

Documentation Succursale

1

Démonstration 1 : Infrastructure : Routage + DMZ + VPN (10%)

Création d'une machine pfSense possédant 2 cartes réseau (1 WAN et 1 LAN). (Dans cette capture d'écran, on ignore la DMZ, le tunnel et les 2 autres interfaces.)

```
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on UPN1 ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.64.101.24/23
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
WG1_TUNEL (opt1) -> tun_wg0  -> v4: 10.10.100.1/24
DMZ (opt2)     -> em2      -> v4: 172.16.10.1/24
SERV1 (opt3)   -> em3      -> v4: 192.168.30.1/24
SERV2 (opt4)   -> em4      -> v4: 192.168.29.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (ssh)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell





Enter an option:
Message from syslogd@UPN1 at Nov 29 18:22:34 ...
php-fpm[15458]: /index.php: Successful login for user 'admin' from: 192.168.1.2
(Local Database)
```

Une fois que pfSense est installé, on va créer une machine Windows 10 pour pouvoir accéder à la configuration du pare-feu. Nous avons utilisé WireGuard. On va donc créer un seul tunnel de la succursale 1 vers la 2, 3, 4.

VPN / WireGuard / Tunnels

Tunnels Peers Settings Status

WireGuard Tunnels

Name	Description	Public Key	Address / Assignment	Listen Port	Peers	Actions
▼ tun_wg0	wg1_tunnel	vyDya8px9hE2qgNkNhd6RdLQgtJdEEC/...	WG1_TUNEL (opt1)	51820	3	   
Peers						
	Description	Public Key	Tunnel	Allowed IPs	Endpoint	
		tmOmTBrqoVPSJzhwpKjbT/nw4j3/SoKQ...	tun_wg0	192.168.2.0/24 (+6)	10.64.101.235:51820	
		dpmAVYzfTWIK1S9\$W97rVBGDu05kFd5x...	tun_wg0	192.168.3.0/24 (+2)	10.64.100.234:51820	
	wg1-4_tunnel	LsZVWS3wgxYrvF24oHaxCh5PPOojMX6X...	tun_wg0	192.168.4.0/24 (+2)	10.64.100.88:51820	

+ Add Tunnel

Sur chaque connexion au tunnel, il faudra allouer les adresses IP suivantes : 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0. Ce sont les adresses de sous-réseaux. De même, pour 10.10.100.1, 10.10.100.2, 10.10.100.3, 10.10.100.4, ce sont les adresses des passerelles (gateways). Les endpoints sont les adresses WAN des pfSense.

3.1.1/wg/vpn_wg_peers_edit.php?peer=0

Peer Configuration

Enable

☒ Enable Peer

Note: Uncheck this option to disable this peer without removing it from the list.

Tunnel

tun_wg0 (wg1_tunnel)

WireGuard tunnel for this peer. (Create a New Tunnel)

Description

Description

Peer description for administrative reference (not parsed).

Dynamic Endpoint

☐ Dynamic

Note: Uncheck this option to assign an endpoint address and port for this peer.

Endpoint

10.64.101.235

51820

Hostname, IPv4, or IPv6 address of this peer. Leave endpoint and port blank if unknown (dynamic endpoints).

Port used by this peer. Leave blank for default (51820).

Keep Alive

1

Interval (in seconds) for Keep Alive packets sent to this peer. Default is empty (disabled).

Public Key

tmOmTBqoVPSJzhwpKjdt/nw4j3/SokQXWigE2+e1gCM=

WireGuard public key for this peer.

Pre-shared Key

Pre-shared Key

Optional pre-shared key for this tunnel. (Copy)

Generate

New Pre-shared Key

Address Configuration

Hint

Allowed IP entries here will be transformed into proper subnet start boundaries prior to validating and saving. These entries must be unique between multiple peers on the same tunnel. Otherwise, traffic to the conflicting networks will only be routed to the last peer in the list.

Allowed IPs	192.168.2.0 / 24	Description	Delete
	10.10.100.2 / 32	Description	Delete
	192.168.1.0 / 24	Description	Delete
	192.168.3.0 / 24	Description	Delete
	192.168.4.0 / 24	Description	Delete
	10.10.100.3 / 32	Description	Delete
	10.10.100.4 / 32	Description	Delete

Add Allowed IP

+ Add Allowed IP

IPv4 or IPv6 subnet or host reachable via this peer.

Description for administrative reference (not parsed).

L'interface du tunnel sur la succursale 1 a comme IP 10.10.100.1, et ainsi de suite pour les autres succursales. Il faudra donc créer une passerelle (gateway) pour chaque succursale, de 2 à 4.

Edit Gateway

Disabled ☐ Disable this gateway
Set this option to disable this gateway without removing it from the list.

Interface
Choose which interface this gateway applies to.

Address Family
Choose the Internet Protocol this gateway uses.

Name
Gateway name

Gateway
Gateway IP address

Gateway Monitoring ☒ Disable Gateway Monitoring
This will consider this gateway as always being up.

Gateway Action ☐ Disable Gateway Monitoring Action
No action will be taken on gateway events. The gateway is always considered up.

Static route ☐ Do not add static route for gateway monitor IP address via the chosen interface
By default the firewall adds static routes for gateway monitor IP addresses to ensure traffic to the monitor IP address leaves via the correct interface. Enabling this checkbox overrides that behavior.

Force state ☐ Mark Gateway as Down
This will force this gateway to be considered down.

State Killing on Gateway Failure
Controls the state killing behavior when this specific gateway goes down. Killing states for specific down gateways only affects states created by policy routing rules and reply-to. Has no effect if gateway monitoring or its action are disabled or if the gateway is forced down. May not have any effect on dynamic gateways during a link loss event.

Description
A description may be entered here for reference (not parsed).

[Display Advanced](#)

[Save](#)

Pour qu'ensuite on puisse créer une route vers les sous-réseaux des autres succursales en empruntant le gateway, c'est-à-dire l'interface de leur tunnel.

Edit Route Entry

Destination network / 24
Destination network for this static route

Gateway
Choose which gateway this route applies to or add a new one first

Disabled ☐ Disable this static route
Set this option to disable this static route without removing it from the list.

Description
A description may be entered here for administrative reference (not parsed).

[Save](#)

Ensuite on a créé une nouvelle interface pour la DMZ avec comme adresse IP 172.16.10.1

General Configuration

Enable

☒ Enable interface

Description

DMZ

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xxxxxxxxxxxx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxx or leave blank.

MTU

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

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

172.16.10.1

/ 24

IPv4 Upstream gateway

None

+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the 'Add' button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by clicking here.

Reserved Networks

Block private networks and loopback addresses

☐

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks

☐

Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

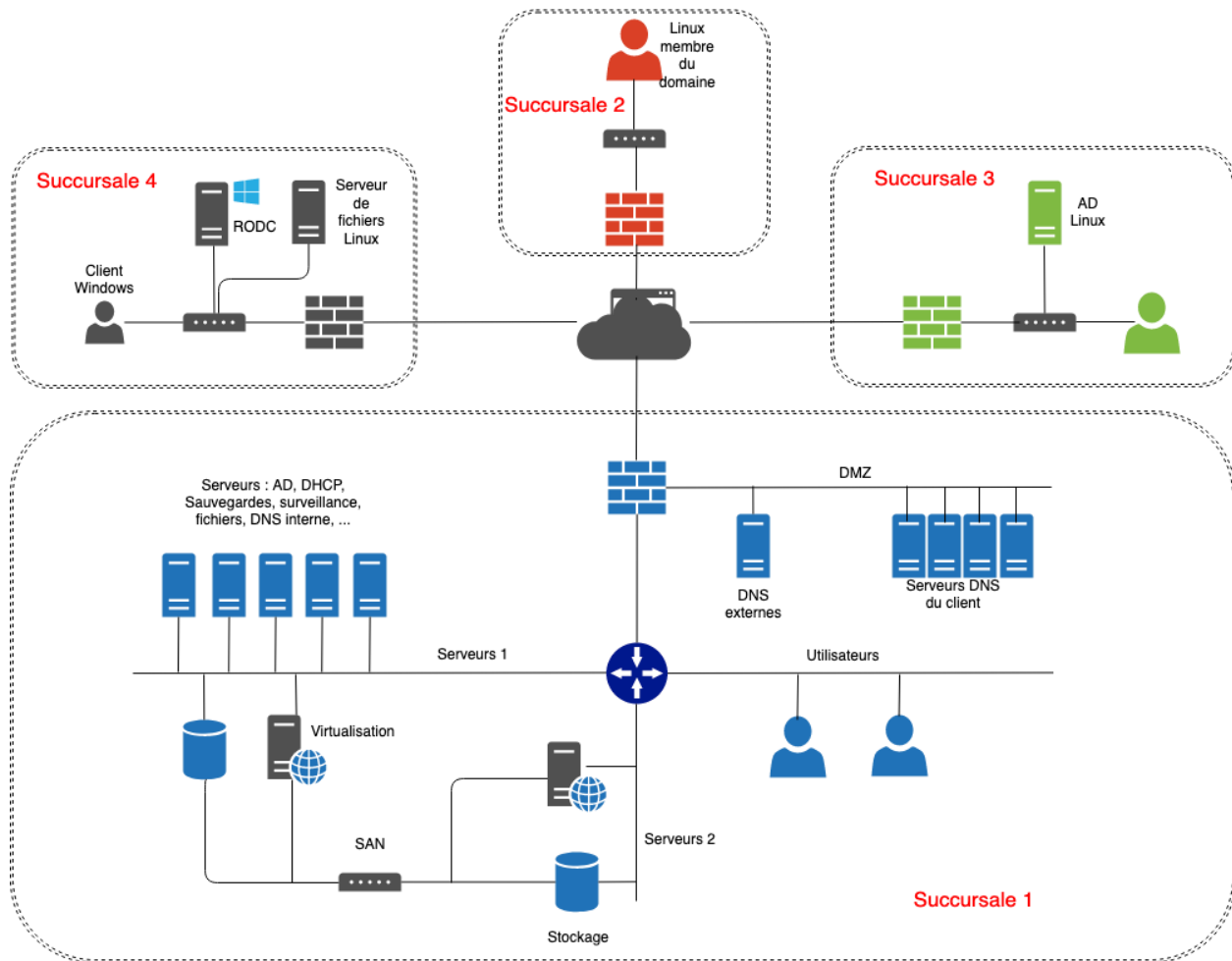
Active Directory

Go to Settings

Activer Windows Defender

Accédez aux paramètres

Démonstration 2 : Active Directory + DNS (15%)



Dans la succursale 1, nous avons décidé d'utiliser le pare-feu comme routeur et donc de créer 3 segments LAN pour les serveurs.

LAN 1 : 192.168.1.0/24

LAN 2 : 192.168.30.0/24

LAN 3 : 192.168.29.0/24

Dans notre topologie, le LAN 2 est notre serveur 1. Nous avons donc créé une machine Windows serveur et installé Active Directory dessus (il est important de lui attribuer une adresse IP fixe avant tout dans le sous-réseau). Dans notre cas, son adresse est 192.168.30.3. Nous avons également configuré un DNS interne. Une fois que c'est fait, sur une machine Linux ayant une adresse dans la DMZ, on a configuré un DNS externe.

Démonstration 3 : Utilisateurs : création, permissions, lecteurs réseaux, stations de travail (15%)

On crée le script de création d'utilisateur, puis on l'exécute.

Ensuite il nous faut un script pour faire le mappage automatique.

Démonstration 4 : Sécurité : Pare-feu, antivirus, sauvegardes, redondance des disques, surveillance (15%)

Pour les règles de pare-feu :

Sur l'interface WAN :

Vers la DMZ, on laisse passer HTTP/HTTPS. On bloque tout vers le LAN.

Sur l'interface DMZ :

On ouvre, par exemple, HTTP. On bloque tout de la DMZ au LAN.

Sur l'interface LAN : Vers la DMZ, on ouvre le DNS, HTTP, SSH. Vers le WAN, c'est personnel donc nous n'avons rien ouvert.

Ensuite, sur la succursale 1, nous avons créé une machine Linux : Nous avons installé ClamAV pour l'antivirus. En ce qui concerne la sauvegarde, il faut installer l'agent de Backup Exec qui n'a pas fonctionné. Ensuite, nous avons fait le RAID en ajoutant 3 disques à la machine et en exécutant cette commande : `bash Copy code mdadm --create /dev/md0 --level=5 --assume-clean --raid-devices=3 /dev/sdb1 /dev/sdc1 /dev/sdd1`

Pour la surveillance, nous avons utilisé Cacti en le configurant à l'aide de MariaDB. Cacti pourra également surveiller la VM Windows.

Démonstration 5 : Stockage, virtualisation (15%)

Nous avons créé 2 machines Linux sur un même segment LAN et effectué le RAID sur les 2 machines. Ensuite, il faut s'attaquer à DRBD pour faire la réplication. On commence par importer les paquets Elrepo, installer DRBD avec `yum install`. Ensuite, il faut désactiver le pare-feu sur les 2 machines. Un redémarrage est nécessaire sur les 2 machines. Ensuite, il faut configurer le fichier de configuration de DRBD (`/etc/drbd.conf`) sur les 2 machines pour y rajouter le protocole C. On enregistre et on crée ensuite un fichier de ressource pour la réplication (`/etc/drbd.d/drbd1.res`) `resource r0 { volume 0 { device /dev/drbd0; # Remplacer par le nom du RAID`

```
disk /dev/sdb;
```

```
meta-disk internal; }
```

```
on node1 { address
```

```
10.0.0.10:7788;
```

```
}
```

```
on node2 {      address  
10.0.0.20:7788;  
  } }
```

Une fois que c'est fait, on sauvegarde sur les 2 machines.

On exécute la commande `drbdadm create-md r0`.

Ensuite, on regarde le statut avec `drbdadm status`.

Il nous faudra configurer une des 2 machines en tant que machine principale avec la commande `drbdadm primary --force r0`.

Configuration du SAN

4 disques de 10Go ont été ajoutés sur la VM Alma.

Ils ont été configurés en deux volumes logiques avec les commandes suivantes :

```
$ pvcreate /dev/sdb /dev/sdc /dev/sdd /dev/sde
```

```
$ vgcreate vg-iscsi /dev/sdb /dev/sdc /dev/sdd /dev/sde
```

```
$ lvcreate -L 20G -n lun0-windows vg-iscsi
```

```
$ lvcreate -L 20G -n lun0-linux vg-iscsi
```

On installe le CLI pour le target iSCSI avec la commande suivante :

```
$ dnf install targetcli
```

On se connecte au client :

```
$ targetcli
```

Configuration de SAN en mode block `create block1`

`/dev/vg-iscsi/lun0-linux` Création du IQN avec le nom Linux

`create iqn.2023-11.ca.qc.cmontmorency:Linux` Se déplacer

sur le IQN créé `cd iscsi/iqn.2023-`

11.ca.qc.cmontmorency:linux/tpg1/ Nous avons changé

l'adresse sur laquelle écoute le serveur :

delete 0.0.0.0 3260 create

192.168.3.10

Création d'une ACL pour autoriser la VM :

acls/ create iqn.VM:VM

Nous pouvons maintenant le voir sur la VM avec la commande :

\$ iscsiadm -m discovery -t st -p 192.168.3.5