

BTS SIO2

# TP-PFSENSE /NTOP/RDP

Nicolas Debut



→Redirection WAN vers le site Web

Accès du LAN vers WAN et DMZ

Accès à la configuration du pfsense

→ Accès de la DMZ vers Internet



**SHEMA** 



## Avant de démarrer votre pfSense pour la première fois, veillez à attribuer 3 interfaces réseau à votre machine. Pour une VM située sur Proxmox, voici comment procéder :

## Allez sur Proxmox, puis dans l'onglet Network. **Cliquez ensuite sur Create puis sélectionnez Linux Bridge.**

∠ ■ Datacenter		Graata	Devert Edit	20mous /	aply Configura	tion		
√ 🌄 proxmox3	O Search	Create V Revent Edit Remove Apply Conliguration						
103 (windows10-damien)		Name 个	Туре	Active	Autostart	VLAN a	F	
😱 104 (Zabbix-Maxime) 🔵	Summary	enet	Natwork Davias	Vee	No	Na		
<ul> <li>105 (wserver-damien)</li> <li>106 (Debian12)</li> <li>107 (pfsense-damien)</li> <li>108 (TEST-OMV-MAX)</li> </ul>	D Notes	enor	Network Device	tes	NO	NO		
	>_ Shell ✿✿ System   ▼	eno2	Network Device	No	No	No		
		eno3	Network Device	No	No	No		
		eno4	Network Device	No	No	No		
201 (wserver-nicolas)	≓ Network	ens1f0	Network Device	No	No	No		
🕞 202 (Pfsense) 🛑	Certificates	ens1f1	Network Device	No	No	No		
🕞 203 (w10-nicolas) 🔵	O DNS	vmbr0	Linux Bridge	Yes	Yes	No	e	
🛶 204 (Apache) 🛑	<b>U</b> bito	vmbr1	Linux Bridge	Yes	Yes	No		
🕞 205 (openmediavault) 🛑	Hosts	vmbr2	Linux Bridge	Yes	Yes	No		

Ports/Slaves	Bond Mode	CIDR	Gateway	Comment
eno1		192.168.20.203/24	192.168.20.254	

Virtual Machine 202 (I	Virtual Machine 202 (Pfsense) on node 'proxmox3' nicolas 🖋			Add: Network Device					
🛢 Summary	Add ~ Remove Edit	Disk Action 🗸 Revert			_				
>_ Console	🚥 Memory	1.00 GiB	Bridge:	vmbr0	<ul> <li>Model:</li> </ul>	VirtIO (paravirtualized)	$\sim$		
🖵 Hardware	Processors	1 (1 sockets, 1 cores) [x86-64-v2-AES]	VLAN Tag:	no VLAN	MAC address:	auto			
Cloud-Init	BIOS	Default (SeaBIOS)			×				
Options	🖵 Display	Default	Firewall:	$\checkmark$					
🔳 Task History	📽 Machine	Default (i440fx)					_		
Monitor	SCSI Controller	VirtIO SCSI single	Disconnect:		Rate limit (MB/s	: unlimited :	0		
⊂ ■ Backup	O CD/DVD Drive (ide2)	local:iso/pfSense-CE-2.7.2-RELEASE-amd64.iso,media=cdrom,size=854172K	MTH	1500 (1 – bridge MTLI)	^ Multiqueue:		~		
	🖨 Hard Disk (scsi0)	VM:vm-202-disk-0,iothread=1,size=20G	MITO.	1000 (1 = blidge MTO)	v Multiquede.		$\sim$		
to Replication		virtio=BC:24:11:91:9C:E9,bridge=vmbr0,firewall=1	_						
Snapshots		virtio=BC:24:11:50:CF:E4,bridge=vmbr1,firewall=1	A Help			Advanced 🖂 Add			
Firewall		virtio=BC:24:11:36:35:46,bridge=vmbr2,firewall=1	0.000						

- Rendez-vous dans l'onglet de votre pfSense, puis dans la catégorie Hardware.
- Cliquez sur Add, puis sur Network Device.
- Sélectionnez l'interface réseau que vous souhaitez, puis cliquez sur Add.
- Vous devriez ensuite voir l'interface que vous avez ajoutée.

➡ Network Device (net0)	virtio=BC:24:11:91:9C:E9,brid
➡ Network Device (net1)	virtio=BC:24:11:50:CF:E4,brid
➡ Network Device (net2)	virtio=BC:24:11:36:35:46,bridg

### dans la catégorie Hardware. ork Device. itez, puis cliquez sur Add. vous avez ajoutée.

ge=vmbr0,firewall=1

lge=vmbr1,firewall=1

e=vmbr2,firewall=1

Should VLANs be set up now [y n]? n	Démarrez ensuite votre VM afin de procéder à l'installat
If the names of the interfaces are not known, auto-detection c be used instead. To use auto-detection, please disconnect all interfaces before pressing 'a' to begin the process.	Une fois celle-ci terminée, associez la bonne interfacan réseau au bon réseau. (Local Database)
Enter the WAN interface name or 'a' for auto-detection (vtnet0 vtnet1 vtnet2 or a): vtnet0	FreeBSD/amd64 (pfSense.nicolasdebut.com) (ttyv0) KVM Guest – Netgate Device ID: 5f117e33bf87bcffc63e
Enter the LAN interface name or 'a' for auto-detection NOTE: this enables full Firewalling/NAT mode. (vtnet1 vtnet2 a or nothing if finished): vtnet1	<pre>* Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense *** WAN (wan) -&gt; vtnet0 -&gt; v4/DHCP4: 192.168.20.161/24 LAN (lan) -&gt; vtnet1 -&gt; v4: 192.168.1.1/24 DMZ (opt1) -&gt; vtnet2 -&gt; v4: 192.168.10.1/24</pre>
Optional interface 1 description found: DMZ Enter the Optional 1 interface name or 'a' for auto-detection (vtnet2 a or nothing if finished): vtnet2	0) Logout (SSH only)9) pfTop1) Assign Interfaces10) Filter Logs2) Set interface(s) IP address11) Restart webConfigurato3) Reset webConfigurator password12) PHP shell + pfSense to4) Reset to factory defaults13) Update from console5) Reboot system14) Enable Secure Shell (s
The interfaces will be assigned as follows:	6) Halt system 15) Restore recent configu 7) Ping host 16) Restart PHP-FPM 8) Shell
WAN -> vtnet0 LAN -> vtnet1 OPT1 -> vtnet2	Enter an option:
Do you want to proceed [yin]? y	

### allation. rface

2 🗖 pfSense - Login	× +								-	Ō	× (	Jn
← C ⊗ Non sécurisé   <del>https</del> ;	//192.168.1.1/index.php			аљ	A	☆	() (	`⊨ @	∞		🗸 🗘	
<b>pf</b> sens	e							Login	to pfSe	ense	a	IC
											A	.cc  '
		SIGN I	N									
		admin										
		•••••	$\bigcirc$									
		SIGN IN										
											!	!!
		<b>v</b>									b	as
											u	n
					Active Accédez	e <mark>r Win</mark> zaux pa	dows ramètres	pour activ		dows.		
	pfSense is dev	eloped and maintained by Netga	ate. © ESF 2004 - 20	024 View license.								
REC1918 Networ	ks											
Block RFC1918	🔽 Block priva	te networks from (	entering via	WAN								
Private Networks	When set, this	option blocks traf	fic from IP :	addresses	that a	are n	eserve	ed for	priva	ate n	etwor	ks :
	172.16/12, 19	2.168/16) as well a	as loopback	k addresse:	s (12	7/8)	This	optior	n sho	uld (	gener	ally
	WAN network	lies in such a priva	ate address	space, too.								

ne fois cela fait, créez une VM en veillant a connecter à l'interface réseau de votre LAN.

cédez ensuite à votre pfSense en entrant 'IP de votre LAN dans votre navigateur. Identifiant par défaut : admin Mot de passe par défaut : pfsense

## N'oubliez pas de vérifier votre configuration.

Ne pas oublier de désactiver l'option en s de la page 4/9 pour permettre d'utiliser réseau privé comme WAN si nécessaire.

s as per RFC 1918 (10/8, ly be left turned on, unless the

### Vous arriverez ensuite sur la page d'accueil de votre pfSense.

	pf	pfSense.nic	olasdebut.com - S	tatu: × +					
C		😣 Non se	écurisé   <del>http:</del>	<del>s</del> ://192.168.1.1					
	Se		System <del>-</del>	Interfaces 🗸	Firewall 🗸	Services -	VPN 🗸	Status 🕶	Diagnostics 🗸
1.000									

### Status / Dashboard

System Inform	nation 🥜 🗭 😒	Netgate Services And Sup
Name	pfSense.nicolasdebut.com	Contract type Comm
User	admin@192.168.1.100 (Local Database)	Comm
System	KVM Guest Netgate Device ID: <b>5f117e33bf87bcffc63e</b>	NETGATE AND pfSens
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 21:10:00 CET 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Wed Sep 25 8:12:36 CEST 2024 €	If you purchased your pfSense ga Community Support at the point hardware, you have access to val the NETGATE RESOURCE LIBR You also may upgrade to a Netga
СРИ Туре	QEMU Virtual CPU version 2.5+ AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No	Support subsorption. We're alway committed to delivering enterprise more than competitive when com
Hardware crypto	Inactive	Upgrade Your Support
Kernel PTI	Enabled	Netgate Global Support FAQ
MDS Mitigation	Inactive	Netgate Professional Services
Uptime	00 Hour 47 Minutes 47 Seconds	
Current date/time	Wed Sep 25 8:59:01 CEST 2024	If you decide to purchase a Ne MUST have your Netgate Dev



### e COMMUNITY SUPPORT RESOURCES

ateway firewall appliance from Netgate and elected t of sale or installed pfSense on your own rious community support resources. This includes RARY.

te Global Technical Assistance Center (TAC) ys on! Our team is staffed 24x7x365 and e-class, worldwide support at a price point that is pared to others in our space.

- Community Support Resources
- Official pfSense Training by Netgate
- es Visit Netgate.com

### Activer Windows

tgate Global TAC Support subscription, you rice ID (NDI) from your firewall in order to

### Un message s'affichera pour vous proposer de changer l'option DHCP. Il est conseillé de passer à la version Kea DHCP, car ISC DHCP n'est plus d'actualité.

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.

### System / Advanced / Networking

Admin Access	Firewall	& NAT	Networking	Miscellaneous	System Tunables	No			
DHCP Options									
Server Backend ISC D that i		• Kea	DHCP	○ ISC DHCP (Deprecated)					
		SC DHCP that includ	has reached end les the most-requ	ed end-of-life and will be removed from a future v st-requested features.					

tifications

Ignore Deprecation Warning

pfSense. Kea DHCP is the newer, modern DHCP distribu

Firewall / Rules / Edit

							man
Edit Firewall Rule							
Action	Pass		~				les
	Choose what to do with pack Hint: the difference between whereas with block the pack	kets that match the criteria specified be a block and reject is that with reject, a p ket is dropped silently. In either case, th	elow. acket (TCP RST or ICMF ae original packet is disc	port unreachable for UDP) is returne arded.	d to the sender,	Pour	les cr
Disabled	Disable this rule						
	Set this option to disable thi	s rule without removing it from the list.					Rul
Interface	LAN		~				
	Choose the interface from w	hich packets must come to match this	; rule.			lan	remi
Address Family	IPv4 Select the Internet Protocol	version this rule applies to.	~				
Protocol	Any Choose which IP protocol th	is rule should match.	~			d'acc	éder
Source							
Source	Invert match	LAN subnets	~	Source Address	VS / V		
				Arronov all arrows		Destination	
						Destination	Invert match
						Extra Options	
The firewall rule configurati The changes must be appli	on has been changed. ed for them to take effect.				Apply Changes	Log	Log packets that a Hint: the firewall has the Status: System Log
III Aprè	s chaqu	e règle sau	vegar	dée, clique	z sur	Description	
Apply	Changes	s. sinon les	règles	que vous	avez		A description may be log.
mi	sos on n	laco no for	action	oront nas	,	Advanced Options	Display Advanced

inises en place ne fonctionnel ont

nt: the firewall has li Status: System Lo description may be ( **Rule Information** Tracking ID 1726648791 Created 9/18/24 10:39:51 by ac 9/18/24 10:39:51 by a

🔒 Save

pas.

### **Il est maintenant temps de configurer** les règles dans pfSense. es créer, allez dans Firewall, puis Rules, et cliquez sur Add. emière règle permettra au LAN der au web via le WAN (ici, notre

réseau de la salle).

	Any	~	Destination Address	/ ~
e handle	d by this rule			
nited loc js: Settin	cal log space. Don't turn on logging for everything. If do igs page).	oing a lo	t of logging, consider using a rem	note syslog server (see
ntered h	ere for administrative reference. A maximum of 52 ch	aracters	will be used in the ruleset and dis	splayed in the firewall
min@19	92.168.1.100 (Local Database)			
lmin@19	92.168.1.100 (Local Database)			

Activer Windows

Firewall / Rules / Edit

### 🗮 📖 🗐 🔞

Edit Firewall Rule								
Action	Pass Choose what to do with packets that match the criteria specified below Hint: the difference between block and reject is that with reject, a pack whereas with block the packet is dropped silently. In either case, the or	• w. tet (TCP RST or ICMP p riginal packet is discar	port unreachable for UDP) is returned to the sender, rded.					
Disabled	Disable this rule Set this option to disable this rule without removing it from the list.			Cette	règle	autorise	les flux	sortants
Interface	DMZ Choose the interface from which packets must come to match this rule	<b>∨</b> e.			•	de la D	MZ.	
Address Family	IPv4 Select the Internet Protocol version this rule applies to.	~						
Protocol	Any Choose which IP protocol this rule should match.	•						
Source								
Source	DMZ subnets	~	Source Address iver Windows / ~	<				
				Destination				
				Destination	Invert match	Any	✓ Destination	Address / V
				Extra Options				
				Log	Log packets that are hand Hint: the firewall has limited the Status: System Logs: Set	<b>dled by this rule</b> local log space. Don't turn on logging for e <mark>ttings</mark> page).	verything. If doing a lot of logging, c	onsider using a remote syslog server (see
				Description	A description may be entered log.	d here for administrative reference. A maxi	mum of 52 characters will be used i	n the ruleset and displayed in the firewall
				Advanced Options	Display Advanced			
				Rule Information				
				Tracking ID	1726650335			
				Created	9/18/24 11:05:35 by admin@	0192.168.1.100 (Local Database)		
				Updated	9/18/24 11:05:35 by admin@	ງ192.168.1.100 (Local Database)		
					Save			

estination						
Destination	Invert match	Any	~	Destination Address	/ ~	
					-	
xtra Options						
Log	<ul> <li>Log packets that are handle</li> </ul>	ed by this rule				
	Hint: the firewall has limited lo	cal log space. Don't turn on logging for everythi	ng. If doing a l	ot of logging, consider using a ren	note syslog server (see	
	the Status: System Logs: Settin	ngs page).				
Description						
	A description may be entered h	nere for administrative reference. A maximum o	f 52 character	s will be used in the ruleset and d	isplayed in the firewall	
	log.					
Advanced Options	Display Advanced					
ule Information						
Tracking ID	1726650335					
Created	9/18/24 11:05:35 by admin@192.168.1.100 (Local Database)					
Updated	9/18/24 11:05:35 by admin@192.168.1.100 (Local Database)					
	D Sava					
	Jave					

### Firewall / NAT / Port Forward / Edit

Edit Redirect Entry						dans Fi	irewa
Disabled	Disable this rule						
No RDR (NOT)	Disable redirection for tra This option is rarely needed.	affic matching this rule Don't use this without thor	ough knowledge of the implication	s.		F	orwa
Interface	WAN Choose which interface this	rule applies to. In most cas	✓ ses "WAN" is specified.			Cette re	edire
Address Family	IPv4 Select the Internet Protocol version this rule applies to.						e se o
Protocol	TCP  Choose which protocol this rule should match. In most cases "TCP" is specified.					imméo	diate
Source	Display Advanced						
Destination	Invert match.	WAN address Type	~	Address/m	nask /	Destination port range	HTTP From port
Destination port range	HTTP  V From port	Custom	HTTP V To port	Custom	Activer Windows Accédez aux paramètres pour activer W	ind: Redirect target ID	Specify the port o
	Specify the port or port range	e for the destination of the	nacket for this manning. The 'to' fi	ld may be left (	empty if only mapping a single port	Redirect target iP	

0

		VVV	<b>EN.</b>	
Destination port range	HTTP 🗸		HTTP	✓
	From port	Custom	To port	Custom
	Specify the port or port range	for the destination of the pac	ket for this mapping. Tl	'he 'to' field may be left empty if only mapping a single port.
		Address or Alice		102 169 10 21
Redirect target IP		Type		Address
	Enter the internal IP address o In case of IPv6 addresses, in n i.e. it is not possible to redirect	f the server on which to map nust be from the same "scop t from link-local addresses s	the ports. e.g.: 192.168 e", cope (fe80:*) to local so	8.1.12 for IPv4 cope (::1)
Redirect target port	HTTP		~	
	Port		Cus	stom
	Specify the port on the machin calculated automatically). This is usually identical to the	ne with the IP address entere "From port" above.	d above. In case of a po	ort range, specify the beginning port of the range (the end port will be
Description				
	A description may be entered l	here for administrative refere	nce (not parsed).	
No XMLRPC Sync	Do not autominically sync t	to other CARP members	a to other CAPP memb	pars. This does NOT prevent the rule from being overwritten on Slave
	This prevents the fulle of Mast	ter norn automatically synch	ig to other oAttr memo	sers. This does not prevent the rule non-being overwritten on slave.
NAT reflection	Use system default		~	
entre de la companya de la comp				
Filter rule association	Rule NAT		~	
	View the filter rule			Activer Windows
Rule Information				Accédez aux paramètres pour activer Wind
Orested	0/10/01 11:50:17 hu admin@1	02 160 1 100 (Local Databa	20)	

### Pour les redirections de port, rendez-vous lans Firewall, puis NAT, et sélectionnez Port Forward. Cliquez ensuite sur Add. ette redirection fera en sorte que, si le WAN ente de se connecter à votre pfSense, il sera immédiatement redirigé vers votre serveur

### 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 processing Outbound NAT rules</li> <li>In most cases this option is not required.</li> </ul>	
Interface	DMZ  The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.	Ici vous
Address Family	■ IPv4 Select the Internet Protocol version this rule applies to.	
Protocol	Any Choose which protocol this rule should match. In most cases "any" is specified.	
Source	DMZ subnets     /     24     Port or Range       Type     Source network for the outbound NAT mapping.     Port or Range	
Destination	WAN subnets     /     24     Port or Range       Type     Destination network for the outbound NAT mapping.     Port or Range	
	Not Not Activer Windows Accédez aux paramètres pour activer Win Nerrt the sense of the destination match.	d Translation Address WAN addr

0

Translation		
Address	WAN address	
	Туре	
	Connections matching this rule will be mapped to the specified address. If specifying a custom network or ali	as, it must be routed to the firewall.
Port or Range	Static Port	
	Enter the external source <b>Port or Range</b> used for remapping the original source port on connections matching the rule.	
	Port ranges are a low port and high port number separated by ":". Leave blank when <b>Static Port</b> is checked.	
Misc		
No XMLRPC Sync	Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule of	rule from being overwritten on Slave.
Description		
	A description may be entered here for administrative reference (not parsed).	
Dula tafana atian		
Rule Information		
Created	9/18/24 10:57:55 by admin@192.168.1.100 (Local Database)	
Updated	9/18/24 10:57:55 by admin@192.168.1.100 (Local Database) Ac	ctiver Windows cédez aux paramètres pour activer Window
	R Save	

### trouvez la règle permettant à Z d'accéder à Internet via le WAN.

### Si, depuis votre WAN, vous entrez l'IP de votre pfSense dans votre navigateur, vous serez redirigé vers votre serveur web situé dans votre DMZ.

2.168.20.161

# NTOP

NTOP est un outil très utile si vous souhaitez superviser l'activité qui se déroule sur votre pfSense, il est inclus dans celui-ci il vous suffit juste de mettre un plugin. Pour l'installer, vous devrez vous rendre dans l'onglet System, puis Package Manager. Cliquez sur Available Packages, recherchez ntop et installez-le.

Syst	System / Package Manager / Available Packages				
Install	ed Packages	Available Packages			
Searc	:h				
Searc	h term	ntop Both			
		Enter a search string or *nix regular expression to search package names and descriptions.			
Packa	ages				
Name	Version	Description			
ntopng	0.8.13_10	ntopng (replaces ntop) is a network probe that shows network usage in a way similar to what top does for displays the network status on the user's terminal. In Web mo∯e it acts as a Web server, creating an HTML NetFlow/sFlow emitter/collector, an HTTP-based client interface for creating ntop-centric monitoring appli traffic statistics.			
		Package Dependencies: webfonts-0.30_14 ntopng-5.6.d20230920,1 libmaxminddb-1.7.1_1 graphviz-8.1.0_1			



### Confirmez l'installation, puis patientez pendant que celle-ci s'effectue.

System / Package Manager / Package Installer
Installed Packages Available Packages Package Installer
Confirmation Required to install package pfSense-pkg-ntopng.
Please wait while the installation of <b>pfSense-pkg-ntopng</b> completes. This may take several minutes. Do not leave or refresh the page!
Installed Packages Available Packages Package Installer
Package Installation
<pre>openpgm: 5.2.122_6 [pfSense] pfSense-pkg-ntopng: 0.8.13_10 [pfSense] png: 1.6.40 [pfSense] psutils: 1.17_5 [pfSense] redis: 7.2.1 [pfSense] tiff: 4.4.0_2 [pfSense] uchardet: 0.0.8 [pfSense] webfonts: 0.30_14 [pfSense] webp: 1.3.2 [pfSense]</pre>
Number of packages to be installed: 38
The process will require 212 MiB more space. 26 MiB to be downloaded. [1/38] Fetching ntopng-5.6.d20230920,1.pkg:



## Une fois installé, allez dans Diagnostics, puis dans ntopng Settings, activez le service et indiquez l'interface à surveiller.

Status 🕶	Diagnostics 🗸	Help 🕇
	ARP Table	_
	Authentication	
	Backup & Restore	
	Command Prompt	t
_	DNS Lookup	_
	Edit File	
	Factory Defaults	
	Halt System	
	Limiter Info	
	NDP Table	
	ntopng	
	ntopng Settings	
	Packet Capture	
	pfInfo	
	pfTop	
	Ping	
	Reboot	
	Routes	
	S.M.A.R.T. Status	Active
	Sockets	Accéde
	States	

moping comingo, intoping comingo ck this to enable ntopng. ntopng settings, graphs and traffic data. disabled, all settings and data will be wiped on package uninstall/ e password for the ntopng GUI. Minimum 5 characters. 6  $\mathbf{T}$ de DNS responses and resolve local numeric IPs only (default) 🔻 res how name resolution is handled. an now be disabled via the ntopng GUI. der all RFC1918 networks local  $\sim$ res how Local Networks are defined. Default: Consider all RFC1918



P Taper ici pour rechercher

nterfac

-

Setting

</>>

۲ Help

### **Cliquez ensuite sur Access ntopng pour** accéder au service ; indiquez votre identifiant et votre mot de passe, et voilà, votre service est installé.



# RDP

# Nous allons maintenant voir comment activer le protocole RDP afin d'accéder à vos appareils à distance. Nous prendrons ici l'exemple d'un Windows Server 2019.

PROPRIÉTÉS Pour WIN-89JMUDSUHOI	Propriétés système	×	CHES		
Nom de l'ordinateur WIN-89JMUD Groupe de travail WORKGROUP	Nom de l'ordinateur     Matériel       Paramètres système avancés     Utilisation à distance		:		
Pare-feu Windows Defender Privé : Actif Gestion à distance Désactivé Bureau à distance Désactivé Association de cartes réseau Désactivé	Autoriser les connexions d'assistance à distance vers cet ordinateur <u>Que se passe-t-il lorsque j'active l'Assistance à</u> <u>distance ?</u> Options avancées		e d'Inte	Comme	nc
Ethernet Adresse IPv4 a	Bureau à distance Choisissez une option, puis spécifiez qui peut se connecter.			de serve	eur
Version du système d'exploitation Microsoft Win Informations sur le matériel BOCHS_BXPC	<ul> <li>Ne pas autoriser les connexions à distance à cet ordinateur</li> <li>Autoriser les connexions à distance à cet ordinateur</li> <li>N'autoriser que la connexion des ordinateurs exécutant le Bureau à distance avec authentification NLA (recommandé)</li> </ul>				
ÉVÉNEMENTS Tous les événements   13 au total	Comment choisir ? Sélectionnez des utilisateurs OK Annuler Appliq	uer	CHES		

### ez depuis votre gestionnaire r en activant l'option Bureau à distance.



Découvrir comment autoriser les de votre réseau local

Port du Bureau à distan

Port actuel du Bureau à distance Découvrir comment modifier le p

### Allez ensuite dans vos paramètres avancés de Bureau à distance pour vérifier, dans un premier temps, s'il est actif, puis le port qui est utilisé (par défaut, le 3389).

	_	×
vancés		
ateurs utilisent l'authentification au onnecter (recommandé)		
ns uniquement avec authentification au		
connexion à distance depuis l'extérieur		
$\searrow$		
nce		
3389 port d'écoute pour le Bureau à distance		

No RDR (NOT)	<ul> <li>Disable redirection for traf</li> <li>This option is rarely needed.</li> </ul>	fic matching this rule Don't use this without thorough k	nowledge of the implication	ns.	
Interface	WAN Choose which interface this r	ule applies to. In most cases "W			
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	Cisplay Advanced				
Destination	Invert match.	WAN address Type	~	Address/mask	
Destination port range	Other From port Specify the port or port range	500 Custom for the destination of the packe	Other To port t for this mapping. The 'to' f	500 Custom ield may be left empty if only mapping a single port.	
Redirect target IP	Enter the internal IP address of IPv6 addresses, in i.e. it is not possible to redired	Address or Alias Type of the server on which to map th must be from the same "scope", ct from link-local addresses scop	✓ ✓ e ports. e.g.: 192.168.1.12 f De (fe80:*) to local scope (::	192.168.10.2 Address for IPv4 1) Activer Windows	
Redirect target port	MS RDP		~	Accédez aux paramètres pour activer Winc	
	Port		Custom		

### Allez ensuite dans votre pfSense afin de configurer une nouvelle redirection de port pour permettre au WAN d'accéder à distance au Windows Server. Pour des raisons de sécurité, j'ai modifié le port de connexion à 500.

	i.e. it is not possible
Redirect target port	MS RDP
	Port
	Specify the port on t
	calculated automation This is usually identi
	This is usually lucitu
Description	accès RDP serveur
	A description may be
No XMLRPC Sync	Do not automatic
	This prevents the rul
NAT reflection	Use system defaul
Filter rule association	Dula NAT accès DD
The full association	Niew the filter rule
	view the filter rule
le Information	
Created	9/25/24 10:51:13 by
Updated	9/25/24 10:51:13 by
	_
	Save

redirect from link-local addresses scope (fe80:*) to local scope (::1)
♥
Custom
e machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be illy). al to the "From port" above.
entered here for administrative reference (not parsed).
Ily sync to other CARP members or Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
~
e serveur srv-nicolas 🗸
dmin@192.168.1.100 (Local Database)
dmin@192.168.1.100 (Local Database)

### Voici ce qui devrait s'afficher ensuite. Attention : n'oubliez pas d'appliquer vos changements.

Firewall / NAT / Port Forward

Th Mo	The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.											
		3										
Port Forward 1:1 Outbound NPt												
Rı	Rules											
$\Box$			Interface	Protocol	Source A	ddress	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT F	
	~	*	WAN	TCP	*		*	WAN address	3389 (MS RDP)	192.168.10.2	3389	
	~	*	WAN	TCP	*		*	WAN address	80 (HTTP)	192.168.10.31	80 (H	

		0
		×
orts	Description	Actions
(MS RDP)	accès RDP serveur srv-nicolas	Ø0
ITTP)		Ø0

### Essayons maintenant de nous connecter depuis notre WAN (j'utilise personnellement Vinagre, mais tout outil permettant la connexion RDP est utilisable).

Visionneur de bureaux distants — 🗆 😣		fa maa daa		<b></b>	
Distant Affichage Signets Aide		Se connecter	و		
差 Se connecter 🔹 🗐	Choisissez Protocole	un bureau distant auquel se connecter e : RDP	ows	V	isionneur de bureaux distants 🛛 🛛 🔊
	Hôte :	Hôte : 192.168.20.161:500		Une authentificatio	on RDP est requise
	Options de	Options de connexion		Hôte :	192.168.20.161
	🗌 Plein é	écran		Nom d'utilisateur	Administrateur
	Options RD	Options RDP		Mat de annue i	
	Mise à	à l'échelle		Mot de passe :	
	Nom d'uti	tilisateur : Administrateur		Domaine :	
	Domaine :				Se souvenir de l'information d'identification
	Largeur :	800 — +			
	Hauteur :	600 - +			S'authentifier
		🗃 Aide 🛛 🕄 Annuler	Se connecter		

### Indiquez ensuite l'IP de votre pfSense avec le port que vous avez configuré, puis spécifiez l'utilisateur avec lequel vous souhaitez vous connecter.

### Vous êtes maintenant connecté à distance à votre Windows Server.



