

**Plateforme de formation -
Doc Admin OPNSense**



PROHACTIVE

Sommaire

Configuration des interfaces	3
Définition de la connexion à l'interface OPNSense	3
Configuration IP des interfaces réseaux	4
Serveurs DHCP	4
Pseudonymes (Aliases)	5
Redirection LemonLDAP	6
Accès Internet	6
Règles Firewall	6
Services de diagnostics	7

- Configuration des interfaces

Interfaces -> Assignments :

Interfaces: Assignments	
Interface	Network port
BOX0	 vmx2 (00:0c:29:53:d6:73) ▼
BOX1	 vmx5 (00:0c:29:53:d6:7d) ▼
BOX2	 vmx7 (00:0c:29:53:d6:87) ▼
BOX3	 vmx0 (00:0c:29:53:d6:91) ▼
BOX4	 vmx3 (00:0c:29:53:d6:9b) ▼
BOX5	 vmx6 (00:0c:29:53:d6:a5) ▼
Formation	 vmx1 (00:0c:29:53:d6:b9) ▼
Interne	 vmx4 (00:0c:29:53:d6:c3) ▼
LAB	 vmx8 (00:0c:29:53:d6:af) ▼

- 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 :

Enabled	<input checked="" type="checkbox"/>
Name	LLDap
Type	Host(s)
Content	10.220.0.4 Clear All Copy
Statistics	<input type="checkbox"/>
Description	LemonLDAP

Ce pseudonyme renseigne l'IP de la vm LemonLDAP.

Enabled	<input checked="" type="checkbox"/>
Name	BOXs
Type	Network(s)
Content	10.255.0.0/21 Clear All Copy
Statistics	<input type="checkbox"/>
Description	Network Box

Ce pseudonyme regroupe tous les réseaux des boxes.

Enabled	<input checked="" type="checkbox"/>
Name	RFC1918
Type	Network(s)
Content	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 Clear All Copy
Statistics	<input type="checkbox"/>
Description	Private Network

Ce pseudonyme regroupe toutes les adresses IP privées.

Enabled	<input checked="" type="checkbox"/>
Name	boxPorts
Type	Port(s)
Content	53 80 123 443 Clear All Copy
Description	box-ports

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 redirigé sur le LemonLDAP :

<input type="checkbox"/>	→ Formation	TCP	*	*	Formation address	80 (HTTP)	LLDap	80 (HTTP)			
<input type="checkbox"/>	→ Formation	TCP	*	*	Formation address	443 (HTTPS)	LLDap	443 (HTTPS)			

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 :

<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description				
<input type="checkbox"/>	LAB	any	*	*	*	Interface address	*	NO	Internet				

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

- Règles Firewall

1. Règles par défaut :

Firewall -> Rules -> Floating :

<input type="checkbox"/>									Automatically generated rules			
<input type="checkbox"/>	→	IPv4	BOXs	*	! RFC1918	boxPorts	*	*	Internet			
<input type="checkbox"/>	→	IPv4	BOXs	*	*	53 (DNS)	*	*	Internet			

Règle 1 : permet aux réseaux des boîtes de communiquer avec toutes les IP qui ne sont pas renseignées dans le pseudonyme RFC1918 (! - Destination / Invert).

Règle 2 : permet aux réseaux des boîtes d'effectuer des requêtes DNS.

2. Règle relative aux réseaux des boîtes :

<input type="checkbox"/>	→	IPv4	*	*	LAB net	*	*	*	BOX > LAB			
--------------------------	---	------	---	---	---------	---	---	---	-----------	--	--	--

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

3. Règles relatives au réseau formation :

<input type="checkbox"/>	→	IPv4 TCP	*	*	LLDap	80 (HTTP)	*	*			
<input type="checkbox"/>	→	IPv4 TCP	*	*	LLDap	443 (HTTPS)	*	*			
<input type="checkbox"/>	→	IPv4 TCP	*	*	Formation address	8443	*	*			

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 :

<input type="checkbox"/>		IPv4 *	Interne net	*	BOXs	*	*	INT > BOXs			
<input type="checkbox"/>		IPv4 TCP	LLDap	*	Interne address	8443	*	Management			
<input type="checkbox"/>		IPv4 TCP/UDP	*	*	! RFC1918	boxPorts	*	Internet			
<input type="checkbox"/>		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 diagnostics

Interfaces -> Diagnostics :

Diagnostics
ARP Table
DNS Lookup
NDP Table
Netstat
Packet Capture
Ping
Port Probe
Trace Route