

CCI Campus de Strasbourg

Travaux pratiques

Comprendre et mettre en œuvre des règles de Firewalling.


CUGNIN Samuel
15/06/2022



Table des matières


1.0. Filtrage : « Deny ALL »	2
2.0. Filtrage : « Internet »	3
3.0. Portail Captive.	4
Annexes.	6

1.0. Filtrage : « Deny ALL ».

- Connexion sur le FW depuis un navigateur. (192.168.2.254). (Voir annexe).
- Création et configuration de l'Alias : (Voir annexe).
 - o Onglet Firewall>Aliases>Ports.
 - o Bouton ADD+.
 - Configuration de l'Alias. (Voir annexe).
- Création et configuration des règles de Firewalling.
 - o Onglet Firewall>Rules>WAN.
 - o Bouton ADD  .
 - Configuration de la règle d'interdiction de « Any » from WAN to LAN.








Edit Firewall Rule	
Action	<div>Block</div> <div>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.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>WAN</div> <div>Choose the interface from which packets must come to match this rule.</div>
Address Family	<div>IPv4+IPv6</div> <div>Select the Internet Protocol version this rule applies to.</div>
Protocol	<div>Any</div> <div>Choose which IP protocol this rule should match.</div>
Source	
Source	<div><input type="checkbox"/> Invert match</div> <div>WAN net</div> <div>Source Address /</div>
Destination	
Destination	<div><input type="checkbox"/> Invert match</div> <div>LAN net</div> <div>Destination Address /</div>
Extra Options	
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <div>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).</div>
Description	<div></div> <div>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.</div>
Advanced Options	<div>Display Advanced</div>
Rule Information	
Tracking ID	1655298313
Created	6/15/22 13:05:13 by admin@192.168.2.10 (Local Database)
Updated	6/15/22 13:14:00 by admin@192.168.2.10 (Local Database)

2.0. Filtrage : « Internet ».

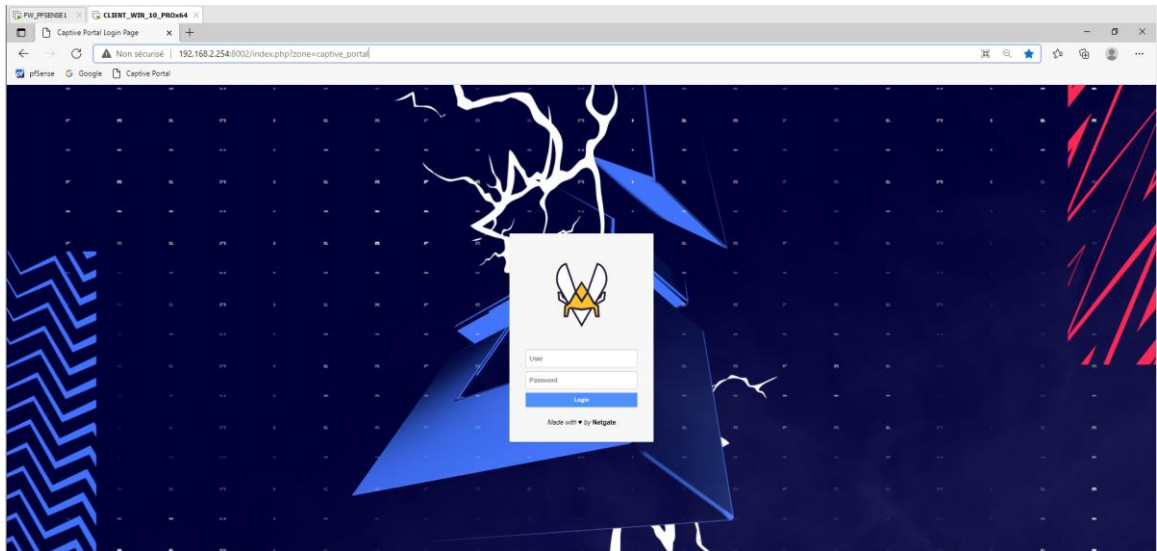
- Création et configuration des règles de Firewalling.
 - o Onglet Firewall>Rules>LAN.
 - o Bouton ADD  .
 - Configuration de la règle d'autorisation TCP/UDP/HTTP(S) from LAN to WAN.

Edit Firewall Rule	
Action	<div>Pass</div> <div>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.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>LAN</div> <div>Choose the interface from which packets must come to match this rule.</div>
Address Family	<div>IPv4+IPv6</div> <div>Select the Internet Protocol version this rule applies to.</div>
Protocol	<div>TCP/UDP</div> <div>Choose which IP protocol this rule should match.</div>
Source	
Source	<div><input type="checkbox"/> Invert match</div> <div>LAN net</div> <div>Source Address /</div>
<div>Display Advanced</div> <div>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.</div>	
Destination	
Destination	<div><input type="checkbox"/> Invert match</div> <div>any</div> <div>Destination Address /</div>
Destination Port Range	<div>(other)</div> <div>ALIAS_TCP_UDP_HTTP.</div> <div>(other)</div> <div>ALIAS_TCP_UDP_HTTP.</div> <div>From Custom To Custom</div> <div>Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.</div>
Extra Options	
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <div>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).</div>
Description	<div></div> <div>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.</div>
Advanced Options	<div>Display Advanced</div>
Rule Information	
Tracking ID	1655298118
Created	6/15/22 13:01:58 by admin@192.168.2.10 (Local Database)
Updated	6/15/22 13:14:39 by admin@192.168.2.10 (Local Database)

3.0. Portail Captive.

- Création et configuration du portail captive.
 - o Onglet Services>Captive Portal.
 - o Bouton ADD .
 - Zone name : CAPTIVE_PORTAL.
 - Zone description : N/A.
 - o Après création du portail captive :
 - Activer « Enable Captive Portal ».
 - Sélectionner l'interface « LAN ».
 - Maximum concurrent connections set to 1.
 - Idle timeout (Minutes) set to 5.
 - Activer « Enable logout popup window ».
 - Définition de « Pre-authentication Redirect URL » to <http://www.google.com>.
 - Définition « After authentication Redirection URL » to <http://www.google.com>.
 - Activer « Disable Concurrent user logins ».
 - Activer « Disable MAC filtering ».
 - Sélectionner « Use an Authentication backend » et sélectionner « Local Database » dans la partie « Authentication Server ».
- Création des groupes.
 - o Onglet System>User Manager>Groups.
 - o Bouton ADD .
 - Renseigner le Nom du Groupe « Agents » et sa description « Delegation Creation Utilisateurs Portail ».
 - Après la création du groupe, éditer le groupe :
 - Bouton ADD  > rubrique « Assigned Privileges ».
 - Sélectionnez dans la liste « WebCfg – System: User Manager ».
 - Revenir à la rubrique « Assigned Privileges » en cliquant sur Bouton ADD .
 - Sélectionnez dans la liste « WebCfg – Status: Captive Portal ».
 - o Bouton ADD .
 - Renseigner le Nom du Groupe « Agents » et sa description « Delegation Creation Utilisateurs Portail ».
 - Après la création du groupe, éditer le groupe :
 - Bouton ADD  > rubrique « Assigned Privileges ».
 - Sélectionnez dans la liste « User – Services: Captive Portal login ».
 -
- Création des utilisateurs.
 - o Onglet System>User Manager>Users.
 - o Bouton ADD .
 - Entrer un Nom d'Utilisateur « agent », son mot de passe et sa description.
 - Sélectionner dans « Group membership » le groupe « Agents » précédemment créé. Cliquez sur « Move to Member of list ».

- Bouton ADD ↱ .
 - Entrer un Nom d'Utilisateur « test », son mot de passe et sa description.
 - Sélectionner dans « Group membership » le groupe « Portail » précédemment créé. Cliquez sur « Move to Member of list ».
- Connexion au portail captif via l'adresse :
http://192.168.2.254:8002/index.php?zone=captive_portal.
-



Annexes.

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.2.10 (Local Database)
System	VMware Virtual Machine Netgate Device ID: dd4b979f7530a0277fe0
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
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 13:16:45 UTC 2022
CPU Type	AMD Ryzen 7 5700U with Radeon Graphics AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	01 Hour 34 Minutes 41 Seconds
Current date/time	Wed Jun 15 14:50:44 UTC 2022
DNS server(s)	<ul style="list-style-type: none">127.0.0.1192.168.1.28.8.8.88.8.4.4
Last config change	Wed Jun 15 13:14:39 UTC 2022
State table size	0% (8/19000) Show states
MBUF Usage	0% (2312/1000000)
Load average	0.08, 0.29, 0.34
CPU usage	6%
Memory usage	72% of 190 MiB
SWAP usage	5% of 1024 MiB

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
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support [here](#).

Interfaces

WAN	↑	1000baseT <full-duplex>	192.168.1.128
LAN	↑	1000baseT <full-duplex>	192.168.2.254

Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
CAPTIVE_PORTAL	LAN	0	V for Victory	Edit Delete

Captive Portal Configuration	
Enable	<input checked="" type="checkbox"/> Enable Captive Portal
Description	<input type="text" value="V for Victory"/> <p>A description may be entered here for administrative reference (not parsed).</p>
Interfaces	<div> <div>WAN</div> <div>LAN</div> </div> <p>Select the interface(s) to enable for captive portal.</p>
Maximum concurrent connections	<input type="text" value="1"/> <p>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.</p>
Idle timeout (Minutes)	<input type="text" value="5"/> <p>Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.</p>
Hard timeout (Minutes)	<input type="text"/> <p>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).</p>
Traffic quota (Megabytes)	<input type="text"/> <p>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.</p>
Pass-through credits per MAC address.	<input type="text"/> <p>Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, 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.</p>
Waiting period to restore pass-through credits. (Hours)	<input type="text"/> <p>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.</p>
Reset waiting period	<input type="checkbox"/> Enable waiting period reset on attempted access <p>If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.</p>
Logout popup window	<input checked="" type="checkbox"/> Enable logout popup window <p>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.</p>
Pre-authentication redirect URL	<input type="text" value="http://www.google.fr"/> <p>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.</p>
After authentication Redirection URL	<input type="text" value="http://www.google.fr"/> <p>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.</p>

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.
Concurrent user logins	<div>Disabled ▼</div> <p>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.</p>
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 checked="" 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 checked="" 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> <input type="text"/> </div> <p>Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out</p>

Authentication

Authentication Method

Use an Authentication backend

Select an Authentication Method to use for this zone. One method must be selected.

- "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

Local Database

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.

Secondary authentication Server

Local Database

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.

Reauthenticate Users

☐ 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 Privileges

☒ Allow only users/groups with "Captive portal login" privilege set

HTTPS Options

Login

☐ Enable HTTPS login

When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

Users				
	Username	Full name	Status	Groups
<input checked="" type="checkbox"/>	Agent	Agent allowed to create user captive portal	✓	
<input type="checkbox"/>	admin	System Administrator	✓	admins
<input type="checkbox"/>	test	Portal user	✓	Portal

User Properties

Defined by

USER

Disabled

☐ This user cannot login

Username

Agent

Password

Password

Confirm Password

Full name

Agent allowed to create user captive portal

User's full name, for administrative information only

Expiration date

Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings

☐ Use individual customized GUI options and dashboard layout for this user.

Group membership

Agent

Portal

admins

Not member of

Member of

➡ Move to "Member of" list

⬅ Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

User Properties

Defined by

USER

Disabled

☐ This user cannot login

Username

test

Password

Password

Confirm Password

Full name

Portal user

User's full name, for administrative information only

Expiration date

Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings

☐ Use individual customized GUI options and dashboard layout for this user.

Group membership

Agent

admins

Not member of

Portal

Member of

» Move to "Member of" list

« Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Groups			
Group name	Description	Member Count	Actions
Agent	Delegation Creation Utilisateurs Portal	0	
Portal	Portal user	1	
admins	System Administrators	1	
all	All Users	3	

Group Properties

Group name

Agent

Scope

Local

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description

Delegation Creation Utilisateurs Portal

Group description, for administrative information only

Group membership

Agent

admin

test

Not members

Members

» Move to "Members"

« Move to "Not members"

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Assigned Privileges		
Name	Description	Action
WebCfg - System: User Manager	Allow access to the 'System: User Manager' page. (admin privilege)	
WebCfg - Status: Captive Portal	Allow access to the 'Status: Captive Portal' page.	
Security notice: Users in this group effectively have administrator-level access		
Add		

Group Properties

Group name

Portal

Scope

Local

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description

Portal user

Group description, for administrative information only

Group membership

Agent
admin

Not members

test

Members

Move to "Members"

Move to "Not members"

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Assigned Privileges

Name	Description	Action
User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.	

Add