



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	4
b. Configuration	7
c. Règles NAT	8
d. Règles Firewall	11
e. Test	
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.

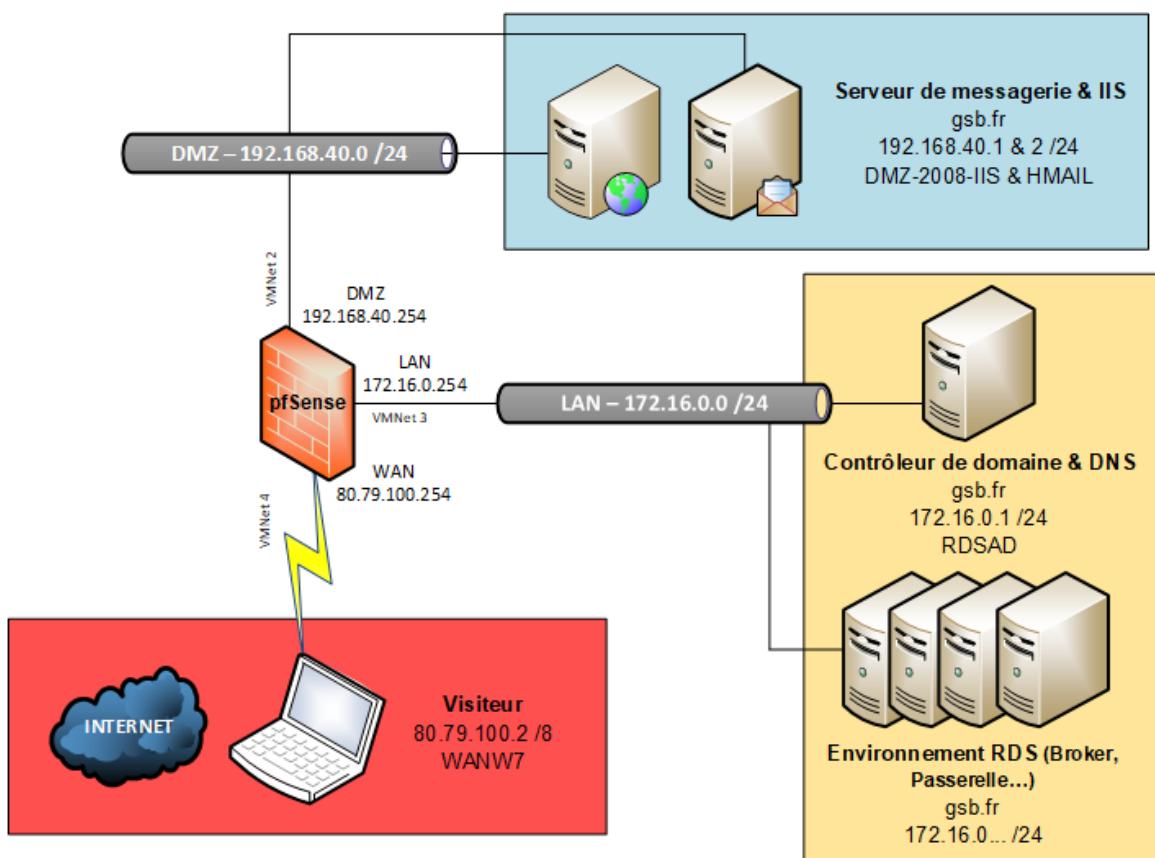
Le serveur de mail GSB devra également être accessible.

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.

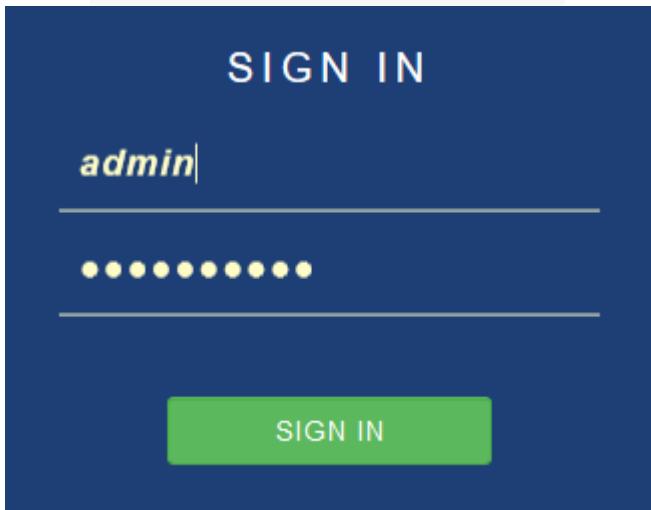
c. Prérequis

- 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

	a. Installation pfSense 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 »
<p>Enter an option: 2</p> <p>Available interfaces:</p> <p>1 - WAN (em0 - dhcp, dhcp6) 2 - LAN (em1 - static)</p> <p>Enter the number of the interface you wish to configure: 2</p> <p>Enter the new LAN IPv4 address. Press <ENTER> for none: > 172.16.0.254</p> <p>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</p> <p>Enter the new LAN IPv4 subnet bit count (1 to 31): > 24</p>	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>b. Configuration</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 & pfSense</p>									
<p>System / General Setup</p> <p>System</p> <p>Hostname pfSense Name of the firewall host, without domain part</p> <p>Domain gsb.fr Do not use '.local' as the final part of the domain (TLD). The '.local' domain is widely used by Bonjour/Rendezvous/Airprint/Airplay, and some Windows systems and networked device Alternatives such as '.local.lan' or '.mylocal' are safe.</p> <p>DNS Server Settings</p> <table border="0"> <tr> <td>DNS Servers</td> <td>172.16.0.1</td> <td>gsb.fr</td> </tr> <tr> <td>Address</td> <td colspan="2">Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.</td> </tr> <tr> <td>Hostname</td> <td colspan="2">Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).</td> </tr> </table>	DNS Servers	172.16.0.1	gsb.fr	Address	Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.		Hostname	Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).		<p>Entrer le nom du pare-feu, le domaine de votre AD et son DNS.</p>
DNS Servers	172.16.0.1	gsb.fr								
Address	Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.									
Hostname	Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).									
<p>Interfaces / Interface Assignments</p> <p>Interface Assignments Interface Groups Wireless</p> <table border="1"> <thead> <tr> <th>Interface</th> <th>Network port</th> </tr> </thead> <tbody> <tr> <td>WAN</td> <td>em0 (00:0c:29:b2:91:d6)</td> </tr> <tr> <td>LAN</td> <td>em1 (00:0c:29:b2:91:e0)</td> </tr> <tr> <td>DMZ</td> <td>em2 (00:0c:29:b2:91:ea)</td> </tr> </tbody> </table>	Interface	Network port	WAN	em0 (00:0c:29:b2:91:d6)	LAN	em1 (00:0c:29:b2:91:e0)	DMZ	em2 (00:0c:29:b2:91:ea)	<p>Ajouter une nouvelle interface pour la DMZ</p>	
Interface	Network port									
WAN	em0 (00:0c:29:b2:91:d6)									
LAN	em1 (00:0c:29:b2:91:e0)									
DMZ	em2 (00:0c:29:b2:91:ea)									

<p>Interfaces / WAN (em0)</p> <p>General Configuration</p> <table> <tr> <td>Enable</td> <td><input checked="" type="checkbox"/> Enable interface</td> </tr> <tr> <td>Description</td> <td>WAN</td> </tr> <tr> <td colspan="2">Enter a description (n:)</td> </tr> <tr> <td>IPv4 Configuration Type</td> <td>Static IPv4</td> </tr> <tr> <td>IPv6 Configuration Type</td> <td>DHCP6</td> </tr> <tr> <td>MAC Address</td> <td>XX:XX:XX:XX:XX:XX</td> </tr> <tr> <td colspan="2">This field can be used Enter a MAC address</td> </tr> <tr> <td>MTU</td> <td></td> </tr> <tr> <td colspan="2">If this field is blank, th</td> </tr> <tr> <td>MSS</td> <td></td> </tr> <tr> <td colspan="2">If a value is entered in</td> </tr> <tr> <td>Speed and Duplex</td> <td>Default (no preferen</td> </tr> <tr> <td colspan="2">Explicitly set speed an</td> </tr> <tr> <td colspan="2">WARNING: MUST be set</td> </tr> </table> <p>Static IPv4 Configuration</p> <table> <tr> <td>IPv4 Address</td> <td>80.79.100.254</td> </tr> </table>	Enable	<input checked="" type="checkbox"/> Enable interface	Description	WAN	Enter a description (n:)		IPv4 Configuration Type	Static IPv4	IPv6 Configuration Type	DHCP6	MAC Address	XX:XX:XX:XX:XX:XX	This field can be used Enter a MAC address		MTU		If this field is blank, th		MSS		If a value is entered in		Speed and Duplex	Default (no preferen	Explicitly set speed an		WARNING: MUST be set		IPv4 Address	80.79.100.254	<p>L'interface LAN a déjà été configurée auparavant.</p> <p>Configurer l'interface WAN avec l'IP 80.79.100.254</p>
Enable	<input checked="" type="checkbox"/> Enable interface																														
Description	WAN																														
Enter a description (n:)																															
IPv4 Configuration Type	Static IPv4																														
IPv6 Configuration Type	DHCP6																														
MAC Address	XX:XX:XX:XX:XX:XX																														
This field can be used Enter a MAC address																															
MTU																															
If this field is blank, th																															
MSS																															
If a value is entered in																															
Speed and Duplex	Default (no preferen																														
Explicitly set speed an																															
WARNING: MUST be set																															
IPv4 Address	80.79.100.254																														
<p>Interfaces / DMZ (em2)</p> <p>General Configuration</p> <table> <tr> <td>Enable</td> <td><input checked="" type="checkbox"/> Enable interface</td> </tr> <tr> <td>Description</td> <td>DMZ</td> </tr> <tr> <td colspan="2">Enter a description</td> </tr> <tr> <td>IPv4 Configuration Type</td> <td>Static IPv4</td> </tr> <tr> <td>IPv6 Configuration Type</td> <td>None</td> </tr> <tr> <td>MAC Address</td> <td>XX:XX:XX:XX:XX:XX</td> </tr> <tr> <td colspan="2">This field can be us Enter a MAC addres</td> </tr> <tr> <td>MTU</td> <td></td> </tr> <tr> <td colspan="2">If this field is blank,</td> </tr> <tr> <td>MSS</td> <td></td> </tr> <tr> <td colspan="2">If a value is entered</td> </tr> <tr> <td>Speed and Duplex</td> <td>Default (no preferen</td> </tr> <tr> <td colspan="2">Explicitly set speed</td> </tr> <tr> <td colspan="2">WARNING: MUST be set</td> </tr> </table> <p>Static IPv4 Configuration</p> <table> <tr> <td>IPv4 Address</td> <td>192.168.40.254</td> </tr> </table>	Enable	<input checked="" type="checkbox"/> Enable interface	Description	DMZ	Enter a description		IPv4 Configuration Type	Static IPv4	IPv6 Configuration Type	None	MAC Address	XX:XX:XX:XX:XX:XX	This field can be us Enter a MAC addres		MTU		If this field is blank,		MSS		If a value is entered		Speed and Duplex	Default (no preferen	Explicitly set speed		WARNING: MUST be set		IPv4 Address	192.168.40.254	<p>Configurer l'interface DMZ avec l'IP 192.168.40.254</p>
Enable	<input checked="" type="checkbox"/> Enable interface																														
Description	DMZ																														
Enter a description																															
IPv4 Configuration Type	Static IPv4																														
IPv6 Configuration Type	None																														
MAC Address	XX:XX:XX:XX:XX:XX																														
This field can be us Enter a MAC addres																															
MTU																															
If this field is blank,																															
MSS																															
If a value is entered																															
Speed and Duplex	Default (no preferen																														
Explicitly set speed																															
WARNING: MUST be set																															
IPv4 Address	192.168.40.254																														

<p>System / Routing / Gateways</p> <p>Gateways Static Routes Gateway Groups</p> <p>Gateways</p> <table border="1"> <thead> <tr> <th>Name</th><th>Default</th><th>Interface</th><th>Gateway</th><th>Monitor IP</th></tr> </thead> <tbody> <tr> <td><input type="checkbox"/> WAN_GTW (default)</td><td><input checked="" type="checkbox"/></td><td>WAN</td><td>80.79.100.254</td><td>80.79.100.254</td></tr> <tr> <td colspan="5"><input checked="" type="checkbox"/> WAN_DHCPC6</td></tr> <tr> <td><input type="checkbox"/> LAN_GTW</td><td><input checked="" type="checkbox"/></td><td>LAN</td><td>172.16.0.254</td><td>172.16.0.254</td></tr> <tr> <td><input type="checkbox"/> DMZ_GTW</td><td><input checked="" type="checkbox"/></td><td>DMZ</td><td>192.168.40.254</td><td>192.168.40.254</td></tr> </tbody> </table>	Name	Default	Interface	Gateway	Monitor IP	<input type="checkbox"/> WAN_GTW (default)	<input checked="" type="checkbox"/>	WAN	80.79.100.254	80.79.100.254	<input checked="" type="checkbox"/> WAN_DHCPC6					<input type="checkbox"/> LAN_GTW	<input checked="" type="checkbox"/>	LAN	172.16.0.254	172.16.0.254	<input type="checkbox"/> DMZ_GTW	<input checked="" type="checkbox"/>	DMZ	192.168.40.254	192.168.40.254	<p>Il faut configurer des passerelles pour que pfSense sert de routeur.</p> <p>Configurer une passerelle pour le LAN, DMZ et WAN avec les mêmes IP.</p>
Name	Default	Interface	Gateway	Monitor IP																						
<input type="checkbox"/> WAN_GTW (default)	<input checked="" type="checkbox"/>	WAN	80.79.100.254	80.79.100.254																						
<input checked="" type="checkbox"/> WAN_DHCPC6																										
<input type="checkbox"/> LAN_GTW	<input checked="" type="checkbox"/>	LAN	172.16.0.254	172.16.0.254																						
<input type="checkbox"/> DMZ_GTW	<input checked="" type="checkbox"/>	DMZ	192.168.40.254	192.168.40.254																						
<p>Propriétés de : intranet</p> <p>Hôte local (A) Sécurité</p> <p>Hôte (utilise le domaine parent si ce champ est vide) : intranet</p> <p>Nom de domaine pleinement qualifié (FQDN) : intranet.gsb.fr</p> <p>Adresse IP : 192.168.40.1</p> <p><input checked="" type="checkbox"/> Mettre à jour l'enregistrement de pointeur (PTR) associé</p>	<p>Créer un nouveau PTR pour l'intranet avec l'IP du serveur IIS.</p>																									

c. Règles NAT

Firewall / NAT / Port Forward									
	Port Forward	1:1	Outbound	NPt					
Rules									
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description
<input type="checkbox"/>	 WAN	TCP	*	*	LAN net	5504	172.16.0.4	5504	Accès au broker
<input 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"/>	 WAN	TCP	*	*	LAN net	88	172.16.0.1	88	Kerberos pour s'authentifier avec un compte de l'AD
<input type="checkbox"/>	 WAN	TCP/UDP	*	*	LAN net	53 (DNS)	172.16.0.1	53 (DNS)	Accès au DNS pour WAN
<input type="checkbox"/>	 WAN	UDP	*	*	LAN net	3391	172.16.0.5	3391	Redirection de port vers la RD Gateway
<input type="checkbox"/>	 WAN	TCP	*	*	LAN net	443 (HTTPS)	172.16.0.5	443 (HTTPS)	Redirection de port vers la RD Gateway
<input type="checkbox"/>	 WAN	TCP	*	*	DMZ address	110 (POP3)	192.168.40.2	110 (POP3)	Accès au serveur HMail
<input type="checkbox"/>	 WAN	TCP	*	*	DMZ address	25 (SMTP)	192.168.40.2	25 (SMTP)	Accès au serveur HMail
<input 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	WAN	LAN	DMZ	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	X	0 /240 B	IPv4 ICMP any	*	*	LAN net	*	*	*	*	*	none		Bloquer les pings vers le LAN
<input type="checkbox"/>	X	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.

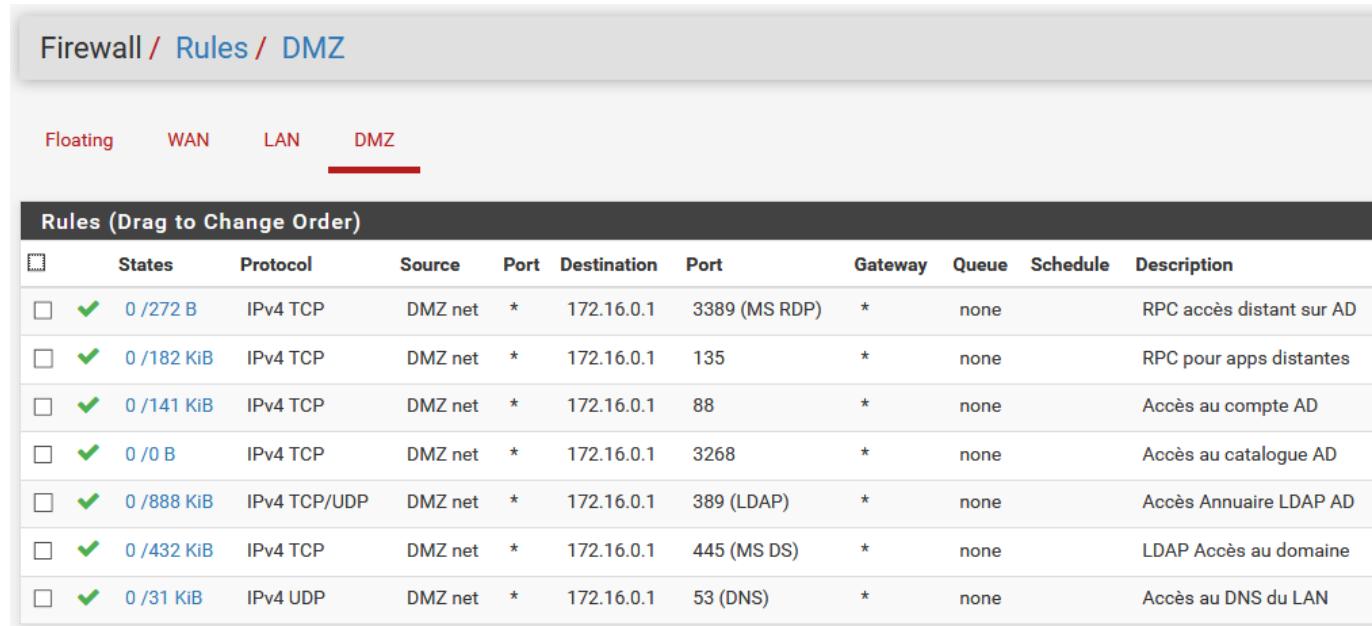
LAN :

Firewall / Rules / LAN										
	Floating	WAN	LAN	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	
✗ ✓ 0 /1.06 MiB	IPv4 TCP	172.16.0.1	*	DMZ net	3389 (MS RDP)	*	none		Autoriser le RDP vers la DMZ	
✗ ✓ 0 /51 KiB	IPv4 ICMP any	172.16.0.1	*	DMZ net	*	*	none		Autoriser le serveur AD à ping vers la DMZ	
✗ ✗ 0 /0 B	IPv4 ICMP any	LAN net	*	DMZ net	*	*	none		Bloquer les pings de la LAN vers la DMZ	
✗ ✓ 0 /5 KiB	IPv4 ICMP any	*	*	*	*	*	none		Autoriser les pings vers tout	
✗ ✓ 0 /0 B	IPv4 TCP	LAN net	*	192.168.40.2	25 (SMTP)	*	none		Accès au serveur HMail pour le LAN	
✗ ✓ 0 /0 B	IPv4 TCP	LAN net	*	192.168.40.2	110 (POP3)	*	none		Accès au serveur HMail pour le LAN	
✗ ✓ 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 autoriser 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 DMZ

Rules (Drag to Change Order)

	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)

The screenshot shows a Windows RemoteApp connection dialog box and a FileZilla interface. The dialog box is titled 'RemoteApp' and displays the following information:

Calculatrice	FileZilla
Dossier actuel : /	
L'éditeur de ce programme RemoteApp ne peut pas être identifié. Voulez-vous vous connecter pour exécuter le programme quand même?	
Ce programme RemoteApp peut endommager votre ordinateur local ou distant. Ne vous connectez pas pour l'exécuter, sauf si vous en connaissez l'origine ou si vous l'avez déjà utilisé.	
Éditeur : Serveur de publication inconnu	
Type : Programme RemoteApp	
Chemin d'accès : filezilla	
Nom : FileZilla	
Ordinateur distant : RDSBROKER.GSB.FR	
Serveur de passerelle : rdspasserelle.gsb.fr	
<input type="checkbox"/> Ne pas me redemander pour les connexions à cet ordinateur	
<input type="button" value="Détails"/>	<input type="button" value="Connexion"/> <input type="button" value="Annuler"/>

The FileZilla interface shows the following details:

- Fichier
- Édition
- Affichage
- Transfert
- Serveur
- Favoris
- ?

Hôte: [] Identifiant: [] Mot de pas

Site local: C:\Users\RDSUser1

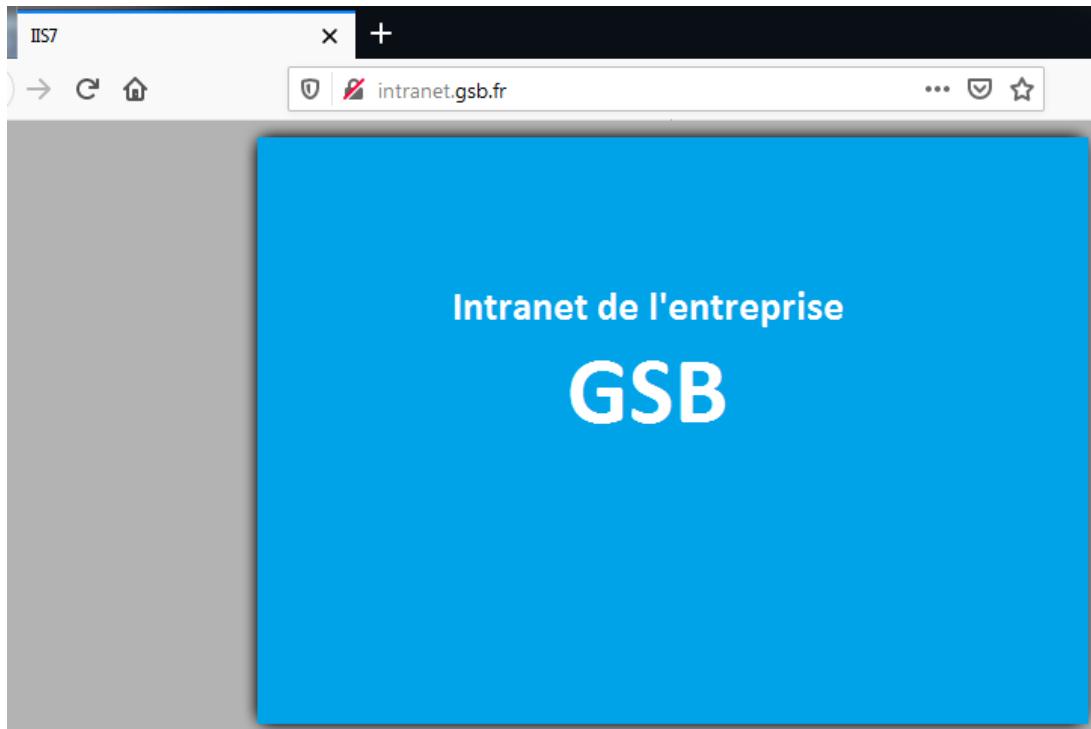
- RDSUser1
- RDSUser1.BACKUP-0
- RDSUser1.BACKUP-1
- TEMP
- TEMP.RDS1
- UvhdCleanupBin
- Windows

D:

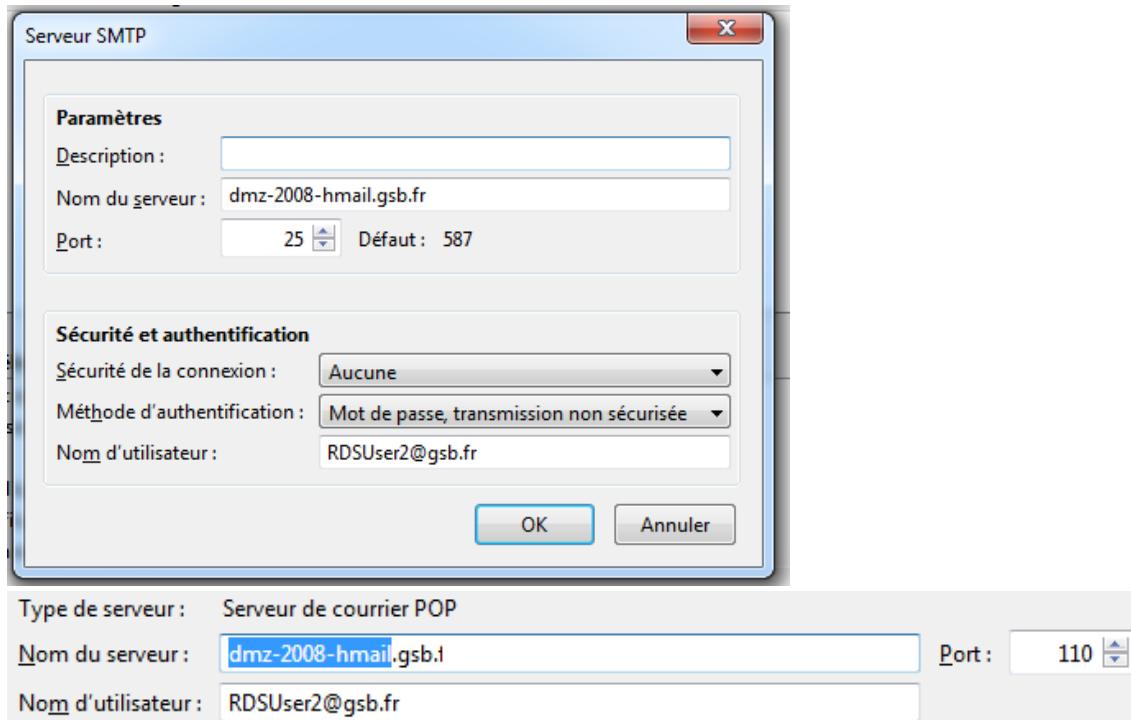
ID de connexion	ID d'utilisateur	Nom d'utilisateur	Connecté le	Durée de la conn...	Durée d...	Ordinateur cible	Adresse IP du client	Port cible	Transport
4:2	GSB\RDSUser1	RDSUser1	29/02/2020 14:55:57	00:00:56	00:00:00	RDS1.gsb.fr	80.79.100.2	3389	RPC-HTTP

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.