

27/10 - 07/11

RAPPORT DE PROJET

Techniques de sécurisation ISR

SOMMAIRE

01

MISE EN PLACE DE
L'ENVIRONEMENT

02

ROUTAGE INTER-
VLAN ET ACL

03

CONFIGURATION
NAT ET PROXY

04

DMZ ET SÉCURITÉ
PÉRIMÉTRIQUE

Mise en place de l'environnement

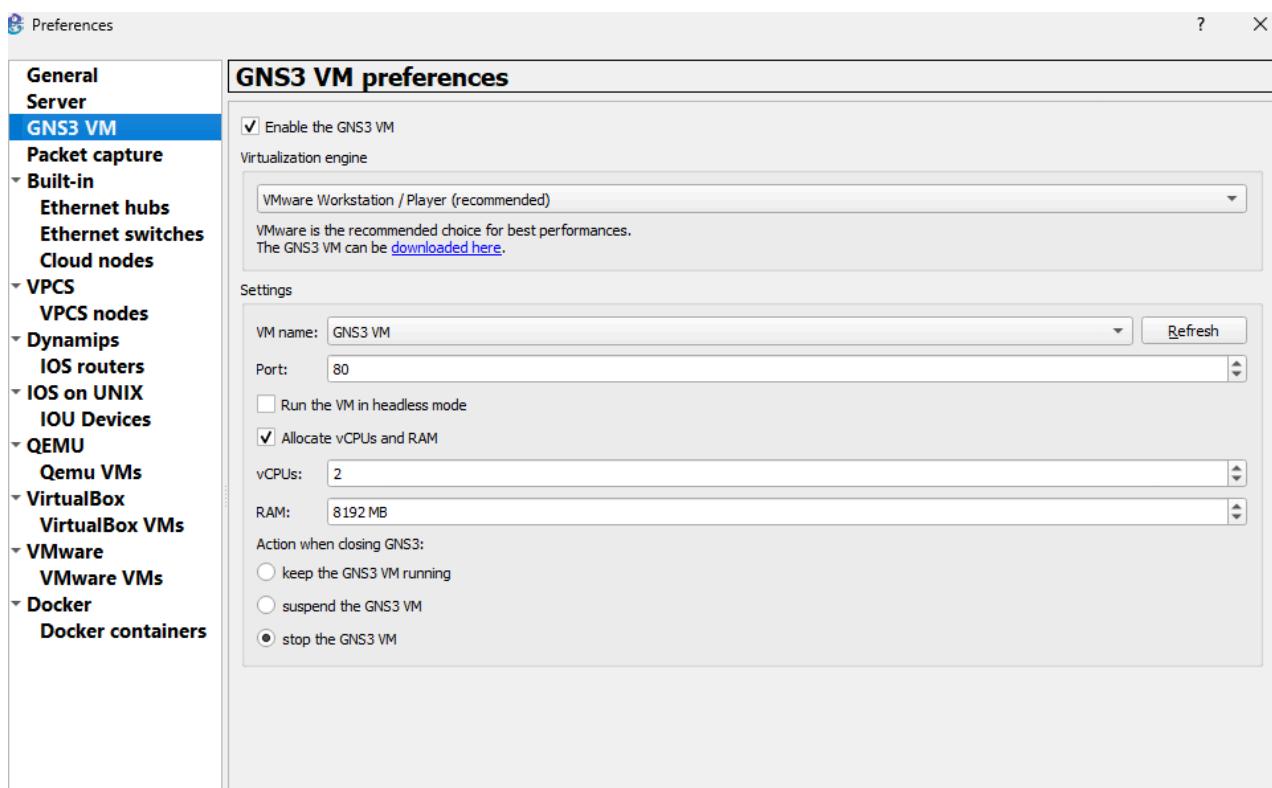
01

Installation

On commence par installer GNS3 pour windows sur <https://www.gns3.com/software/download> en se créant un compte.

Ensuite on installe GNS3 VM pour VMware sur <https://www.gns3.com/software/download-vm>.

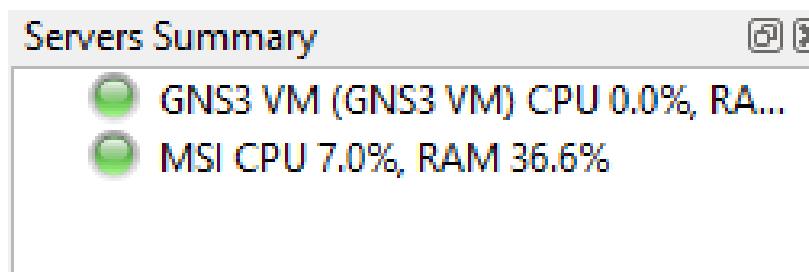
Une fois l'installation de GNS3 terminé, on se rend dans Edit > Préférences > GNS3 VM, on coche Enable the GNS3 VM, ensuite dans Virtualization engine on selection VM Ware, puis on appuie sur le bouton Refresh et on sélectionne GNS3 VM, pour finir on appuie sur Apply et OK



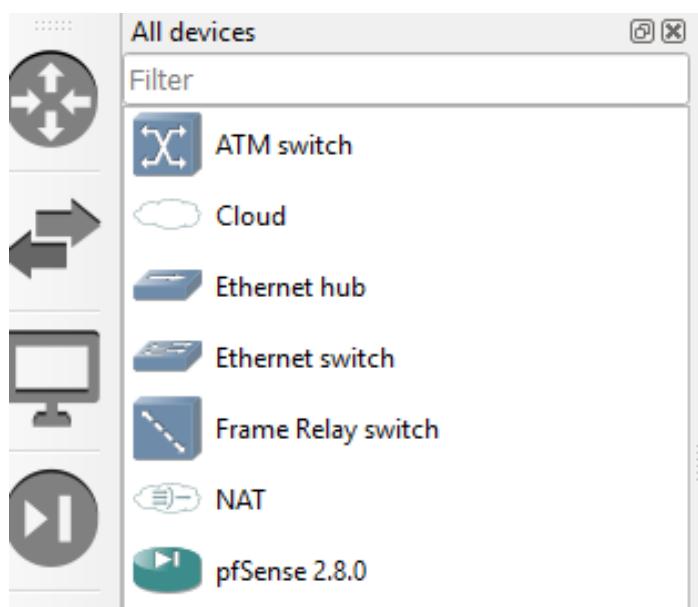
Mise en place de l'environement

01

On peut vérifier que la connexion entre notre machine virtuelle GNS3 VM et GNS3 en regardant en bas à droite si un rond vert apparaît devant le nom de la machine virtuelle.



Ensuite on installe **pfSense**, dans la listes de tous les dispositifs, on clique sur **New template**, puis on sélectionne la première options (**Install an appliance from the GNS3 server**), on se rend dans l'onglet Firewalls on clique sur pfSense on sélectionne /bin/qemu/-system-x86_64(v8.0.4), installé plus tôt, ensuite on clique sur **Create a new version**, on marque le numéro de la version (**2.8.0**), et enfin on importe l'image de pfSense et on valide.

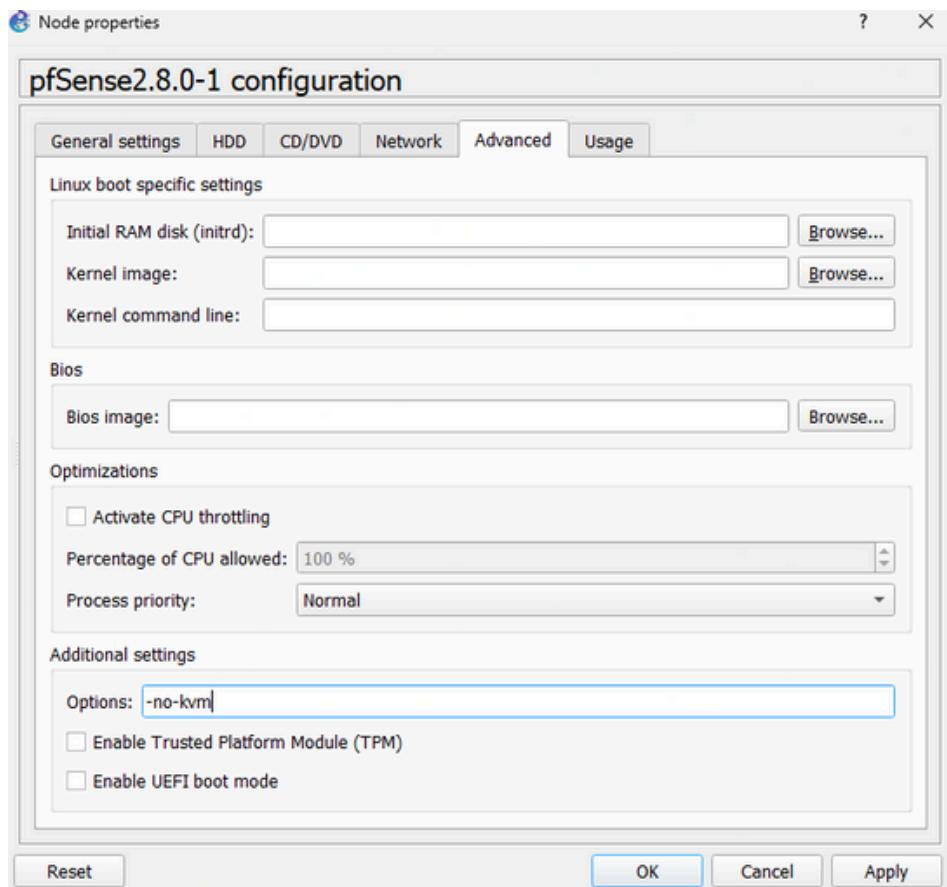


Mise en place de l'environnement

01

Erreur KVM

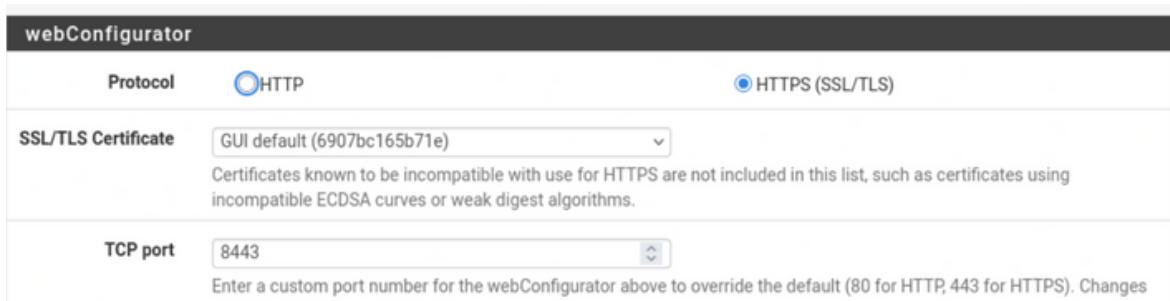
On glisse **pfSense** sur le tableau de bord et on le lance, à cette étape nous avons rencontré un problème **KVM**, pour y remédier nous avons été dans les **options** avancées de pfSense et à la ligne options nous avons écrit **-no-kvm**, ce qui a résolu le problème, après ça nous avons pu le lancer pour le configurer.



Mise en place de l'environement

01

Configuration



Après son lancement nous l'avons **configurer**, pour cela on a sélectionné l'interface réseau **em0** que nous avons laissé en dhcp qui nous sert de réseau WAN, puis l'interface réseau **em1** que nous avons laissé en statique qui sera l'interface où se trouvera notre **réseau LAN**, après cela nous avons d'abord relié l'interface **em0** à un **cloud**, mais nous n'arrivons pas à installer pfSense car ça bloquait, nous avons alors remplacé le cloud par un **NAT**, ce qui a résolu le problème ensuite nous avons pu finir d'installer pfSense.

Pour finir cet objectif nous avons **installer** le Switch de niveau 3

Configurer les interfaces réseau et l'adressage IP de base.

```
root@webterm-1:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=3.67 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=3.15 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2.52 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=2.57 ms
^C
```

```
root@webterm-1:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=14.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=28.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=32.7 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 13.986/25.048/32.704/8.012 ms
```

Routage inter-VLAN et ACL

02

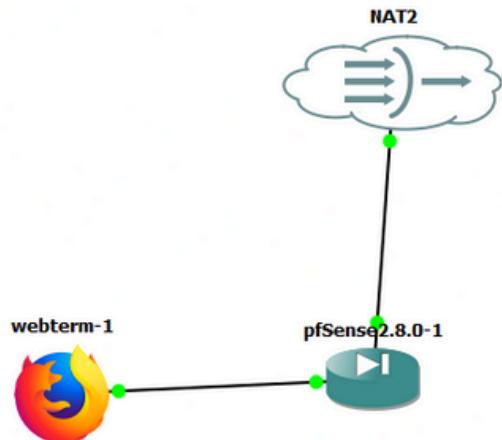
Après ça on peut accéder a pfSense en marquant 192.168.1.1 dans la barre de recherche de Firefox pour ensuite commencer la créations et la configurations des VLans

Pour cela on se rend dans Interfaces puis VLANs on clique sur pour créer un VLAN,

En Parent Interface on met em1 (...) –lan, en VLAN Tag on met le numéro 10 pour le VLAN Admin et 30 pour le VLAN clients et en description le nom du VLAN

Création et configuration des VLans

Pour configurer pfSense on relit un Webterm a l'interface em1 de pfSense.



Dans le terminal du webterm on lui donne **192.168.1.50/24** comme adresse ip, **192.168.1.1** comme passerelle par défaut et 8.8.8.8 comme DNS.

```
root@webterm-1:~# ip addr add 192.168.1.50/24 dev eth0
root@webterm-1:~# ip route add default via 192.168.1.1
root@webterm-1:~# echo "nameserver 8.8.8.8" > /etc/resolv.conf
```

Routage inter-VLAN et ACL

02

Pour commencer nous avons été dans la **console du Switch** et nous avons créé deux VLans (un Vlan est un sous réseau virtuel qui permet de **découper** un LAN physique en plusieurs LAN logiques, pour **isoler** les différents domaines et réseaux et limiter le broadcast), une nommée VLAN_Admin et une nommée VLAN_Clients.

VLAN Configuration

<u>Parent Interface</u>	em1 (0c:c7:8f:97:00:01) - lan
Only VLAN capable interfaces will be shown.	
<u>VLAN Tag</u>	30
802.1Q VLAN tag (between 1 and 4094).	
<u>VLAN Priority</u>	0
802.1Q VLAN Priority (between 0 and 7).	
<u>Description</u>	VLAN_CLIENTS
A group description may be entered here for administrative reference (not parsed).	
<input type="button" value="Save"/>	

Sur cette image on a créer le VLAN clients, on fait pareil pour le VLAN admin en changeant les valeurs expliqué plus haut.

VLAN Interfaces				
Interface	VLAN tag	Priority	Description	Actions
em1 (lan)	10		VLAN_ADMIN	
em1 (lan)	30		VLAN_CLIENTS	

On peut ensuite voir que les VLANs ont bien été créés.

Routage inter-VLAN et ACL

02

Configuration des VLans

Interface Assignments	Interface Groups	Wireless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges	LAGGs
Interface					Network port				
WAN			em0 (0c:87:57:c3:00:00)						
LAN			em1 (0c:87:57:c3:00:01)					 Delete	
VLAN_ADMIN			VLAN 10 on em1 - lan (VLAN_ADMIN)					 Delete	
VLAN_CLIENTS			VLAN 30 on em1 - lan (VLAN_CLIENTS)					 Delete	
Available network ports:		em4 (0c:87:57:c3:00:04)					 Add		

General Configuration

Enable	<input type="checkbox"/> Enable interface
Description	VLAN_CLIENTS Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	XX:XX:XX:XX:XX:XX This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: XX:XX:XX:XX:XX:XX or leave blank.
MTU	1500 If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	1460 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration	
IPv4 Address	192.168.30.1 / 32

Sur cette image on a configuré le VLAN_Clients et on a fait de même pour le VLAN_Admin en changeant la description par VLAN_Admin et l'IPv4 Address par 192.168.10.1

Puis on finit la configuration pfSense en configurant le DHCP sur chaque VLAN, pour cela on se rend dans services dhcp et pour chaque VLAN on coche l'option **Enable DHCP server** sur VLAN_ADMIN (ou VLAN_CLIENTS selon les VLAN qu'on configure) interface et dans Address Pool Range on configure la plage ip du dhcp de 192.168.x.10 à 192.168.x.20 (x -> numéro du VLAN, 10 pour VLAN_ADMIN et 30 pour VLAN_CLIENT).

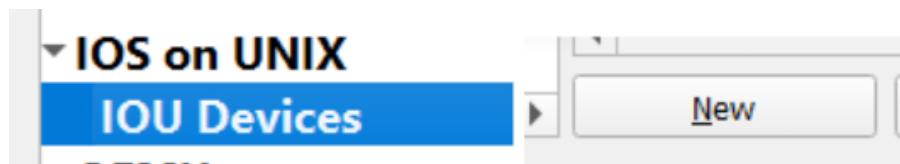
Routage inter-VLAN et ACL

02

The screenshot shows the pfSense DHCP Server configuration for the VLAN_ADMIN interface. The 'VLAN_ADMIN' tab is selected. Under 'General Settings', the DHCP Backend is set to ISC DHCP, and the 'Enable' checkbox is checked. The 'Deny Unknown Clients' dropdown is set to 'Allow all clients'. Under 'Ignore Denied Clients', the 'Ignore denied clients rather than reject' checkbox is unchecked. Under 'Ignore Client Identifiers', the 'Do not record a unique identifier (UID) in client lease data if present in the client DHCP request' checkbox is unchecked. In the 'Primary Address Pool' section, the Subnet is 192.168.10.0/24, and the Subnet Range is 192.168.10.1 - 192.168.10.254. The Address Pool Range is set from 192.168.10.10 to 192.168.10.20. A note states: 'The specified range for this pool must not be within the range configured on any other address pool for this interface.'

Après avoir créer et configurer les VLans sur pfSense on les créer et les configures aussi sur le switch de niveau 3 depuis son terminal.

On commence par télécharger le switch de niveau 3 avec l'image :



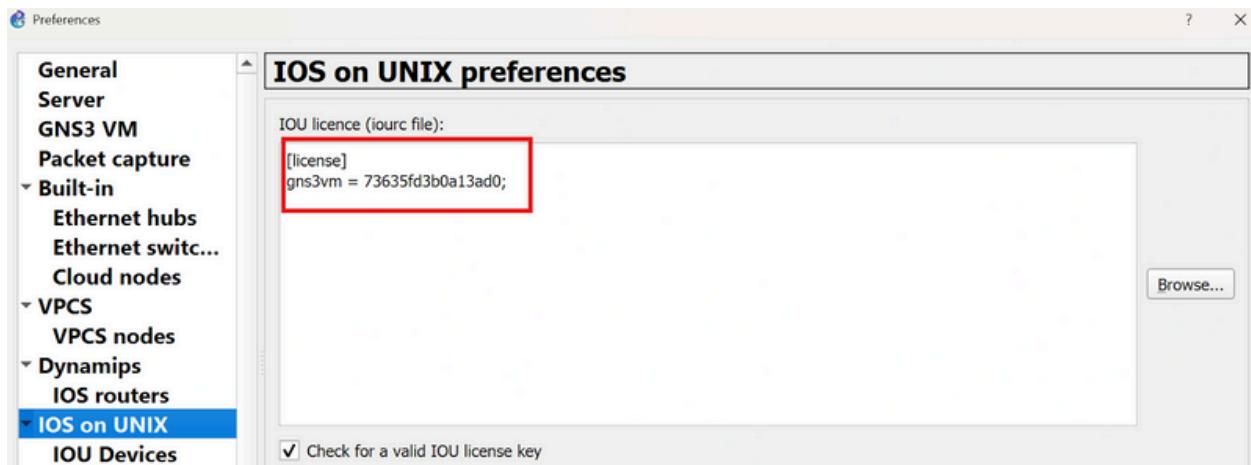
Aller dans IOU devices > new et sélectionnez l'image

The screenshot shows the 'New' dialog for creating a new IOU device. The 'Name' field is filled with 'SWITCHL3'. Under the 'Image' section, the 'Type' is set to 'L3 image'. There are two radio buttons: 'Existing image' (unchecked) and 'New Image' (checked). The 'IOU image:' field is empty, and there is a 'Browse...' button next to it.

Routage inter-VLAN et ACL

02

Et enfin mettre la license :



Pour cela, on tape cette suite commande :

- conf t
- vlan 10
- name VLAN_Admin
- exit

Puis on fait de même pour créer le VLAN clients :

- vlan 30
- name VLAN_Client
- exit
- exit

On peut faire la commande show vlan pour voir les VLAN qu'on vient de mettre en place.

```
SWITCH-LAN#show vlan
VLAN Name                               Status    Ports
----+-----+-----+-----+-----+-----+
1   default                             active   Et0/0, Et0/1, Et0/2, Et0/3
                                         Et1/0, Et1/1, Et1/2, Et1/3
10  VLAN_Admin                         active
30  VLAN_Clients                       active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fdnet-default                     act/unsup
1005 trnet-default                     act/unsup

VLAN Type      SAID      MTU      Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1   enet      100001   1500      -       -       -       -       0       0
10  enet      100010   1500      -       -       -       -       0       0
30  enet      100030   1500      -       -       -       -       0       0
1002 fddi     101002   1500      -       -       -       -       0       0
1003 tr       101003   1500      -       -       -       -       0       0
1004 fdnet    101004   1500      -       -       ieee   -       0       0
1005 trnet    101005   1500      -       -       ibm   -       0       0

Primary Secondary Type          Ports
----+-----+-----+-----+-----+
```

Routage inter-VLAN et ACL

02

Ensute on configure la liaison entre pfSense et le switch en mode trunk :

```
SWITCH-LAN(config)#int et0/0
SWITCH-LAN(config-if)#switchport trunk encapsulation dot1q
SWITCH-LAN(config-if)#switchport mode trunk
SWITCH-LAN(config-if)#switchport trunk allowed vlan 10,30
SWITCH-LAN(config-if)#desc Trunk vers pfSense
SWITCH-LAN(config-if)#exit
SWITCH-LAN(config)#exit
SWITCH-LAN#
*Nov  2 20:41:50.156: %SYS-5-CONFIG_I: Configured from console by console
SWITCH-LAN#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 2008 bytes to 1112 bytes[OK]
```

Nous allons alors tenter d'obtenir une adresse ip avec le dhcp que nous venons configurer avec la commande **ip dhcp**,
Depuis le pc situer sur le VLan admin :

```
ip dhcp
DDORA IP 192.168.10.10/24 GW 192.168.10.1
PC1> █
```

Et depuis le **pc** situ  sur le VLan clients :

```
ip dhcp
DDORA IP 192.168.30.10/24 GW 192.168.30.1
PC1> █
```

Routage inter-VLAN et ACL

02

Ensuite nous avons mis en place des règles de filtrage pour pouvoir avoir accès au vlan clients depuis le **VLAN_ADMIN** mais pas l'inverse.

Pour cela nous avons configuré des règles de base Pour avoir un accès complet au sein de chaque vlan, puis nous avons mis en place une règle qui bloque la connexion du **VLAN_CLIENTS** vers le VLAN admin en faisant comme sur les images ci dessous :

The screenshot shows the 'Edit Firewall Rule' dialog box. The 'Action' dropdown is set to 'Pass'. The 'Disabled' checkbox is unchecked. The 'Interface' dropdown is set to 'VLAN_ADMIN'. The 'Address Family' dropdown is set to 'IPv4'. The 'Protocol' dropdown is set to 'Any'. In the 'Source' section, the 'Source' dropdown is set to 'VLAN_ADMIN subnets' and the 'Destination' dropdown is set to 'Any'. In the 'Extra Options' section, the 'Log' checkbox is unchecked. The 'Description' field contains the text 'Admin FULL ACCESS'.

Sur cette image nous avons configuré l'accès complet au sein du VLan admin, nous avons fait exactement pareil pour le VLan client en changeant seulement l'interface par **VLAN_CLIENTS** et la source par **VLAN_CLIENTS** subnets et pour commentaire « **Clients FULL ACCESS** »

Routage inter-VLAN et ACL

02

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	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	VLAN_CLIENTS		
Choose the interface from which packets must come to match this rule.			
Address Family	IPv4		
Select the Internet Protocol version this rule applies to.			
Protocol	Any		
Choose which IP protocol this rule should match.			
Source			
Source	<input type="checkbox"/> Invert match	VLAN_CLIENTS subnets	Source Address
Destination			
Destination	<input type="checkbox"/> Invert match	VLAN_ADMIN subnets	Destination Address
Extra Options			
Log	<input type="checkbox"/> 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	Bloque VLAN_CLIENTS > VLAN_ADMIN		

Et sur cette image nous pouvons voir la configuration que nous avons réalisées pour bloquer la connexion du VLANs clients vers le VLAN admin.

Nous pouvons donc voir avec les images qui suivent que les règles ont bien été configurées :

Floating	WAN	LAN	VLAN_ADMIN	VLAN_CLIENTS						
Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	X 0/0 B	IPv4 *	VLAN_CLIENTS subnets	*	VLAN_ADMIN subnets	*	*	none	Bloque VLAN_CLIENTS > VLAN_ADMIN	
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv4 *	VLAN_CLIENTS subnets	*	*	*	*	none	Clients FULL ACCESS	

Floating	WAN	LAN	VLAN_ADMIN	VLAN_CLIENTS						
Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv4 *	VLAN_ADMIN subnets	*	*	*	*	none	Admin FULL ACCESS	

Routage inter-VLAN et ACL

02

Pour finir nous avons testé la communication et le filtrage, pour cela nous avons fait un ping depuis un VLAN vers un autre, sur la première image on voit bien que depuis le **VLAN_Admin(192.168.10.1)** on peut ping le **VLAN_Clients(192.168.30.1)**.

```
PC2> ping 192.168.30.11
84 bytes from 192.168.30.11 icmp_seq=1 ttl=63 time=6.844 ms
84 bytes from 192.168.30.11 icmp_seq=2 ttl=63 time=5.089 ms
```

A l'inverse sur cette deuxième image nous voyons que nous ne pouvons pas faire l'inverse (depuis le **VLAN_Clients** on ne peut pas ping le **VLAN_Admin**).

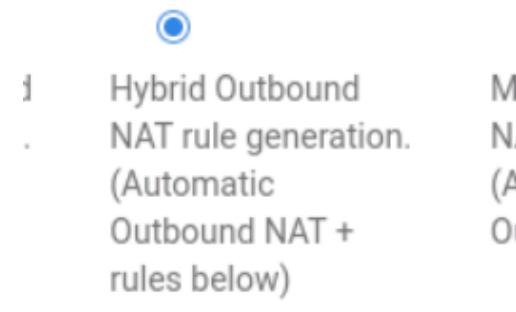
```
?C1> ping 192.168.10.10
192.168.10.10 icmp_seq=1 timeout
192.168.10.10 icmp_seq=2 timeout
```

Configuration NAT et Proxy

03

Configuration du NAT

Pour configurer le NAT on se rend dans **Firewall > NAT > onglet "Outbound"** et on sélectionne **Hybrid Outbound...**



Ensuite on se rend dans **Port Forward** et on fait:

Disabled Disable this rule

No RDR (NOT) Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface: DMZ
Choose which interface this rule applies to. In most cases 'WAN' is specified.

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

Protocol: TCP
Choose which protocol this rule should match. In most cases 'TCP' is specified.

Source: Hide Advanced
Source port range: Any / Any
From port: Any / Custom To port: Any / Custom
Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be 'any'). The 'to' field may be left empty if only filtering a single port.

Destination: Invert match.
Type: This Firewall (self)
Destination port range: HTTPS / HTTPS
From port: Custom To port: Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP: Address or Alias
Type: Address
Address: 127.0.0.1
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope".
I.e. it is not possible to redirect from link-local addresses scope (fe80::) to local scope (::1)

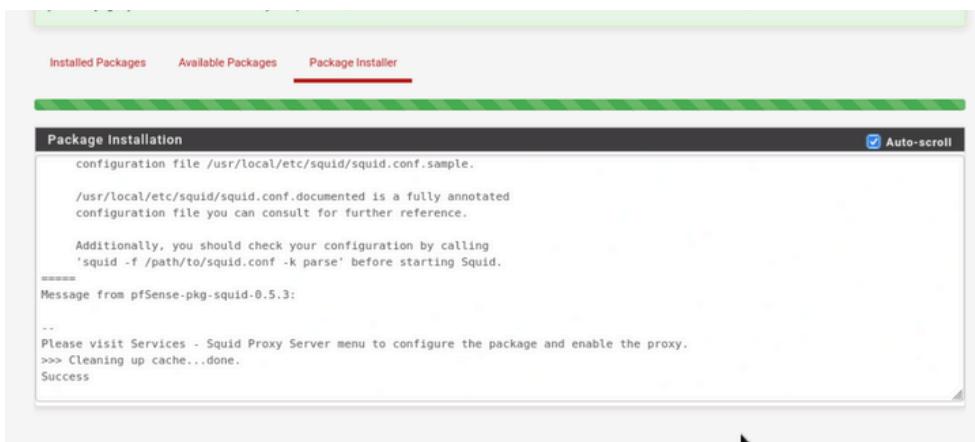
Redirect target port: Other
Port: 3129
Custom

Configuration NAT et Proxy

03

Installation et configuration du proxy Squid:

Pour installer Squid depuis pfSense nous avons fait **Services > Packet Manager > Available > squid > download**



Une fois squid fini d'installer on vas créer une certification d'autorisation pour Squid, pour ça on se rend sur **System > Certificates > Authorities > Edit**, puis dans **Descriptive Name** on écrit **SQUID_CA** et dans méthode on sélectionne **Create an internal Certificate Authority**

WARNING:
The password for this account is insecure. Password is currently set to the default value (pfSense).
Change the password as soon as possible.

System / Certificates / Authorities / Edit

Authorities Certificates Revocation

Create / Edit CA

Descriptive name: SQUID_CA

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, *, '

Method: Create an internal Certificate Authority

Trust Store: Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial: Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type: RSA

2048

The length to use when generating a new DCA key in bits

Configuration NAT et Proxy

03

Après nous avons pu commencer à configurer Squid, pour cela nous avons été dans **Services > Squid Proxy Server > General** puis nous avons

Squid General Settings

Enable Squid Proxy	<input checked="" type="checkbox"/> Check to enable the Squid proxy. Important: If unchecked, ALL Squid services will be disabled and stopped.
Keep Settings/Data	<input checked="" type="checkbox"/> 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 DMZ VLAN_ADMIN The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
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	<input checked="" type="checkbox"/> 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.

Transparent Proxy Settings

Transparent HTTP Proxy	<input checked="" type="checkbox"/> Enable transparent mode to forward all requests for destination port 80 to the proxy server. <small>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.</small>
Transparent Proxy Interface(s)	WAN LAN DMZ VLAN_ADMIN The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.
Bypass Proxy for Private Address Destination	<input checked="" type="checkbox"/> 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 Interception	<input checked="" type="checkbox"/> 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 DMZ VLAN_ADMIN 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	SQUID_CA Select Certificate Authority to use when SSL interception is enabled. Click Info for details.

Configuration NAT et Proxy

03

Puis on a ajouter des sites internet dans la **Blacklist**, comme par exemple netflix.com



Après avoir blacklisté **netflix.com** on a tenté d'y accéder mais nous n'y êtes pas parvenu ce qui prouve que le filtrage est fonctionnel.

ERROR: The requested URL could not be retrieved — Mozilla Firefox

Problem loading page x ERROR: The requested URL x +

Not Secure http://netflix.com

Firefox automatically sends some data to Mozilla so that we can improve your experience. Choose What I Share X

ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: <http://netflix.com/>

Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

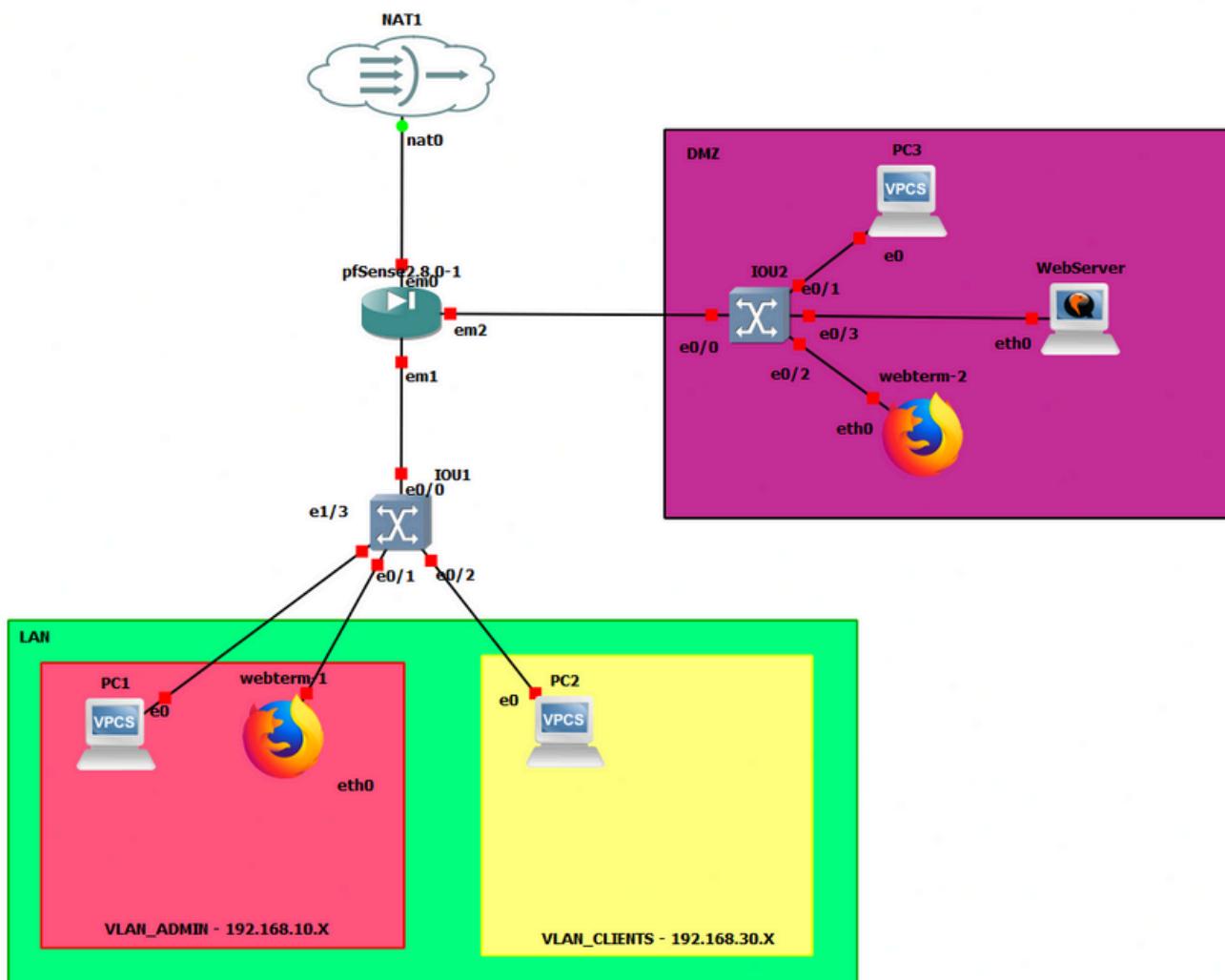
Your cache administrator is admin@localhost.

Generated Thu, 06 Nov 2025 09:56:07 GMT by localhost (squid/6.12)

DMZ et sécurité pérимétrique

04

DMZ



Nous avons ensuite rajouté un **switch** qui s'occupera de la **DMZ**, et ensuite un **serveur web** avec apache, un **pc** et un **webterm** pour effectuer des tests.

DMZ et sécurité périphérique

04

The screenshot shows a firewall rule configuration interface. At the top, there are tabs for Floating, WAN, LAN, DMZ (which is selected), VLAN_ADMIN, and VLAN_CLIENTS. Below the tabs is a table titled "Rules (Drag to Change Order)". The table has columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are five rows in the table:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/1020 B	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		BLOCK DMZ -> LAN	
0/252 B	IPv4 *	DMZ subnets	*	VLAN_ADMIN subnets	*	*	none		BLOCK DMZ -> VLAN_ADMIN	
0/0 B	IPv4 *	DMZ subnets	*	VLAN_ADMIN subnets	*	*	none		BLOCK DMZ -> VLAN_CLIENTS	
0/1.38 MiB	IPv4 *	DMZ subnets	*	*	*	*	none		DMZ PASS ALL	

At the bottom of the interface are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

Nous **bloquons** toute requête venant de la **DMZ** au **LAN**, et aux **VLANs**.
Et les **VLANs Admin** et **Clients** peuvent communiquer avec la **DMZ**.

```
PC3> ip dhcp
DDORA IP 192.168.90.10/24 GW 192.168.90.1

PC3> ping 192.168.10.10
192.168.10.10 icmp_seq=1 timeout
192.168.10.10 icmp_seq=2 timeout
192.168.10.10 icmp_seq=3 timeout
192.168.10.10 icmp_seq=4 timeout
192.168.10.10 icmp_seq=5 timeout

PC3>
```

```
PC1>
PC1> ping 192.168.90.10
84 bytes from 192.168.90.10 icmp_seq=1 ttl=63 time=3.789 ms
84 bytes from 192.168.90.10 icmp_seq=2 ttl=63 time=2.714 ms
84 bytes from 192.168.90.10 icmp_seq=3 ttl=63 time=3.337 ms
84 bytes from 192.168.90.10 icmp_seq=4 ttl=63 time=3.138 ms
84 bytes from 192.168.90.10 icmp_seq=5 ttl=63 time=15.614 ms

PC1>
```

Nous pouvons **vérifier** que la DMZ est bien isolée avec les pings, le PC1 de la VLAN_ADMIN peut communiquer avec la DMZ mais pas l'inverse.

MERCI !