# DÚ DOMOTech TECH

# CONFIGURATION DE PFSENSE

PROCEDURE

Date de création : 01/03/2022 Version : 1.1 Pour validation : DSI A destination : DSI Mode de diffusion : SharePoint Nombre de pages : 15

# Métadonnées

Diffusion				
Périmètre de diffusion	Contrôlé	Interne	Libre	

Historique des évolutions			
Auteur	Version	Objet de la version et liste des modifications	
Dylan Chau	1.0	Initialisation du document	
Dylan Chau	1.1	Mise à jour	

Validation					
Réda	cteur	Validateur			
Nom	Date	Nom	Date		
Dylan Chau	01/03/2023	DSI	01/03/2023		
Date d'application : 01/03/2023					

#### Sommaire

Méto	adonnées	2
Prére	equis	3
Prés	entation	4
I)	Création des interfaces réseaux	5
II)	Configuration Outbound	8
III)	Configuration du firewall PFSense10	0
a.	Création des Aliases10	0
b.	Règles du pare-feu12	2
c.	Configuration des règles de pare-feu12	2
IV)	Cahier de tests	5

## Prérequis

- Un routeur/FW PFSense avec une carte réseau WAN, et les cartes réseaux LAN (au moins une). Dans notre cas, il s'agit du réseau DMT SRV et DMT USER.
- La matrice de flux des services DOMOTech.

### Présentation

pfSense est une solution de pare-feu et de routage open-source basée sur le système d'exploitation FreeBSD. Il offre une multitude de fonctionnalités avancées pour sécuriser et gérer les réseaux informatiques de toutes tailles, allant des petites entreprises aux environnements d'entreprise complexes.

Parmi ses fonctionnalités, on peut retrouver :

- Pare-feu
- Routage
- VPN
- Journalisation et surveillance

#### Création des interfaces réseaux

Nous allons créer l'ensemble des interfaces réseaux afin de permettre la connectivité entre les différents LANs.

/!\ Il est important d'avoir une carte réseau LAN configuré afin de pouvoir accéder à l'interface PFSense et de configurer les autres.



Cliquer sur « Interfaces ». \_

admin@102.169.66.2 (Local Database)

- Cliquer sur l'interface réseau à configurer

Interface Assignments	Interface Groups	Wireless	VLANs	Qin
Interface	Network	port		
WAN	em0 (0	0:0c:29:da:29:8f	)	
LAN_SRV	em1 (0	0:0c:29:da:29:99	9)	
LAN_USER	em2 (0	0:0c:29:da:29:a3	3)	
R Save				

- Cliquer sur « Enable interface » pour activer l'interface réseau.

Interfaces / OPT	2 (em3)	≡ ₩ 0
General Configuration	n	
Enable	Enable interface	
Description	Ian_uset Enter a description (name) for the interface here.	
IPv4 Configuration Type	None v	
Pv6 Configuration Type	None	
MAC Address	8000000000	

- Mettre dans « Description » le nom du réseau (Par exemple, ici LAN\_USER).

of sense	System -	Interfaces -	Firewall •	Services -	VPN -	Status -	Diagnostics -	Help •	(+
Interfaces /	OPT2	(em3)							≞ ⊯ 0
General Confi	iguration								
	Enable	Enable interface					_		
Desc	cription	lan_uset Enter a description (	name) for the in	terface here.					
IPv4 configuratio	on Type	None				~			
11v6 Configuratio	on Type	None				~			
<b>/</b>									

- Dans « IPv4 Configuration Type », mettre en « Static IPv4 ».

COMMUNITY EDITION	Interfaces • Firewal	Services	VPN • Status •	Diagnostics •	Help +	60	
Interfaces / OPT2	(em3)					≢ ⊯ <b>0</b>	
General Configuration							
Enable	Enable interface						
Description	Ian_user Enter a description (name) for	the interface here.					
IPv4 Configuration Type	Static IPv4		v				
IPv6 Consuration Type	None	Ð	v				¢
MAC Address	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	y ('spoof') the MAC ad owing format xxxxxxx	dress of this interface. xxxxxxx or leave blank.				
MTU			10				

- Renseigner l'adresse IP de la passerelle et le masque.

IPv4 Address	192.168.66.254		1	24	~
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.				

- Cliquer sur Save pour sauvegarder votre configuration de l'interface réseau.

ite address space, too.
ks traffic from reserved IP addres ing table, and so should not appe option should only be used on er r: The update frequency can be cl

- Cliquer maintenant sur « Apply change » tout en haut de la page pour appliquer les changements.

Don't forget to adjust the DHCP Server range if needed after applying.	The LAN_USER configuration has been changed. The changes must be applied to take effect. Don't forget to adjust the DHCP Server range if needed after applying.	Apply Changes
------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------

- Réitérer l'opération pour l'ensemble des interfaces réseaux à ajouter.

#### II) Configuration Outbound

Les Outbound sur pfSense font référence à la configuration des règles de pare-feu sortantes pour les paquets qui quittent le réseau local vers Internet ou un autre réseau distant.

Nous allons configurer la communication entre le LAN SERVER et LAN USER.

- Cliquer sur « Firewall ».



- Cliquer ensuite sur « NAT ».

DI SENSE	System + Interfaces +	Firewall 🕶	Services + VPI
		Aliases	
Status /	Dashboard	NAT	
		Rules	
System Inf	ormation	Schedules	· • •
Name	pfSenseDMT.domotech.priv	Traffic Shape	r
User	admin@192.168.66.2 (Local E	Virtual IPs	
System	VMware Virtual Machine		

- Cliquer sur « Outbound ».

pfSenseDMT.domotech.priv	- Fir x +			
🔺 🔥 Non sécurisé	https://192.168.66.2	254/firewall_n	at_out.php	
		System <del>+</del>	Interfaces <del>-</del> F	irewall <del>+</del> Services <del>+</del>
	Firewall /	NAT / O	utbound	
	Port Forward	1:1	Outbound NPt	
	Outbound N	AT Mode		
		Mode	0	0
			Automatic outbound NA rule generation. (IPsec passthrough included)	T Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)

- Cliquer sur le mode « Manual » pour configurer nous-même.

NAT /	Outbound			
1:1	Outbound NPt			
T Mode				
Mode	0	0	۲	
	Automatic outbound NAT	Hybrid Outbound NAT	Manual Outbound NAT	D
	rule generation.	rule generation.	rule generation.	п 0
	included)	NAT + rules below)	Outbound NAT)	0
_	B Save			

- Cliquer sur « Add » avec une flèche vers le bas pour que ce soit plus lisible



- Choisir le réseau à qui nous voulons donner accès à d'autre réseau (Il s'agit de nos différents LAN USER et SERVER).

Firewall / NAT / Outbound / Edit						
Edit Advanced Outbo	und NAT Entry					
Disabled	Disable this rule					
Do not NAT	<ul> <li>Enabling this option will disable NAT for traffic matching this rule and stop In most cases this option is not required.</li> </ul>					
Interface	LAN_SRV V					
Address Family	WAN at et LAN_SRV LAN_USER Select the Internet Protocol version this rule applies to.					

- Renseigner l'IP réseau des réseaux que l'on a configurés.

			Choose which protocol this rule should mate	ch. In most cases "any" is specified.		
_	$\rightarrow$	Source	Network 🗸	192.168.66.0 Source network for the outbound NAT mapping.	/ 24	~
		Destination	Any		/ 24	~

- Cliquer ensuite sur « Save » et créer toutes les entrées que vous voulez



### III) Configuration du firewall PFSense

#### a. Création des Aliases

Les Aliases sont des noms uniques qui permettent de regrouper plusieurs adresses IP, noms et ports afin de simplifier la configuration des règles du pare-feu.

- Cliquer sur « Firewall ».

pfSenseDMT.domotech.priv - Firit × +		
C A Non sécurisé   https://192.168.21.254/firewall_rules.php?if=lan		
	Firewall - Ser	vices - V
Firewall / Rules / LAN_SRV	Aliases NAT Rules	
Floating WAN LAN_SRV LAN_U	Schedules Traffic Shaper	
Rules (Drag to Change Order)	Virtual IPs	
States Protocol Source	Port Destination	Port
• Ø 0 /0 P • •	* IAN COV	244

- Cliquer sur « Aliases ».

pfSenseDMT.domotech.priv - Fire 🗙 🕂 C A Non sécurisé https://192.168.21.254/firewall\_rules.php?if=lan *of* sense Firewall -System -Interfaces -Services -COMMUNITY EDITION Aliases Firewall / Rules / LAN NAT Rules Schedules Floating WAN LAN\_SRV LAN\_U Traffic Shaper Virtual IPs Rules (Drag to Change Order)  $\Box$ Source States Protocol Port Destination Port . . O /O P . \* LAN COV 449

- Cliquer sur « Ports »

pfSenseDMT.domotech.priv -	Fire × +			
C 💧 Non sécurisé	https://192.168.21.254/	firewall_alias	es.php?tab=port	
		System <del>-</del>	Interfaces 🗸	Firewall 👻
	Firewall / A	liases /	Ports	
	IP Ports	URLs	All	

- Cliquer sur « + ADD » pour ajouter un aliases.



- Renseigner un nom, une description, le type et les ports à regrouper par exemple. Les aliases peuvent aussi regrouper des noms, et également des IP.

pfSenseDMT.domotech.priv - Fire × +							
C 🔺 Non sécurisé   https://192.168.21.254/fire	wall_aliases_edit.php?tab=pc	rt					A
COMMUNITY EDITION	stem 👻 Interfaces 👻	Firewall - Services -	VPN -	Status 🗸	Diagnostics -	Help 🗸	<b>‡</b> 2
Firewall / Alia	ases / Edit						
Properties							
Na	Aliases The name of the alia	s may only consist of the chara	icters "a-z, A-Z,	, 0-9 and _".			
Descript	Test A description may be	entered here for administrativ	e reference (no	ot parsed).			
T	Port(s)			*			
Port(s)							
	lint Enter ports as desire	d, with a single port or port ran	ge per entry. P	ort ranges can b	e expressed by sep	arating with a colon.	
F	Port 80		H	ГТР			🛅 Delete
	Port		De	escription			Delete
	Save + Add	Port					

- Dans l'infrastructure de DOMOTech, les aliases suivants ont été créés afin d'être utilisé pour la mise en place de la matrice de flux de services.

Firewall Aliases Ports					
Name	Values	Description	Actions		
AD	389, 88	Authentification AD	e 🗋 🖉		
Browsing	80, 443, 8080, 53	List of Browsing Ports	e 🗋 🖉		
File_Transfer	20, 21, 22	Transfert de fichiers	e 🗋 🖉		
Mail_Access	143, 993, 110, 995	Accès au courrier	e 🗋 🖉		
RemoteMGMT	80, 22, 3389	For management access	e 🗋 🖉		
			🕂 Add 🔔 Import		

#### b. Règles du pare-feu

Plusieurs règles ont été mises en place pour sécuriser le réseau de DOMOTech. Ces règles sont présentes dans le document « Matrice de flux des services » (Annexe 3).

#### c. Configuration des règles de pare-feu

Une règle de pare-feu est une instruction ou un ensemble d'instructions qui permet de contrôler le trafic réseau entrant ou sortant d'un système informatique. Le pare-feu analyse chaque paquet de données qui entre ou sort du réseau et décide si le paquet doit être autorisé ou bloqué en fonction des règles de pare-feu configurées. La matrice de flux des services DOMOTech apportent des détails sur les services autorisés.

Nous allons configurer la communication entre le LAN SERVER et LAN USER, et le WAN.

- sense Interfaces -Firewall -Services + VPN System + UNITY EDITION Aliases Status / Dashboard NAT Rules 600 System Information Schedules Name pfSenseDMT.domotech.priv Traffic Shaper admin@192.168.66.2 (Local E User Virtual IPs System VMware Virtual Machine
- Cliquer sur « Firewall ».

- Cliquer ensuite sur « Rules ».

pfSenseDMT.domotech.priv - Fin × +		
C A Non sécurisé   https://192.168.21.254/firewall_rules.php		
COMMUNITY EDITION	<b>Firewall →</b> S	ervices <del>-</del>
Firewall / Rules / WAN	Aliases NAT	
	Rules	
Floating WAN LAN_SRV LAN_U	Schedules Traffic Shaper	
Rules (Drag to Change Order)	Virtual IPs	

- Cliquer sur un LAN.



- Les règles fonctionnent en commençant par la plus haute à la plus basse.

Il est également possible de créer des « separator » afin d'avoir une meilleure visibilité et gestion sur les règles.

La première règle sera de bloquer toutes les connexions du LAN vers les autres afin de les débloquer en utilisant la matrice.

Add	🕽 Add	🔟 Delete	F Save	+ Separator
-----	-------	----------	--------	-------------

- Cliquer sur « Add »

×		∕∕↓ ā
*		✓ □
	1 Add 1 Add 🛅 Dele	te 🖬 Save

- Pour cette règle,
  - Action : Block
  - Protocol : Any
  - Source : LAN USER NET, Destination : Any

Edit Eirowell Bule			_	_		_	
Edit Filewall Kule							
Action	Pass		~				
	Pass						
	Block		TCP RST	or ICMP port unre	eachable for UDP) is return	ed to the sender,	
	Reject		hal packet	is discarded.			
Disabled	<ul> <li>Disable this rule</li> </ul>						
	Set this option to disable this	rule without removing it from t	he list.				
Interfece							
interface	LAN_USER		<b>*</b>				
	Choose the interface from wh	ich packets must come to mat	ch this rule.				
Address Family	IPv4		~				
	Select the Internet Protocol v	ersion this rule applies to.					
Protocol	TOD						
10000	Observation International International	and a shared discovered.	•				
	Choose which IP protocol this	rule should match.					
Source							
Source	Invert match	any		✓ Source	e Address	1	~
ource							
	Display Advanced						
	The Source Port Range for a its default value, any	connection is typically random	and almost never equa	I to the destinatio	n port. In most cases this	setting must rema	lin at
	no deradit valde, any.						
Destination							
Destination	Invert match	any		✓ Destir	nation Address	1	~
Destination							
Destination Port Range	(other) 🗸		(other)	▼			

- Cliquer ensuite sur « Save »



- Configurer l'ensemble des autres règles en utilisant la matrice de flux des services et le cahier de test pour vérifier le bon fonctionnement de chaque règle.

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
Internet	t Access										Ô
- ~	14 /2.17 MiB	IPv4 TCP/UDP	192.168.21.0/24	•	*	Browsing	*	none		Allow Browsing	<b>∛</b> ∥⊡©
	0/0B	IPv4 ICMP any	LAN_USER net	*	*	*	*	none		Test de connectivité	
Active [	Directory										Î
- ~	6 /71 KiB	IPv4 TCP/UDP	LAN_USER net	•	192.168.0.0/27	AD	*	none		Authentification AD	<b>₩</b> /00
Other											Ô
• •	0 /592 B	IPv4 UDP	LAN_USER net	*	*	123 (NTP)	*	none		Heure	\$∥©©
- ~	0/08	IPv4 TCP	LAN_USER net	•	*	Mail_Access	*	none		Accès au courrier électronique	£
- ~	0/0B	IPv4 TCP	LAN_USER net	•	*	RemoteMGMT	*	none		Remote MGMT	€#©©
	0/0B	IPv4 TCP	LAN_USER net	•	*	File_Transfer	*	none		Transfert de fichiers	₽₽©0
~	1 /50 KiB	IPv4 TCP	LAN_USER net	*	192.168.0.0/27	445 (MS DS)	*	none		Partage de fichiers	€ø©©
Server /	Access										Î
	0/0 B	IPv4 TCP/UDP	LAN_USER net	•	192.168.0.0/27	53 (DNS)	*	none		Allow DNS Access	<b>₽</b> ₽₽00
	0/0B	IPv4 UDP	LAN_USER net	68	192.168.0.0/27	67	*	none		Allow DHCP Access	€#©©
Allow F	irewall Acces	is									Î
	0/08	IPv4 TCP	LAN_USER net	*	192.168.21.254	443 <mark>(H</mark> TTPS)	*	none		Mgmt Access to firewall	±≠00
Block F	irewall Acces	s									Ō
<b>×</b>	0/0B	IPv4 *		*	192.168.21.254	*	*	none		Block other IPv4 access to firewall	₽₽00
Die els A	mething Dula										m

Après configuration des règles sur le LAN\_USER

#### IV) Cahier de tests

L'ensemble des tests pour la mise en place de nouvelles règles seront réalisés sur les équipements terminaux.

- DNS : Vérifier la résolution de noms avec nslookup
- HTTP : Tester la connectivité à un site en http
- HTTPS : Tester la connectivité à un site en https
- HTTP PROXY : Faire un speedtest (qui utilise le port 8080)
- LDAP : Vérifier l'authentification avec un compte user et mot de passe
- Kerberos : Vérifier l'authentification avec un compte user et mot de passe
- SMB : Se connecter à un filer
- NTP : Vérifier l'heure système
- ICMP : Réaliser un ping
- RDP : Se connecter à un serveur avec « mstsc.exe »
- SSH : Se connecter à un serveur distant avec « PuTTY.exe »
- FTP : Tester un transfert de fichier FTP
- SFTP : Tester un transfert de fichier SFTP
- RPC : Tester VEEAM
- SMTP : Vérifier l'envoi de courriels via le protocole SMTP depuis un client de messagerie.
- IMAP : Vérifier l'envoi de courriels via le protocole SMTP depuis un client de messagerie.
- IMAPS : Vérifier la récupération de courriels via le protocole IMAPS depuis un client de messagerie.
- POP3 : Vérifier la récupération de courriels via le protocole IMAPS depuis un client de messagerie.
- POP3S : Vérifier l'envoi de courrier électronique chiffré via SMTPS depuis un client de messagerie.

Ce cahier de test donne la liste des tests à effectuer pour les divers protocoles de la matrice de flux et dans les différents sens indiqués par celle-ci.

La première règle bloquant tout, il est important de réaliser le cahier de test en même temps que la configuration des règles. (Troubleshooting)