

SKY-FUTURE

VOUS PRÉSENTE

L'installation de PfSense

Tutoriel réalisé par luo

Version 1.0.0 du 22/02/14

**Cette version est temporaire.
De nombreuses corrections vont être effectuées dans les prochains jours.**

Pour toutes informations veuillez adresser un mail à l'auteur à :

luo@sky-future.net

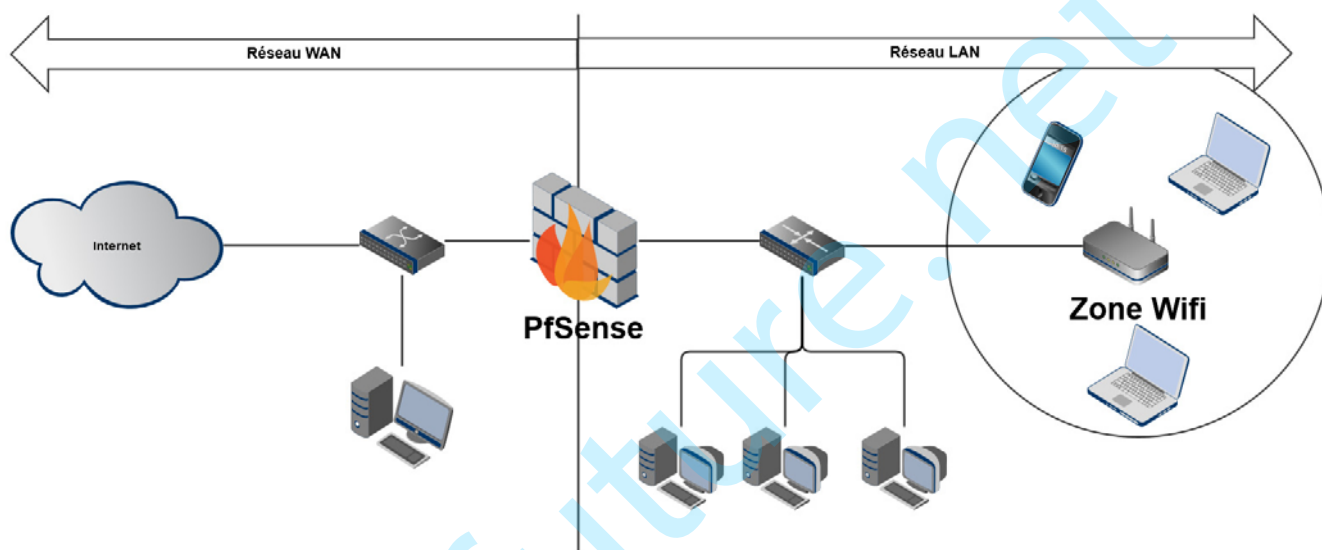
**Toute reproduction, même partielle, est interdite sans l'accord de l'auteur.
© Sky-future.net, 2014**

Introduction

PfSense est un routeur / pare-feu open source basé sur FreeBSD. Il a pour particularité de gérer nativement les VLAN (802.1q). Et dispose de très nombreuses fonctionnalités tels que faire VPN ou portail captif.

Dans ce tutoriel, je vais vous expliquer comment installer rapidement la distribution pfsense. La version que nous utiliserons pour ce tutoriel est la 2.1.

Voici l'architecture avec laquelle peut être utilisée pfsense (ici représenté par le pare-feu).



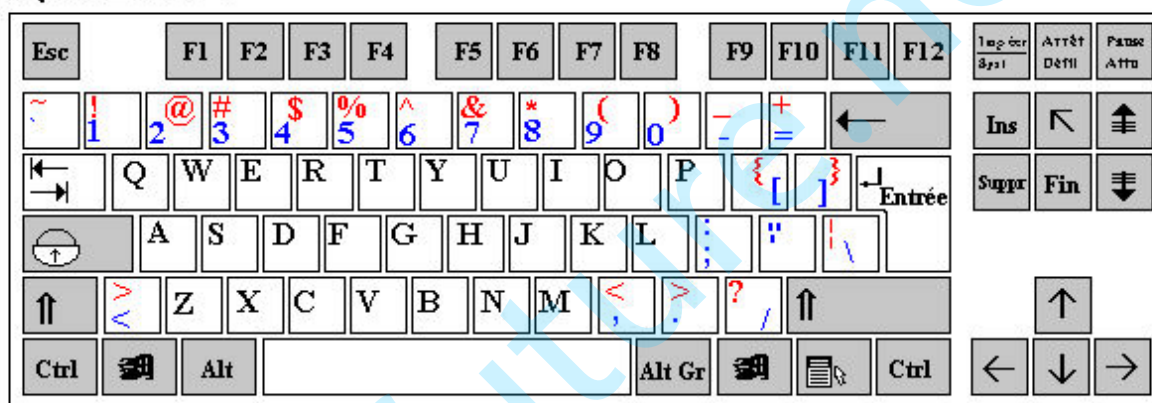
Prérequis

Un serveur ou ordinateur disposant d'au moins deux cartes réseaux. Une pour l'interface LAN (du côté du réseau local) et l'autre pour l'interface WAN (du côté du réseau relié à internet). Vous pouvez bien entendu utiliser un serveur virtuel. Mais cela pourra poser des problèmes au niveau des interfaces.

Le clavier français et en azerty, vous aurez donc besoin de connaître l'emplacement des touches du clavier anglais (qwerty) car lors de l'installation et la configuration via la ligne de commande le clavier est en qwerty. Et malheureusement même en modifiant les options lors de l'installation le clavier azerty n'est pas pris en compte.

Voici donc les deux claviers vous en aurez besoin (n'utilisez pas le pavé numérique):

QWERTY



AZERTY

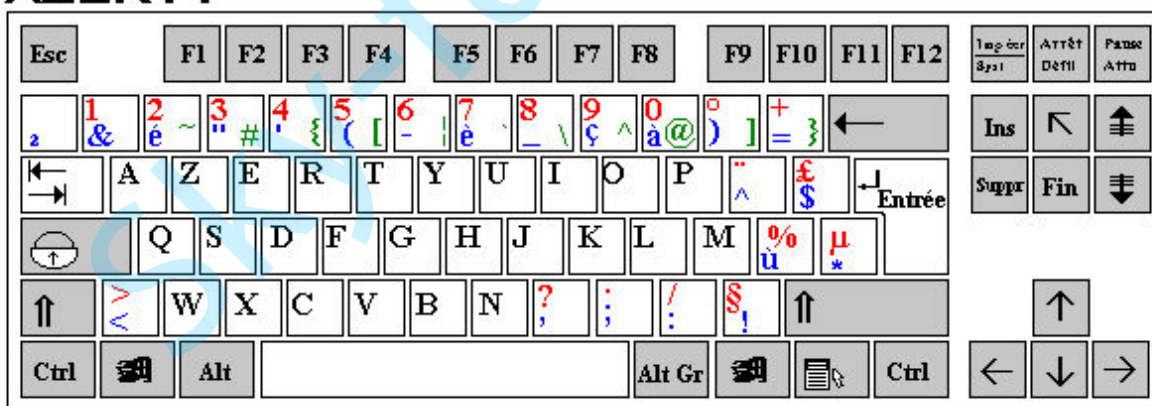


Illustration 1: comparaison des claviers

Installation de PfSense

Pour commencer, télécharger [l'iso par ici](#).

Une fois l'iso téléchargé gravé la sur un CD ou mettez-là dans un lecteur cd virtuel (pour une machine virtuelle par exemple.)

Pour ce tutoriel, j'utilise une machine virtuelle disposant de deux cartes réseaux une reliée en pont pour l'interface WAN et l'autre branchée sur un commutateur virtuel relié à différents ordinateurs.

Pour commencer, insérez le cd dans le serveur ou donnez l'iso au serveur pour démarrer l'installation.

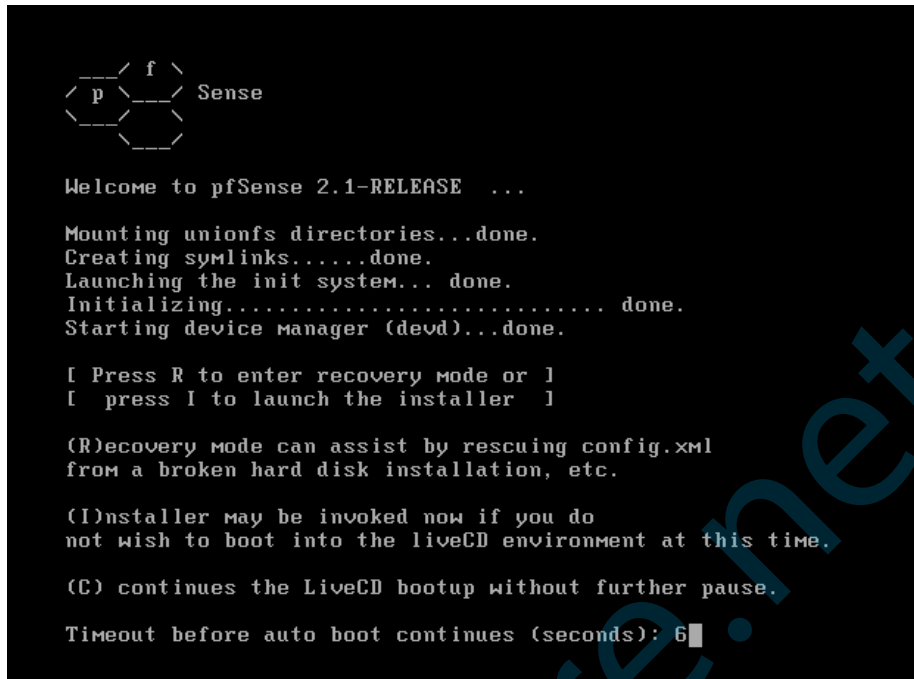
Une fois lancé, vous devriez arriver sur l'écran suivant :



Illustration 2: écran au lancement du cd

Appuyez sur entrer (c'est l'option 1 par défaut), ou patientez 10 secondes.

Normalement, si tout va bien, vous verrez alors cela :



```

  f \
  p  \ Sense

Welcome to pfSense 2.1-RELEASE ...

Mounting unionfs directories...done.
Creating symlinks.....done.
Launching the init system... done.
Initializing..... done.
Starting device manager (devd)...done.

[ Press R to enter recovery mode or ]
[ press I to launch the installer ]

(R)ecovery mode can assist by rescuing config.xml
from a broken hard disk installation, etc.

(I)nstaller may be invoked now if you do
not wish to boot into the liveCD environment at this time.

(C)ontinues the LiveCD bootup without further pause.

Timeout before auto boot continues (seconds): 6█
```

Illustration 3: choix de démarrage du CD

Encore un choix à faire, nous, nous désirons faire une installation, mais par défaut le système s'exécute en liveCD. Pour lancer l'installation appuyez sur « i ».

Maintenant nous obtenons cela :

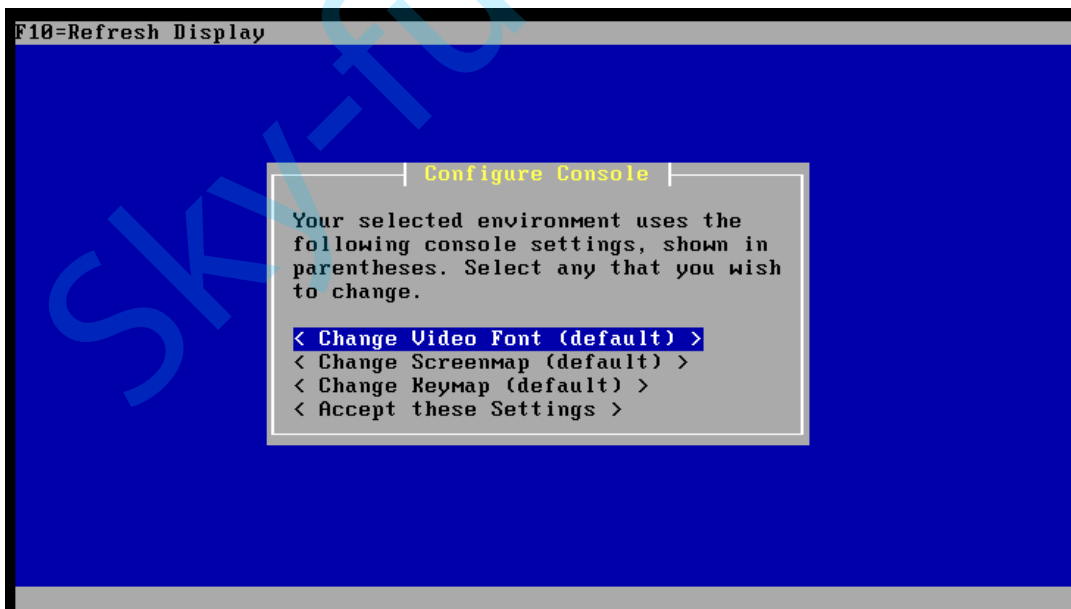


Illustration 4: écran d'installation 1

Déplacez le curseur sur « Accept these Settings », puis appuyez sur entrer.

Nous arrivons sur l'écran du choix du type d'installation.

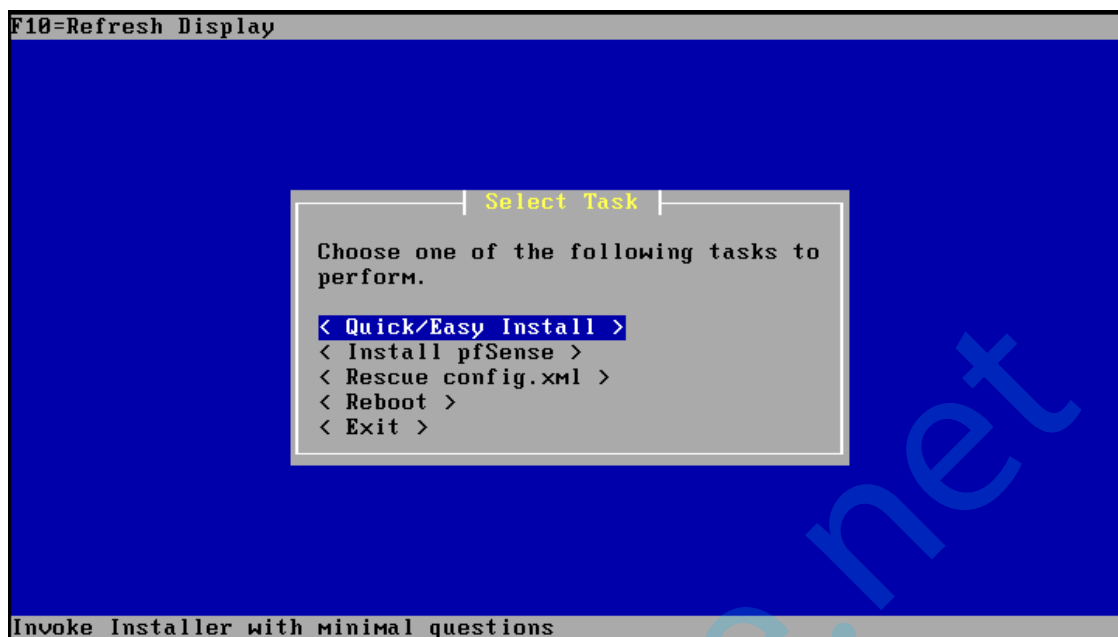


Illustration 5: écran d'installation 2

Nous allons sélectionner « Quick/Easy Install », pour éviter une installation trop longue via la console. On nous demande ensuite confirmation il faut donc faire « Ok ».

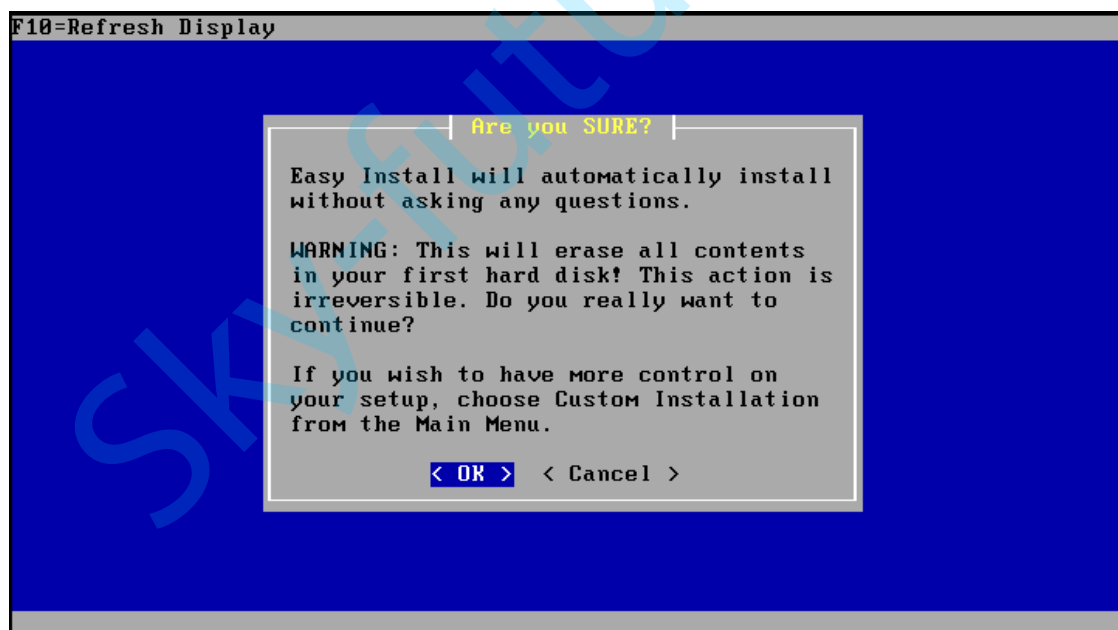


Illustration 6: écran d'installation 3

Patiencez quelques minutes, avant d'arriver à l'écran suivant.

Sur ce nouvel écran, on nous demande si l'on désire installer un kernel personnalisé. Nous allons sélectionner « Standard Kernel ».

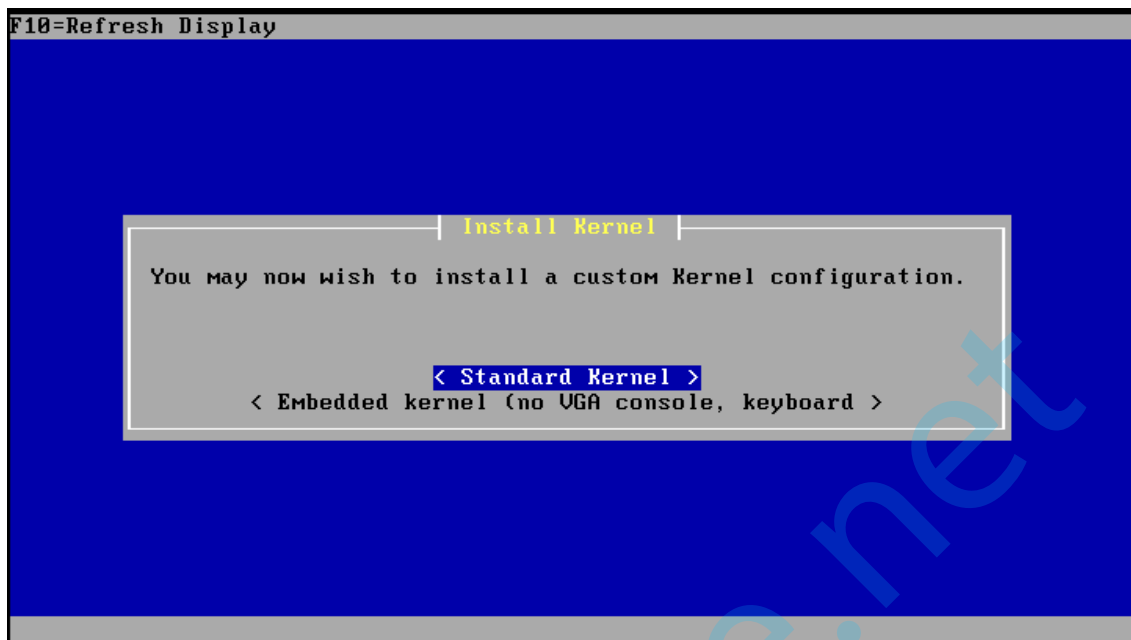


Illustration 7: écran d'installation 4

Ensuite, sur l'écran suivant appuyez sur « Reboot » pour continuer l'installation.

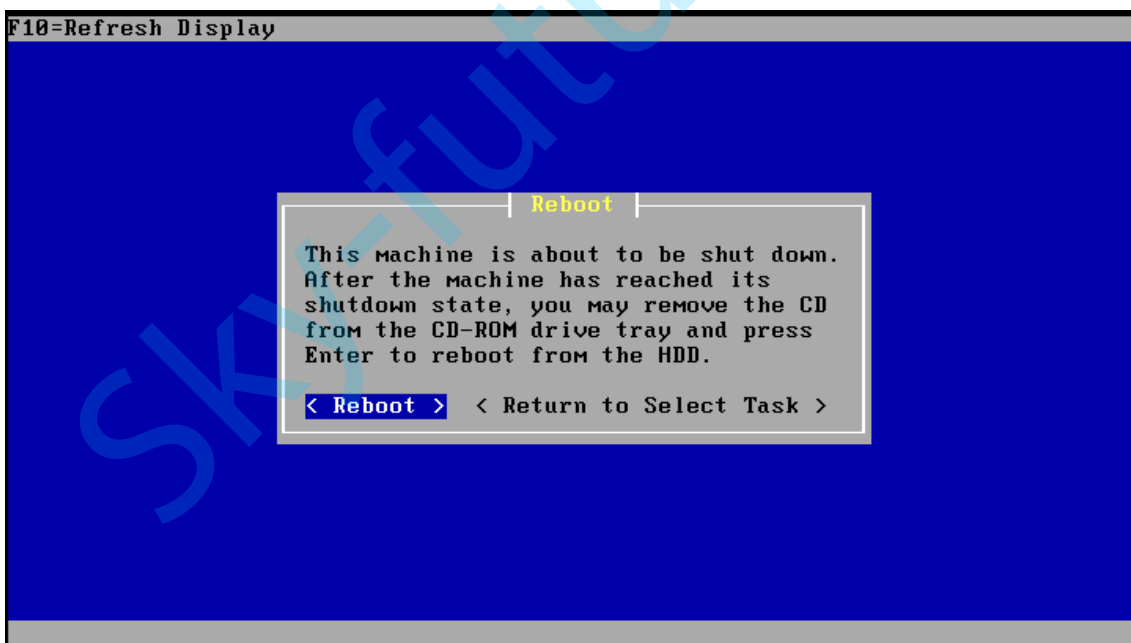


Illustration 8: écran d'installation 5

L'ordinateur est en cours de ré-démarrage, veuillez à éjecter le CD, ou l'image iso. Normalement au démarrage vous aurez l'écran suivant :



Illustration 9: écran de boot 1

Vous pouvez attendre ou appuyez sur F1. Vous arriverez de nouveau sur l'écran suivant :

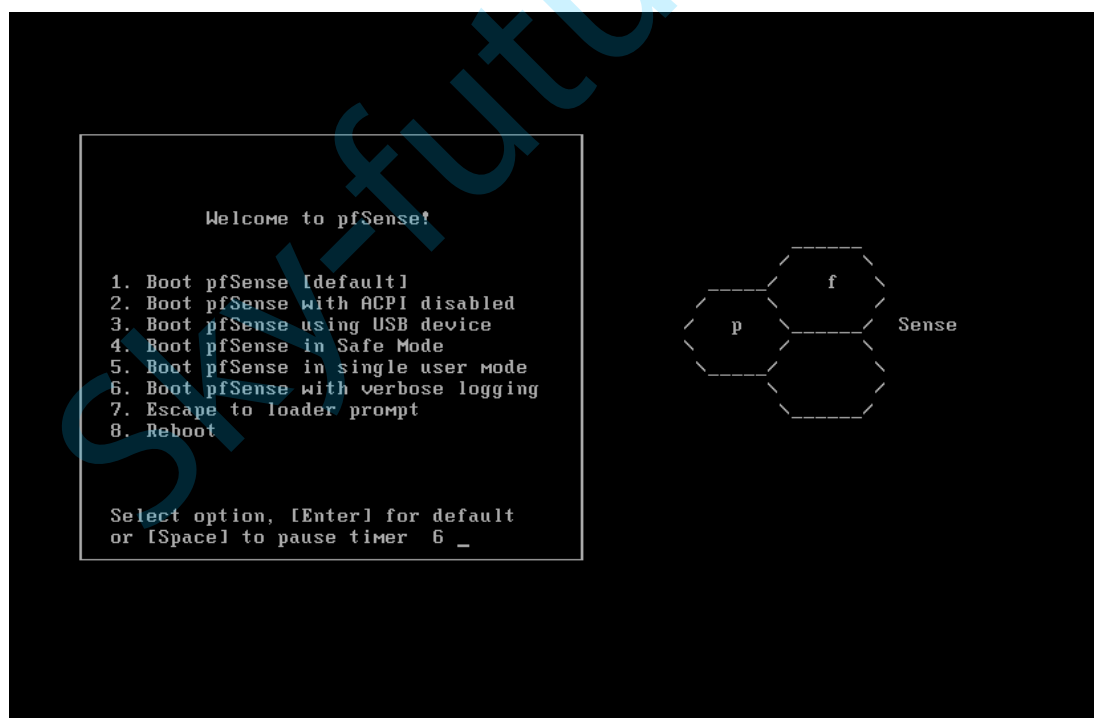


Illustration 10: écran de boot 2

Vous pouvez aussi attendre ou appuyer sur entrer.

Une fois effectuée, vous aurez alors l'écran suivant :

```
Welcome to pfSense 2.1-RELEASE ...

No core dumps found.
Creating symlinks.....done.
External config loader 1.0 is now starting...
Launching the init system... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.

Default interfaces not found -- Running interface assignment option.
le0: link state changed to UP

Valid interfaces are:

em0  00:0c:29:0e:c1:ca  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.4
le0  00:0c:29:0e:c1:d4  (up) AMD PCnet-PCI

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y!n]? █
```

Illustration 11: écran de configuration vlan

Avant de nous lancer sur la suite, nous devons noter des informations, j'ai entouré en rouge les interfaces qui sont disponibles qui seront indispensables à la configuration un peu plus loin. Ici l'interface em0 est l'interface WAN et le0 est l'interface LAN. Les interfaces ne sont pas toujours nommées de la même façon, il va falloir que vous testiez la configuration car vous pouvez avoir aussi em0, em1 ainsi que le0 et le1. Pour savoir laquelle est la bonne. Ne vous inquiétez pas si vous vous trompez vous le saurez assez vite et il est possible de les changer assez facilement.

Maintenant passons à la dernière ligne de la capture. Elle permet de configurer les VLANs nous indiquerons non (n). Vous pouvez faire oui si vous utilisez des VLAN ou attendre la fin de l'installation pour configurer ceci par l'interface web.

Ensuite, nous devons configurer les interfaces, ici la WAN où je rentre em0 :

```
Valid interfaces are:

em0  00:0c:29:0e:c1:ca  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.4
le0  00:0c:29:0e:c1:d4  (up) AMD PCnet-PCI

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y!n]? n

*NOTE*  pfSense requires *AT LEAST* 1 assigned interface(s) to function.
        If you do not have *AT LEAST* 1 interfaces you CANNOT continue.

        If you do not have at least 1 *REAL* network interface card(s)
        or one interface with multiple VLANs then pfSense
        *WILL NOT* function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: █
```

Illustration 12: configuration de l'interface WAN

Ensuite, c'est le tour de l'interface LAN où je rentre le0 :

```
If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): le0
```

Illustration 13: configuration de l'interface LAN

Si vous disposez d'une autre interface c'est ici qu'il faut l'indiquer sinon appuyez sur entree :

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

Illustration 14: interface supplémentaire

Ensuite, on nous demande confirmation donc on fait « y ».

Nous voilà à l'écran principal :

```
Starting DHCPv6 service...done.
Configuring firewall.....done.
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
Bootup complete

FreeBSD/i386 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.1-RELEASE-pfSense (i386) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.12/24
LAN (lan)      -> le0      -> v4: 192.168.1.1/24

0) Logout (SSH only)          8) Shell
1) Assign Interfaces          9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults  12) pfSense Developer Shell
5) Reboot system              13) Upgrade from console
6) Halt system                 14) Disable Secure Shell (sshd)
7) Ping host                   15) Restore recent configuration

Enter an option: 
```

Illustration 15: écran principal

Comme vous pouvez le constater, vous pouvez faire de nombreuses modifications d'ici. Mais pour l'instant, nous allons continuer l'installation qui n'est pas encore terminée.

Si vous regardez les IP vous remarquerez que l'ip WAN donné par ma box au serveur est 192.168.1.1 et que l'ip du lan est en 192,168,1,1

Donc je vais devoir changer cela pour pouvoir accéder à l'interface web sinon je vais toujours tomber sur la page de ma box.

Type de réseau	WAN	LAN
IP de l'interface	192.168.1.12 (attribué par le DHCP)	10.10.10.254
IP de la passerelle et du DHCP	192.168.1.1	10.10.10.254
Masque de sous réseau	255.255.255.0	255.255.255.0
Début de la plage DHCP (LAN)		10.10.10.20
Fin de la plage DHCP (LAN)		10.10.10.50

Les informations WAN sont celle par défaut et donc ne seront pas changées. Par contre, j'ai décidé arbitrairement des informations du réseau LAN. Vous pouvez changer l'ip du serveur, le masque de sous réseau ainsi que la plage du DHCP. Ce sont les valeurs que je vais utiliser pour le tutoriel.

Sur l'écran principal, choisissons l'option 2 (puis entrer).

Il nous indique alors les interfaces disponibles et laquelle configurer. Nous allons configurer l'interface LAN, car les paramètres de celle de l'interface WAN sont attribuées par le DHCP.

```
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (le0 - static)
Enter the number of the interface you wish to configure: █
```

Illustration 16: choix de l'interface

Entrons « 2 » pour configurer les paramètres ip de l'interface LAN.

Ensuite, nous rentrons les informations demandés tel que nous les avons vu précédemment dans le récapitulatif.

Nous commençons par l'ip de l'interface LAN, puis nous entrons le masque de sous réseau sous la forme de son CIDR. Ici nous devons mettre le masque 255.255.255.0 alors nous entrons 24.

Puis-je rentre la passerelle, ici la passerelle est l'ip du serveur.

Pour les IPv6, je fais entrer, car on va les laisser de côté. (je n'ai pas d'ipv6 sur le port WAN)

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.10.10.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8

Enter the new LAN IPv4 subnet bit count:
> 24

Enter the new LAN IPv4 gateway address. Press <ENTER> for none:
> 10.10.10.254

Enter the new LAN IPv6 address. Press <ENTER> for none:
> █
```

Illustration 17: configuration interface LAN

Ensuite, on active le serveur DHCP, puis il faut entrer les adresses IP de début et de fin de la plage IP utilisé par le serveur DHCP.

Puis, on vous propose d'activer le service de configuration web (webConfigurator). Faites « y » puis nous obtenons alors l'url qui doit être entré dans un navigateur du côté LAN, qui est ici l'ip du serveur.

```
Do you want to enable the DHCP server on LAN? [y;n] y
Enter the start address of the IPv4 client address range: 10.10.10.20
Enter the end address of the IPv4 client address range: 10.10.10.50
Disabling DHCPD...Done!

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to LAN... Reloading filter...
DHCPD... restarting webConfigurator...

The IPv4 LAN address has been set to 10.10.10.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://10.10.10.254/

Press <ENTER> to continue. █
```

Illustration 18: configuration du DHCP et activation de l'interface web

L'adresse pour se connecter à l'interface web est : <http://10.10.10.254/> (dans mon cas)

Finalement, nous nous retrouvons avec l'interface de départ.

Nous n'utiliserons plus cette interface en console sauf en cas de problème.

Fin de l'installation et interface web

Dans la première partie nous avons installé le serveur via la console. Maintenant il est temps de finir l'installation via l'interface web.

Pour y accéder entrez l'adresse web suivante :

URL du serveur web (côté LAN)	http://10.10.10.254/
Identifiant	admin
Mot de passe	pfsense

Voilà la page de connexion à l'interface web :



Illustration 19: page de connexion de l'interface web

Identifiez vous avec les identifiants indiqués ci-dessus.
Une fois identifiée, vous arriverez sur la page suivante qui nous indique que la configuration initiale va débiter :

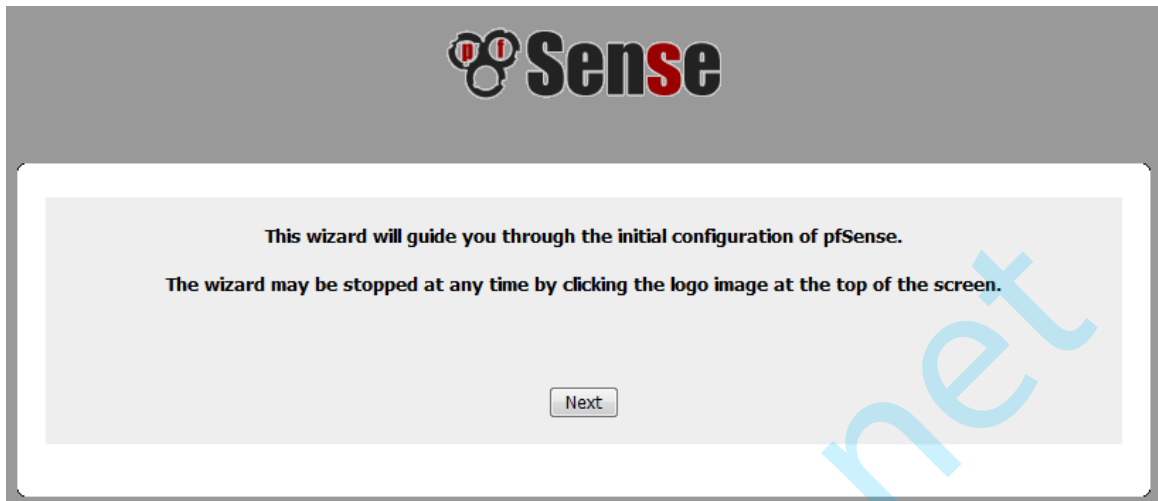


Illustration 20: page web avant la configuration

Cliquez sur next, nous arrivons sur la première page de configuration.
Nous entrons le nom du serveur pour moi j'ai choisi « srv », puis le domaine sur lequel se trouve le serveur ici « sky-future.eu ». Ensuite, il faut indiquer les serveurs DNS, j'ai choisi d'indiquer [les serveurs DNS d'OpenDNS](#). Puis laissez la dernière case cochée.



Illustration 21: 1er page de configuration web

Sur la page suivante, il faut ajouter le serveur de temps NTP, j'ai choisi celui de gandi :ntp.deuza.net
Liste de serveur NTP disponible ici : https://services.renater.fr/ntp/serveurs_francais
Choisissez la bonne zone de temps (normalement Europe/Paris).



The screenshot shows the PfSense web configuration interface. At the top, the PfSense logo is displayed. Below it, a message reads "Please enter the time, date and time zone." The main form area is titled "Time Server Information" and contains two fields: "Time server hostname:" with a text input field containing "ntp.deuza.net" and a sub-label "Enter the hostname (FQDN) of the time server.", and "Timezone:" with a dropdown menu set to "Europe/Paris". A "Next" button is located at the bottom of the form.

Illustration 22: 2ème page de configuration web

La page suivante traite de la configuration de l'interface WAN que je laisse en DHCP, je laisse les autres champs vide ou par défaut.

On this screen we will configure the Wide Area Network information.

Configure WAN Interface

SelectedType: DHCP

General configuration

MAC Address: This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU: Set the MTU of the WAN interface. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS: If you enter a value in this field, then MSS damping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

IP Address: / 1

Gateway:

DHCP client configuration

DHCP Hostname: The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

PPPoE configuration

PPPoE Username:

PPPoE Password:

PPPoE Service name: Hint: this field can usually be left empty

PPPoE Dial on demand: This option causes the interface to operate in dial-on-demand mode, allowing you to have a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected. Enable Dial-On-Demand mode

PPPoE Idle timeout: If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

RFC1918 Networks

Block RFC1918 Private Networks: When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too. Block private networks from entering via WAN


Block bogon networks

Block bogon networks: When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive. Block non-Internet routed networks from entering via WAN

Next

Illustration 23: configuration de l'interface WAN

Nous voilà sans surprise sur la page de configuration de l'interface LAN, nous n'avons normalement rien à modifier, car nous l'avons fait précédemment dans la console.



On this screen we will configure the Local Area Network information.

Configure LAN Interface

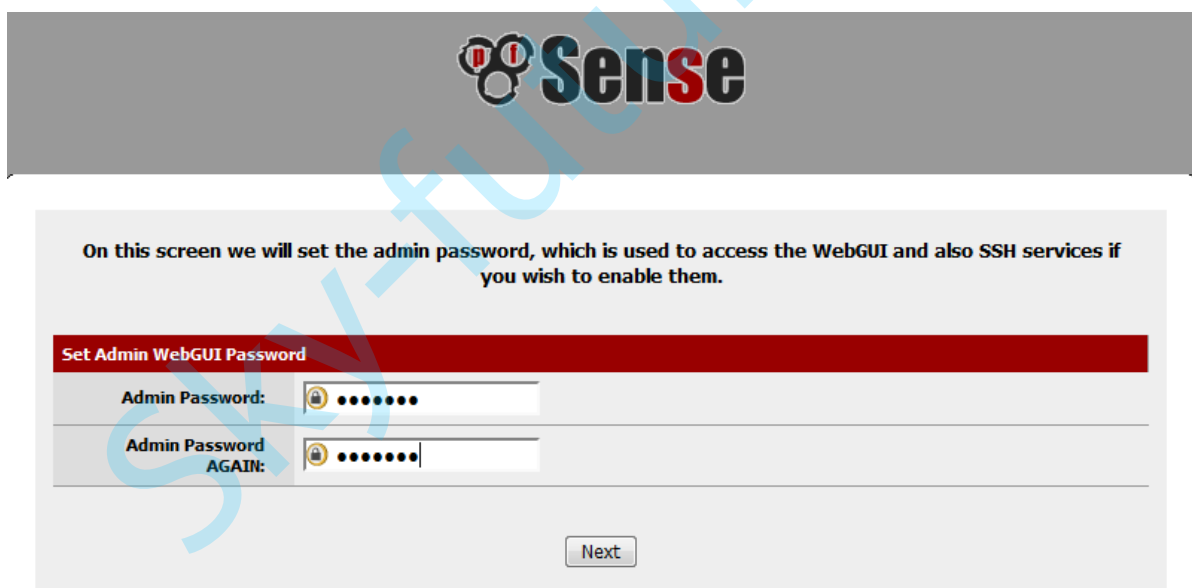
LAN IP Address: Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask:

Next

Illustration 24: configuration de l'interface LAN

Maintenant on nous demande de changer le mot de passe, il serait idiot de se faire pirater le serveur à cause un mot de passe par défaut.



On this screen we will set the admin password, which is used to access the WebGUI and also SSH services if you wish to enable them.

Set Admin WebGUI Password

Admin Password:

Admin Password AGAIN:

Next

Illustration 25: changement de mot de passe

Cliquez sur reload, pour que les modifications soient appliqués.



Illustration 26: page de chargement

Maintenant vous pouvez cliquer sur la partie surligné en jaune pour accéder à l'interface web :



Illustration 27: Fin de la configuration

Finalement, on est enfin arrivé à l'interface web :

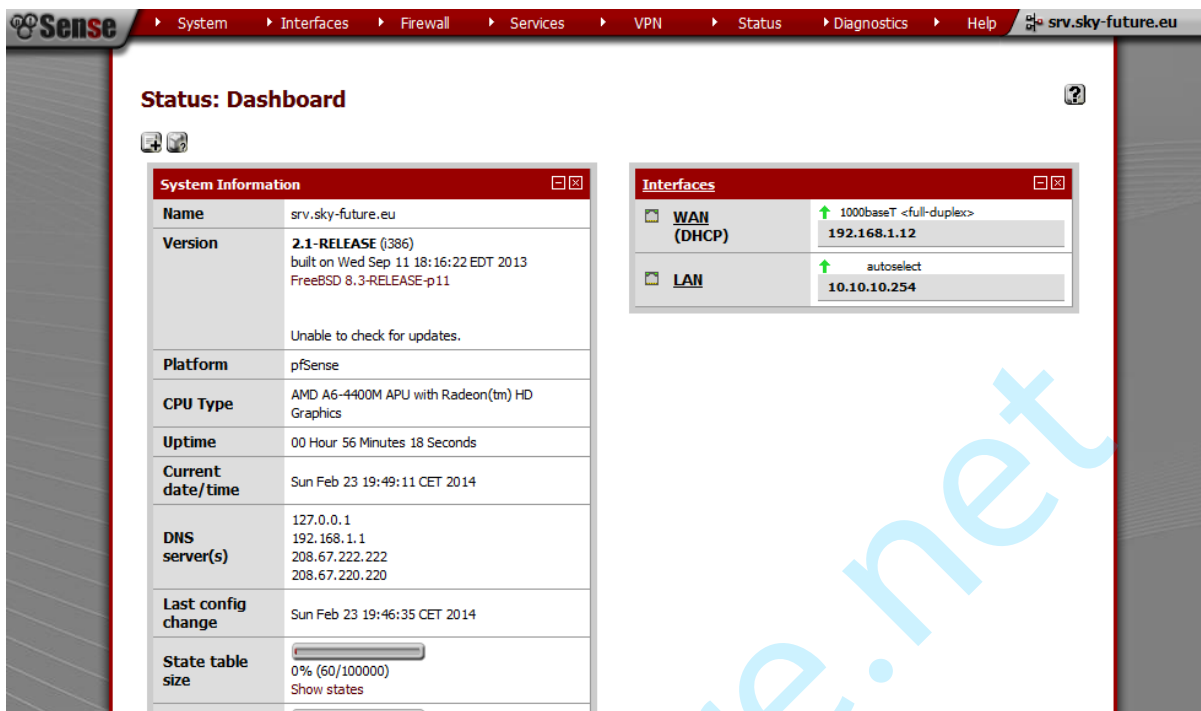


Illustration 28: Interface web

Configuration minimum

Je ne vais pas vous laisser comme cela, je vais vous expliquer très rapidement la configuration minimum à effectuer pour éviter que des petits malin branchés sur le LAN essayent de se connecter à l'interface web.

Rendez-vous dans System > Advanced. Les numéros, sont visibles sur la capture présente à la page suivante.

1. Activer le https pour que la connexion entre vous et le serveur soit chiffré.
2. Changer le numéro de port pour accéder à l'interface web. (supérieur à 49152)
3. Cochez la case pour supprimez la redirection automatique vers l'interface web lors de la connexion à l'adresse ip du serveur sur le port 80.
4. Activer le SSH pour éviter de passer par la console.
5. Entrez un numéro de port supérieur à 49152 différent du port de l'interface web choisi ci-dessus.
6. Cochez la case si vous désirez que le mot de passe de l'interface web soit demandé lors de l'accès à la console.

Une fois configuré, l'accès à l'interface web dans mon cas se fera alors avec l'adresse :
<https://10.10.10.254:55555>

Pour se connecter en SSH je me connecte avec l'ip du serveur sur le port 54321. L'identifiant pour vous connecter est : root et le mot de passe celui de l'interface web. Il en est de même si vous avez coché la

case en 6 avec la console.

System: Advanced: Admin Access



Admin Access Firewall / NAT Networking Miscellaneous System Tunables Notifications

NOTE: The options on this page are intended for use by advanced users only.

webConfigurator

Protocol **1** HTTP HTTPS

SSL Certificate webConfigurator default

TCP port **2**
Enter a custom port number for the webConfigurator above if you want to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

Max Processes
Enter the number of webConfigurator processes you want to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.

WebGUI redirect **3** **Disable webConfigurator redirect rule**
When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.

WebGUI Login Autocomplete **Disable webConfigurator login autocomplete**
When this is unchecked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to disable autocomplete on the login form so that browsers will not prompt to save credentials (NOTE: Some browsers do not respect this option).

WebGUI login messages **Disable logging of webConfigurator successful logins**
When this is checked, successful logins to the webConfigurator will not be logged.

Anti-lockout **Disable webConfigurator anti-lockout rule**
When this is unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure you have a firewall rule in place that allows you in, or you will lock yourself out!) *Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.*

DNS Rebind Check **Disable DNS Rebinding Checks**
When this is unchecked, your system is protected against DNS Rebinding attacks. This blocks private IP responses from your configured DNS servers. Check this box to disable this protection if it interferes with webConfigurator access or name resolution in your environment.

Alternate Hostnames
Alternate Hostnames for DNS Rebinding and HTTP_REFERER Checks
Here you can specify alternate hostnames by which the router may be queried, to bypass the DNS Rebinding Attack checks. Separate hostnames with spaces.

Browser HTTP_REFERER enforcement **Disable HTTP_REFERER enforcement check**
When this is unchecked, access to the webConfigurator is protected against HTTP_REFERER redirection attempts. Check this box to disable this protection if you find that it interferes with webConfigurator access in certain corner cases such as using external scripts to interact with this system. More information on HTTP_REFERER is available from Wikipedia.

BEAST Attack Protection **Mitigate the BEAST SSL Attack**
When this is checked, the webConfigurator can mitigate BEAST SSL attacks. This option is off by default because Hifn accelerators do NOT work with this option, and the GUI will not function. It is possible that other accelerators have a similar problem that is not yet known/documented. More information on BEAST is available from Wikipedia.

Secure Shell

Secure Shell Server **4** **Enable Secure Shell**

Authentication Method **Disable password login for Secure Shell (RSA/DSA key only)**
When enabled, authorized keys need to be configured for each user that has been granted secure shell access.

SSH port **5**
Note: Leave this blank for the default of 22.

Serial Communications

Serial Terminal **Enables the first serial port with 9600/8/N/1 by default, or another speed selectable below.** Note: This will redirect the console output and messages to the serial port. You can still access the console menu from the internal video card/keyboard. A null modem serial cable or adapter is required to use the serial console.

Serial Speed bps
Allows selection of different speeds for the serial console port.

Console Options

Console menu **6** **Password protect the console menu**
Changes to this option will take effect after a reboot.

Conclusion

L'objectif de ce tutoriel est terminé, je vous laisse essayer de configurer pfsense comme bon vous semble. Dans les futures tutoriels sur pfsense, nous verrons comment configurer le portail captif entre le WAN et LAN, comment régler le par feu les différentes règles qui peuvent être appliqués en entré et en sortie. Ou même la configuration d'un VPN.

Si vous remarquez des erreurs et/ou des remarques veuillez me les adresser par mail à :

luo@sky-future.net

SKY-future.net