



# Mise en place d'un périmètre et solution de sécurité (pfSense)

Mounir OURIBI – Quentin GARNIER – Raphael LEBLET

## **SOMMAIRE**

I. pfSense	2
1. Présentation	
a. Objectifs	
b. Rôle de pfSense	
c. Prérequis	
2. Mode opératoire pfSense	3
a. Installation pfSense	
b. Configuration	4
c. Règles NAT	7
d. Règles Firewall	8
e. Test	11
3. Conclusion	14

# I. pfSense

## 1. Présentation

### a. Objectifs

Nous avons pour objectif d'installer et de configurer une solution du firewall pfSense en respectant la mise en place d'une DMZ qui hébergera un serveur web (IIS) et un serveur de messagerie (HMail). L'accès au serveur web devra être accessible pour les utilisateurs du LAN de GSB ainsi que pour les visiteurs médicaux se trouvant dans le WAN.

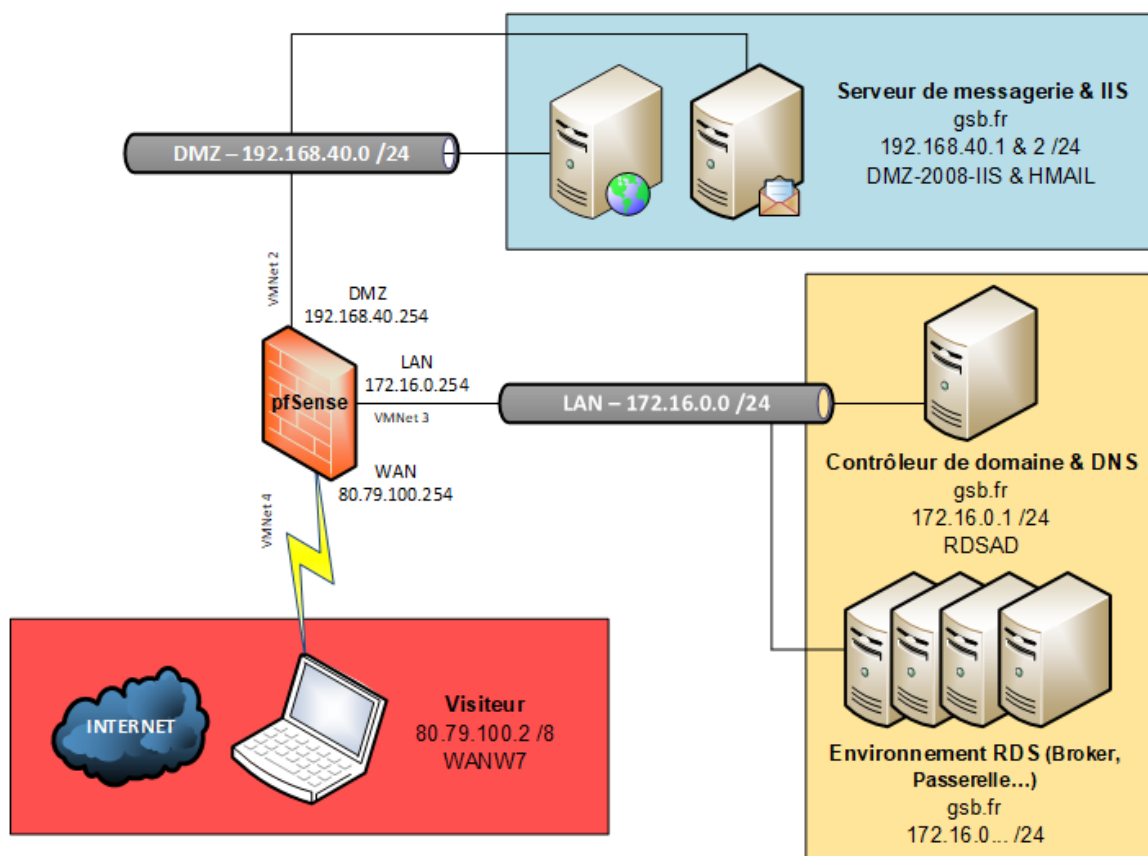
Le serveur de mail GSB devra également être accessible.

### b. Rôle de pfSense.

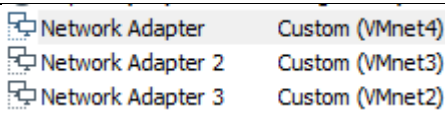
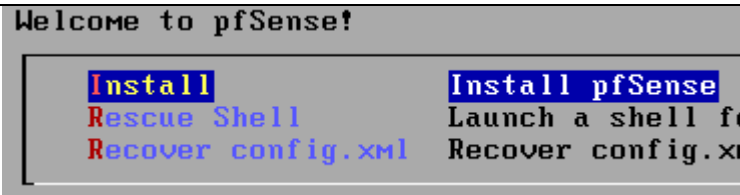
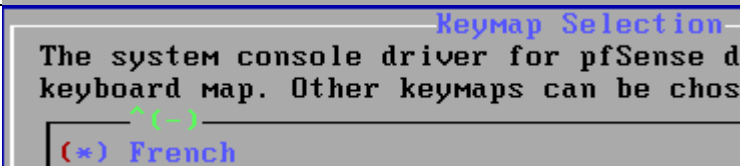
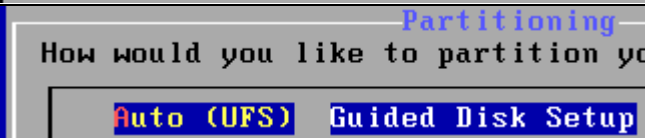
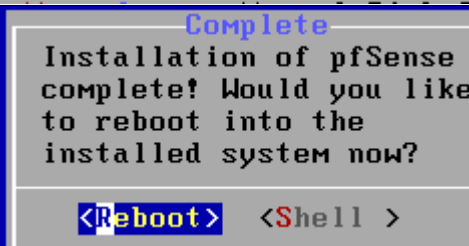
Nous utiliserons donc un routeur/pare-feu open source pfSense basé sur l'OS FreeBSD afin de configurer les règles de filtrage et le NAT/PAT qui assureront la sécurité de GSB.

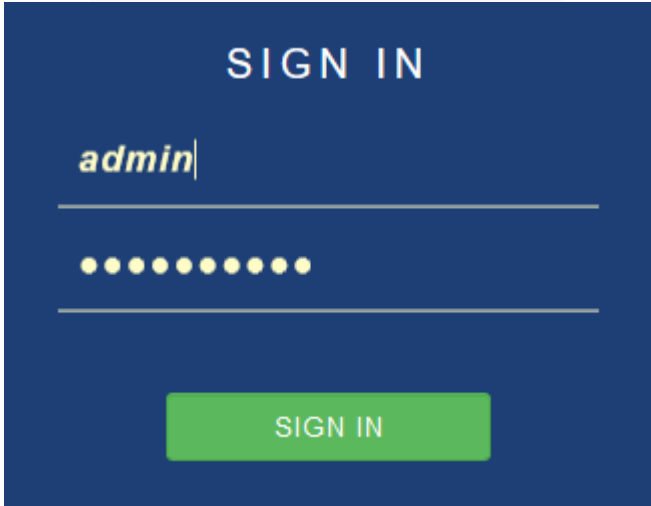
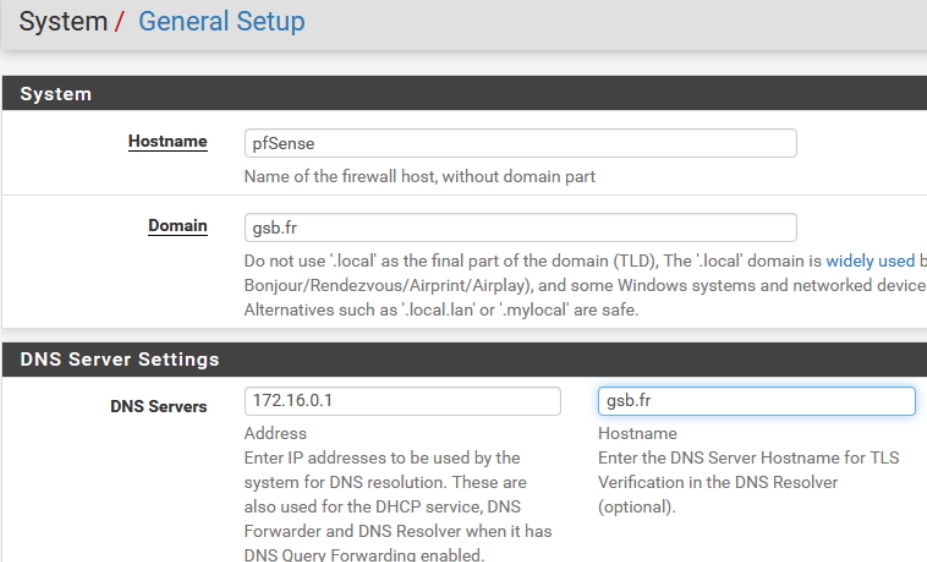
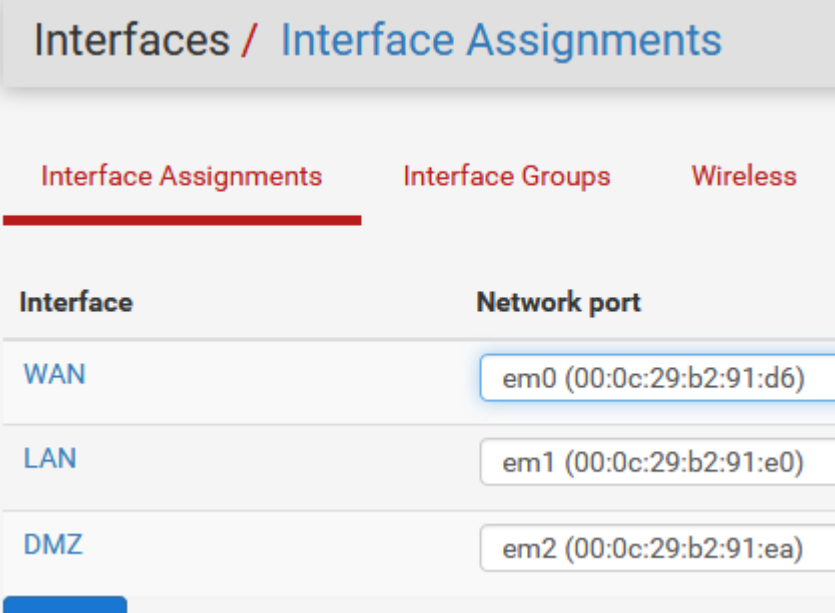
### c. Prérequis

- Un serveur routeur/pare-feu pfSense :
  - 3 cartes réseau (LAN, DMZ, WAN) → 172.16.0.1 /24,
  - VMNet (2,3,4)
- Deux serveurs W2008 R2 pour la DMZ avec IIS et l'autre HMail
  - IP fixe → 192.168.40.1 & 2 /24, 172.16.0.1 en DNS primaire
  - VMNet (2)
- Un serveur AD et un environnement RDS dans le LAN
  - IP fixe → 172.16.0.1 /24, 172.16.0.1 en DNS primaire
  - VMNet (3)
- Une machine cliente test Windows 7 dans le WAN
  - IP fixe → 80.79.100.2 /8, 172.16.0.1 en DNS primaire
  - VMNet (4)



## 2. Mode opératoire pfSense

	<b>a. Installation pfSense</b> Créer une nouvelle VM sous FreeBSD 11 64 bits et y ajouter 3 interfaces avec l'ISO de pfSense
	« Install »
	Sélectionner le clavier FR
	« Auto (UFS) Guided Disk Setup »
	Enlever l'ISO de pfSense et « Reboot »
<pre> Enter an option: 2  Available interfaces:  1 - WAN (em0 - dhcp, dhcp6) 2 - LAN (em1 - static)  Enter the number of the interface you wish to configure: 2  Enter the new LAN IPv4 address. Press &lt;ENTER&gt; for none: &gt; 172.16.0.254  Subnet masks are entered as bit counts (as in CIDR notation) e.g. 255.255.255.0 = 24     255.255.0.0   = 16     255.0.0.0     = 8  Enter the new LAN IPv4 subnet bit count (1 to 31): &gt; 24 </pre>	Taper « 2 » et entrer  Sélectionner l'interface LAN ici 2  Entrer la nouvelle IP du LAN, ici 172.16.0.254  Entrer le masque de l'interface LAN, ici /24

 <p>The image shows the pfSense login page. At the top, the URL is https://172.16.0.254/index.php. The page has a dark blue background with the text 'SIGN IN' in large white letters. Below this, the username 'admin' is entered in a white text box. The password field is represented by a series of yellow dots. At the bottom, there is a green button labeled 'SIGN IN'.</p>	<p><b>b. Configuration</b></p> <p>Mettre son AD sur la même interface que l'interface LAN de pfSense, ici VMNet 3</p> <p>Mettre 172.16.0.254 en passerelle de l'AD</p> <p>Se connecter à 172.16.0.254 et rentrer admin &amp; pfsense</p>
 <p>The image shows the 'System / General Setup' page in pfSense. The 'System' section has a 'Hostname' field with 'pfSense' and a 'Domain' field with 'gsb.fr'. The 'DNS Server Settings' section has a 'DNS Servers' field with '172.16.0.1' and a 'Hostname' field with 'gsb.fr'.</p>	<p>Entrer le nom du pare-feu, le domaine de votre AD et son DNS.</p>
 <p>The image shows the 'Interfaces / Interface Assignments' page in pfSense. It has three tabs: 'Interface Assignments', 'Interface Groups', and 'Wireless'. The 'Interface Assignments' tab is selected. It shows a table with two columns: 'Interface' and 'Network port'. The table has three rows: 'WAN' with 'em0 (00:0c:29:b2:91:d6)', 'LAN' with 'em1 (00:0c:29:b2:91:e0)', and 'DMZ' with 'em2 (00:0c:29:b2:91:ea)'.</p>	<p>Ajouter une nouvelle interface pour la DMZ</p>

	<div>Interfaces / WAN (em0)</div> <div>General Configuration</div> <div> <div>Enable <input checked="" type="checkbox"/> Enable interface</div> <div> <div>Description</div> <div>WAN</div> <div>Enter a description (n</div> </div> <div> <div>IPv4 Configuration Type</div> <div>Static IPv4</div> </div> <div> <div>IPv6 Configuration Type</div> <div>DHCP6</div> </div> <div> <div>MAC Address</div> <div>XX:XX:XX:XX:XX:XX</div> <div>This field can be used</div> <div>Enter a MAC address</div> </div> <div> <div>MTU</div> <div></div> <div>If this field is blank, th</div> </div> <div> <div>MSS</div> <div></div> <div>If a value is entered in</div> </div> <div> <div>Speed and Duplex</div> <div>Default (no preferen</div> <div>Explicitly set speed ar</div> <div>WARNING: MUST be s</div> </div> <div>Static IPv4 Configuration</div> <div> <div>IPv4 Address</div> <div>80.79.100.254</div> </div> </div>	<p>L'interface LAN a déjà été configurée auparavant.</p> <p>Configurer l'interface WAN avec l'IP 80.79.100.254</p>
	<div>Interfaces / DMZ (em2)</div> <div>General Configuration</div> <div> <div>Enable <input checked="" type="checkbox"/> Enable interface</div> <div> <div>Description</div> <div>DMZ</div> <div>Enter a description</div> </div> <div> <div>IPv4 Configuration Type</div> <div>Static IPv4</div> </div> <div> <div>IPv6 Configuration Type</div> <div>None</div> </div> <div> <div>MAC Address</div> <div>XX:XX:XX:XX:XX:XX</div> <div>This field can be us</div> <div>Enter a MAC address</div> </div> <div> <div>MTU</div> <div></div> <div>If this field is blank,</div> </div> <div> <div>MSS</div> <div></div> <div>If a value is entered</div> </div> <div> <div>Speed and Duplex</div> <div>Default (no prefer</div> <div>Explicitly set speed</div> <div>WARNING: MUST b</div> </div> <div>Static IPv4 Configuration</div> <div> <div>IPv4 Address</div> <div>192.168.40.254</div> </div> </div>	<p>Configurer l'interface DMZ avec l'IP 192.168.40.254</p>

## Gateways

	Name	Default	Interface	Gateway	Monitor IP
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN_GTW (default)		WAN	80.79.100.254	80.79.100.254
	<input checked="" type="checkbox"/> WAN_DHCP6		WAN		
<input type="checkbox"/>	<input checked="" type="checkbox"/> LAN_GTW		LAN	172.16.0.254	172.16.0.254
<input type="checkbox"/>	<input checked="" type="checkbox"/> DMZ_GTW		DMZ	192.168.40.254	192.168.40.254

Il faut configurer des passerelles pour que pfSense sert de routeur.

Configurer une passerelle pour le LAN, DMZ et WAN avec les mêmes IP.

## Propriétés de : intranet

Hôte local (A)

Sécurité

Hôte (utilise le domaine parent si ce champ est vide) :

intranet

Nom de domaine pleinement qualifié (FQDN) :

intranet.gsb.fr

Adresse IP :

192.168.40.1

☒ Mettre à jour l'enregistrement de pointeur (PTR) associé

Créer un nouveau PTR pour l'intranet avec l'IP du serveur IIS.

## c. Règles NAT

Firewall / NAT / Port Forward

Port Forward1:1OutboundNPT

Rules

			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	LAN net	5504	172.16.0.4	5504	Accès au broker
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP/UDP	*	*	LAN net	389 (LDAP)	172.16.0.1	389 (LDAP)	Permettre d'autoriser l'user de l'AD
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	LAN net	88	172.16.0.1	88	Kerberos pour s'authentifier avec un compte de l'AD
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP/UDP	*	*	LAN net	53 (DNS)	172.16.0.1	53 (DNS)	Accès au DNS pour WAN
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	UDP	*	*	LAN net	3391	172.16.0.5	3391	Redirection de port vers la RD Gateway
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	LAN net	443 (HTTPS)	172.16.0.5	443 (HTTPS)	Redirection de port vers la RD Gateway
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	DMZ address	110 (POP3)	192.168.40.2	110 (POP3)	Accès au serveur HMail
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	DMZ address	25 (SMTP)	192.168.40.2	25 (SMTP)	Accès au serveur HMail
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	DMZ address	80 (HTTP)	192.168.40.1	80 (HTTP)	Accès au serveur WEB IIS de la DMZ

Nous avons créé des règles NAT pour que les Visiteurs médicaux puissent accéder au serveur WEB IIS, envoyer des emails grâce au serveur HMail et puissent utiliser les applications distantes.



## d. Règles Firewall

Toutes les règles ont une description pour savoir à quoi elles correspondent.

Nous avons mis des règles pour le LAN et WAN qui ont donc l'accès à l'intranet et peuvent envoyer des mails grâce aux serveurs situés dans la DMZ.

WAN :

Firewall / Rules / WAN										
Floating <b>WAN</b> LAN    DMZ										
Rules (Drag to Change Order)										
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	✗ 0/240 B	IPv4 ICMP any	*	*	LAN net	*	*	none		Bloquer les pings vers le LAN
<input type="checkbox"/>	✗ 0/660 B	IPv4 ICMP any	*	*	DMZ net	*	*	none		Bloquer les pings vers la DMZ
<input type="checkbox"/>	✓ 0/2 KiB	IPv4 ICMP any	*	*	*	*	*	none		Autoriser les pings vers tout
<input type="checkbox"/>	✓ 0/269 KiB	IPv4 TCP	*	*	192.168.40.1	80 (HTTP)	*	none		NAT Accès au serveur WEB IIS de la DMZ
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	192.168.40.2	25 (SMTP)	*	none		NAT Accès au serveur HMail
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	192.168.40.2	110 (POP3)	*	none		NAT Accès au serveur HMail
<input type="checkbox"/>	✓ 0/1.06 MiB	IPv4 TCP	*	*	172.16.0.5	443 (HTTPS)	*	none		NAT Redirection de port vers la RD Gateway
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	172.16.0.5	3391	*	none		NAT Redirection de port vers la RD Gateway
<input type="checkbox"/>	✓ 1/174 KiB	IPv4 TCP/UDP	*	*	172.16.0.1	53 (DNS)	*	none		NAT Accès au DNS pour WAN
<input type="checkbox"/>	✓ 0/21 KiB	IPv4 TCP	*	*	172.16.0.1	88	*	none		NAT Kerberos pour s'authentifier avec un compte de l'AD
<input type="checkbox"/>	✓ 0/332 B	IPv4 TCP/UDP	*	*	172.16.0.1	389 (LDAP)	*	none		NAT Permettre d'autoriser l'user de l'AD
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	172.16.0.4	5504	*	none		NAT Accès au broker










Les règles NAT sont automatiquement intégrées dans les règles firewall.

Pour plus de sécurité nous avons empêché les pings vers le LAN & la DMZ mais autorisé le ping vers le reste.

Afin que le WAN puisse accéder aux applications distantes en passant par la passerelle et le broker nous avons créé un certain nombre de règles et de redirections en nous aidant du site <https://techcommunity.microsoft.com/t5/enterprise-mobility-security/rd-gateway-deployment-in-a-perimeter-network-firewall-rules/ba-p/246873> qui expliquait quels ports configurer dans un environnement RDS.

Nous n'avons pas mis d'accès RDP du WAN vers la DMZ car nous n'en voyons pas l'utilité.

## LAN :

Firewall / Rules / LAN										
Floating   WAN <b>LAN</b> DMZ										
Rules (Drag to Change Order)										
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	0 / 2.14 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	 0 / 1.06 MiB	IPv4 TCP	172.16.0.1	*	DMZ net	3389 (MS RDP)	*	none		Autoriser le RDP vers la DMZ
<input type="checkbox"/>	 0 / 51 KiB	IPv4 ICMP <u>any</u>	172.16.0.1	*	DMZ net	*	*	none		Autoriser le serveur AD à ping vers la DMZ
<input type="checkbox"/>	 0 / 0 B	IPv4 ICMP <u>any</u>	LAN net	*	DMZ net	*	*	none		Bloquer les pings de la LAN vers la DMZ
<input type="checkbox"/>	 0 / 5 KiB	IPv4 ICMP <u>any</u>	*	*	*	*	*	none		Autoriser les pings vers tout
<input type="checkbox"/>	 0 / 0 B	IPv4 TCP	LAN net	*	192.168.40.2	25 (SMTP)	*	none		Accès au serveur HMail pour le LAN
<input type="checkbox"/>	 0 / 0 B	IPv4 TCP	LAN net	*	192.168.40.2	110 (POP3)	*	none		Accès au serveur HMail pour le LAN
<input type="checkbox"/>	 0 / 0 B	IPv4 TCP	*	*	192.168.40.1	80 (HTTP)	*	none		Accès au serveur WEB IIS de la DMZ

Concernant le LAN, nous avons autorisé le serveur AD pour qu'il puisse ping et prendre la main à distance sur les serveurs de la DMZ mais nous avons bloqué pour le reste.

Nous avons seulement autorisé le RDP vers le DMZ depuis le serveur AD.

## DMZ :

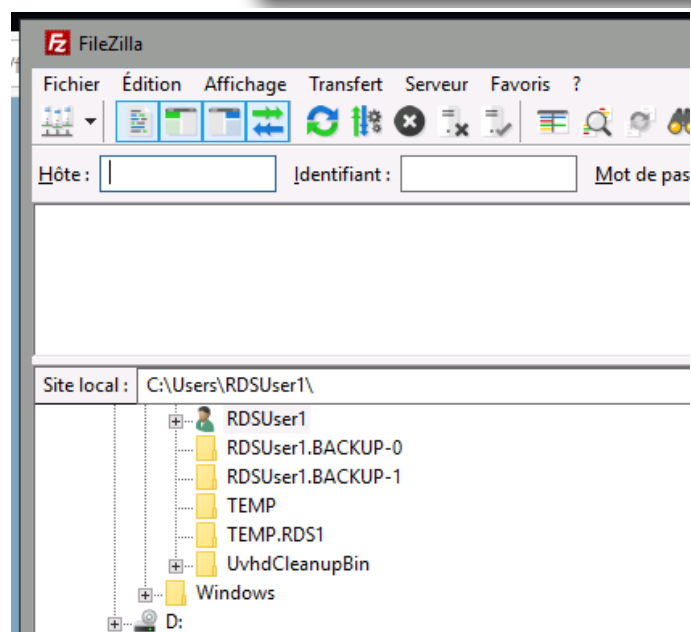
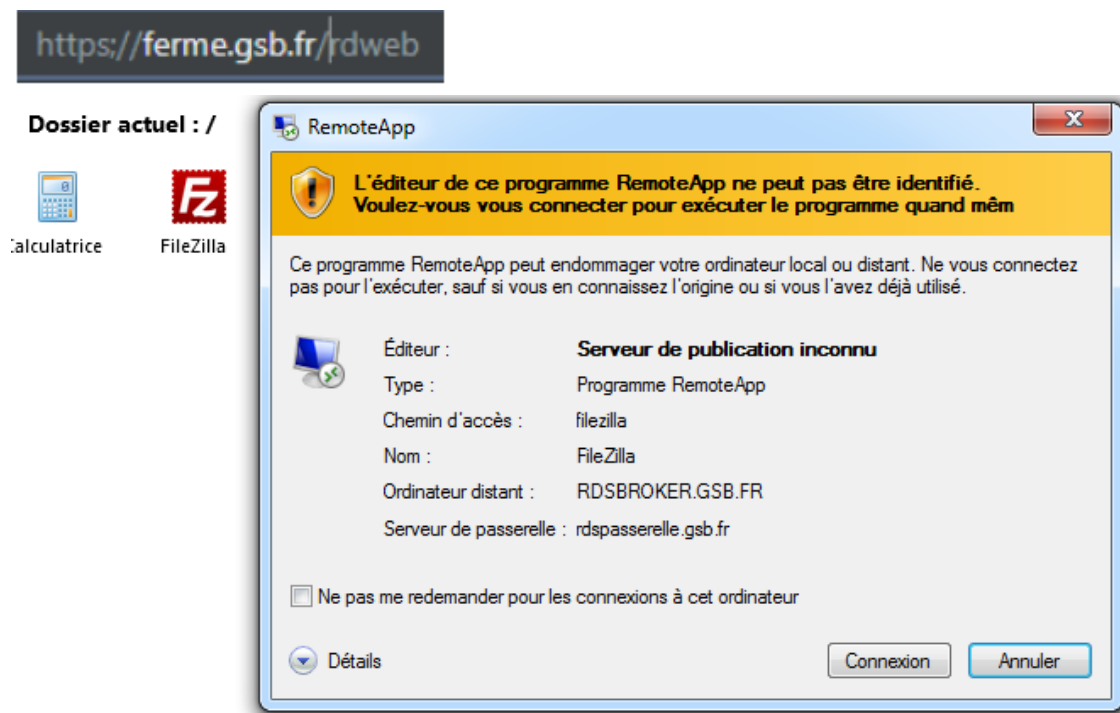
Firewall / Rules / DMZ										
Floating   WAN   LAN <u>DMZ</u>										
Rules (Drag to Change Order)										
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	✓ 0 / 272 B	IPv4 TCP	DMZ net	*	172.16.0.1	3389 (MS RDP)	*	none		RPC accès distant sur AD
<input type="checkbox"/>	✓ 0 / 182 KiB	IPv4 TCP	DMZ net	*	172.16.0.1	135	*	none		RPC pour apps distantes
<input type="checkbox"/>	✓ 0 / 141 KiB	IPv4 TCP	DMZ net	*	172.16.0.1	88	*	none		Accès au compte AD
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	DMZ net	*	172.16.0.1	3268	*	none		Accès au catalogue AD
<input type="checkbox"/>	✓ 0 / 888 KiB	IPv4 TCP/UDP	DMZ net	*	172.16.0.1	389 (LDAP)	*	none		Accès Annuaire LDAP AD
<input type="checkbox"/>	✓ 0 / 432 KiB	IPv4 TCP	DMZ net	*	172.16.0.1	445 (MS DS)	*	none		LDAP Accès au domaine
<input type="checkbox"/>	✓ 0 / 31 KiB	IPv4 UDP	DMZ net	*	172.16.0.1	53 (DNS)	*	none		Accès au DNS du LAN

Nous avons ici autorisé l'accès à plusieurs composants de l'AD pour que notre serveur mail puisse créer des emails en rapport avec les comptes de l'Active Directory.

## e. Test

### Test sur un client WAN :

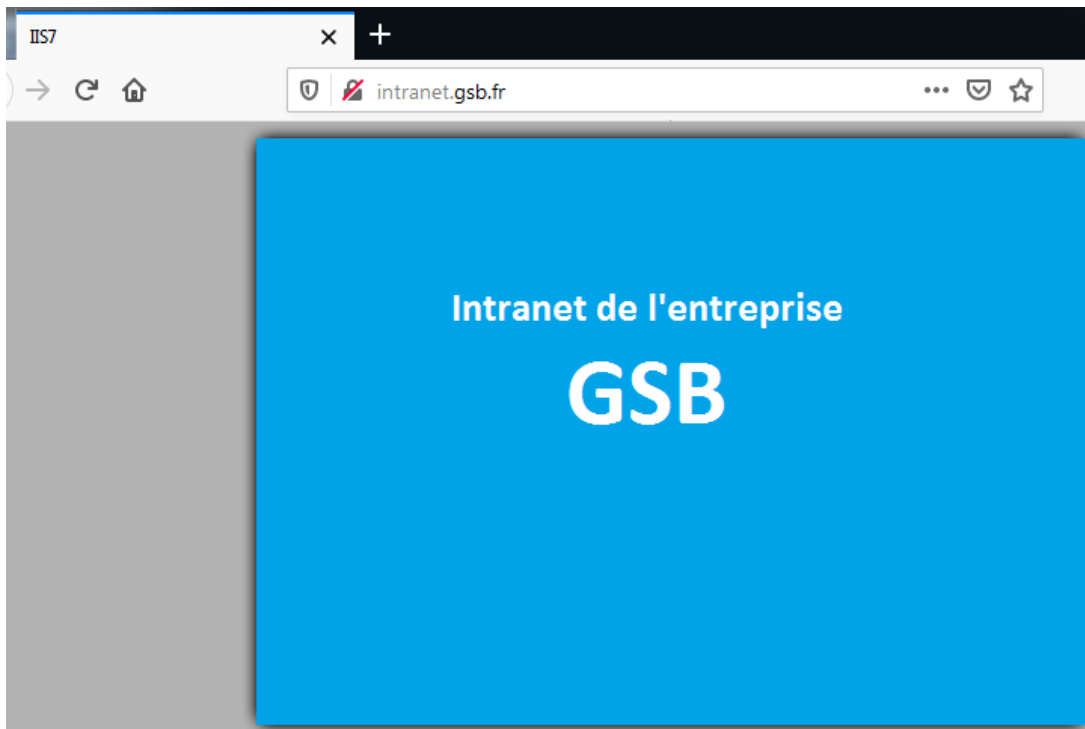
1. Applications distantes (ne pas oublier de mettre le certificat issu de la passerelle dans le client)



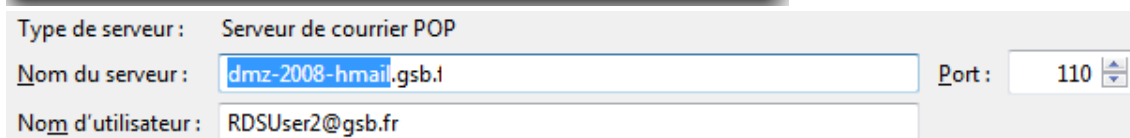
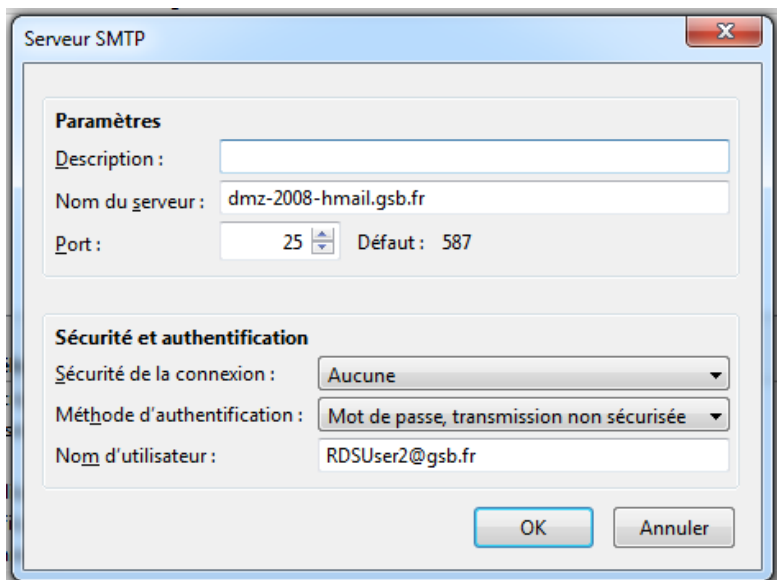
ID de connexion	ID d'utilisateur	Nom d'utilisateur	Connecté le	Durée de la connex...	Durée d...	Ordinateur cible	Adresse IP du client	Port cible	Transport
4-2	GSB\RDSUser1	RDSUser1	29/02/2020 14:55:57	00:00:56	00:00:00	RDS1.gsb.fr	80.79.100.2	3389	RPC-HTTP


Vérification du fonctionnement de la passerelle


## 2. Intranet GSB (Serveur IIS)









## 3. Mail entre LAN et WAN



 Courrier entrant

 Test e-mail WAN --> LAN -

 Relever |   Écrire |   Messagerie instantanée  Adress

De RDSUser2 <RDSUser2@gsb.fr> ★


Sujet **Test e-mail WAN --> LAN**

Pour Moi★

Test

 Courrier entrant

 Test e-mail LAN --> WAN -

 Relever |   Écrire |   Messagerie instantanée  Adress

De Administrateur <administrateur@gsb.fr> ★

Sujet **Test e-mail LAN --> WAN**

Pour Moi★

Test

#### **4. Conclusion**

L'installation et la configuration d'un serveur pfSense sont essentielles pour toutes les entreprises.

Ce routeur/pare-feu open source est réputé dans le monde pour sa fiabilité et sa sécurité.

Il est adaptable à tous types d'infrastructures et ne nécessite que peu de ressources.

Une fois sa mise en place effectuée, les employés GSB pourront effectuer leur travail et leurs échanges sur internet de façon sécurisée.