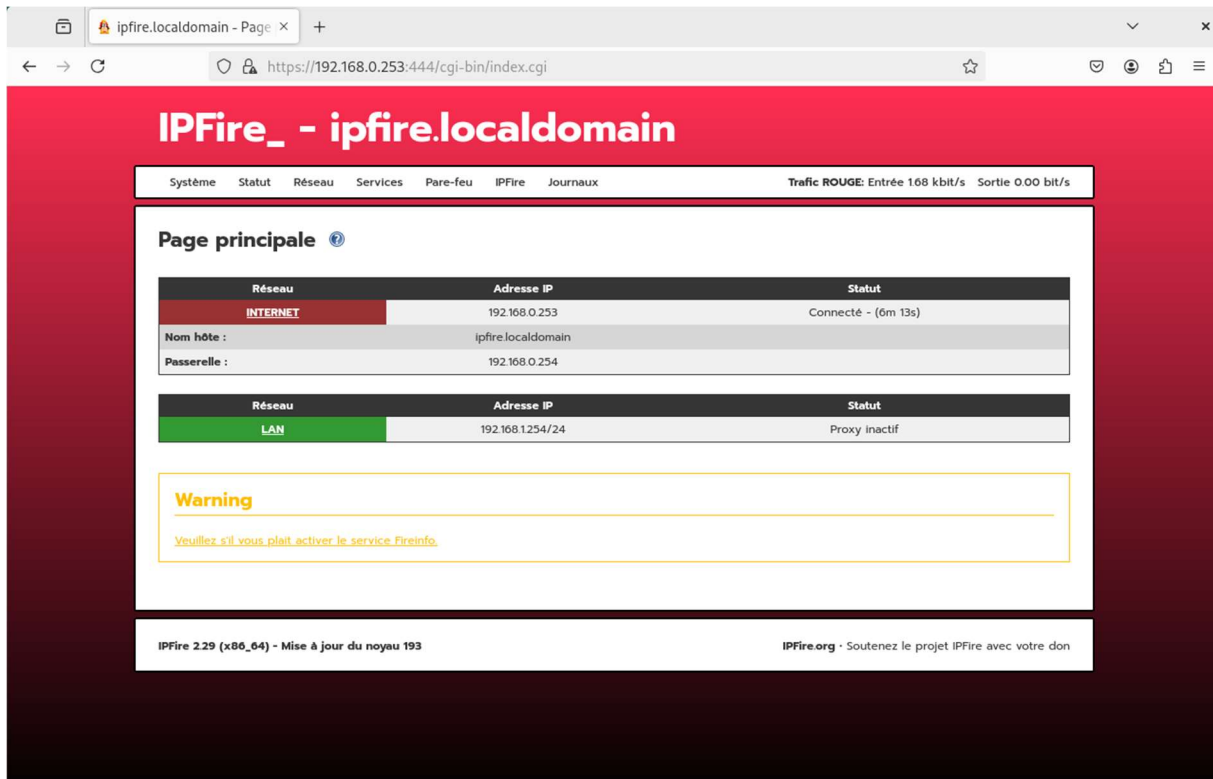
IPFire - www.ipfire.org

Le paramétrage est terminé.

OK

Pour accéder à l'interface graphique du logiciel **IPFIRE**, il nous faut nous rendre dans un navigateur sur une autre machine et taper l'adresse IP de notre carte réseau **RED** :

https://Adresse_IP_RED:444



Nous pouvons vérifier le bon fonctionnement du Pare-Feu **IPFIRE** et du service **DHCP** de celui-ci en tapant la commande **ip a** dans le terminal d'une machine se trouvant dans le réseau **GREEN**. Notre adresse IP correspond à la plage DHCP configurée auparavant.

```

user@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:ea:17:3d brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.1.10/24 brd 192.168.1.255 scope global dynamic noprefixroute ens33
        valid_lft 3511sec preferred_lft 3511sec
    inet6 fe80::20c:29ff:feea:173d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

```

CONFIGURATION D'UN ACCES SSH SUR UNE MACHINE LINUX

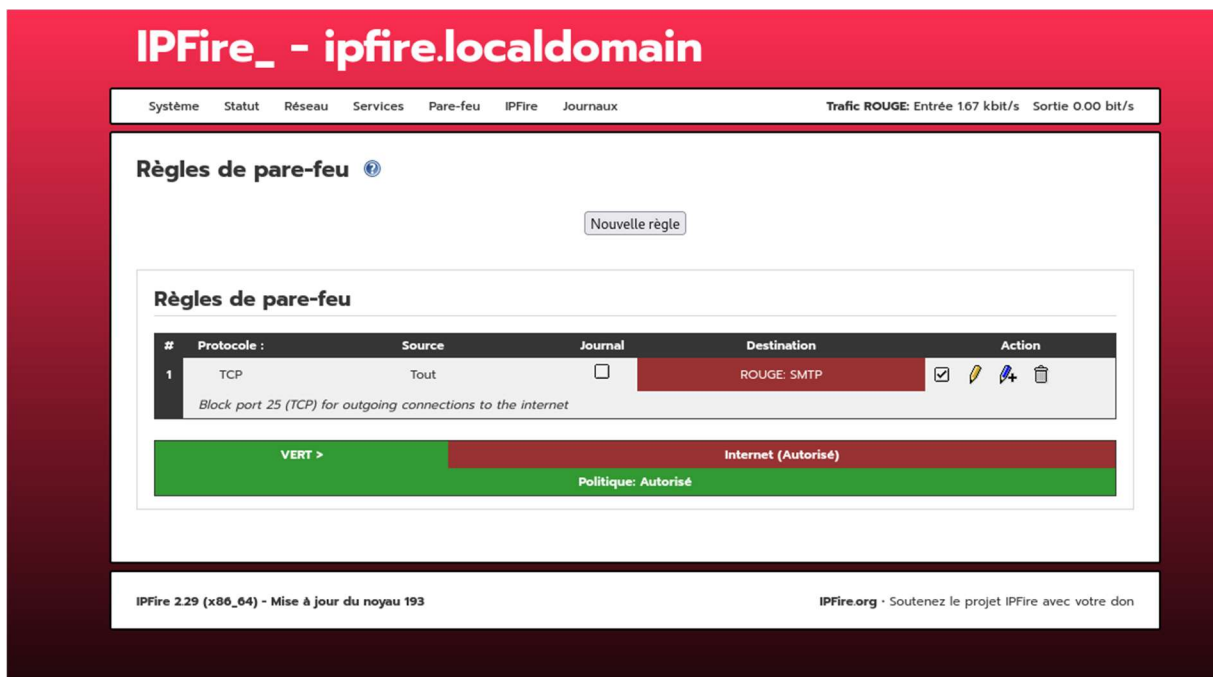
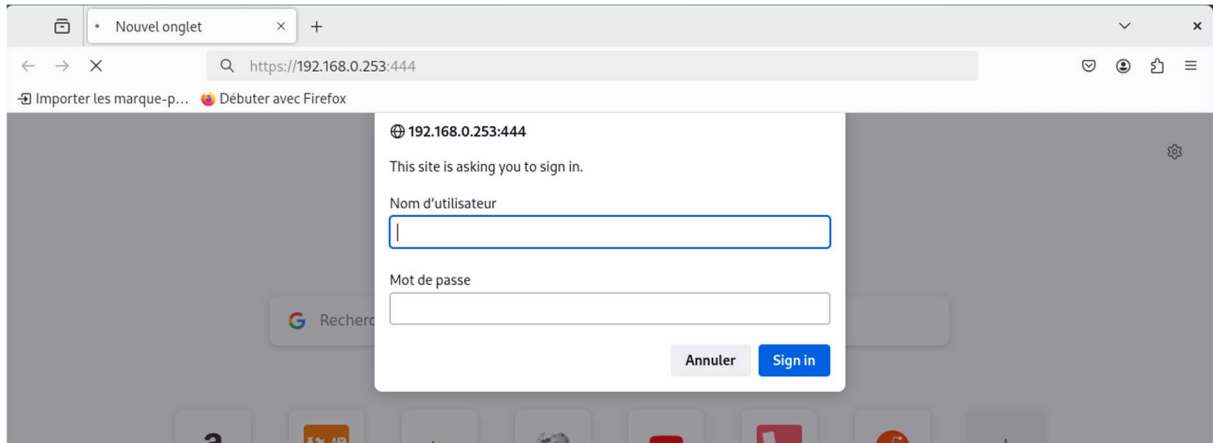
Pour pouvoir accéder à notre machine Linux via SSH nous devons dans un premier temps l'installer sur celle-ci.

```
user@debian:~$ sudo apt install openssh-server -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Paquets suggérés :
  molly-guard monkeysphere ssh-askpass ufw
Les NOUVEAUX paquets suivants seront installés :
  openssh-server
0 mis à jour, 1 nouvellement installés, 0 à enlever et 2 non mis à jour.
Il est nécessaire de prendre 457 ko dans les archives.
Après cette opération, 1 976 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 openssh-server amd64 1:9.2p1-2+deb12u5 [457 kB]
457 ko réceptionnés en 0s (8 730 ko/s)
Préconfiguration des paquets...
Sélection du paquet openssh-server précédemment désélectionné.
(Lecture de la base de données... 154756 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../openssh-server_1%3a9.2p1-2+deb12u5_amd64.deb ...
Dépaquetage de openssh-server (1:9.2p1-2+deb12u5) ...
Paramétrage de openssh-server (1:9.2p1-2+deb12u5) ...
rescue-ssh.target is a disabled or a static unit not running, not starting it.
ssh.socket is a disabled or a static unit not running, not starting it.
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
```

Nous nous assurons ensuite que le service SSH est bien démarré sur notre machine Linux.

```
user@debian:~$ systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-04-28 19:22:16 CEST; 1min 17s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
    Main PID: 5290 (sshd)
      Tasks: 1 (limit: 4590)
    Memory: 1.4M
       CPU: 14ms
    CGroup: /system.slice/ssh.service
            └─5290 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

Nous pouvons désormais configurer une règle sur notre Pare-Feu IPFIRE à l'aide de l'interface graphique sur le navigateur. Lors de la première connexion à l'interface nous rentrons les informations de l'utilisateur **admin**. Puis nous nous rendons dans **Pare-Feu > Règles de pare-feu > Nouvelle règle** pour configurer une règle.



Puis nous configurons une redirection de port pour pouvoir accéder à notre machine Linux en SSH via une autre machine.

Règles de pare-feu ⓘ

Source

☒ Adresse source (adresse MAC/IP ou réseau) :

☐ Firewall Tous

☐ Réseaux standards : ROUGE

☐ Localisation A1 - Anonymous Proxy

NAT

☒ Utiliser la traduction d'adresses réseau (NAT)

☒ Destination NAT (redirection de port)

☐ Source NAT

Interface pare-feu: - Automatique -

Destination

☒ Adresse IP de destination (adresse IP ou réseau) :

☐ Firewall Tous

☐ Réseaux standards : ROUGE

☐ Localisation A1 - Anonymous Proxy

Protocole

TCP

Port source :

Port de destination :

Port externe (NAT):

Paramètres additionnels

Remarque :

Position de règle :

☐ Journalisation de la règle

☐ Enable SYN Flood Protection (TCP only)

☐ Utiliser les contraintes horaires

☐ Limiter les connexions simultanées par adresse IP

☐ Limiter le nombre des nouvelles connexions

Ajouter Retour

Après avoir ajouté cette nouvelle règle nous appliquons les changements

Règles de pare-feu ?



Sur une machine de notre réseau local nous pouvons nous rendre dans un terminal pour initialiser une connexion SSH vers notre machine Linux. **ssh user@adresse_ip_red**

Pour une première connexion SSH notre machine du réseau local ne connaît pas le fingerprint de la machine Linux.

Nous pouvons vérifier qu'il s'agit bien de notre machine Linux en tapant la commande : **ip a** pour obtenir l'adresse IP. Dans notre cas l'adresse IP est bien celle que nous avons obtenus par **IPFIRE**

```
user@debian: ~  
C:\Users\Moi>ssh user@192.168.0.253  
The authenticity of host '192.168.0.253 (192.168.0.253)' can't be established.  
ED25519 key fingerprint is SHA256:exHCntAzUIk4+Wg8Cnc6fkIrrlwe+Ea3rD8UvHJvz8g.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.0.253' (ED25519) to the list of known hosts.  
user@192.168.0.253's password:  
Linux debian 6.1.0-33-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.133-1 (2025-04-10) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
user@debian:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:ea:17:3d brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.1.10/24 brd 192.168.1.255 scope global dynamic noprefixroute ens33  
        valid_lft 2282sec preferred_lft 2282sec  
    inet6 fe80::20c:29ff:feea:173d/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
user@debian:~$
```