PRÉSENTÉ PAR DRUELLE NICOLAS

TP-PFSENSE

CAHIER DES CHARGES

-Mise en place du Pfsense -Configuration des interfaces (WAN,LAN,DMZ) -Configuration des règles -Configuration du portforward Autorisation du WAN et du LAN d'accès au serveur sur la DMZ

-Mise en place du serveur web -Configuration du serveur dans la DMZ

-Réalisation des tests -Test LAN vers WAN et DMZ -Test WAN vers LAN et DMZ -Test DMZ vers LAN et WAN



TOPOLOGIE





ADRESSAGE IP

Nom	Adresse IP
PFSENSE (LAN)	192.168.202.20
PFSENSE (WAN)	192.168.20.86
PFSENSE (DMZ)	192.168.22.1
Serveur LAMP	192.168.22.2
Poste client LAN	192.168.202.11



MISE EN PLACE DU PFSENSE



INSTALLATION PFSENSE

	Add V Remove Edit [Disk Action V Revert
	Memory	2.00 GiB
۲	Processors	1 (1 sockets, 1 cores) [x86-64-v2-AES]
	BIOS	Default (SeaBIOS)
Ţ	Display	Default
¢,	Machine	Default (i440fx)
8	SCSI Controller	VirtIO SCSI single
0	CD/DVD Drive (ide2)	local:iso/pfSense-CE-2.5.2-RELEASE-amd64.iso,media=cdrom,size=636498K
a	Hard Disk (scsi0)	local-lvm:vm-204-disk-0,iothread=1,size=10G
₽	Network Device (net0)	virtio=BC:24:11:54:4A:21,bridge=vmbr0,firewall=1
Ħ	Network Device (net1)	virtio=BC:24:11:71:D3:9C,bridge=vmbr0,firewall=1
1	Network Device (net2)	virtio=BC:24:11:5D:DA:6D,bridge=vmbr0,firewall=1

Dans un premier temps je vais installer PFSENSE sur le Proxmox en ajoutant 2 interfaces réseau supplémentaire



INSTALLATION PFSENSE

Install	Install pfSense
Rescue Shell	Launch a shell for rescue operations
Recover config.xml	Recover config.xml from a previous install



ZFS Con	figuration
Configure Options:	Proceed with Installation
>>> Install	stripe: 0 disks
T Pool Type/Disks:	*
- Rescan Devices	*
- Disk Info	pfSense
N Pool Name	YES
4 Force 4K Sectors?	NO
E Encrypt Disks?	GPT (BIOS)
P Partition Scheme	2g
S Swap Size	NO
M Mirror Swap?	NO
W Encrypt Swap?	NO
<mark>⟨S</mark> elect≻	<cancel></cancel>



Une fois les interfaces ajouter je démarre la VM et procède à l'installation

INSTALLATION PFSENSE

stripe	Stripe - No Redundancy Minnon - n-Way Minnoning
raid10	RAID $1+0 - n \times 2-Wau$ Mirrors
raidz1	RAID-Z1 - Single Redundant RA
r aidz2	RAID-Z2 - Double Redundant RA
r aidz3	RAID-Z3 - Triple Redundant RA
L	
	<pre>< DK > <cancel></cancel></pre>









(Local Database)

reeBSD/amd64 (pfSensenicolas.home.arpa) (ttyv0)

KVM Guest - Netgate Device ID: 38df5bb6885c0c08f512

Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSensenicolas ***

-> v4/DHCP4: 192.168.20.86/24 \rightarrow utnet0 WAN (wan) LAN (lan) -> v4: 192.168.202.20/24 -> vtnet1 -> vtnet2 -> v4: 192.168.22.1/24 OPT1 (opt1) 9) pfTop 10) Filter Logs 0) Logout (SSH only) 1) Assign Interfaces Set interface(s) IP address 11) Restart webConfigurator
 12) PHP shell + pfSense tools 3) Reset webConfigurator password 4) Reset to factory defaults 13) Update from console 14) Enable Secure Shell (sshd) 5) Reboot system 15) Restore recent configuration 6) Halt system 7) Ping host 8) Shell 16) Restart PHP-FPM

Enter an option: 1

Valid interfaces are:

vtnet0 bc:24:11:54:4a:21 (up) VirtIO Networking Adapter vtnet1 bc:24:11:71:d3:9c (up) VirtIO Networking Adapter vtnet2 bc:24:11:5d:da:6d (up) VirtIO Networking Adapter

Do VLANs need to be set up first? ? ULANs will not be used, or only for optional interfaces, it is typical to ay no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [yin]? n

If the names of the interfaces are not known, auto-detection can be used instead. To use auto-detection, please disconnect all interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection (vtnet0 vtnet1 vtnet2 or a): vtnet0

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

Optional interface 1 description found: OPT1 Enter the Optional 1 interface name or 'a' for auto-detection (vtnet2 a or nothing if finished): vtnet2

The interfaces will be assigned as follows:

WAN -> vtnet0 LAN -> vtnet1 OPT1 -> vtnet2

Do you want to proceed [yin]? y

Une fois l'installation fini j'assigne le LAN, WAN et la DMZ à une interface créer précédemment avec l'option "1"



WAN	(wan)	->	vtnet0	->	v4/DHCP4: 192.168.20.86/24
LAN	(lan)	->	vtnet1	\rightarrow	v4: 192.168.202.20/24
OPT1	(opt1)	\rightarrow	vtnet2	\rightarrow	v4: 192.168.22.1/24



Ensuite avec l'option "2" je donne une ip en suivant le tableau d'adressage en page 4 sur chacune des interfaces

8 Non sécurisé	https://192.168.202.20/wizard.php?xml=setup_wizard.xml
sense Sustan	n v Interfaces v Firewall v Services v VPN v Status v Diagnostics v Haln v Partice v Partices v Haln v Partices v
ARNING: The 'admin' ac	count password is set to the default value. Change the password in the User Manager.
Vizard / pfSens	e Setup / O
fSense Setup	
	Welcome to pfSense® software!
	This wizard will provide guidance through the initial configuration of pfSense.
	The wizard may be stopped at any time by clicking the logo image at the top of the screen.
	>> Next
Step 2 of 9	
eneral Information	
	On this screen the general pfSense parameters will be set.
Hostname	pfSenseNicolas
	EXAMPLE: myserver
Domain	home.arpa
	EAAMPLE: mydomain.com
	manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.
Primary DNS Server	
Secondary DNS Server	
Override DNS	
overnae bits	Allow DNS servers to be overridden by DHCP/PPP on WAN
	>> Next
ard / pfSense	Setup / Time Server Information
Step 3	3 of 9
e Server Informati	ion
	Please enter the time, date and time zone.
ne server hostname	2 pfsense pool ato ora
	Enter the hostname (FQDN) of the time server.
Timezone	Europe/Paris v

Une fois les adresses ip mise sur les interfaces avec le poste client LAN je me connecte au site du PFSENSE afin de commencer la configuration

Dans un premier temps je renseigne les configurations de base comme le nom de l'hôte et la plage horaire



PPTP Remote IP Address	
PPTP Dial on demand	Enable Dial-On-Demand mode
	This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
PPTP Idle timeout	
	If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.
RFC1918 Networks	
Block RFC1918 Private Networks	Block private networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.
Block bogon network	s
Block bogon networks	Block non-Internet routed networks from entering via WAN
	When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.
	» Next

zard / prSense Setup / Configure LAN Interface		•
	Step 5 of 9	
igure LAN Interf	ace	
	On this screen the Local Area Network information will be configured.	
LAN IP Address	192.168.202.20	
	Type dhcp if this interface uses DHCP to obtain its IP address.	
Subnet Meek	24	

Ensuite on passe la configuration des interface. Sur l'interface WAN on décoche "block rfc1918 private networks" afin d'avoir une ip privée sur celle-ci

Après l'interface WAN, c'est au tour de l'interface LAN on vérifie donc si l'ip mise précédemment est bien la bonne



	Step 6 of 9	
et Admin WebGUI Pa	assword	
	On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enable	ed.
Admin Password	[]	
dmin Password AGAIN	Image: Constraint of the second sec	

Une fois cela fait je peux accéder à la page d'accueil du serveur





Enfin la dernière configuration est le changement du mot de passe par défaut car il ne faut jamais laissé le mot de passe de base sur un serveur

bard	+ 0
۶ <i>۲</i> ۵ ۵	Netgate Services And Support 🗢 😒
pfSensenicolas.home.arpa	Contract type Community Support
admin@192.168.202.11 (Local Database)	Community Support Only
KVM Guest Netgate Device ID: 38df5bb6885c0c08f512	NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
2.5.2-RELEASE (amd64) built on Fri Jul 02 15.33:00 EDT 2021 FreeBSD 12.2-STABLE Obtaining update status 🌣	If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBERRY.
QEMU Virtual CPU version 2.5+ AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No	You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
Enabled	Upgrade Your Support Community Support Resources
Inactive	Netgate Global Support FAQ Official pfSense Training by Netgate
23 Hours 29 Minutes 12 Seconds	Netgate Professional Services Visit Netgate.com
Sat Sep 28 17:43:48 CEST 2024	Activer Windows
 127.0.0.1 185.156.80.7 	If you decide to purchase a Netgate Global TAC Support Subscription, you were Windows. MUST have your Netgate Device ID (NDI) from your frewall in order to

EXPLICATION RÈGLE

ACTION: PASS (AUTORISER), BLOCK (BLOQUER SANS RETOUR), OU REJECT (BLOQUER AVEC NOTIFICATION). **INTERFACE:** SUR QUELLE INTERFACE LA RÈGLE S'APPLIQUE : LAN, WAN, DMZ, ETC. **PROTOCOL**: TYPE DE PROTOCOLE FILTRÉ : TCP, UDP, ICMP (PING), OU ANY (TOUS LES PROTOCOLES). **SOURCE**: ORIGINE DU TRAFIC : ANY (TOUT), SINGLE HOST OR ALIAS (ADRESSE IP UNIQUE), OU NETWORK (UN SOUS-RÉSEAU). **DESTINATION:** DESTINATION DU TRAFIC, AVEC LES MÊMES OPTIONS QUE POUR LA SOURCE. **PORTS**: SOURCE PORT ET DESTINATION PORT : PLAGES DE PORTS SPÉCIFIQUES À FILTRER (EX.: 80 POUR HTTP, 443 POUR HTTPS). **DESCRIPTION:** CHAMP POUR NOMMER LA RÈGLE POUR MIEUX L'IDENTIFIER.



CONFIGURATION RÈGLE LAN

dit 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 packet (TCP RST or ICMP port unreachable for U whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	Disable this rule
	Set this option to disable this rule without removing it from the list.
Associated filter rule	This is associated with a NAT rule. Editing the interface, protocol, source, or destination of associated filter rules is not permitted. View the NAT rule
Interface	LAN
	Choose the interface from which packets must come to match this rule.
Address Family	IPv4 V
	Select the Internet Protocol version this rule applies to.
Protocol	TCP
	Choose which IP protocol this rule should match.

	Source				
	Source	Invert match	any	~	Source Address
		Display Advanced The Source Port Range for a co its default value, any.	onnection is typically random a	and almost never equal to the d	estination port. In most
	Destination				
	Destination	Invert match	Single host or alias	~	192.168.22.2
	Destination Port Range	HTTP (80) ¥	Custom	HTTP (80) 🗸	Custom
•		Specify the destination port or	port range for this rule. The "To	o" field may be left empty if only	r filtering a single port.
	Extra Options				
	Log	Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If d the Status: System Logs: Settings page).			
	Description NAT A description may be entered here for administrative reference. A maximum of 52 characters will be used in log.				s will be used in the rule



JDP) is returned to the sender,



CONFIGURATION RÈGLE WAN

Edit Firewall Kule 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, apacket (TCP RST or ICMP p whereas with block the packet is dropped silently. In either case, the original packet is discan Disabled Disable this rule Set this option to disable this rule without removing it from the list. Interface WAN Choose the interface from which packets must come to match this rule. Address Family IPv4 Set this option to disable this rule applies to. Protocol TCP Choose which IP protocol this rule should match. Source Invert match Source Invert match Source Invert match Bestination Invert match Bestination Invert match Single host or alias Interface From Custom To Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Interface for administrative reference. A maximum of 52 characters log. Description A description may be entered here for administrative reference. A maximum of 52 characters log. </th <th></th>	
Action Pasa Choose what to do with packets that match the oriteria specified below. Hint: the difference between block and reject is that with reject, a packet (TGP RST or ICMP p Whereas with block the packet is dropped silently. In either case, the original packet is discar Disabled Disable this rule Set this option to disable this rule without removing it from the list. Interface WAN Choose which the interface from which packets must come to match this rule. Address Family IPv4 Select the Internet Protocol version this rule applies to. Protocol TCP Choose which IP protocol this rule should match. Source Invert match any Invert match Destination Invert match Destination Invert match Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Log Log Log packets that are handled by this rule Hint: the freewall has limited local log space. Don't turn on logging for everything. If doing a log the Status: System Logs: Settings page).	
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP p whereas with block the packet is dropped silently. In either case, the original packet is discare Disabled Disable this rule Set this option to disable this rule without removing it from the list. Interface WAN Choose the interface from which packets must come to match this rule. Address Family IP4 Select the Internet Protocol version this rule applies to. Protocol TCP Choose which IP protocol this rule ehould match. Ource Source Invert match any Destination Destination Invert match Single host or alias HTTP (80) From Custom To Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Log Log packets that are handled by this rule Hint: the frewall has limited local log space. Don't turn on logging for everything. If doing a log the Status: System Logs: Settings page).	
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP p whereas with block the packet is diopped allently. In either case, the original packet is discard by the packet is option to disable this rule Disabled Disable this rule Set this option to disable this rule without removing it from the list. Interface WAN Choose the interface from which packets must come to match this rule. Address Family IPv4 Select the Internet Protocol version this rule applies to. Protocol TCP Choose which IP protocol this rule should match. Ource Choose which IP protocol this rule should match. Ource Invert match any Source Invert match any Destination Invert match single host or alias Destination Invert matc	
whereas with block the packet is dropped silently. In either case, the orginal packet is discard Disabled Disable this rule Set this option to disable this rule without removing it from the list. Interface WAN WAN • Choose the interface from which packets must come to match this rule. Address Family IPv4 Select the Internet Protocol version this rule applies to. Protocol TCP Choose which IP protocol this rule should match. Purce Source Invert match any Destination Destination Invert match Single host or alias V Destination Invert match Single	ort unreachable fo
Disabled Disable this rule Set this option to disable this rule without removing it from the list. Interface WAN Choose the interface from which packets must come to match this rule. Address Family IPv4 Select the Internet Protocol version this rule applies to. Protocol TCP Choose which IP protocol this rule should match. Urce Choose Port Range for a connection is typically random and almost never equal to the de its default value, any. Destination Invert match Invert match <li< td=""><td>led.</td></li<>	led.
Set this option to disable this rule without removing it from the list. Interface WAN Choose the interface from which packets must come to match this rule. Address Family IPv4 Select the Internet Protocol version this rule applies to. Protocol TOP Choose which IP protocol this rule should match. urce Source Invert match Invert match any Statistion Invert match Single host or alias To Postination Invert match Single host or alias To From Custom To Specify the destination port or port range for this rule. The 'To' field may be left empty if only Extra Options Log Log Log packets that are handled by this rule Hint: the freewall has limited local log space. Don't turn on logging for everything. If doing a log the Status' System Logs' Settings page). Description A description may be entered here for administrative reference. A maximum of 52 characters log.	
Interface WAN ▼ Choose the interface from which packets must come to match this rule. Address Family IPv4 Address Family IPv4 ▼ Select the Internet Protocol version this rule applies to. ▼ Protocol TCP ▼ Choose which IP protocol this rule should match. ▼ Urce ▼ Choose which IP protocol this rule should match. Urce ▼ Invert match any Postination Invert match any ▼ Destination Invert match Single host or alias ▼ Destination Port Range HTTP (80) ▼	
Interface WAN Choose the interface from which packets must come to match this rule. Address Family IPv4 Select the Internet Protocol version this rule applies to. Protocol TCP Choose which IP protocol this rule should match. urce Choose which IP protocol this rule should match. Urce Invert match any Integrave for a connection is typically random and almost never equal to the de its default value, any. Destination Invert match Single host or alias From Custom To Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Log Log packets that are handled b	
Choose the interface from which packets must come to match this rule. Address Family IPv4 Select the Internet Protocol version this rule applies to. Protocol TCP Choose which IP protocol this rule should match. Urce Source Invert match any Comparing for a connection is typically random and almost never equal to the de its default value, any. Destination Destination Invert match Single host or alias From Custom To Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Log Log Description Adscription may be entered here for administrative reference. A maximum of 52 characteres log.	
Address Family IPv4 Select the Internet Protocol version this rule applies to. Protocol TCP Choose which IP protocol this rule should match. urce Source Invert match any Display Advanced The Source Port Range for a connection is typically random and almost never equal to the derits default value, any. Destination Invert match Single host or alias Destination <td></td>	
Select the Internet Protocol version this rule applies to. Protocol TCP Choose which IP protocol this rule should match. urce Source Invert match any Chopse Port Range for a connection is typically random and almost never equal to the de its default value, any. Destination Invert match Single host or alias Destination Port Range HTTP (80) From Custom Cog Log packets that are handled by this rule. Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot the Status: System Loge: Settings page). Description	
Protocol TCP Choose which IP protocol this rule should match. urce Source Invert match any Display Advanced The Source Port Range for a connection is typically random and almost never equal to the de its default value, any. Destination Invert match Single host or alias Descriptions Extra Options HTTP (80) Log Log packets that are handled by this rule Hint: the firewall has limited local log s	
Protocol TCP ▼ Choose which IP protocol this rule should match. urce Source Invert match any ▼ Source Invert match any ▼ Display Advanced The Source Port Range for a connection is typically random and almost never equal to the de its default value, any. Destination Invert match Single host or alias ▼ From Custom T	
Choose which IP protocol this rule should match.	
Source Invert match any Display Advanced The Source Port Range for a connection is typically random and almost never equal to the derits default value, any. Destination Destination Invert match Single host or alias Prom Custom To Destination Invert match Single host or alias Prom Custom To Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Iog Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot the Status: System Loge: Settings page). Description A description may be entered here for administrative reference. A maximum of 52 characters log.	
Source Invert match any Invert match any Image Source Display Advanced The Source Port Range for a connection is typically random and almost never equal to the device of the source Port Range for a connection is typically random and almost never equal to the device of the source Port Range for a connection is typically random and almost never equal to the device of the source Port Range Destination Invert match Single host or alias Image of the source Port Range of the source Port Range of the source Port Range of the source of the	
Source Invert match any Display Advanced The Source Port Range for a connection is typically random and almost never equal to the de its default value, any. Destination Invert match Single host or alias Destination Invert match Single host or alias Destination Port Range HTTP (80) From Custom To Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Log Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot the Status: System Logs: Settings page). Description	(a
Image: Display Advanced The Source Port Range for a connection is typically random and almost never equal to the det its default value, any. Destination Invert match Single host or alias Image: Control of the status of the	Source Address
Display Advanced The Source Port Range for a connection is typically random and almost never equal to the de its default value, any. Destination Destination Destination Destination Port Range HTTP (80) From Custom To Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Log Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot the Status: System Logs: Settings page). Description A description may be entered here for administrative reference. A maximum of 52 characters log.	
The Source Port Range for a connection is typically random and almost never equal to the detits default value, any. Destination Destination Invert match Single host or alias Destination Port Range HTTP (80) Item (80) </td <td></td>	
Destination Destination Invert match Single host or alias Destination Port Range HTTP (80) HTTP (80) From Custom To Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Log Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a log the Status: System Logs: Settings page). Description A description may be entered here for administrative reference. A maximum of 52 characters log.	stination port. In r
Destination Invert match Single host or alias Image Destination Port Range HTTP (80) HTTP (80) Image From Custom To Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Log Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a log the Status: System Logs: Settings page). Description A description may be entered here for administrative reference. A maximum of 52 characters log.	
Destination Destination Invert match Single host or alias Destination Port Range HTTP (80) HTTP (80) From Custom To Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Log Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a log the Status: System Logs: Settings page). Description A description may be entered here for administrative reference. A maximum of 52 characters log.	
Destination Invert match Single host or alias Destination Port Range HTTP (80) From Custom To <th></th>	
Destination Port Range HTTP (80) HTTP (80) To From Custom To Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Log Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a log the Status: System Logs: Settings page). Description A description may be entered here for administrative reference. A maximum of 52 characters log.	192.168.22.2
From Custom To Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Log Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a log the Status: System Logs: Settings page). Description A description may be entered here for administrative reference. A maximum of 52 characters log.	
Specify the destination port or port range for this rule. The "To" field may be left empty if only Extra Options Log Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a log the Status: System Logs: Settings page). Description	Custom
Extra Options Log Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a log the Status: System Logs: Settings page). Description A description may be entered here for administrative reference. A maximum of 52 characters log.	filtering a single pe
Extra Options Log Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a log the Status: System Logs: Settings page). Description A description may be entered here for administrative reference. A maximum of 52 characters log.	intening a single po
Log Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a log the Status: System Logs: Settings page). Description A description may be entered here for administrative reference. A maximum of 52 characters log.	
Log packets that are native by this the Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lo the Status: System Logs: Settings page). Description A description may be entered here for administrative reference. A maximum of 52 characters log.	
Description A description may be entered here for administrative reference. A maximum of 52 characters log.	of logging, consid
Description A description may be entered here for administrative reference. A maximum of 52 characters log.	or 1099.119, 0011010
Description A description may be entered here for administrative reference. A maximum of 52 characters log.	
A description may be entered here for administrative reference. A maximum of 52 characters log.	
iog.	will be used in the
Advanced Options	



UDP) is returned to the sender,



ost cases this setting must remain at



QU'EST CE QUE LE PORTFORWARD

Le "port forwarding" (redirection de port) est une technique permettant de rediriger le trafic réseau destiné à une adresse IP publique et un port spécifique vers une adresse IP privée et un port sur un réseau interne (comme un LAN ou une DMZ). Cela permet d'accéder à des services internes (serveurs web) depuis l'extérieur du réseau, tout en conservant la sécurité offerte par le pare-feu et le NAT (Network Address Translation).

CONFIGURATION PORT FORWARD LAN

Interface	LAN Choose which interface this m	ule applies to. In most cases "\	✓ NAN" is specified.	
Address Family	IPv4 Select the Internet Protocol ve	ersion this rule applies to.	v	
Protocol	TCP Choose which protocol this ru	le should match. In most case	▼ s "TCP" is specified.	
Source	Display Advanced			
Destination	Invert match.	LAN address Type	*	Address/mask
Destination port range	HTTP From port Specify the port or port range	Custom for the destination of the pack	HTTP To port tet for this mapping. The 'to' fie	Custom Id 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	Single host Type of the server on which to map t must be from the same "scope at from link-local addresses sc	the ports. e.g.: 192.168.1.12 fo ", ope (fe80:*) to local scope (::1)	192.168.22.2 Address r IPv4

Redirect target port	HTTP 👻		
	Port Cus	stom	
	Specify the port on the machine with the IP address entered above. In case of a per- calculated automatically). This is usually identical to the "From port" above.	ort range, specify the beginning port of the range (the end port will be	
Description	A description may be entered here for administrative reference (not parsed).		
No XMLRPC Sync	 Do not automatically sync to other CARP members This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave. 		
NAT reflection	Use system default		
Filter rule association	Rule NAT 👻		
	View the filter rule		

Pour la configuration du port forward sur le lan on redirige l'adresse LAN vers l'ip du serveur ici "192.168.22.2" sur le port 80 (HTTP)

CONFIGURATION PORTFORWARD WAN

Disabled	Disable this rule					
No RDR (NOT)	OT) Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.					
Interface	WAN	WAN				
	Choose which interface	this rule applies to. In most	cases "WAN" is specified.			
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	Display Advanced					
Destination	 Invert match. 	WAN address		~		/
Destination		-			Address/mask	
Destination	_	Туре				
Destination Destination port range	HTTP	v Ivpe	HTTP	~		
Destination Destination port range	HTTP From port	V Custom	HTTP To port	~	Custom	
Destination Destination port range	HTTP From port Specify the port or port r	Custom	HTTP To port the packet for this mapping. Th	► 'to' field	Custom d may be left empty if only ma	apping a single port.

Redirect target port	HTTP	~	
	Port		Custom
	Specify the port on the machine with the IP address entered calculated automatically). This is usually identical to the "From port" above.	above. In case of	f a port range, specify the beginning port of the range (the end port will be
Description	A description may be entered here for administrative referen	nce (not parsed).	
No XMLRPC Sync	Do not automatically sync to other CARP members This prevents the rule on Master from automatically syncing	g to other CARP m	nembers. This does NOT prevent the rule from being overwritten on Slave.
NAT reflection	Use system default	•	
Filter rule ssociation	Rule NAT	~	
	View the filter rule		

Pour la configuration du port forward sur le lan on redirige l'adresse WAN vers l'ip du serveur ici "192.168.22.2" sur le port 80 (HTTP)





TEST PING LAN

```
C:\Users\Windows>ping 192.168.20.86
Envoi d'une requête 'Ping' 192.168.20.86 avec 32 octets de données :
Réponse de 192.168.20.86 : octets=32 temps<1ms TTL=64
Réponse de 192.168.20.86 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.20.86 : octets=32 temps<1ms TTL=64
Réponse de 192.168.20.86 : octets=32 temps<1ms TTL=64
Statistiques Ping pour 192.168.20.86:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = Oms, Maximum = 2ms, Moyenne = Oms
```

```
Ping vers WAN
```

```
Envoi d'une requête 'Ping' 192.168.22.2 avec 32 octets de données :
Réponse de 192.168.22.2 : octets=32 temps=1 ms TTL=63
Réponse de 192.168.22.2 : octets=32 temps=2 ms TTL=63
Réponse de 192.168.22.2 : octets=32 temps=1 ms TTL=63
Réponse de 192.168.22.2 : octets=32 temps=1 ms TTL=63
Statistiques Ping pour 192.168.22.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```



C:\Users\Windows>ping 192.168.22.2

Ping vers DMZ

TEST PING WAN

C:\Users\Nico>ping 192.168.202.11 Envoi d'une requête 'Ping' 192.168.202.11 avec 32 octets de données : Délai d'attente de la demande dépassé. Délai d'attente de la demande dépassé.

Délai d'attente de la demande dépassé. Délai d'attente de la demande dépassé.

Ping vers LAN



C:\Users\Nico>ping 192.168.22.2

Envoi d'une requête 'Ping' 192.168.22.2 avec 32 octets de données : Délai d'attente de la demande dépassé. Délai d'attente de la demande dépassé. Délai d'attente de la demande dépassé. Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.22.2: Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%)

Ping vers DMZ

TEST PING DMZ

root@debian:~# ping 192.168.202.20 PING 192.168.202.20 (192.168.202.20) 56(84) bytes of data. -- 192.168.202.20 ping statistics --packets transmitted, 0 received, 100% packet loss, time 5103ms

Ping vers LAN



oot@debian:~# ping 192.168.20.86 PING 192.168.20.86 (192.168.20.86) 56(84) bytes of data.

-- 192.168.20.86 ping statistics --packets transmitted, 0 received, 100% packet loss, time 3072ms

Ping vers WAN

TEST CONNECTION SITE



C : A Non sicurist 192.168.20.86 code 💿 Accueil | Microsoft... 📼 SIO Sair

Connection avec le LAN





Connection avec le WAN