# Installation OPNSense



# Table des matières :

Configuration Windows :	3
Installation des logiciels	3
Formatage de la clé :	5
Configuration du Pare-feu via Tabby :	6
Tabby :	6
Bios	7
Installation de l'image Opensense	
Configuration OPNSense	
Changement du mot de passe Admin / langue	21
MDP Admin firewall	21
Changement de la langue	
Sauvegarde / restauration	24
Sauvegarde	24
Restauration	
Rester en mode usine	27
Sauvegarde	
Rester	
Restauration	
Configuration du webfiltering	
Configuration	
Activer le SSH	
Activer le SSH	
Test	

# **Configuration Windows :**

### Installation des logiciels

Il faut d'abord commencer par récupérer l'iso de opensense sur le site officiel (cliquer sur le lien ou il est marqué « Download » pour aller plus vite :



#### On fera attention à bien installer la version serial :

#### Fast download selector

#### Architecture

System architecture.

amd64

#### Select the image type:

~

- dvd: ISO installer image with live system capabilities running in VGA mode. On amd64, UEFI boot is supported as well.
   vga: USB installer image with live system capabilities running in VGA mode as GPT boot. On amd64, UEFI boot is supported as well.
- serial: USB installer image with live system capabilities running in serial console (115200) including UEFI support...
- nano: a preinstalled serial image for USB sticks, SD or CF cards as MBR boot. These images are 3G in size and automatically adapt to the installed media size after first boot. ~

serial

#### Mirror Location

OPNsense can be downloaded from a large range of mirrors located in different countries, you may want to select the fastest options for your location. LeaseWeb ~

Download

#### Checksum verification

Checksum files next to the images may not prove authenticity of images on any particular mirror. The checksums can also be found in the forum annoucements, mailing lists, blog posts or GitHub. Please double-check

OPNsense-24.7-serial-amd64.img.bz2 (SHA256) : a94207c3515389c3fab5c6d72eeda4951526f9f50f06794ad9a4c1478bc8e8d0

Puis on installe Tabby qui nous permettra de rentrer sur le pare-feu :



Ici on renseigne juste si le logiciel doit être installer sur tous les utilisateurs de la machine.

Installation de Tabby	—		×
Choisis les options d'installation Pour qui cette application doit-elle être installée ?			>
Choisis pour qui ce logiciel doit être accessible : pour tous les utilisateurs	ou juste	e pour toi	i?
O Pour tous ceux qui utilisent cet ordinateur (tous les utilisateurs)			
Nouvelle installation uniquement pour l'utilisateur actuel.			
Tabby 1.0.207 —	nt >	Ann	uler

# Formatage de la clé :

On commence par formater la clé en mettant L'iso télécharger précédemment (Le logiciel que l'on utilise ici est Rufus).

A Rufus 4.2.2074	- 0	×	1
Options de Périphérique			
Périphérique			
Ventoy (E:) [64 Go]		~	
Type de démarrage			
OPNsense-24.1-serial-amd64.img.bz2		I  ▼	
Schéma de partition	Système de destination		
GPT ~	UEFI (non CSM)	~ ?	
✓ Afficher les options de périphérique avance	ées		
Options de Formatage —			
Nom de volume			
Ventoy			
Système de fichiers	Taille d'unité d'allocation		+
Large FAT32 (Défaut) 🗸 🗸	32 kilo-octets (Défaut)	$\sim$	L
<ul> <li>Afficher les options de formatage avancées</li> </ul>	;		
Statut			
PRE	T		þr
Ø () 🌣 🗐			
	DEMARKER		
Image utilisée : OPNsense-24.1-serial-amd64.im	g.bz2		
Image utilisée : OPNsense-24.1-serial-amd64.im	g.bz2	×	
Image utilisée : OPNsense-24.1-serial-amd64.im	g.bz2	×	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique	g.bz2	×	(
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique Périphérique	g.bz2	×	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique Périphérique EFISYS (Disque 1) [64 Go]	g.bz2	×	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 <b>Options de Périphérique</b> Périphérique EFISYS (Disque 1) [64 Go] Type de démarrage	g.bz2	×	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique Périphérique EFISYS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2	g.bz2	× ~ •	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique Périphérique EFISYS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition	g.bz2 — — — — — — — — — — — — — — — — — — —	× ~ DN   <del>•</del>	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique Périphérique EFISYS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR	g.bz2 – Sýstème de destination BIOS (ou UEFI-CSM)	× • •	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique EFISYS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR V Afficher les options de périphérique avan	g.bz2 — — — — — — — — — — — — — — — — — — —	× ~ ОN   <del>-</del>	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique EFISYS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR V Afficher les options de périphérique avan Options de Formatage	g.bz2 — — — — — — — — — — — — — — — — — — —	× ~ ⊃N  ▼	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique Périphérique EFISYS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR Afficher les options de périphérique avan Options de Formatage — Nom de volume	g.bz2 — — — — — — — — — — — — — — — — — — —	× ~ ⊃	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique Périphérique EFISYS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR MBR MBR MBR MBR MBR MBR MBR	g.bz2 — — — — — — — — — — — — — — — — — — —	× ОN (+	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique Périphérique EFISYS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR Afficher les options de périphérique avan Options de Formatage — Nom de volume EFISYS Système de fichiers	g.bz2  Sýstème de destination BIOS (ou UEFI-CSM) cées Taille d'unité d'allocation	× ↓ ↓	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique EFISYS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR Afficher les options de périphérique avan Options de Formatage Nom de volume EFISYS Système de fichiers Large FAT32 (Défaut)	g.bz2 	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique Périphérique EFISYS (Disque 1) [64 Go] Type de démarage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR MBR Afficher les options de périphérique avan Options de Formatage FISYS Système de fichiers Large FAT32 (Défaut)	g.bz2 	× ~ ~ ~ ~	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique Périphérique EFISYS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR Afficher les options de périphérique avan Options de Formatage — Nom de volume EFISYS Système de fichiers Large FAT32 (Défaut) Afficher les options de formatage avancé Statut	g.bz2 	× ▼ ▼	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique EfISYS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR MBR Afficher les options de périphérique avan Options de Formatage EFISYS Système de fichiers Large FAT32 (Défaut)	g.bz2 — Sýstème de destination BIOS (ou UEFI-CSM)) ccées Taille d'unité d'allocation 32 kilo-octets (Défaut) es	× • •	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique EFISVS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR Afficher les options de périphérique avan Options de Formatage EFISVS Système de fichiers Large FAT32 (Défaut) Afficher les options de formatage avancé Statut	g.bz2 	X DN I	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique EFISYS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR Afficher les options de périphérique avan Options de Formatage EFISYS Système de fichiers Large FAT32 (Défaut) Afficher les options de formatage avancé Statut	g.bz2 		
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique EFISVS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR Afficher les options de périphérique avan Options de Formatage FISVS Système de fichiers Large FAT32 (Défaut) Afficher les options de formatage avancée Statut PR Statut	g.bz2 	DN V	
Image utilisée : OPNsense-24.1-serial-amd64.im Rufus 4.2.2074 Options de Périphérique EFISYS (Disque 1) [64 Go] Type de démarrage OPNsense-24.1-serial-amd64.img.bz2 Schéma de partition MBR Afficher les options de périphérique avan Options de Formatage — Nom de volume EFISYS Système de fichiers Large FAT32 (Défaut) Afficher les options de formatage avancé Statut PI © ① 章 I	g.bz2 G. SÉLECTION Système de destination BIOS (ou UEFI-CSM) cées Taille d'unité d'allocation 32 kilo-octets (Défaut) es SÉT DÉMARRER FERM		

# Configuration du Pare-feu via Tabby :

### Tabby:

Sur le logiciel tabby on change de port de connexion dans "Profilés & connections", on cherchera le Serial (COM7(Pour savoir quel port utiliser on peut aller dans le gestionnaire des périphériques et aller dans la catégorie « Ports (COM et LPT) »)).





On passera la vitesse de lecture a 9600 bauds (car cela correspond à la vitesse du bios mais non le reste de l'image).



### Bios

A savoir : Le BIOS est un programme indépendant, stocké dans la mémoire de la carte mère (du pare-feu), qui permet de tester et d'initialiser tous les périphériques au démarrage avant de charger le système d'exploitation

On cherchera donc à aller sur le bios, il faudra appuyer sur la console (on fait ça pour pouvoir faire un impute car si cette action n'est pas faite les touches presser ne sont pas pris en compte par le logiciel) puis sur F2 au moment du boot du pare-feu (sur l'image ci-dessous vous pouvez voir le moment ou il faut faire les actions).



Une fois sur l'étapes précédente réussie le BIOS s'ouvre. Pour commencer dans le BIOS pour activer le LAN ByPass sur les ports. (Le LAN ByPass est une fonction qui permet de garantir la continuité du trafic réseau en reliant directement deux ports LAN en cas de défaillance de l'appareil, assurant ainsi une connexion sans interruption.)

1 Serial: FTDI B0033LQ1	+ 🗇		ŝ	-	<
🔵 СОМ6 (9600)					
Aptio Setup Utilit Main Advanced Chips	ty - Copyright (C) 2013 Am set Boot Security Save	erican Megatrends, Inc. & Exit Server Mgmt			
BIOS Information BIOS Vendor Core Version Compliancy Project Version Build Date and Time	American Megatrends 4.6.5.4 UEFI 2.3.1; PI 1.2 3250E118 x64 02/12/2014 19:05:01	Choose the system  default language 			
Memory Information Total Memory	4096 MB (DDR3 1333)	 			
System Language     System Date	[English] [Mon 06/17/2024]	<pre>&gt;&gt;: Select Screen   ^v: Select Item   Enter: Select</pre>			
System Time     Access Level	[14:13:05] Administrator	+/-: Change Opt.    F1: General Help    F2: Previous Values			
   		F4: Save & Exit    ESC: Exit			
Version 2.15.1230	5. Copyright (C) 2013 Amer	ican Megatrends, Inc. AB			

Pour ce faire on ira dans : Advanced -> LAN ByPass Configuration-> LAN3 & LAN4, LAN5 & LAN6 ByPass et on les mettra en NO BYPASS



Consequent de la consequencia de la consequenci	1 Serial: FTDI B0033LQ1	+ 🖸		ŵ -	o x
Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.         Advanced         Orboard LAW ByPass Configuration       Set LAN3 and LAVA         LAN3 & LAWA ByPass [No ByPass]       ByPass capability.         LAN5 & LAN6 ByPass [No ByPass]       ByPass setting, molify         Lis & LAN6 ByPass [No ByPass]       ByPass setting.         Version 2.15.1236. Copyright (C) 2013 American Megatrends, Inc.	🔵 СОМ6 (9600)				🐺 Unpin
Onboard LAW ByPass Configuration       Set LAW3 and LAW4         LAW3 & LAW6 ByPass       [No ByPass]         LAW5 & LAW6 ByPass       [No ByPass]         ByPass capability.       Luser AP setting, will use user AP setting.         LAW5 & LAW6 ByPass       [No ByPass]         ByPass setting.       Luser AP setting.         X: Select Screen       X: Select Screen         Y: Select Item       Enter: Select         H*: Charge Opt.       F1: General Help         F2: Previous Values       F3: Optimized Defaults         F3: Set kit       ESC: Exit         Version 2.15.1236. Copyright (C) 2013 American Megatrends, Inc.       AB	Aptio Setup Utility Advanced	- Copyright (C) 2013 Amer	ican Megatrends, Inc.		
+: Change Opt.  F1: General Help  F2: Previous Values  F3: Optimized Defaults  F4: Save & Exit  ESC: Exit Version 2.15.1236. Copyright (C) 2013 American Megatrends, Inc. AB	Onboard LAN ByPass Conf LAN3 & LAWA ByPass LAN5 & LAN6 ByPass	iguration [No ByPass] [No ByPass]	Set LAN3 and LAN4 [ByPass capability. [Bypass setting will use luser AP setting, modify this item will clear [user AP setting. 		
	Version 2.15.1236.	Copyright (C) 2013 Americ	+/:: Change Opt.    F1: General Help    F2: Previous Values    F3: Optimized Defaults    F3: Optimized Defaults    F4: Save & Exit    ESC: Exit     Am Megatrends, Inc. AB		

Puis on ira dans la page « Boot », on sélectionnera avec la touche « Entre » et on montera la clé USB en première position dans Boot option Priorities, ensuite on ira dans la catégorie « Hard drive BBS priorities » ou on montera la clé en première option de la même manière que l'on a fait précédemment.

	Aptio Setup Utility Main Advanced Chipse	- Copyright (C) 2013 Ameri t Boot Security Save & E	can Megatrends, Inc. xit Server Mgmt
/-     	Boot Configuration Setup Prompt Timeout Bootup NumLock State	3 [0n]	Sets the system boot
	Quiet Boot Fast Boot	[Disabled] [Disabled]	
i.	Boot Option Priorities		
i.	Boot Option #1	[UEFI: SanDisk SanDi]	
i.	Boot Option #2	[P4: HGST HTE725032A]	<pre>&gt;&lt;: Select Screen</pre>
Ì.	Boot Option #3	[UEFI: Built-in EFI]	^v: Select Item
			Enter: Select
	Hard Drive BBS Prioriti	es	+/-: Change Opt.
>	CSM16 Parameters		F1: General Help
	CSM parameters		F2: Previous Values
			F3: Optimized Defaults
			F4: Save & Exit
			ESC: Exit
/-	Voncion 2 15 1226	Converight (C) 2012 Amonica	+/
	Version 2.15.1250.	Copyright (C) 2015 America	In Megachenus, The.
			AD

1 Serial: FTDI B0033LQ1	+ 🗇		ŝ	-	×
🔵 СОМ6 (9600)					ipin 🕴
Aptio Setup Utility	- Copyright (C) 2013 Ameri Boot	can Megatrends, Inc.			
Boot Option #1 Boot Option #2 Boot Option #3	<pre>[P4: HGST HTE725032A] [SanDisk SanDisk 3.2] [P5: INTEL SSD5C2BB1] Boot Option #2</pre>	<pre>&gt; &gt; &gt; &gt; &gt; &gt; &gt; &gt;-</pre>			
Version 2.15.1236.	Copyright (C) 2013 America	n Megatrends, Inc. AB			

Ici on est retourné dans la catégorie « Hard drive BBS priorities » pour vérifier que la clé est bien montée.

1 Serial: FTDI	B0033LQ1	+	Ē		ŝ	-	×
🔶 СОМб (9600)							pin
Aptio S	etup Utility	- Copy Boot	right (C) 2013 Ameri	can Megatrends, Inc.			
Boot Option Boot Option Boot Option	: #1 #2 #3	[SanDi: [P4: HK [P5: II	sk SanDisk 3.2] SST HTE725032A] VTEL SSDSC2BB1]	Sets the system boot lorder			
 \Versio	n 2.15.1236.	Copyri	ght (C) 2013 America	ESC: Exit   +/ nn Megatrends, Inc.			
				AB			

Pour finir on ira dans la rubrique « Save & Exit », dans « save changes and Exit » et avec Entrer faite « Yes »

1 Serial: FTDI B0033LQ1 + 📋	
СОМБ (9600)	
Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc. Main Advanced Chipset Boot Security Save & Exit Server Mgmt	
Save Changes and Exit       Exit system setup after         Discard Changes and Exit       Isaving the changes.         Save Changes and Reset       Isaving the changes.         Discard Changes and Reset       Isaving the changes.         Save Options       / Save & Exit Setup         Save Changes       Isave configuration and exit?	
Restore Defaults       Select Screen         Save as User Defaults       Select Screen         Restore User Defaults       Select Item         r: Select       Select Item         Boot Override       +/-: Change Opt.         UEFI: Built-in EFI Shell       F1: General Help         UEFI: SanDisk SanDisk 3.2 Gen1DL17       F2: Previous Values         SanDisk SanDisk 3.2 Gen1DL17       F3: Optimized Defaults         F4: Save & Exit       ESC: Exit	
Version 2.15.1236. Copyright (C) 2013 American Megatrends, Inc. AB	

### Installation de l'image Opensense

Après avoir configurer le BIOS et l'avoir quitté le pare-feu va redémarrer donc pendant de temps il va falloir d'abord mettre la clé avec l'ISO et ensuite passer la vitesse de lecteur a 115200bauds (le plus important est de mettre la clé car le changement de vitesse n'a rien à vois avec le redémarrage, si vous n'avez pas réussi pas de soucis coupé le pare-feu est recommencer)



Il faudra se connecter avec c'est identifiant :

Identifiant = Installer

Mdp par défaut = opnsense

A savoir : Une fois connecter il faut savoir que comme depuis le debut la souris ne sera pas utiliser seulement les touche du clavier (ici sois on utilise le plus est le moins ou les flèches directionnel pour naviguer, la touche enter pour sélectionner mais aussi pour les touches « ok » ou « Yes » et le reste des touches pour écrire).

On arrive ensuite sur cette page ou on sélectionnera le clavier voulu donc ici « French ».



Une fois le clavier sélectionné on arrive sur cette page ou on devra sélectionner « Install (ZFS) ».

A savoir : Le ZFS (Zettabyte File System) est un système de fichiers avancé qui a été conçu pour offrir une gestion robuste, fiable et performante des données.



On ne sélectionne pas de mode miroir et pas de redondance.

A Savoir : pour faire un miroir il faut un deuxième disque dure car tout ce qu'est fait sur le premier et répliquer sur le second et la redondance est utile pour assurer une haute disponibilité exemple : si le disque dure principale lâche le deuxième prend le relais pour avoir un taux de disponibilité élever.



On sélectionne avec espace l'emplacement où l'on veut que la configuration soit installée (ici on veut mettre la configuration ZFS sur le disk HDD nommé « HGST HTE... »).



Puis descendre avec les touches directionnelles sur « ok ».

Après avoir sélectionner l'emplacement de la configuration un message pour nous prévenir que tout ce qu'il y avait sur le disk va être écrasé. Pour passer il faut appuyer sur « Entré »

1 C:\WINDOWS\SYSTE 2 Serial: FTDI B0033LQ1 + 📋	¢ –	пх
COM6 (115200)		
OPNsense Installer		
700 Confirmation		
Last Chance! Are you sure you want to destroy		
the current contents of the following disks:		
ada0		
< YES > < NO >		
[Press arrows, TAB or ENTER]		

Quand la barre de chargement est à 100% on peut alors enlever la clé :



Un fois le chargement terminé on clique sur change root password (question de sécurité).



Et on confirme le MDP (en tapant le même).

1 C:\WINDOWS\SYSTE 2 Serial: FTDI B0033LQ1 +	
COM6 (115200)	🐺 Unpin
OPNsense Installer	
Set Password	
Please confirm the password for the system management account (root):	
****	
<u> </u>	

Puis on sélectionne exit and reboot :

1 C:\WINDOWS\SYSTE	2 Serial: FTDI B0033LQ1	+	Ē	ŵ − □	X L
🔶 СОМ6 (115200)					🐺 Unpin
OPNsense Installer					-
Setup of complete Comp omp	Final Configuration your OPNsense system is nea Password Change root pa lete Install Exit and rebox	arly assword			
	Li				
1 C:\WINDOWS\SYSTE	2 Serial: FTDI B0033LQ1		Ē		
COM6 (115200)					
The installation finishe	d successfully.				
After reboot, open a wet https://192.168.1.1 (or can also be used to set Your browser may report and ask you to accept it certificate will be self an external root authori	<ul> <li>browser and navigate to the LAN IP address). The a different LAN IP.</li> <li>the HTTPS certificate as un the HTTPS is normal, as the effective resigned and cannot be value ty.</li> </ul>	console ntruste default dated by	d V		
Rebooting in 5 seconds.	CTRL-C to abort				
					I

Ensuite il faudra retourner dans le bios pour mettre le HDD en priorité.

### **Configuration OPNSense**

A savoir : pendant la configuration, il y a des propositions oui ou non en marquant [y/N] : s'il n'y a rien marqué après les points, c'est que c'est la lettre en majuscule qui est sélectionnée par défaut.

Pour commencer la configuration il faut aller dans l'option 1 pour assigner les ports.



Pour les deux prochaines questions on fait « Entrée » car on ne veut pas configurer pour l'instant.



A la deuxième étape on nous présente les ports (sous forme d'interface) configurables, ici on nous demande quel port sera le WAN, pour configurer un port il faut marquer le numéro de port ici « igb4 » si on sait lequel correspond auquel sinon il faut brancher un équipement en RJ45 au port que le veut configurer et écrie « a »

Valid interfac	es are:
igb0 igb1	00:0e:b6:c0:e4:5c Intel(R) I347-AT4 DH89XXCC 00:0e:b6:c0:e4:5d Intel(R) I347-AT4 DH89XXCC 00:0e:b6:c0:e4:5d Intel(R) I347-AT4 DH89XXCC
TRDS	00:00:00:00:00:04:50 Inter(K) 1347-A14 DH89XXCC
igb3	00:0e:b6:c0:e4:5f Intel(R) I347-AT4 DH89XXCC
igb4	00:0e:b6:5b:ff:f0 Intel(R) I210 (Copper)
igb5	00:0e:b6:5b:ff:f1 Intel(R) I210 (Copper)
If you do not auto-detection hitting 'a' to	know the names of your interfaces, you may choose to use . In that case, disconnect all interfaces now before initiate auto detection.
Enter the WAN	interface name or 'a' for auto-detection: igb4

Ici on nous demande quel port sera sur le LAN de la même manière que précédemment dans notre cas « igb5 ».

Enter the LAN interface name or 'a' for auto-detection NOTE: this enables full Firewalling/NAT mode. (or nothing if finished): igb5

Ici on ne met rien car on ne veut pas d'interface supplémentaire.

```
Enter the Optional interface 1 name or 'a' for auto-detection (or nothing if finished):
```

Un message nous dit quelle interface sera attribuée à quoi et si on veut procéder à l'assignation en mettant un « y ».



Maintenant, on va mettre des adresses IP sur les interfaces que l'on a configurées avant.



Là, on nous montre les interfaces configurables. On commence par le LAN en mettant « 1 »

Available interfaces: 1 - LAN (igb5 - static, track6) 2 - WAN (igb4 - dhcp, dhcp6) Enter the number of the interface to configure: 1

Là, on fait « entrée » car on ne veut pas mettre de DHCP sur le port LAN.

Configure IPv4 address LAN interface via DHCP? [y/N]

Maintenant on rentre l'adresse IP du port LAN, dans ce cas-là on met « 192.168.60.254 »

Enter the new LAN IPv4 address. Press <ENTER> for none: > 192.168.60.254

Là, on rentre le nombre de bits du masquer. Dans notre cas, on rentre 24 car l'adresse IP est en classe C.



lci on fait juste « Entrée ».



A la prochaine étape, on écrit « n » car on ne veut mettre d'IPv6 sur le LAN via le WAN.

Configure IPv6 address LAN interface via WAN tracking? [Y/n] n

Maintenant on appuie sur « Entrée » car on ne veut pas mettre d'IPv6 sur le LAN via DHCP6.

Configure IPv6 address LAN interface via DHCP6? [y/N]

Ici on ne veut toujours pas d'IPv6 donc « Entrée »



À cette étape, on va écrire un « y » car on veut mettre un DHCP sur le LAN.

Do you want to enable the DHCP server on LAN? [y/N] y

Maintenant on vient rentrer la plage d'IP que l'on veut.

Enter the start address of the IPv4 client address range: 192.168.60.100 Enter the end address of the IPv4 client address range: 192.168.60.200

Est-ce pour finir aux trois prochaines questions faites « Entrée » car on ne veut pas ces options.

Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] Do you want to generate a new self-signed web GUI certificate? [y/N] Restore web GUI access defaults? [y/N]

A la fin de la configuration, on peut voir qu'une adresse IP apparaît. Elle va être utilisée pour se connecter à l'interface web de OPNSense.

You	can now access the web GUI by opening
the	following URL in your web browser:
	https://192.168.60.254

# Changement du mot de passe Admin / langue

A savoir : changer le mot de passe Admin est super important car tout le monde peut connaître le mot de passe Admin en regardant la documentation du logiciel. On le change donc pour des questions de sécurité.

Aussi par défaut le logiciel est en anglais, donc pour pouvoir mieux s'orienter quand on ne connaît pas très bien l'anglais, il est important de changer la langue.

# MDP Admin firewall

Sur le menu pour aller changer le mot de passe admin, il faut prendre l'option 3 (à écrire sur la ligne « Enter an option : »).



Ici, on nous demande si on veut procéder au changement du mot de passe root, donc on met alors un « y » en minuscule pour signifier yes.



Et il nous est demandé de mettre le nouveau MDP deux fois pour le confirmer.



# Changement de la langue.

Pour changer la langue, il faut déjà aller sur la page d'accueil du pare-feu en tapant dans l'URL l'adresse IP du pare-feu (on a obtenu cette IP à la fin de l'installation) et en rentrant les identifiants de notre compte Admin.



Ensuite, à gauche, il faut aller cliquer sur la rubrique « System ».



Puis cliquer sur « Settings ».

Routes	ŧ
Settings	¢°
Administration	
Cron	
General	
Logging	
Logging / targets	
Miscellaneous	
Tunables	

Et aller dans la catégorie « Général ».



Puis sur le reste de l'écran, il faut aller dans la partie « Language » et mettre la langue voulue.

6 Language

Portuguese (Brazil)

.

Et pour finir, il faut aller en bas de la page pour cliquer sur le bouton où il est écrit « Sauvegarder ».



# Sauvegarde / restauration

A savoir : Il est essentiel de faire des sauvegardes régulières afin de pouvoir revenir à une version antérieure en cas de mauvaise manipulation. Cela garantit que, même en cas de problème, le pare-feu restera opérationnel pour assurer la sécurité et le filtrage du réseau. Il est également important de savoir comment restaurer rapidement une sauvegarde pour gagner du temps et minimiser les interruptions de service.

# Sauvegarde

Pour faire une sauvegarde, il faut déjà aller sur la page d'accueil du pare-feu en tapant dans l'URL l'adresse IP du pare-feu (on a obtenu cette IP à la fin de l'installation) et en rentrant les identifiants de notre compte Admin.



Ensuite, à gauche, il faut aller cliquer sur la rubrique « Système ».

🖵 Accueil	
📥 Rapports	
🗮 Système	
Accès	<u></u>
Configuration	୭
Firmware	
Passerelles	1
Haute disponibilité	0
Routes	ŧ
Paramètres	¢
Gestion des Certificats	٠
Assistant	Y
Fichiers journaux	۲
Diagnostics	(Ē)
📥 Interfaces	
🚯 Pare-feu	
VPN	
Services	
🖋 Alimentation	
Aide	

#### Puis cliquer sur « Configuration ».



#### Et aller dans la catégorie « Sauvegarde ».

🗃 Système	
Accès	<u>e</u>
Configuration	5
Sauvegardes	

Puis sur le reste de l'écran, il faut aller dans la partie « Téléchargement » et appuyer sur « Télécharger la configuration ».

Système: Configura	tion: Sauvegardes
Nombre de sauvegardes	
	Entrez le nombre de configurations à conserver dans le cache local des sauvegardes.
Sauvegarder	Soyez conscient de la quantité d'espace utilisée par les sauvegardes avant d'ajuster cette valeur. Espace actuellement utilisé: 256K
Téléchargement	
✓ Ne pas sauvegarder les donn ☐ Chiffrer ce fichier de configur	ées RRD. ration
Télécharger la configuration	
Cliquer sur ce bouton pour télée	charger la configuration système au format XML.

On peut voir en haut à droite que le fichier s'est bien téléchargé.



# Restauration

Pour faire la restauration, il faut être sur la même page que pour la sauvegarde et descendre pour aller dans la catégorie « Sauvegarde ».

lestauration	
lestore areas:	
Tout (recommandé) 👻	
Choisir un fichier Aucun fichier choisi	
Redémarrer après une restauration réalisée avec succès.	
Exclure les paramètres de la console de l'importation.	
Flush (full) local configuration history.	
☐Le fichier de configuration est chiffré.	
Restaurer la configuration	
Nuvrir un fichier de configuration XML puis cliquez sur le bo	outon ci dessous pour restaurer la configuration
Juvin un nemer de configuration AME puis cliquez sur le bo	outon ci-dessous pour restaurer la configuration.

Ensuite, on va cliquer sur le bouton « choisir un fichier ».



Et on sélectionne le fichier que l'on a téléchargé.



Et pour finir, il faut cliquer sur le bouton « Restaurer la configuration ».

estore areas:	
Tout (recommandé)	•
Choisir un fichier config-0341.xml	
Redémarrer après une restauration réalise	ée avec succès.
Exclure les paramètres de la console de l'i	mportation.
Flush (full) local configuration history.	
Le fichier de configuration est chiffré	

#### Pour vérifier que tout s'est bien passé, tout en haut de la page, un message s'affiche.

La configuration a été restaurée. Le système est en cours de redémarrage. Cela peut prendre une minute.

# Rester en mode usine

A savoir : Il est utile de rester en mode usine en cas de mauvaise configuration, en cas de panne et dysfonctionnements. Avant de faire ceci, il est important de faire une sauvegarde au préalable, ensuite rester en mode usine, puis il est possible de faire une restauration de la sauvegarde faite précédemment pour minimiser les interruptions de service.

### Sauvegarde

Pour faire une sauvegarde, il faut déjà aller sur la page d'accueil du pare-feu en tapant dans l'URL l'adresse IP du pare-feu (on a obtenu cette IP à la fin de l'installation) et en rentrant les identifiants de notre compte Admin.



Ensuite, à gauche, il faut aller cliquer sur la rubrique « Système ».

Rapports         Système         Accès         Configuration         Passerelles         Passerelles         Haute disponibilité         Routes         Paramètres         Gestion des Certificats         Assistant         Fichilers journaux         Diagnostics         Pare-feu         VPN         Services         Álimentation         Jade	😐 Accueil	
Système       Accès       Image: Système         Accès       Image: Système         Configuration       D         Firmware       Image: Système         Passerelles       Image: Système         Passerelles       Image: Système         Haute disponibilité       Image: Système         Routes       Image: Système         Paramètres       Image: Système         Gestion des Certificats       Image: Système         Assistant       Image: Système         Diagnostics       Image: Services         Pare-feu       VPN         Services       Alimentation         Image: Alimentation       Aide	陆 Rapports	
Accès <ul> <li>Configuration</li> <li>Pirmware</li> <li>Passerelles</li> <li>Passerelles</li> <li>Haute disponibilité</li> <li>Routes</li> <li>Routes</li> <li>Paramètres</li> <li>Gestion des Certificats</li> <li>Gestion des Certificats</li> <li>Assistant</li> <li>Fichiers journaux</li> <li>Diagnostics</li> <li>Interfaces</li> <li>Pare-feu</li> <li>VPN</li> <li>Services</li> <li>Alimentation</li> <li>Aide</li> </ul>	😂 Système	
Configuration     Image: Second	Accès	꺌
Firmware     Image: Constraint of the co	Configuration	5
Passerelles     1       Haute disponibilité     2       Routes     7       Paramètres     5       Gestion des Certificats     6       Assistant     7       Fichiers journaux     7       Diagnostics     1       Interfaces     1       9     Pare-feu       VPN     Services       1     Alimentation       1     Aide	Firmware	
Haute disponibilité     C       Routes     T       Paramètres     S       Gestion des Certificats     Image: S       Assistant     Image: S       Fichiers journaux     Image: S       Diagnostics     Image: S       Interfaces     Image: S       Pare-feu     Image: S       Services     Image: S       Image: Alimentation     Image: S       Aide     Image: S	Passerelles	1
Routes     +       Paramètres     •       Gestion des Certificats     •       Assistant     *       Fichiers journaux     •       Diagnostics     •       Interfaces       •     Pare-feu       •     Services       *     Aimentation       •     Aide	Haute disponibilité	C
Paramètres     \$       Gestion des Certificats     •       Assistant     \$       Fichiers journaux     •       Diagnostics     •       Interfaces       •     Pare-feu       •     Services       •     Alimentation       •     Aide	Routes	ŧ
Gestion des Certificats       Assistant       Fichiers journaux       Diagnostics       Interfaces       Pare-feu       VPN       Services       Alimentation       Aide	Paramètres	¢;
Assistant	Gestion des Certificats	•
Fichiers journaux       Diagnostics       Diagnostics       Interfaces       Pare-feu       VPN       Services       Alimentation       Aide	Assistant	Y
Diagnostics       Interfaces       Pare-feu       VPN       Services       Mimentation       Aide	Fichiers journaux	۲
A Interfaces     Pare-feu     VPN     Services     Alimentation     Aide	Diagnostics	Ô
<ul> <li>Pare-feu</li> <li>VPN</li> <li>Services</li> <li>Alimentation</li> <li>Aide</li> </ul>	🚠 Interfaces	
<ul> <li>VPN</li> <li>Services</li> <li>Alimentation</li> <li>Aide</li> </ul>	🚯 Pare-feu	
<ul> <li>Services</li> <li>Alimentation</li> <li>Aide</li> </ul>	VPN	
<ul><li>Alimentation</li><li>Aide</li></ul>	Services	
Aide	🖋 Alimentation	
	Aide	

Puis cliquer sur « Configuration ».

Système	
Accès	<u> </u>
Configuration	5
Sauvegardes	
Par défaut	
Historique	
Firmware	

#### Et pour finir, dans aller dans la catégorie « Sauvegarde ».

Configuration	5
Sauvegardes	
Par défaut	
Historique	

Sur la page, il va falloir aller dans la partie « Téléchargement » et cliquer sur « Télécharger la configuration ».

Téléchargement
✓ Ne pas sauvegarder les données RRD. □ Chiffrer ce fichier de configuration
Télécharger la configuration
Cliquer sur ce bouton pour télécharger la configuration système au format XML.

Après avoir téléchargé la configuration, un pop-up s'affiche en haut à droite montrant le téléchargement.



### Rester

Pour passer la configuration du pare-feu en mode usine, il faut déjà aller sur la page d'accueil du pare-feu.



Ensuite, à gauche, il faut aller cliquer sur la rubrique « Système ».



#### Par la suite, il faut aller dans « Configuration ».

Système	
Accès	<u></u>
Configuration	5
Sauvegardes	
Par défaut	
Historique	
Firmware	

#### Et cliquer sur la catégorie « Par défaut ».

Configuration	୭
Sauvegardes	
Par défaut	
Historique	

Sur le reste de la page, un message vient s'afficher pour prévenir de ce qui va être modifié. Et un pour pouvoir mettre la configuration par défaut, il faut cliquer sur le bouton « oui ».

# Système: Configuration: Par défaut

Si vous cliquez "Oui", le système va:

- Retour aux paramètres d'usine
- L'adresse IP LAN sera réinitialisée en 192.168.1.1
- Le système sera configuré en tant que serveur DHCP sur l'interface LAN par défaut
- L'interface WAN sera configurée pour obtenir automatiquement une adresse depuis un serveur DHCP
- Nom d'utilisateur et mot de passe de l'administrateur seront réinitialisés.
- Éteindre une fois les changements terminés

Êtes-vous certain de vouloir continuer?



Une fois que l'on a cliqué sur le bouton, un message s'affiche pour dire que le mode usine est en cours d'application.

Votre appareil est en cours d'extinction	
Le système a été réinitialisé avec les paramètres usine et est en cours d'extinction.	

# Restauration

Pour faire la restauration, il faut être sur la même page que pour la sauvegarde et descendre pour aller dans la catégorie « Sauvegarde ».

Restauration
Restore areas:
Tout (recommandé) 🔹
Choisir un fichier Aucun fichier choisi
Redémarrer après une restauration réalisée avec succès.
Exclure les paramètres de la console de l'importation.
✓ Flush (full) local configuration history.
Le fichier de configuration est chiffré.
Restaurer la configuration
Ouvrir un fichier de configuration XML puis cliquez sur le bouton ci-dessous pour restaurer la configuration.

Ensuite, on va cliquer sur le bouton « choisir un fichier ».



Et on sélectionne le fichier que l'on a téléchargé.



Et pour finir, il faut cliquer sur le bouton « Restaurer la configuration ».

Restauration
Restore areas:
Tout (recommandé) 🔹
Choisir un fichier config-0341.xml
<ul> <li>Redémarrer après une restauration réalisée avec succès.</li> <li>Exclure les paramètres de la console de l'importation.</li> </ul>
Flush (full) local configuration history.
Le lichier de configuration est chiffe.
Restaurer la configuration

Pour vérifier que tout s'est bien passé, tout en haut de la page, un message s'affiche.

La configuration a été restaurée. Le système est en cours de redémarrage. Cela peut prendre une minute.

# Configuration du webfiltering

A savoir : le webfiltering est utilisé car il peut bloquer l'accès à certains sites internet sur le réseau de l'entreprise.

### Configuration

Pour activer le service de webfilterning, il faut déjà aller sur la page d'accueil du pare-feu en tapant dans l'URL l'adresse IP du pare-feu (on a obtenu cette IP à la fin de

CPO <mark>sense" &lt;</mark>					root@OPNsense.localdomain	
ccuell	Assurable Tableau de boud					
apports	Accuell: Tableau de bord				O Ad	Jd Widget Restore default layout
stème						
terfaces	System Information *	Mémoire # Disque #	Statistiques des Interfaces	*	CPU #	Passerelles
re-feu					Intel(R) Xeon(R) CPU @ 2.50GHz (4 cores,	
1	Nom	11.33% 0%			4 threads)	WAN_DHCP6
rices	OPNsense.localdomain				Total	~
rentation	Versions	Graphique du trafic 🍡 🛪				WAN_DHCP
	FreeBSD 14.1-RELEASE-p2	Traffic In	WAN		Interrupt	192.168.0.254
	OpenSSL 3.0.14	140.00 K				
	Nises à jour	120.00 K			e	
	Cliquer pour vérifier les mises à jour.	80.00 K			Utilisateur	
	Durée de fonctionnement	60.00 K				
	V0442-39	20.00 K	Pare-feu	×	Système	
	Date/heure actuelle Wed Oct 2 10:59:26 UTC 2024			-		
	Last configuration change	Traffic Out				
	Non Sep 23 14:31:15 UTC 2024	160.00 K	let out anything from firewall host it		Announcements #	
		120.00 K	anti-lockout rule			
		80.00 K	let out anything from firewall host it allow thcov6 client out WAN		Ber Offitiente 24.7.5 released	
		40.00 K	Elock private networks from VIAN		A hotfix release was issued as	
			Block bogon IPv4 networks from Vi		24.7.5_3:	
					o system: due to observed timing	
					o openvpn: fix "auth-gen-token"	
					being supplied in server mode	
					OPNsense 24.7.5 released	
					A good day to you all,	

### l'installation) et en rentrant les identifiants de notre compte Admin.

Puis sur le menu à gauche, il faut aller dans la catégorie « Services ».

😐 Accueil	
📐 Rapports	
🗃 Système	
🚠 Interfaces	
🚯 Pare-feu	
VPN	
Services	
Portail Captif	A
DHCRelay	۲
DNS Dnsmasq	۲
Détection d'Intrusion	U
ISC DHCPv4	۲
ISC DHCPv6	۲
Kea DHCP [new]	۲
Monit	••
Heure réseau	0
OpenDNS	۲
Unbound DNS	۲
🖌 Alimentation	
Aide	

Puis cliquer sur « Unbound DNS ».

Unbound DNS	۱
Général	
Contournements	
Avancé	
Listes d'accès	
Liste de blocage	
Transmission des requêtes	
DNS sur TLS	
Statistiques	
Fichier journal	

Et aller dans la catégorie « Liste de blocage ».



Une fois sur la page, on peut avoir accès à des listes de blocage déjà intégrées dans OPNSense qui se trouvent dans « Types de DNSBL » telles que des sites pornos, la cryptomonnaies et bien d'autres. Il est aussi possible de bloquer un site en particulier en rentrant l'URL dans « Domaines en liste bloquée ».

🕐 mode avancé	
1 Activer	
1 Forcer SafeSearch	
Type de DNSBL	Liste de tous les pornos 🔹
ODD Domaines de la liste blanche	🛇 Tout effacer 🖓 Copie 🖺 Pâte 🖹 Texte
O Domaines en liste bloquée	pornhub.com ×           O Tout effacer ᠿ Copie
0 Domaines Wildcard	🛇 Tout effacer 街 Copie 🚯 Pâte 🗟 Texte
Appliquer	

Aussi, quand on clique sur le bouton « mode avancée » il est possible d'ajouter une liste de blocage dans « URLs des listes de blocage » que l'on peut trouver sur internet comme l'URL : <u>https://sebsauvage.net/hosts/hosts</u>

Activer	
Forcer SafeSearch	
Type de DNSBL	Liste de tous les pornos 🗸
	😮 Tout effacer 🛛 Sélectionner tout
URLs des listes de blocage	https://sebsauvage.net/hosts/hosts ×
	😆 Tout effacer 🖆 Copie 📑 Pâte 📄 Texte
Domaines de la liste blanche	
	😮 Tout effacer 🥙 Copie   🖻 Pâte 📄 Texte
Domaines en liste bloquée	pornhub.com ×
	😮 Tout effacer 🥙 Copie   🗈 Pâte 📄 Texte
Domaines Wildcard	
	🛿 Tout effacer 🥙 Copie 📭 Pâte 📄 Texte
Adresse de destination	
Retour NXDOMAIN	

Une fois la configuration faite comme souhaité, il faut appuyer sur le bouton « Appliquer » qui se trouve en bas de la page.



# Activer le SSH

A savoir : Sur le pare-feu, il y a la possibilité d'activer le service SSH qui est utile pour prendre main sur le pare-feu à distance sans passer par le câble console et sans interface graphique.

### Activer le SSH

Pour activer le service SSH, il faut déjà aller sur la page d'accueil du pare-feu en tapant dans l'URL l'adresse IP du pare-feu (on a obtenu cette IP à la fin de l'installation) et en rentrant les identifiants de notre compte Admin.

← → C O Non securited Amport/192.1	68.60.254/us/core/dashboard				÷ 0 10 3
SOPOsenso" <				root@OPNserse.localdomain 0 Q	
교 Accuell L Rapports 國 Système	Accueil: Tableau de bord			O Ada	Widget Restore default layout
à ventos à Pentos O VTN O VTN I Sinnestan I Alizentan O Aria	System Information e e Single Constraints (Constraints) Writes (	Banda & Bage + Construction of the second s	Existing de statutes	OU 20 2010 INCRUINCE 4 DESCRIPTION 4 DESCRIPTION	Rug, SIGN     View, SIGN     Vi
	OPhisense (c) 2004-2004 Deciso B.X.				

Ensuite, à gauche, il faut aller cliquer sur la rubrique « Système ».

😐 Accueil	
Rapports	
Système	
Accès	<u>88</u>
Configuration	୭
Firmware	
Passerelles	1
Haute disponibilité	C
Routes	ŧ
Paramètres	o°,
Gestion des Certificats	٠
Assistant	P
Fichiers journaux	۲
Diagnostics	(Ē)
📥 Interfaces	
🚯 Pare-feu	
VPN	
Services	
🖌 Alimentation	
Aide	

#### Puis cliquer sur « Paramètres »

Haute disponibilité	0
Routes	ŧ
Paramètres	¢
Gestion des Certificats	٠
Assistant	1

Et aller dans la catégorie « Administration ».

Paramètres	o°,
Administration	
Cron	
Général	
Journalisation	
Divers	
Optimisations	
Gestion des Certificats	٠
Assistant	1

Puis sur le reste de l'écran, il faut descendre jusqu'à « Port SSH », dans le rectangle à côté il faut rentrer 22 et cocher les cases « Activer le Shell sécurisé, Autoriser la connexion de l'utilisateur root, Autoriser les connexions avec mot de passe ».

Shell Sécurisé	
O Serveur Shell sécurisé	✓ Activer le Shell sécurisé
<b>1</b> Groupe de connexion	wheel, admins -
Oconnexion root	✓ Autoriser la connexion de l'utilisateur root
Méthode d'authentification	✓ Autoriser les connexions avec mot de passe
() Port SSH	22
Interfaces d'écoute	Tout (recommandé) 🔹
Avancé	Afficher les dérogations cryptographiques

Pour finir, il faut aller tout en bas de la page pour cliquer sur le bouton « Sauvegarder »



Une fois que la sauvegarde de la configuration est bonne, un message s'affiche.



#### Test

Pour tester si la connexion marche bien, on vient utiliser l'invite de commande et taper la commande ssh utilisateur@IP (dans notre cas ssh root@192.168.60.254)

C:\Users\Loïc≻ssh root@192.168.60.254 The authenticity of host '192.168.60.254 (192.168.60.254)' can't be established. ED25519 key fingerprint is SHA256:APsIDEGW9aG/ipSHnDXZo9J/S6XkIA2giGyhG57+EPw. This key is not known by any other names Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.60.254' (ED25519) to the list of known hosts. (root@192.168.60.254) Password: Last login: Wed Oct 2 10:39:24 2024 Hello, this is OPNsense 24.7 രെ Website: https://opnsense.org/ https://docs.opnsense.org/ https://forum.opnsense.org/ https://github.com/opnsense Handbook: Forums: Code: Twitter: https://twitter.com/opnsense \*\*\* OPNsense.localdomain: OPNsense 24.7 \*\*\* LAN (igb5) -> v4: 192.168.60.254/24 WAN (igb4) -> v4/DHCP4: 192.168.0.242/24 HTTPS: sha256 B6 06 75 15 27 02 48 BD 0A BD 3A 81 93 10 54 7D B1 CB E2 FB F8 0E D1 78 81 25 DD 8F 27 A9 36 42 SHA256 4CCdeICX+xHCcb/ONyZsCg+9D6t4n4JsDejImDWzLsI (ECDSA) SSH: SHA256 APsIDEGW9aG/ipSHnDXZo9J/S6XkIA2giGyhG57+EPw (ED25519) SSH: SSH: SHA256 fLKtuYrFbqiSpOPJmcaO9ib9nRPcq5MHz+AIGGuuqSI (RSA) Ping host
 Shell 0) Logout 1) Assign interfaces 2) Set interface IP address 9) pfTop 3) Reset the root password 10) Firewall log 4) Reset to factory defaults 11) Reload all services 5) Power off system 12) Update from console 6) Reboot system 13) Restore a backup Enter an option: