Plateforme de formation - Doc Admin OPNSense

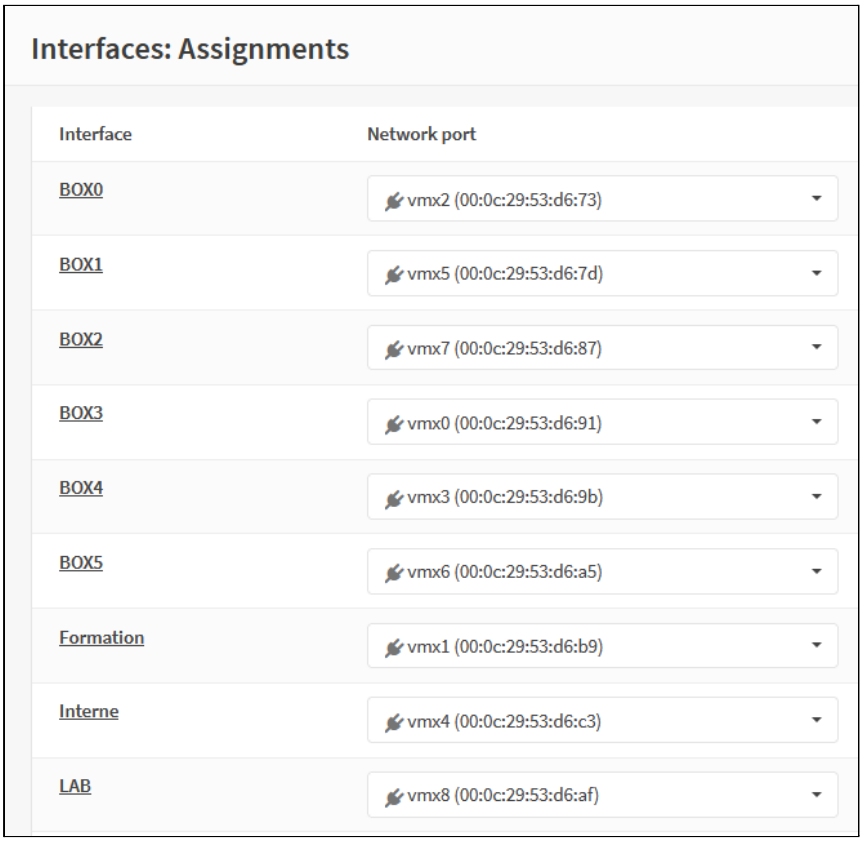
PROHACKTIVE

Mathis Scaffidi Fonti

Sommaire

- Configuration des interfaces

Interfaces -> Assignments :



- Définition de la connexion à l'interface OPNSense

System → Settings → Administration :

- **TCP port** : port d'écoute d'OPNSense (ici : 8443)
- **DNS Rebind Check** : Lorsque cette option n'est pas cochée, votre système est protégé contre les attaques DNS Rebinding. Cela bloque les réponses IP privées de vos serveurs DNS configurés.
- **HTTP_REFERER** enforcement : Lorsque cette case n'est pas cochée, l'accès à l'interface graphique Web est protégé contre les tentatives de redirection **HTTP_REFERER**. Il est utile de cocher cette case dans certains cas particuliers, comme l'utilisation de scripts externes pour interagir avec ce système.
- **Listen interfaces** : interface sur laquelle doit écouter d'OPNSense (ici : toutes)

- Configuration IP des interfaces réseaux

Interfaces -> <nomInterface> :
Enable : branchement de l'interface
Description : nom de l'interface
IPv4 Configuration Type : choix de l'ip de l'interface (static ou attribution DHCP)

Si IPv4 Configuration Type = Static IPv4 :
IPv4 address : Définition de l'IP de l'interface
IPv4 Upstream Gateway : choix de l'auto détection de la passerelle

BOX<n°> : static -> 10.255.<n°>.254
Formation : static -> 172.17.0.126
Interne : static -> 10.220.0.254
LAB : DHCP

- Serveurs DHCP

Services -> DHCPv4 -> <nomInterface> :
Enable : lancement du serveur DHCP
Range : définition d'un range d'adresse IP que le serveur DHCP va pouvoir distribuer

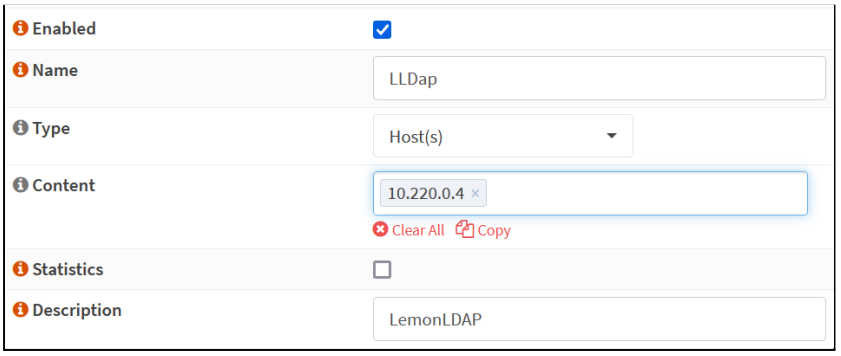
Services -> DHCPv4 -> <nomInterface> -> DHCP Static Mappings for this interface :
MAC address : renseigner l'adresse MAC de la machine cible
IP address : définition de l'adresse IP statique de la machine cible
Hostname : hostname de la machine cible
Gateway : passerelle de la machine cible

Les réseaux suivants ont un serveur DHCP actifs : BOX[0-5] et Interne.
Le serveur DHCP interne comprend une IP statique (celle du LemonLDAP) :

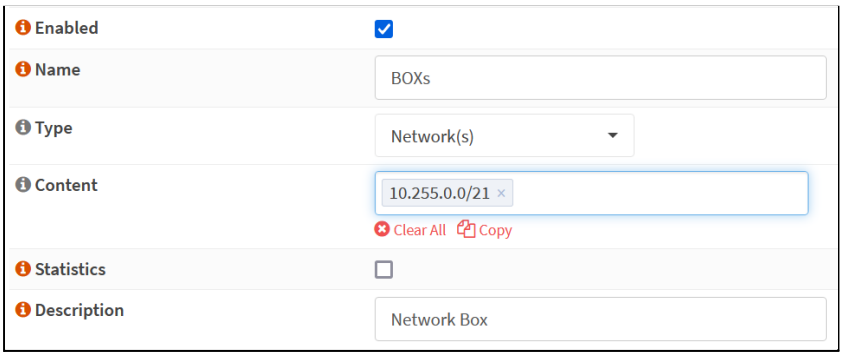
MAC address	IP address	Hostname	Description
00:0c:29:a2:cf:ca	10.220.0.4	lemonLDAP	LemonLDAP

- Pseudonymes (Aliases)

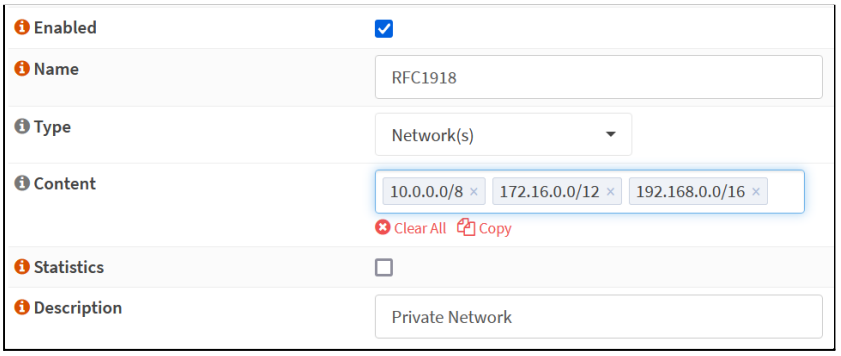
Firewall -> Aliases :



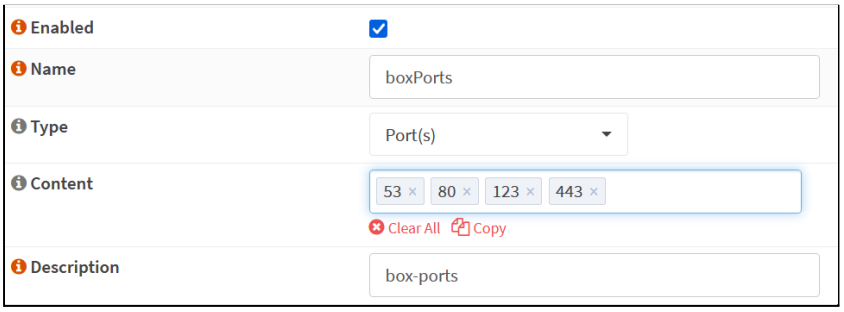
Ce pseudonyme renseigne l'IP de la vm LemonLDAP.



Ce pseudonyme regroupe tous les réseaux des boxes.



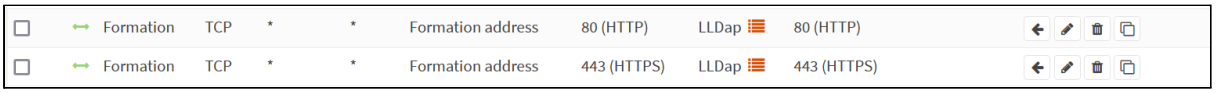
Ce pseudonyme regroupe toutes les adresses IP privées.



Ce pseudonyme regroupe les différents ports avec lesquels nous devons communiquer (53 : DNS, 80 : HTTP, 123 : NTP, 443 : HTTPS).

- Redirection LemonLDAP

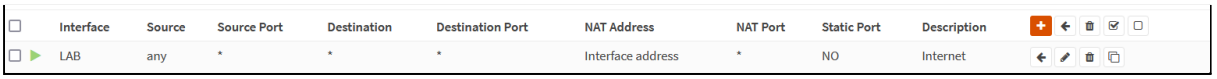
Firewall -> NAT -> Port Forward :
Quand l'utilisateur côté formation essaye de se connecter à l'IP de l'OPNSense, il est directement redirigée sur le LemonLDAP :



Règle 1 : Si l'utilisateur envoie une requête sur le port 80 de l'OPNSense, il est redirigé sur le port 80 du LemonLDAP.
Règle 2 : Si l'utilisateur envoie une requête sur le port 443 de l'OPNSense, il est redirigé sur le port 443 du LemonLDAP.

- Accès Internet

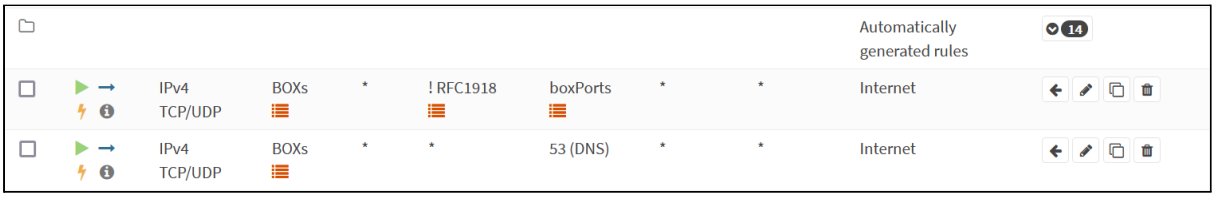
Firewall -> NAT -> NAT Outbound :



Cette règle permet de mapper tous les paquets sur l'adresse IP "interface address".

- Règles Firewall

1. Règles par défaut :
Firewall -> Rules -> Floating :

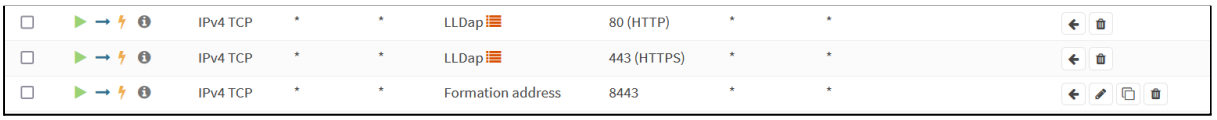


Règle 1 : permet aux réseaux des boxes de communiquer avec toutes les IP qui ne sont pas renseignées dans le pseudonyme RFC1918 (! - Destination / Invert).
Règle 2 : permet aux réseaux des boxes d'effectuer des requêtes DNS.

2. Règle relative aux réseaux des boxes :

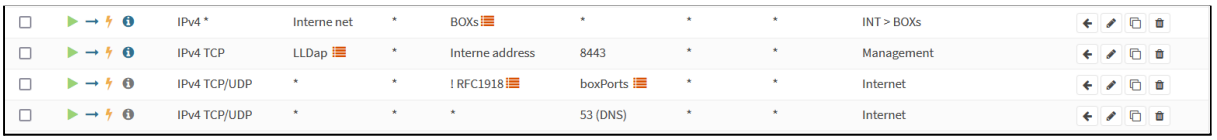
Le réseau de la boxe à accès au réseau LAB sur n'importe quel port.

3. Règles relatives au réseau formation :



Règle 1 et 2 : saisie automatiquement lors de la création de la redirection vers le LemonLDAP.
Règle 3 : permettre l'accès à l'IP de l'OPNSense sur le port 8443.

4. Règles relatives au réseau interne :



IPv4 *	Interne net	*	BOXs	*	*	*	INT > BOXs	
IPv4 TCP	LLDap	*	Interne address	8443	*	*	Management	
IPv4 TCP/UDP	*	*	! RFC1918	boxPorts	*	*	Internet	
IPv4 TCP/UDP	*	*	*	53 (DNS)	*	*	Internet	

Règle 1 : le réseau interne peut communiquer avec les réseaux des boxes sur n'importe quel port.
Règle 2 : le LemonLDAP peut communiquer avec l'IP de l'OPNSense sur le port 8443.
Règle 3 : le réseau interne peut communiquer avec toutes les IP qui ne sont pas renseignées dans le pseudonyme RFC1918 (! - Destination / Invert).
Règle 4 : le réseau interne peut effectuer des requêtes DNS.

5. Il n'y a pas de règles spécifiques au réseau LAB.

- Services de diagnostiques

Interfaces -> Diagnostics :