

Documentation technique PFsense



Sommaire :

Table des matières

1.	Installation de PfSense :	3
2.	Accès a l'interface web de PfSense :	6
3.	Mise en place d'un filtrage « Deny all »	9
4.	Mise en place d'un portail captif :	12

1. Installation de PfSense :

Configuration de la VM et ses interface réseaux :

Général

Nom : VM-PFSense
Système d'exploitation : Windows 7 (64-bit)

System

Mémoire vive : 3072 Mo
Ordre d'amorçage : Disquette, Optique, Disque dur
Accélération : VT-x/AMD-V, Pagination imbriquée, Paravirtualisation Hyper-V

Affichage

Mémoire vidéo : 27 Mo
Contrôleur graphique : VBoxSVGA
Serveur de bureau à distance : Désactivé
Enregistrement : Désactivé

Stockage

Contrôleur : SATA
Port SATA 0 : VM-PFSense.vdi (Normal, 11,58 Gio)

Audio

Pilote hôte : Windows DirectSound
Contrôleur : Intel Audio HD

Réseau

Interface 1: Intel PRO/1000 MT Desktop (NAT)
Interface 2: Intel PRO/1000 MT Desktop (Réseau privé hôte, 'VirtualBox Host-Only Ethernet Adapter')

USB

Contrôleur USB : OHCI
Filtres de périphérique : 0 (0 actif)

Dossiers partagés

Aucun

Description

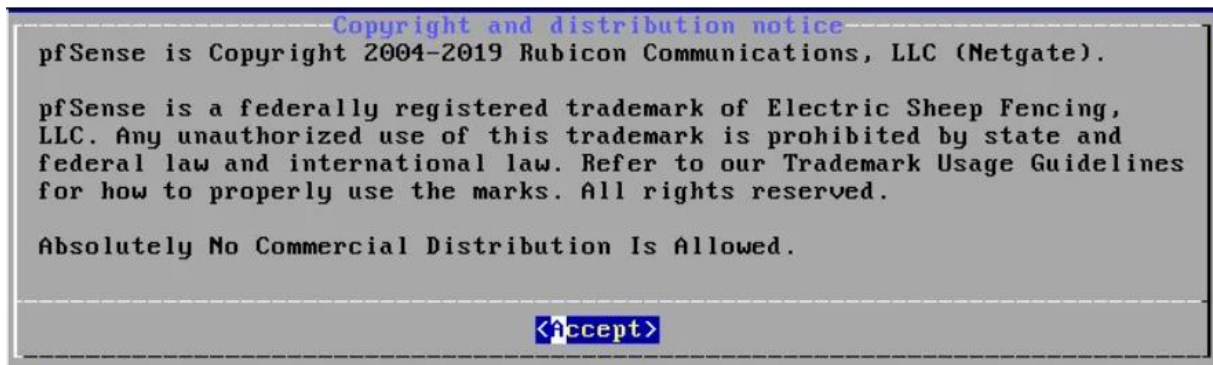
Aucune

Prévisualisation

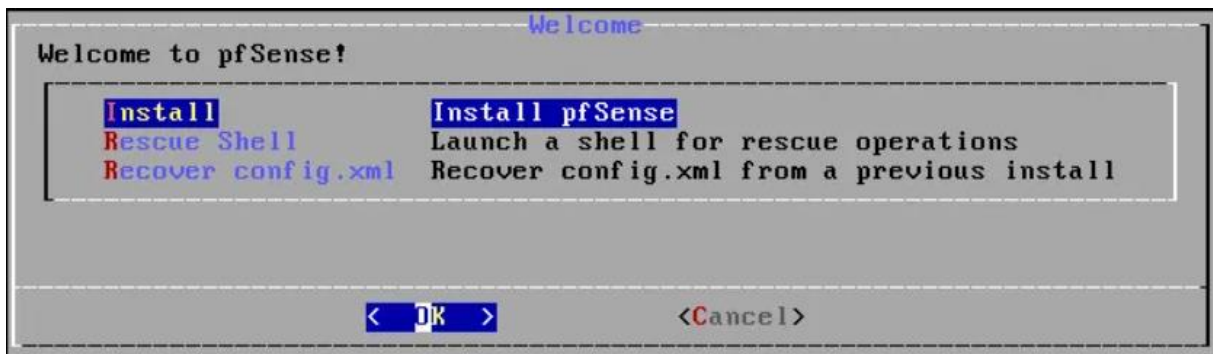
Ensuite on lance la VM :



Accepter le contrat de licence utilisateur final PFsense :

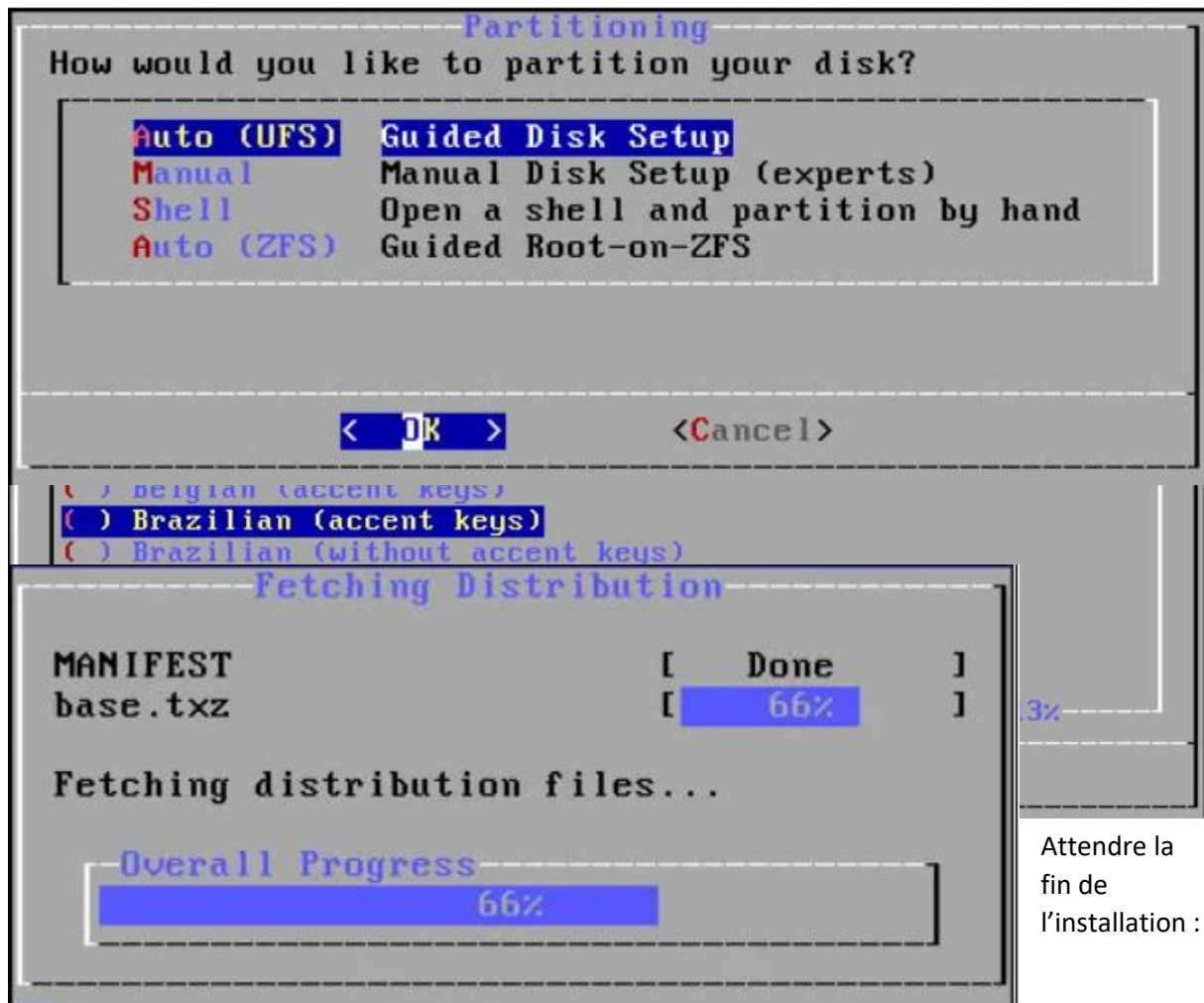


Choisir installer PFsense :

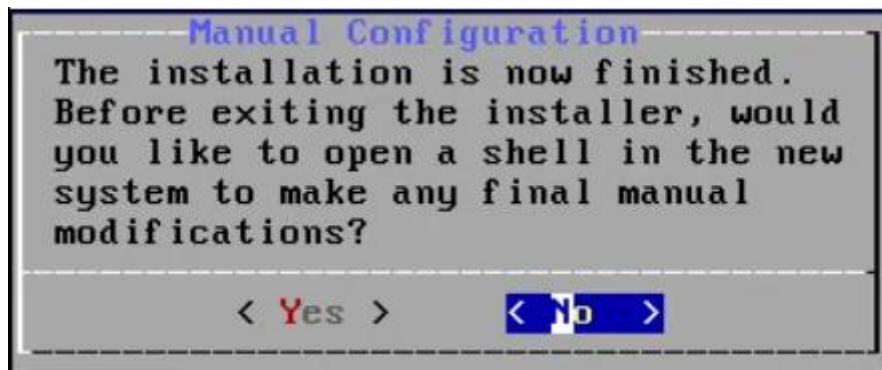


Sélectionner le clavier que l'on souhaite :

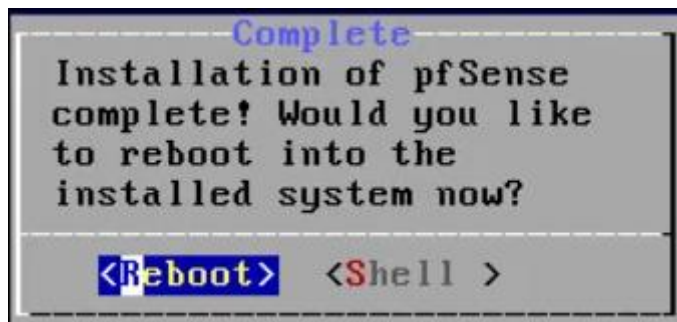
Choisir le partitionnement du disque automatiquement :



Sélectionner non pour l'écran de configuration manuelle :



Choisir reboot et enlever le support d'installation :

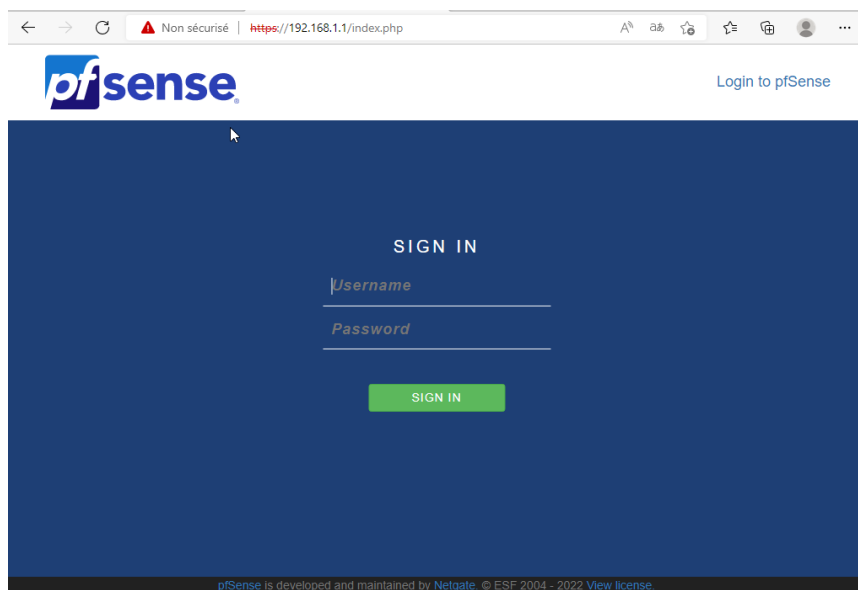


Ensuite nous arrivons sur le menu de PfSense et c'est good :



2. Accès à l'interface web de PfSense :

Il faut avoir un client dans le même réseau que notre serveur PfSense et ensuite taper l'adresse LAN de notre serveur PfSense et on accède à l'interface :



Le nom d'utilisateur et le mot de passe par défaut sont :

Nom d'utilisateur : admin

Mot de passe : pfsense

Nous arrivons sur la page de configuration de pfsense :

The screenshot displays the pfSense Community Edition dashboard. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into two panels. The left panel, titled 'System Information', contains a table with details about the system, including the name, user, system type, BIOS information, version, CPU type, and hardware crypto status. The right panel, titled 'Netgate Services And Support', shows the contract type as 'Community Support' and provides links to various support resources, including the Netgate Resource Library, upgrade options, and community support resources.

System Information	
Name	pfSense.home.arpa
User	admin@192.168.1.120 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 0d73e621b219924abae4
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE The system is on the latest version. Version information updated at Wed Jun 15 6:45:32 UTC 2022
CPU Type	Intel(R) Core(TM) i7-10870H CPU @ 2.20GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel DTU	Disabled

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Visit Netgate.com

(Ne pas oublier de changer le mot de passe admin)

3. Mise en place d'un filtrage « Deny all »

Il faut se rendre dans firewall -> Rules puis LAN et ensuite il faut créer une règle ou l'on block toutes les connexions dans le LAN :

Firewall / Rules / Edit

Edit Firewall Rule

Action

Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4+IPv6

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

any

Source Address

/

Destination

Destination

☐ Invert match

any

Destination Address

/

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Deny all

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Rule Information

Tracking ID

1655285481

Created

6/15/22 09:31:21 by admin@192.168.1.100 (Local Database)

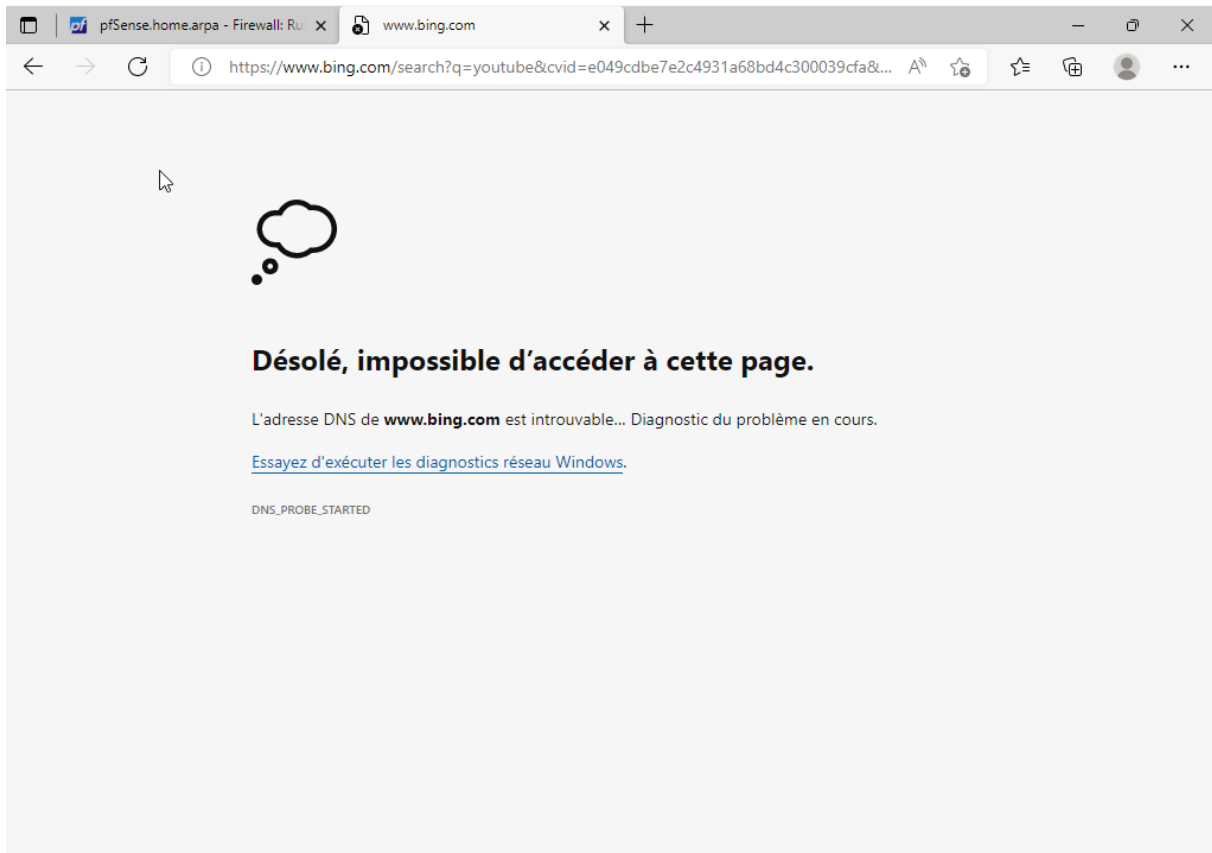
Updated

6/15/22 11:03:52 by admin@192.168.1.100 (Local Database)

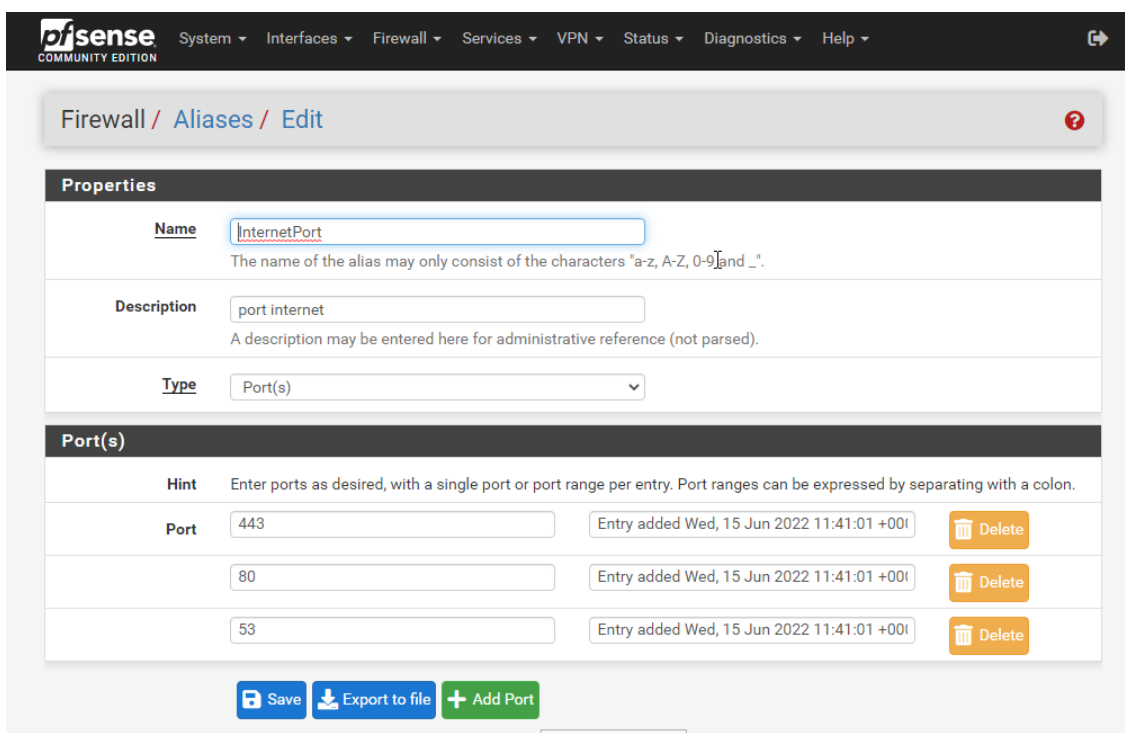
Save

Parler à Cortana

Voilà qui est fait ! (Screen de ma machine de test) :



Maintenant nous voulons avoir accès seulement à internet donc nous allons créer un alias pour inclure les ports d'internet :



Ensuite nous allons créer une règle qui inclut cet alias en destination et en source « LAN net » :

Choose the interface from which packets must come to match this rule.

Address Family IPv4+IPv6
Select the Internet Protocol version this rule applies to.

Protocol TCP/UDP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match LAN net Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

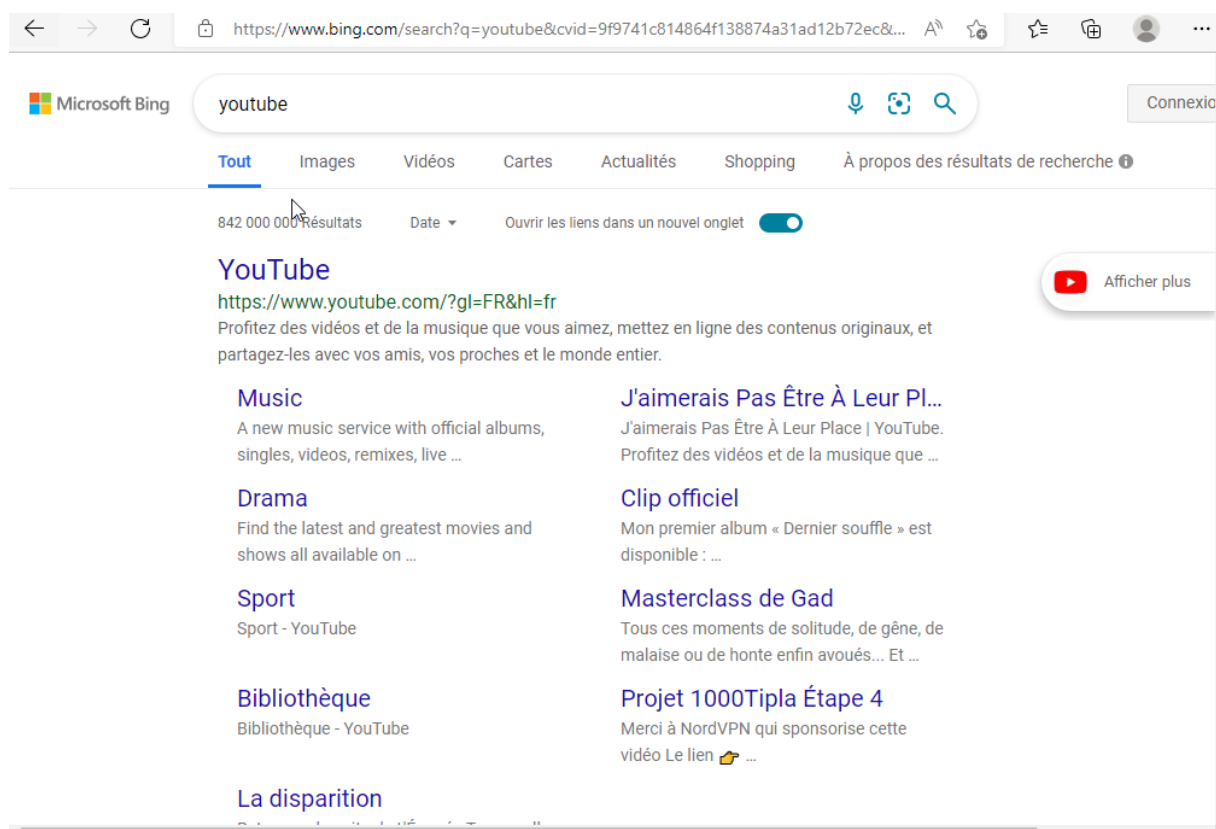
Destination ☐ Invert match any Destination Address /

Destination Port Range

From (other) InternetPort To (other) InternetPort
Custom Custom

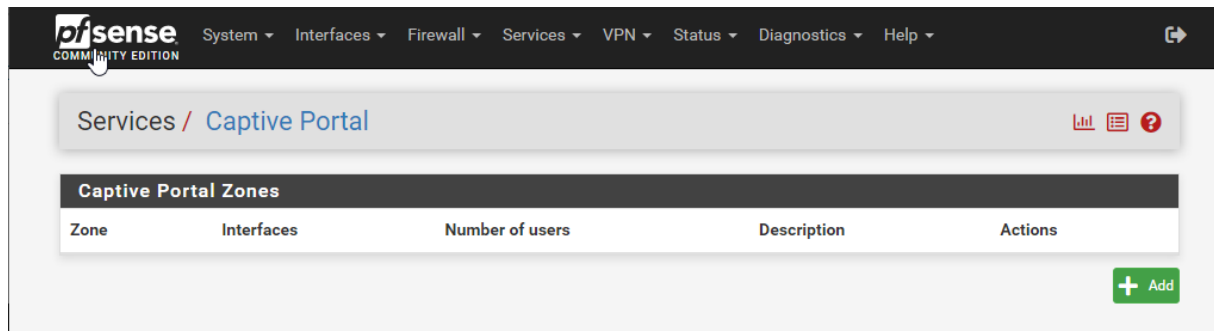
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Et voila nous avons maintenant accès qu'a internet :



4. Mise en place d'un portail captif :

Pour créer un portail captif il faut aller dans services -> Captive Portal :



Ensuite add et mettre le nom que l'on souhaite :


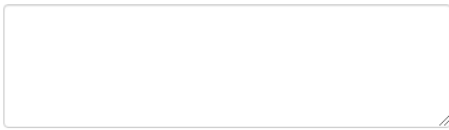
The screenshot shows the 'Add Captive Portal Zone' form. The form has two main sections: 'Zone name' and 'Zone description'. The 'Zone name' field contains 'TP_PFsense' and has a note: 'Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.' The 'Zone description' field contains 'Portail Captif' and has a note: 'A description may be entered here for administrative reference (not parsed)'. At the bottom of the form is a blue 'Save & Continue' button.

Puis nous arrivons dans la configuration du portail (suivre les captures d'écrans) :

The screenshot shows the 'Captive Portal Configuration' form. The form has several sections: 'Enable' with a checked checkbox 'Enable Captive Portal'; 'Description' with the text 'Portail Captif' and a note: 'A description may be entered here for administrative reference (not parsed)'; 'Interfaces' with a dropdown menu showing 'WAN' and 'LAN' selected, and a note: 'Select the interface(s) to enable for captive portal.'; 'Maximum concurrent connections' with a value of '1' and a note: 'Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.'; 'Idle timeout (Minutes)' with a value of '5' and a note: 'Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.'; 'Hard timeout (Minutes)' with a blank field and a note: 'Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).'; and 'Traffic quota (Megabytes)' with a blank field and a note: 'Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.'

	the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.
Waiting period to restore pass-through credits. (Hours)	<input type="text"/> Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.
Reset waiting period	<input type="checkbox"/> Enable waiting period reset on attempted access If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.
Logout popup window	<input checked="" type="checkbox"/> Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
Pre-authentication redirect URL	<input type="text" value="http://www.google.fr"/> Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRECTURL\$ variable in captiveportal's HTML pages.
After authentication Redirection URL	<input type="text" value="http://www.google.fr"/> Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.
Blocked MAC address redirect URL	<input type="text"/> Blocked MAC addresses will be redirected to this URL when attempting access.
Preserve users database	<input type="checkbox"/> Preserve connected users across reboot If enabled, connected users won't be disconnected during a pfSense reboot.

Preserve users database	<input type="checkbox"/> Preserve connected users across reboot If enabled, connected users won't be disconnected during a pfSense reboot.
Concurrent user logins	<input type="text" value="Disabled"/> Disabled: Do not allow concurrent logins per username or voucher. Multiple: No restrictions to the number of logins per username or voucher will be applied. Last login: Only the most recent login per username or voucher will be granted. Previous logins will be disconnected. First login: Only the first login per username or voucher will be granted. Further login attempts using the username or voucher will not be possible while an initial user is already active.
MAC filtering	<input checked="" type="checkbox"/> Disable MAC filtering If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.
Pass-through MAC Auto Entry	<input type="checkbox"/> Enable Pass-through MAC automatic additions When enabled, a MAC passthrough entry is automatically added after the user has successfully authenticated. Users of that MAC address will never have to authenticate again. To remove the passthrough MAC entry either log in and remove it manually from the MAC tab or send a POST from another system. If this is enabled, the logout window will not be shown.
Per-user bandwidth restriction	<input type="checkbox"/> Enable per-user bandwidth restriction
Use custom captive portal page	<input type="checkbox"/> Enable to use a custom captive portal login page If set a portal.html page must be created and uploaded. If unchecked the default template will be used
Captive Portal Login Page	
Display custom logo image	<input type="checkbox"/> Enable to use a custom uploaded logo

Use custom captive portal page	<input type="checkbox"/> Enable to use a custom captive portal login page If set a portal.html page must be created and uploaded. If unchecked the default template will be used
Captive Portal Login Page	
Display custom logo image	<input type="checkbox"/> Enable to use a custom uploaded logo
Logo Image  <div> <input type="button" value="Choisir un fichier"/> Aucun fichier n'a été sélectionné </div> <p>Add a logo for use in the default portal login screen. File will be renamed captiveportal-logo.* The image will be resized to fit within the given area, It can be of any image type: .png, .jpg, .svg This image will not be stored in the config. The default logo will be used if no custom image is present.</p>	
Display custom background image	<input type="checkbox"/> Enable to use a custom uploaded background image
Background Image <div> <input type="button" value="Choisir un fichier"/> Aucun fichier n'a été sélectionné </div> <p>Add a background image for use in the default portal login screen. File will be renamed captiveportal-background.* The background image will fill the screen. This image will not be stored in the config. The default background image will be used if no custom background is present.</p>	
Terms and Conditions	<div>  </div> <p>Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out</p>

Authentication Method	<div> <input type="button" value="Choisir un fichier"/> Aucun fichier n'a été sélectionné </div> <p>Select an Authentication Method to use for this zone. One method must be selected.</p> <ul style="list-style-type: none"> - "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers. - "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button. - "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.
Authentication Server	<div> <input type="button" value="Choisir un fichier"/> Aucun fichier n'a été sélectionné </div> <p>You can add a remote authentication server in the User Manager. Vouchers could also be used, please go to the Vouchers Page to enable them.</p>
Secondary authentication Server	<div> <input type="button" value="Choisir un fichier"/> Aucun fichier n'a été sélectionné </div> <p>You can optionally select a second set of servers to to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.</p>
Reauthenticate Users	<input type="checkbox"/> Reauthenticate connected users every minute If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests.
Local Authentication	<input checked="" type="checkbox"/> Allow only users/groups with "Captive portal login" privilege set

Et enfin faite SAVE.

Après il faut créer des utilisateurs :

System / User Manager / Users

Users Groups Settings Authentication Servers

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input checked="" type="checkbox"/>	agent		✓	Agent	
<input type="checkbox"/>	test	un utilisateur pour le portail	✓	Portail	

Cliquer sur Add et créer un utilisateur pour la gestion des comptes qui auront accès au portail captif (ici c'est agent qui est cet utilisateur)

Il dispose des privilèges ci-dessous :

Effective Privileges

Inherited from	Name	Description	Action
Agent	WebCfg - System: User Manager	Allow access to the 'System: User Manager' page. (admin privilege)	
Agent	WebCfg - Status: Captive Portal	Allow access to the 'Status: Captive Portal' page.	

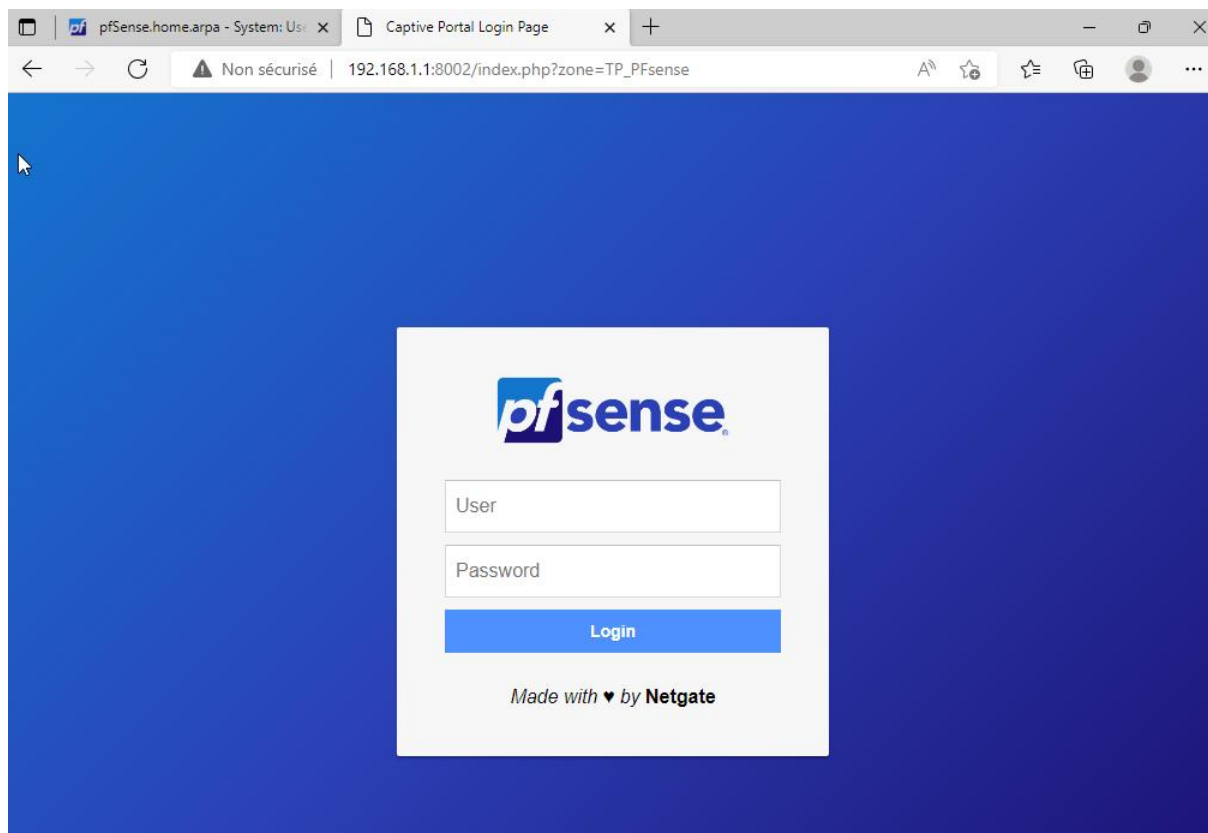
Security notice: This user effectively has administrator-level access

Ensuite il faut créer un groupe pour autoriser les utilisateurs à utiliser le portail captif

Groups

Group name	Description	Member Count	Actions
Agent	Creation utilisateur pour portail	1	
Portail	Utilisateur du portail	1	
admins	System Administrators	1	
all	All Users	3	

Et enfin pour accéder au portail il faut taper l'adresse :
http://192.168.1.1:8002/index.php?zone=TP_PFSense



Ensuite la personne n'a qu'à se connecter avec ses identifiants.