

Rapport de Test

Configuration du routeur Pfsense

Configuration dur routeur avec les OPT1 qui est mon vlan 2 et OPT2 qui est mon vlan 3 :

```
VirtualBox Virtual Machine - Netgate Device ID: 4c187d5073644e33ab19

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.1.44.121/16
LAN (lan)      -> em1      -> v4: 192.168.10.254/24
OPT1 (opt1)    -> em2      -> v4: 192.168.20.254/24
OPT2 (opt2)    -> em3      -> v4: 192.168.30.254/24
```

Configuration du serveur

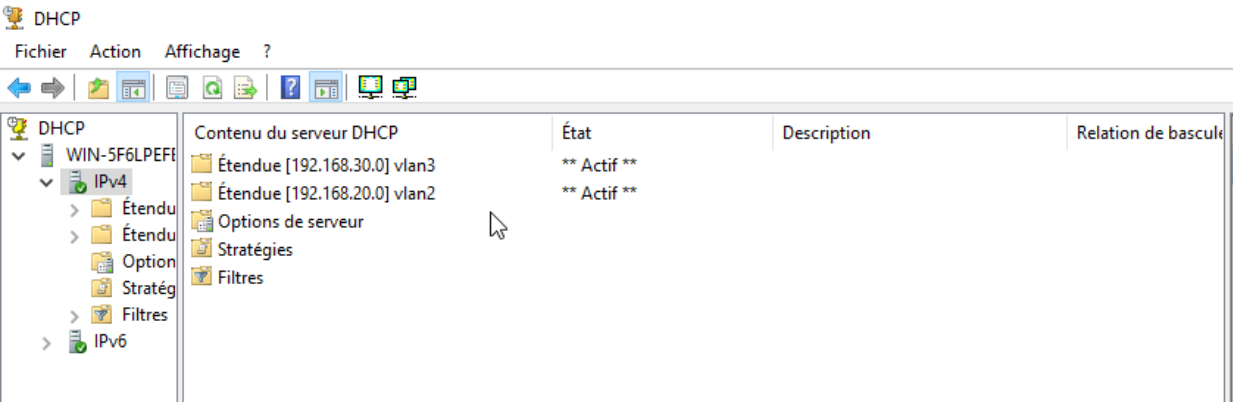
Configuration de mon serveur DHCP et DNS :

```
Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Adresse physique . . . . . : 08-00-27-1A-E9-9D
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::2867:b7b5:ec84:8a71%17(préfééré)
Adresse IPv4. . . . . : 192.168.10.1(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.10.254
IAID DHCPv6 . . . . . : 101187623
DUID de client DHCPv6. . . . . : 00-01-00-01-2E-E1-09-15-08-00-27-1A-E9-9D
Serveurs DNS. . . . . : 192.168.10.1
                        8.8.8.8
NetBIOS sur Tcpi. . . . . : Activé
```

Configuration du server DHCP

Configuration des pools dhcp pour mon vlan 2 et mon vlan 3 :



Configuration du relay DHCP

Configuration de mon DHCP relay :

←↻🔴 Non sécurisé | https://192.168.10.254/services_dhcp_relay.php

🔍🔖🏠🔖🔖

Services / DHCP Relay

The changes have been applied successfully.

DHCP Relay Configuration

Enable

☒ Enable DHCP Relay

Downstream Interfaces

WAN

LAN

OPT1

OPT2

Interfaces without an IPv4 address will not be shown.

CARP Status VIP

none

DHCP Relay will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.

☐ Append circuit ID and agent ID to requests

Append the circuit ID (interface number) and the agent ID to the DHCP request.

Upstream Servers

192.168.10.1

+ Add Upstream Server

Configuration du PC

Configuration de mon pc sur le vlan 2 :

```
Carte Ethernet Ethernet 2 :
Suffixe DNS propre à la connexion. . . :
Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter #2
Adresse physique . . . . . : 08-00-27-47-AA-90
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::e881:2dd2:a0a3:3ee7%6(préfééré)
Adresse IPv4. . . . . : 192.168.20.1(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : mercredi 4 décembre 2024 10:11:11
Bail expirant. . . . . : jeudi 12 décembre 2024 10:11:12
Passerelle par défaut. . . . . : 192.168.20.254
Serveur DHCP . . . . . : 192.168.10.1
IAID DHCPv6 . . . . . : 319291431
DUID de client DHCPv6. . . . . : 00-01-00-01-2E-E1-09-15-08-00-27-1A-E9-9D
Serveurs DNS. . . . . : 192.168.10.1
                        8.8.8.8
NetBIOS sur Tcpi. . . . . : Activé
```

Configuration de mon pc sur le vlan 3 :

```
Carte Ethernet Ethernet 3 :

Suffixe DNS propre à la connexion. . . . :
Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter #3
Adresse physique . . . . . : 08-00-27-2D-A3-DE
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::4cd5:c5f4:4ba2:eb3d%11(préfééré)
Adresse IPv4. . . . . : 192.168.30.1(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : mercredi 4 décembre 2024 10:11:15
Bail expirant. . . . . : jeudi 12 décembre 2024 10:11:16
Passerelle par défaut. . . . . : 192.168.30.254
Serveur DHCP . . . . . : 192.168.10.1
IAID DHCPv6 . . . . . : 336068647
DUID de client DHCPv6. . . . . : 00-01-00-01-2E-E1-09-15-08-00-27-1A-E9-9D
Serveurs DNS. . . . . : 192.168.10.1
                        8.8.8.8
NetBIOS sur Tcpi. . . . . : Activé
```

Configuration du serveur proxy:

DHCP

Fichier Action Affichage ?

DHCP

WIN-5F6LPEFF

IPv4

Étendu

Étendu

Option

Stratég

Filtres

IPv6

Contenu du serveur DHCP

État

Description

Relation de bascule

Étendue [192.168.30.0] vlan3

Étendue [192.168.20.0] vlan2

Options de serveur

Stratégies

Filtres

** Actif **

** Actif **

pfSense

COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Package / Proxy Server: General Settings / General

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status Sync

Squid General Settings

Enable Squid Proxy

☒ Check to enable the Squid proxy.

Important: If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data

☒ If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.

Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

Listen IP Version

IPv4

Select the IP version Squid will use to select addresses for accepting client connections.

CARP Status VIP

none

Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.

Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization.

Proxy Interface(s)

WAN LAN OPT1 OPT2

Outgoing Network Interface

Default (auto)

The interface the proxy server will use for outgoing connections.

Proxy Port

3128

This is the port the proxy server will listen on. Default: 3128

ICP Port

This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

Allow Users on Interface

☒ If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy.
There will be no need to add the interface's subnet to the list of allowed subnets.

Patch Captive Portal

This feature was removed - see Bug #5594 for details!

Resolve DNS IPv4 First

☒ Enable this to force DNS IPv4 lookup first.
This option is very useful if you have problems accessing HTTPS sites.

Disable ICMP

☐ Check this to disable Squid ICMP pinger helper.

Use Alternate DNS Servers for the Proxy Server

To use DNS servers other than those configured in System > General Setup, enter the IP(s) here. Separate entries by semi-colons (;)

Extra Trusted CA

none

Select extra Trusted CA certificate in addition to the default root certificate bundle.
Warning: This option may only be required if the upstream proxy is using SSL/MITM mode and could be a security issue in other cases.

Transparent HTTP Proxy

☒ Enable transparent mode to forward all requests for destination port 80 to the proxy server.

Transparent proxy mode works without any additional configuration being necessary on clients.
Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.
Hint: In order to proxy both HTTP and HTTPS protocols **without intercepting SSL connections**, configure WPAD/PAC options on your DNS/DHCP servers.

Transparent Proxy Interface(s)

WAN
LAN
OPT1
OPT2

The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.

Bypass Proxy for Private Address Destination

☐ Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations.
Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.

Bypass Proxy for These Source IPs

Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall.
Applies only to transparent mode. Separate entries by semi-colons (;)

Bypass Proxy for These Destination IPs

Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall.
Applies only to transparent mode. Separate entries by semi-colons (;)

SSL Man In the Middle Filtering

HTTPS/SSL

☒ Enable SSL filtering.

SSL Man In the Middle Filtering

HTTPS/SSL Interception

☒ Enable SSL filtering.

SSL/MITM Mode

Splice All

The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled.
Default: Splice Whitelist, Bump Otherwise. [Click Info for details.](#)

SSL Intercept Interface(s)

WAN
LAN
OPT1
OPT2

The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.

SSL Proxy Port

3129

This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129

SSL Proxy Compatibility Mode

Modern

The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. [Click Info for details.](#)

DHParams Key Size

2048 (default)

DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.

CA

CA-Réseau

Select Certificate Authority to use when SSL interception is enabled.

SSL Certificate

Enable Access Logging

☒ This will enable the access log.
Warning: Do NOT enable if available disk space is low.

Log Store Directory

/var/squid/logs

The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs
Important: Do NOT include the trailing / when setting a custom location.

Rotate Logs

365

Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Log Pages Denied by SquidGuard

☐ Makes it possible for SquidGuard denied log to be included on Squid logs.
[Click Info for detailed instructions.](#)

Headers Handling, Language and Other Customizations

Visible Hostname

ProxyIT-Connect

This is the hostname to be displayed in proxy server error messages.

Administrator's Email

admin@it-connect.fr

This is the email address displayed in error messages to the users.

Error Language

en

Select the language in which the proxy server will display error messages to users.

X-Forwarded Header Mode

(on)

Choose how to handle X-Forwarded-For headers. Default: on

Squid Cache General Settings

Disable Caching

☐ Disable caching completely.
This may be required if Squid is only used as a proxy to audit website access.

Cache Replacement Policy

Heap LFUDA

The cache replacement policy decides which objects will remain in cache and which objects are replaced to create space for the new objects. Default: heap LFUDA

Low-Water Mark in %

90

The low-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm.

High-Water Mark in %

95

The high-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm.

Do Not Cache

Enter domain(s) and/or IP address(es) that should never be cached. Put each entry on a separate line.

Enable Offline Mode

☐ Enable this option and the proxy server will never try to validate cached objects.
Offline mode gives access to more cached information than normally allowed (e.g., expired cached versions where the origin server should have been contacted otherwise).

External Cache Managers

Hard Disk Cache Size

1024

Amount of disk space (in megabytes) to use for cached objects.

Hard Disk Cache System

ufs

This specifies the kind of storage system to use.

Clear Disk Cache NOW

Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron.
If you wish to clear cache immediately, click this button once:

Clear Disk Cache NOW

Level 1 Directories

16

Specifies the number of Level 1 directories for the hard disk cache.

Hard Disk Cache Location

/var/squid/cache

This is the directory where the cache will be stored. Default: /var/squid/cache

Minimum Object Size

0

Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)

Maximum Object Size

4

Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB)

Squid Memory Cache Settings

Memory Cache Size

64

Specifies the ideal amount of physical RAM (in megabytes) to be used for In-Transit objects, Hot Objects and Negative-

04-12-2024

Copyright © 2024 Mathys DOMERGUE - All Right Reserved

6/10

General settingsCommon ACLGroups ACLTarget categoriesTimesRewritesBlacklistLogXMLRPC Sync

General Options

Enable

☒ Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See [this link for details](#).
The Save button at the bottom of this page must be clicked to save configuration changes.
To activate squidGuard configuration changes, **the Apply button must be clicked**.

☒ Apply

SquidGuard service state: **STARTED**

LDAP Options

Enable LDAP Filter

☐ Enable options for setup ldap connection to create filters with ldap search

LDAP DN

Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)

LDAP DN Password

Password must be initialize with letters (Ex: Change123), valid format: [a-zA-Z_\.\-\!\@\#\%\&'*\+\,\;\:\|\~\`\{\}\|\+\?\=\&]

LDAP Cache Time

Number of seconds to cache LDAP Results (recommended value: 300)

Strip NT domain

☐ Strip NT domain name component from user names (/ or \ separated).

Service options

Rewrite process children

Maximum number of SquidGuard redirector processes that Squid may spawn. Using too few of these helper processes (a.k.a. "helpers") creates request queues. Using too many helpers wastes your system resources. (Default: 16)

Rewrite process children startup

Sets a minimum of how many SquidGuard processes are to be spawned when Squid starts or reconfigures. (Default: 8)

Rewrite process children idle

Sets a minimum of how many SquidGuard processes Squid is to try and keep available at all times. (Default: 4)

Logging options

Enable GUI log

☒ Check this option to log the access to the Proxy Filter GUI.

Enable log

☒ Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.

Enable log rotation

☐ Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.

Miscellaneous

Clean Advertising

☐ Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.

Blacklist options

Blacklist

☒ Check this option to enable blacklist

Proxy Denied Error

The first part of the error message displayed to clients when access was denied. Defaults to **Request denied by g_get(product_name) proxy**.

Redirect mode

int error page (enter error message)

Select redirect mode here.
Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible.
Options: [ext url err page](#), [ext url redirect](#), [ext url as 'move'](#), [ext url as 'found'](#).

Redirect info

Enter external redirection URL, error message or size (bytes) here.

Use SafeSearch engine

☒ Enable the protected mode of search engines to limit access to mature content.
At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search, Bing, DuckDuckGo, OneSearch, Rambler, Ecosia and Qwant. Make sure that the search engines can be accessed. It is recommended to prohibit access to others.
Note: This option overrides 'Rewrite' setting.

Rewrite

none (rewrite not defined)

Enter the rewrite condition name for this rule or leave it blank.

Log

☒ Check this option to enable logging for this ACL.

Save

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license](#).

La preuve que mon proxy bloque les réseaux sociaux, voici ce qui se passe quand j'essaye d'accéder à des réseaux sociaux :

