

DynFi 3.0 Configurer des règles DNAT SSH/HTTP

MODULE 3

DynFi[®]

DYNAMIC FIREWALLS

SOMMAIRE

- 1. CONFIGURER UN REGLE SSH DANS LE PARE-FEU DYNFI**
 - a. Installation des services SSH sur Debian
 - b. Modification du port SSH
 - c. Ajout d'un utilisateur au groupe "sudo"
 - d. Création d'une règle d'accès SSH dans DynFi
- 2. CONFIGURER UNE REGLE HTTP DANS LE PARE-FEU DYNFI**
 - a. Installation du serveur web Apache 2.4 sur Debian
 - b. Création d'une règle d'accès HTTP dans DynFi
 - c. Test d'accès au serveur web depuis l'extérieur

© tutos-info.fr - 07/2024

DIFFICULTE



UTILISATION COMMERCIALE INTERDITE

Note importante :

Pour réaliser ce tutoriel, vous devez avoir suivi les 2 premiers modules (voir sur <https://tutos-info.fr>), à savoir :

- création d'un routeur DynFi avec 2 interfaces réseau WAN + LAN
- un accès au routeur (soit depuis une machine du réseau LAN, soit depuis l'interface WAN)

Notre environnement de travail, ici, est Proxmox mais ce tutoriel est transposable à d'autres logiciels de virtualisation (Virtualbox, vmWare Player).

1 – CREATION D'UNE REGLE SSH DANS LE PARE-FEU DE DYNFI 3.0

Dans ce tutoriel nous allons expliquer comment accéder en SSH à une machine Debian connectée sur l'interface LAN de notre réseau (pour rappel, nous avons configuré un routeur DynFi avec une interface WAN et une interface LAN).

- Créez une machine virtuelle Debian 12 et connectez-la au "vubr" correspondant à l'interface LAN de votre routeur DynFi. (le "vubr6" ici correspond à l'interface "LAN" de notre machine DynFi) :

	Ajouter ▾	Supprimer	Éditer	Action disque ▾	Revenir en arrière
Résumé					
Console					
Matériel					
Cloud-Init					
Options					
Historique des tâches					
Moniteur					
Sauvegarde					
Réplication					
Mémoire					2.00 Gio
Processeurs					2 (1 sockets, 2 cores) [x86-64-v2-AES]
BIOS					Par défaut (SeaBIOS)
Affichage					Par défaut
Machine					Par défaut (i440fx)
Contrôleur SCSI					VirtIO SCSI single
Lecteur CD/DVD (ide2)					local:iso/debian-12-6.iso,media=cdrom,size=631M
Disque dur (scsi0)					local:801/vm-801-disk-0.qcow2,discard=on,iosthread=1,size=32G
Carte réseau (net0)					virtio=BC:24:11:A3:F9:59,bridge=vubr6

- Installez Debian sur la machine puis lancez-la en vous connectant en tant que "root"

A – INSTALLATION DES SERVICES SSH SUR DEBIAN 12

- Installez les services SSH à l'aide de la commande suivante :

```
apt install openssh-server -y
```

- Assurez-vous que le service est en fonctionnement à l'aide de la commande suivante :

```
systemctl status ssh
```

B – MODIFICATION DU PORT SSH (par sécurité)

Par convention, le port SSH est défini sur "22". Ce port étant très connu des utilisateurs malveillants et des "bots", il est recommandé de le modifier par un port TCP supérieur à 1024.

Dans ce tutoriel, nous allons modifier le port d'écoute SSH par défaut (22) par le port 2220 par exemple.

- Editez le fichier `"/etc/ssh/sshd_config"` à l'aide de la commande suivante :

nano /etc/ssh/sshd_config

- Modifiez le port d'écoute en décommentant la ligne `"#Port"`, saisissez le nouveau port d'écoute SSH, quittez et sauvegardez les modifications (**CTRL + X – Oui – "Entrée"**) :

```
Port 2220
#AddressFamily any
#ListenAddress 0.0.0.0
```

- Relancez les services SSH avec la commande suivante :

systemctl restart ssh

- Vérifiez, avec la commande `"systemctl status ssh"` que le port modifié `"2220"` est bien en écoute :

```
root@debianlabo:~# systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Thu 2024-07-04 15:08:24 CEST; 4s ago
    Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 494 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 495 (sshd)
   Tasks: 1 (limit: 2305)
  Memory: 1.4M
     CPU: 19ms
  CGroup: /system.slice/ssh.service
          └─495 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

juil. 04 15:08:24 debianlabo systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
juil. 04 15:08:24 debianlabo sshd[495]: Server listening on 0.0.0.0 port 2220.
juil. 04 15:08:24 debianlabo sshd[495]: Server listening on :: port 2220.
juil. 04 15:08:24 debianlabo systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

C – AJOUT D'UN UTILISATEUR DEBIAN AU GROUPE "SUDO"

Par mesure de sécurité, il est vivement déconseillé d'autoriser l'accès SSH au `"root"` (super utilisateur du système). Il convient donc d'autoriser SSH à un utilisateur qui sera doté des droits `"sudo"` (droits privilégiés). Attention, les manipulations suivantes nécessitent d'être connecté en tant que `"root"` sur la machine Debian :

- Listez vos utilisateurs Debian avec la commande `"cat /etc/group"` et repérez un utilisateur auquel vous souhaitez affecter les droits `"sudo"`
- Saisissez la commande suivante : `"usermod -aG sudo debianxxx"` (debianxxx étant l'utilisateur)
- Vérifiez que votre utilisateur est bien dans le groupe `"sudo"` avec la commande suivante :

groups debianxxx

Logiquement le groupe `"sudo"` doit être affiché :

```
root@debianlabo:~# groups debianlabo
debianlabo : debianlabo cdrom floppy sudo audio dip video plugdev users netdev
```

- Installez `"sudo"` avec la commande suivante : `apt install sudo -y`

D – CREATION D'UNE REGLE D'ACCES SSH DEPUIS L'INTERFACE WAN DE DYNFI

Ici, nous souhaitons accéder à la machine Debian en SSH (avec l'utilisateur ayant les droits "sudo") depuis une machine externe au réseau local LAN virtuel et via l'interface WAN de DynFi. Pour cela, nous devons créer une règle DNAT qui autorisera le flux SSH à destination de la machine Debian du réseau LAN.

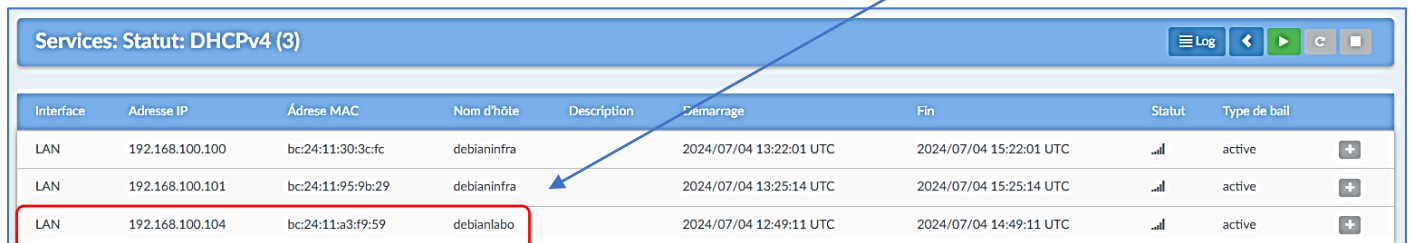
- Connectez-vous à votre console de gestion DynFi

Consultez l'adresse IP dynamique qui a été allouée à votre machine Debian par DynFi en consultant les services DHCP de DynFi :

- Cliquez "**Services**" – "**DHCPv4**" et cliquez sur "**LAN**"
- Cliquez le bouton "**Statut**" en haut à droite de la fenêtre :



Les "baux" DHCP s'affichent et notre machine "Debianlabo" a bien une IP dynamique locale (192.168.100.104 en ce qui nous concerne) :

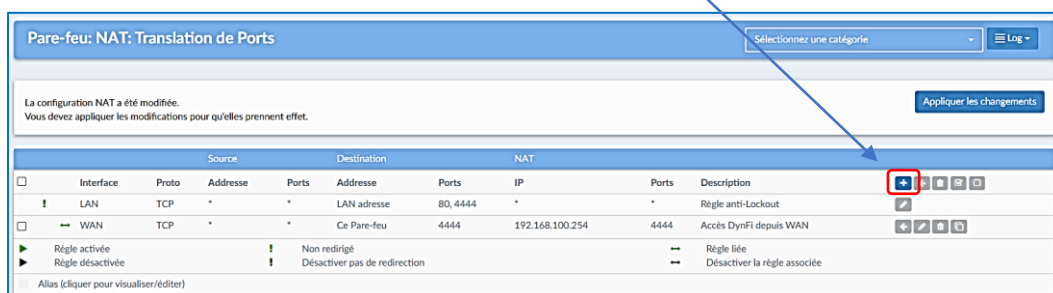


Interface	Adresse IP	Adresse MAC	Nom d'hôte	Description	Démarrage	Fin	Statut	Type de bail
LAN	192.168.100.100	bc:24:11:30:3cfc	debianinfra		2024/07/04 13:22:01 UTC	2024/07/04 15:22:01 UTC	📶	active
LAN	192.168.100.101	bc:24:11:95:9b:29	debianinfra		2024/07/04 13:25:14 UTC	2024/07/04 15:25:14 UTC	📶	active
LAN	192.168.100.104	bc:24:11:a3:f9:59	debianlabo		2024/07/04 12:49:11 UTC	2024/07/04 14:49:11 UTC	📶	active

Note : vous pouvez aussi vous connecter à votre machine Debian et saisir la commande "**ip a**" pour vérifier l'adresse dynamiquement allouée (192.168.100.104) :

```
root@debianlabo:~# 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: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:a3:f9:59 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.100.104/24 brd 192.168.100.255 scope global dynamic ens18
        valid_lft 4792sec preferred_lft 4792sec
    inet6 fe80::be24:11ff:fea3:f959/64 scope link
        valid_lft forever preferred_lft forever
```

- Dans la console de gestion DynFi, cliquez "**Pare-feu**" – "**NAT**" – "**Translation de ports**"
- Dans la fenêtre qui s'affiche, cliquez le petit "+" sur fond bleu pour créer une nouvelle règle :



- Configurez la règle DNAT ainsi :

Pare-feu: NAT: Translation de Ports Log ▾

Modifier entrée de Redirection aide complète 🟢

🔴 Désactivé Désactiver cette règle
Sélectionnez cette option pour désactiver cette règle sans la retirer de la liste.

🔴 Pas de RDR (SANS)
Activer cette option permet de désactiver la redirection du trafic correspondant à cette règle.
Suggestion : dans la plupart des cas, vous devriez utiliser WAN ici.

🔴 Interface WAN
Choisissez sur quelle interface cette règle sera appliquée.
Suggestion : dans la plupart des cas, vous devriez utiliser WAN ici.

🔴 Version TCP/IP IPv4
Sélectionnez la version d'IP qui s'applique à cette règle.

🔴 Protocole TCP
Choisissez à quel protocole IP cette règle doit correspondre.
Suggestion : dans la plupart des cas, vous devriez spécifier TCP ici.

On sélectionne, ici, l'interface des flux entrants en l'occurrence la "WAN", et le protocole TCP (IPv4) concerné.

Source Avancés
Afficher l'adresse source et la plage de ports

🔴 Destination / Inverseur
Cette option permet d'inverser le sens de la correspondance.

🔴 Destination WAN adresse

🔴 Plage de ports de destination
(autres) (autres)
Lors de l'utilisation des protocoles TCP ou UDP, spécifiez le port ou la plage de ports destination pour cette correspondance.

On indique, ici, la plage de ports concernés par la règle DNAT (ici le port 2220).

🔴 Rediriger l'IP de destination Hôte unique ou Réseau
192.168.100.104
Indiquez l'adresse IP interne du serveur sur lequel vous souhaitez accéder.
ex. 192.168.1.12

On indique, ici, l'IP de destination (en l'occurrence la machine du réseau LAN sur laquelle on souhaite accéder en SSH).

🔴 Rediriger le port cible (autres)
Indiquez le port de la machine correspondant à l'adresse IP de destination.
Suggestion : ceci est généralement identique au port 'de début' renseigné précédemment.

On indique, ici, le port TCP concerné (pour rappel nous avons modifié le port d'écoute SSH de 22 à 2220).

- Saisissez une brève description de la règle :

🔴 Description On saisit, ici, une brève description de la règle DNAT créée.
Vous pouvez saisir ici une description à titre de référence.

- Cliquez le bouton "Sauvegarde" :

Sauvegarde Annuler

Un message s'affiche et indique que des modifications ont été détectées, cliquez le bouton "Appliquer les changements" pour que la règle soit activée :

La configuration NAT a été modifiée.
Vous devez appliquer les modifications pour qu'elles prennent effet.

Appliquer les changements

La nouvelle règle s'affiche :

	Interface	Proto	Source		Destination		NAT		Description	
			Adresse	Ports	Adresse	Ports	IP	Ports		
<input type="checkbox"/>	LAN	TCP	*	*	LAN adresse	80, 4444	*	*	Règle anti-Lockout	
<input type="checkbox"/>	WAN	TCP	*	*	Ce Pare-feu	4444	192.168.100.254	4444	Accès DynFi depuis WAN	
<input type="checkbox"/>	WAN	TCP	*	*	WAN adresse	2220	192.168.100.104	2220	Accès Debian SSH via WAN	

! Règle activée
! Règle désactivée

! Non redirigé
! Désactiver pas de redirection

↔ Règle liée
↔ Désactiver la règle associée

Alias (cliquer pour visualiser/éditer)

- Testez l'accès SSH à votre machine Debian (connectée à l'interface LAN de votre routeur DynFi) en procédant ainsi :
 - Ouvrez un terminal sur votre machine Windows (**Windows + R – cmd**)
 - Saisissez la commande (**avec le port SSH modifié**) "**ssh debianxxx@ipWAN -p 2220**"

Si la connexion est acceptée, un échange de clés est proposé ; saisissez "yes" et pressez "Entrée" :

```
C:\Users\pc>ssh debianlabo@212.83.149.1 -p 2220
The authenticity of host '[212.83.149.1]:2220 ([212.83.149.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:EbgdFNY5ZkrAgCzEkr4i+m/eJVdBbZxRr65pt4GjFhI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

- Saisissez le mot de passe de votre machine Debian et pressez la touche "Entrée" :

```
Warning: Permanently added '[212.83.149.1]:2220' (ED25519) to the list of known hosts.
debianlabo@212.83.149.1:~$
```

- Vous êtes logué(e) en SSH sur votre machine Debian ; si vous saisissez la commande "**ip a**" vous pouvez vérifier que l'IP est bien celle de votre machine locale :

```
debianlabo@debianlabo:~$ 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: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether bc:24:11:a3:f9:59 brd ff:ff:ff:ff:ff:ff
   altname enp0c18
   inet 192.168.100.104/24 brd 192.168.100.255 scope global dynamic ens18
       valid_lft 6268sec preferred_lft 6268sec
   inet6 fe80::be24:11ff:fea3:f959/64 scope link
       valid_lft forever preferred_lft forever
debianlabo@debianlabo:~$
```

- Saisissez la commande "**exit**" et pressez la touche "Entrée" pour quitter la session SSH :

```
debianlabo@debianlabo:~$ exit
```

2 – ACTIVATION D'UN SERVEUR WEB APACHE 2 ET CREATION DE LA REGLE DNAT DANS DYNFI 3.0

Dans cette partie, nous allons installer un serveur web Apache 2.4 sur notre machine Debian connectée à l'interface LAN du routeur DynFi et nous testerons l'accès depuis l'interface WAN en créant une règle DNAT dans le pare-feu.

A – INSTALLATION DU SERVEUR WEB

- Connectez-vous sur votre machine Debian (en SSH) avec l'utilisateur ayant les droits "sudo"
- Installer le serveur web Apache 2.4 à l'aide de la commande suivante :

```
sudo apt install apache2 -y
```

```
debianlabo@debianlabo:~$ sudo apt install apache2 -y
[sudo] Mot de passe de debianlabo : |
```

- Vérifiez que votre serveur web est bien actif avec la commande "systemctl status apache2" :

```
debianlabo@debianlabo:~$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Thu 2024-07-04 16:16:59 CEST; 28s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 1178 (apache2)
    Tasks: 55 (limit: 2305)
  Memory: 9.4M
     CPU: 35ms
   CGroup: /system.slice/apache2.service
           └─1178 /usr/sbin/apache2 -k start
             └─1179 /usr/sbin/apache2 -k start
               └─1180 /usr/sbin/apache2 -k start
```

B – CREATION DE LA REGLE DNAT POUR ACCEDER AU SERVEUR WEB DEPUIS L'INTERFACE WAN DE DYNFI

- Connectez-vous à la console de gestion DynFi
- Cliquez "Pare-feu" – "NAT" – "Translation de ports"
- Cliquez le petit "+" sur fond bleu (en haut à droite de la fenêtre) et configurez la règle DNAT :

❌ Désactivé Désactiver cette règle
Sélectionnez cette option pour désactiver cette règle sans la retirer de la liste.

❌ Pas de RDR (SANS)
Activer cette option permet de désactiver la redirection du trafic correspondant à cette règle.
Suggestion : cette option est rarement nécessaire, ne l'utilisez pas sauf si vous savez ce que vous faites.

📌 Interface
Choisissez sur quelle interface cette règle sera appliquée.
Suggestion : dans la plupart des cas, vous devriez utiliser WAN ici.

📌 Version TCP/IP
Sélectionnez la version d'IP qui s'applique à cette règle.

📌 Protocole
Choisissez à quel protocole IP cette règle doit correspondre.
Suggestion : dans la plupart des cas, vous devriez spécifier TCP ici.

Source
Afficher l'adresse source et la plage de ports

📌 Destination / Inverseur
Cette option permet d'inverser le sens de la correspondance.

📌 Destination

📌 Plage de ports de destination
Lors de l'utilisation des protocoles TCP ou UDP, spécifiez le port ou la plage de ports destination pour cette correspondance.

Rediriger l'IP de destination

Hôte unique ou Réseau

192.168.100.104

Indiquez l'adresse IP interne du serveur sur lequel vous souhaitez accéder au serveur web Apache (en spécifiant le port 80 "http").
ex. 192.168.1.12

Rediriger le port cible

HTTP

Indiquez le port de la machine correspondante à l'adresse IP de destination (le port de fin sera calculé automatiquement).
Suggestion : ceci est généralement identique au port de destination.

Description

Accès serveur web Apache

Vous pouvez saisir ici une description à titre de référence.

Définir une balise locale

Vous pouvez marquer un paquet correspondant à cette règle et utiliser cette marque pour faire correspondre d'autres règles NAT / filtre.

Correspondance du tag local

Vous pouvez faire correspondre un paquet à une marque placée précédemment sur une autre règle.

Pas de Sync XMLRPC

Astuce : Cela empêche la règle sur le Maître de se synchroniser automatiquement avec les autres membres CARP. Cela n'empêche PAS l'écrasement de la règle sur l'Esclave.

Réflexion NAT

Utiliser les paramètres système par défaut

Association de règle de filtrage

Rule Accès serveur web Apache

Information de la règle

Créé(e) le 4/7/24 16:24:36 (root@78.243.49.182)

Mise à jour le 4/7/24 16:24:36 (root@78.243.49.182)

Sauvegarde Annuler

On indique, ici, l'IP de destination (en l'occurrence la machine du réseau LAN sur laquelle on souhaite accéder au serveur web Apache (en spécifiant le port 80 "http").

On saisit, ici, une brève description de la règle DNAT créée.

- Cliquez le bouton "**Sauvegarde**" pour valider votre règle
- Cliquez le bouton "**Appliquer les changements**" pour activer la règle :

La configuration NAT a été modifiée.
Vous devez appliquer les modifications pour qu'elles prennent effet.

Appliquer les changements

La règle DNAT pour permettre l'accès à votre serveur web s'affiche :

	Source	Destination	NAT		Description					
	Interface	Proto	Adresse	Ports	Adresse	Ports	IP	Ports		
<input type="checkbox"/>	LAN	TCP	*	*	LAN adresse	80, 4444	*	*	Règle anti-Lockout	
<input type="checkbox"/>	WAN	TCP	*	*	Ce Pare-feu	4444	192.168.100.254	4444	Accès DynFi depuis WAN	
<input type="checkbox"/>	WAN	TCP	*	*	WAN adresse	2220	192.168.100.104	2220	Accès Debian SSH via WAN	
<input type="checkbox"/>	WAN	TCP	*	*	WAN adresse	80 (HTTP)	192.168.100.104	80 (HTTP)	Accès serveur web Apache	
<input checked="" type="checkbox"/>	Règle activée		!		Non redirigé		--		Règle liée	
<input type="checkbox"/>	Règle désactivée		!		Désactiver pas de redirection		--		Désactiver la règle associée	

- Testez l'accès à votre serveur web depuis une machine externe. Pour cela, ouvrez un navigateur et saisissez l'adresse IP WAN de votre routeur DynFi : <http://ipWAN> (en http car nous ne gérons pas ici le protocole HTTPS !) ; la page par défaut du serveur web Apache doit s'afficher :

