

Ajout d'un routeur pfSense

On ajoute un routeur à notre configuration, opérant comme une box ADSL. Cette VM, basée sur FreeBSD, est gérée au moyen d'une interface web pour router et filtrer des paquets du WAN vers l'interface LAN. Il nous permettra de faire du NAT/Port Forwarding vers la `lxle`¹. On finira par des aspects plus "joueurs".

1 Installation

Téléchargez l'ISO de pfSense 2.7.2 (Community Edition). Allouez 3Go de disque, activez 2 interfaces réseau, une en NAT (ou équivalent VirtualBox²), l'autre en host only (ou Internal Network de VirtualBox) sans dhcp. J'ai dû créer un nouveau réseau virtuel sans serveur dhcp pour déléguer ce service à pfSense. 512Mo de RAM et un cœur suffisent. Procédez à l'installation en Auto UFS / GPT. Une fois l'installation terminée et le routeur redémarré, il reste quelques problèmes à résoudre pour accéder à l'interface de gestion web qui n'est normalement accessible que depuis une machine du LAN.

Notez bien l'adresse WAN (connectée sur votre NAT) qui devra correspondre à l'interface `em0` et l'adresse LAN (connectée en host only) correspondant à l'interface `em1`. L'adresse LAN est définie par l'interface réseau virtuelle activée par votre gestionnaire de VM (sur mes exemples, l'adresse LAN est 192.168.40.0).

1.1 Clavier français et accès web

Pour avoir un clavier français, depuis le menu principal de la console, faire le choix 8) Shell puis saisir la commande :

```
root: kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.acc.kbd
```

Il vous sera ensuite possible de saisir plus facilement la commande qui permet de désactiver le firewall et d'autoriser la connexion sur l'interface de gestion web depuis le WAN :

```
root: pfctl -d
```

Vous devriez alors avoir accès à l'interface de gestion web depuis le WAN. Essayez depuis un navigateur de votre machine physique. Le login/mdp par défaut de pfSense est admin/pfsense.

1.2 Premiers pas

Le Setup wizard démarre automatiquement. Saisissez les informations demandées avec comme nom de domaine `cs.sr`, choisissez 1.1.1.1 pour le DNS primaire et 8.8.8.8 pour le secondaire³. À l'étape 4, décochez seulement le blocage des réseaux privés et des bogon nets tels que spécifiés par la RFC1918, mettez à jour l'adresse IP du LAN telle que définie par votre gestionnaire de machine virtuelle (en prenant en compte que certains attribuent la première adresse réseau à la machine physique). Changez le mot de passe admin à l'étape 6 et vous êtes prêt à utiliser votre routeur. À la fin de la configuration par le Setup wizard, vous serez peut-être déconnecté de l'interface web du routeur par le firewall. Pour y accéder à nouveau, saisissez à nouveau `pfctl -d` dans la console.

Une fois reconnecté, changez la configuration du clavier de façon pérenne : installez le paquet `Shellcmd` (choix System/Package Manager des menus). Sélectionnez ensuite Services/Shellcmd et remplissez les champs :

```
Command : kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbd
```

```
Shellcmd Type : shellcmd
```

```
Description : clavier azerty
```

Installez aussi le paquet `open-vm-tools`. Au redémarrage, la console utilisera le clavier français.

Il faut ensuite ajouter les règles de firewall pour autoriser l'accès au serveur web de pfsense depuis un navigateur de votre machine physique connectée sur le WAN. Je me suis inspiré du [tutoriel](#) pour ajouter les règles de firewall qui devraient apparaître comme ci-dessous :

1. J'ai conservé le nom `lxle` pour me conformer aux captures écran.

2. Reportez-vous éventuellement à un [tutoriel](#).

3. Sur le réseau de l'université, le dns est 134.59.1.7

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 2 / 48 KIB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			  
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			  

2 Configuration minimale

Le routeur nous permet d'avoir un serveur dhcp et un serveur dns pour les machines du LAN.

2.1 Activer le dhcp

Choisissez le menu `Services/DHCP Server` et mettez à jour les informations du LAN cf. ci-dessous :

General Options	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny unknown clients	<input type="text" value="Allow all clients"/> <p>When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.</p>
Ignore denied clients	<input type="checkbox"/> Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers	<input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Subnet	192.168.40.0
Subnet mask	255.255.255.0
Available range	192.168.40.1 - 192.168.40.254
Range	<input type="text" value="192.168.40.10"/> <input type="text" value="192.168.40.245"/> From To

Ajoutez au besoin dans `DNS Servers` l'adresse LAN du routeur, mettez à jour le `Domain name` : `cs.sr` et ajoutez tout en bas dans la partie `DHCP Static Mappings for this Interface` votre machine `lxle` avec son adresse MAC et l'adresse IP que vous lui destinez.

DHCP Static Mappings for this Interface (total: 2)					
Static ARP	MAC address	Client Id	IP address	Hostname	Description
	f2:18:98:3f:bc:65	pfsense	192.168.40.1	pfsense	 
	00:0c:29:d8:0a:9a	lxle	192.168.40.2	lxle	 

2.2 Activer le dns

Attention ! le dns que nous allons activer ne servira que la zone locale côté LAN. Tout l'adressage côté WAN restera sans résolution de nom.

Choisissez dans le menu `Services/DNS Resolver`. Celui-ci est normalement activé et il n'y a que des modifications à y apporter. Je n'ai fait que cocher les options `Enable DNS resolver`, `Enable Forwarding Mode`, `Register DHCP static mappings in the DNS Resolver` et ajouté nos machines dans la rubrique `Host Overrides` comme ci-dessous (mon nom de domaine est `cs.sr`) :

Host Overrides				
Host	Parent domain of host	IP to return for host	Description	Actions
lxle	cs.sr	192.168.40.2	lxle	 
pfsense	cs.sr	192.168.40.1	pfsense	 

A la fin de la page de configuration, vous devez trouver un bouton “Dislay/Hide Custom Options” qui permet d’ajouter un champ MX (pour le mail) en ajoutant les commandes comme décrit ci-dessous (normalement la première ligne n’est pas utile) :

```

Custom options
server: local-zone: "cs.sr" type:transparent
server: local-data: "cs.sr IN MX 10 lxle.cs.sr."
server: local-data: "lxle.cs.sr IN A 192.168.40.2"

```

Enter any additional configuration parameters to add to the DNS Resolver configuration here, separated by a newline.

3 Utilisation

3.1 Test de bon fonctionnement

Il est temps de vérifier le bon fonctionnement ! Pour cela, sur votre gestionnaire de VM, changez la configuration de l’interface réseau de votre lxle connectée en NAT au TP1 pour la mettre sur l’interface virtuelle Host Only. Sa nouvelle configuration réseau sera alors compatible avec le LAN de votre routeur. Si tout s’est bien passé, après le boot de lxle, celle-ci devrait acquérir une IP assignée par le serveur dhcp du routeur que vous avez spécifiée en activant le dhcp par le mappage statique. Vérifiez par un ifconfig sur la lxle votre IP puis le fonctionnement du dns par dig

- sur la zone locale en cherchant l’IP du routeur ;
- sur une machine extérieure (p.e. du domaine univ-cotedazur.fr).

3.2 Activer un NAT/Port forwarding

L’intérêt d’un routeur est de pouvoir associer un service LAN à une IP WAN. Si le premier TP a été correctement finalisé, vous devriez avoir des services actifs sur la lxle pour http(s) en écoute sur les ports 80 et 443. Nous allons faire en sorte que toute requête sur pfsense.8080 soit redirigée vers lxle.80 et celles sur pfsense.1443 soient redirigées vers lxle.443. Le firewall va réaliser cette traduction d’adresse en choisissant l’entrée du menu Firewall/NAT pour arriver à la configuration :

Rules										
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	8080	192.168.40.2	80 (HTTP)		 
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	1443	192.168.40.2	443 (HTTPS)		 

Vérifiez le bon fonctionnement de ces règles de traduction d’adresse réseau en vous connectant depuis un navigateur de votre machine physique (en http et https) pour voir le formulaire de connexion du TP1.

4 Reconnaissance

Une phase importante du pentesting est la phase de reconnaissance qui est facilité par la kali. Démarrez-la et faites une reconnaissance du réseau du côté WAN du routeur pour trouver les machines actives, une détection de leur OS et les ports ouverts.

Une fois trouvé le(s) port(s) web, retrouvez le serveur correspondant et son numéro de version.

Connectez ensuite votre kali côté LAN et faites une reconnaissance comparable. Notez les différences...