

FLORENTIN BRACQ-FLABAT, BTS 2 SIO

TP B2 Pfsense / DMZ



Topologie réseau





Installation Pfsense

Création de l'interface LAN dans proxmox

Avant de passer à l'installation de la VM, il faut créer l'interface LAN dans proxmox, cliquer sur créer, puis Linux Bridge

Pour prendre en compte les modifications, penser à cliquer sur Appliquer la configuration

Source :

https://www.youtube.com/watch?v=2YZ C8Ze0CM

| xmox2" rcher | Créer ~ | Revenir en arrière | | | Appliquer la cor | | | | |
|---|---|--|--|--|--|---|--|--|--|
| rcher Ié | Créer ~ | Revenir en artière | | | Apoliquer la cor | | | | |
| | eno2 eno3 | Carte réseau Carte réseau Carte réseau | Actif Oul Non Non | Démarr Non Non Non | Gère le Non Non Non | Ports/escla | Mode d'agr | CIDR | Passerelle |
| eau | vmbr0 | Linux Bridge | Oui | Oui | Non | eno1 | | 192.168.20.202/24 | 192 168 20 254 |
| ancatas S sos re tem Log à jour ← dts eu ▶ | | | | | | | | | |
| | ficats is ons em Log em Log ti jour ♥ ôts iu ♥ | nficats vmibr1 s s re em Log elijour v ofts s | Afficats vmbr1 Linux Bridge is ans re am Log ljour • dos su • | ificats vmbr1 Linux Bridge Oui is nons re em Log bjour → dts nu ▶ | aficats <u>vmbr1 Linux Bridge Oui Oui</u> is ons re em Log ljour ♥ dfs uu ♥ | Aficats vmbr1 Linux Bridge Oui Oui Non ← is is is ans re am Log bjour ← dfs iu ▶ | Aficats vmbr1 Linux Bridge Oui Oui Non s ns re am Log t jour → dfs nu ▶ | aficats vmbr1 Linux Bridge Oui Oui Non s ns ns re am Log tjour ↓ dfs u ↓ | aficats vmbr1 Linux Bridge Oui Oui Non ← |



Ajout de l'interface LAN sur la VM

Pour connecter l'interface LAN à la VM, il faut ajouter une nouvelle carte réseau pour connecter l'interface LAN. Dans mon cas la carte net0 est le WAN sur l'interface vmbr0 et la carte net1 est le LAN sur l'interface vmbr1

PROXMOX Virtual Environment 8.2.2 Rechercher Machine virtuelle 108 (Pfsense florentin) sur le nœud proxmox2 Aucune étiquette Vue serveur Centre de données Résumé Ajouter v Supprimer Éditer Action disque v proxmox2 103 (WIN-SRV-FLORENTIN) >_ Console 2.00 Gio 104 (WIN-SERV-SAM) Matériel 1 (1 sockets, 1 cores) [x86-64-v2-AES] 105 (windows samael) BIOS Par défaut (SeaBIOS) Cloud-Init 106 (windows florentin) Affichage Par défaut Options 107 (pfsensegatien) OS Machine Par défaut (i440fx) 108 (Pfsense florentin) Historique des tâches Contrôleur SCSI VirtIO SCSI single 109 (WIN-SRV-Flo-Supervision) Moniteur local iso/pfSense-CE-2.5.2-RELEASE-amd64 iso.media=cdrom.size=636498K 110 (W10-B2-Florentin) Sauvegarde 111 (pfsensegatiendeleau) local-lvm:vm-108-disk-0,iothread=1,size=32G Disque dur (scsi0) 201 (WinServ-Nicolas) 13 Réplication virtio=BC:24:11:3E:A2:5F,bridge=vmbr0,firewall=1 202 (Win10-Nicolas) virtio=BC:24:11:69:90:C4,bridge=vmbr1,firewall=1 😅 Carte réseau (net1) Instantanés 203 (Zabbix-Nicolas) D Pare-feu 204 (pfsense-nicolas) 100 (debian) Permissions 101 (Windows10) 102 (Windows-server-2019) 200 (Debian-12) Iocalnetwork (proxmox2) local (proxmox2) Iocal-lvm (proxmox2)

Installation de Pfsense

Laissez-vous guider pendant l'installation en suivant les captures d'écran suivantes, jusqu'au redémarrage



Configuration de Pfsense

Après le redémarrage, répondre aux différentes questions, comme sur la capture d'écran, puis indiquer la fonction des différentes interfaces <u>ATTENTION !!! à ne pas inverser,</u> <u>sinon le serveur DHCP peut se</u> <u>retrouver sur le WAN !</u> Dans mon cas le WAN est sur vtnet0 et mon LAN est sur vtnet1

Juste après avoir validé, on peut voir certaines informations, notamment les @IP qui ont été attribuées au WAN (serveur DHCP de la salle) et le LAN (par défaut 192.168.1.1/24)

vtnet1 bc:24:11:f4:c9:15 (down) VirtIO Networking Adapter

Do VLANs need to be set up first? If VLANs will not be used, or only for optional interfaces, it is typical to say 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 or a): vtnet0

Enter the LAN interface name or 'a' for auto-detection NOTE: this enables full Firewalling/NAT mode. (vtnet1 a or nothing if finished): vtnet1

The interfaces will be assigned as follows:

WAN -> vtnet0 LAN -> vtnet1

Do you want to proceed [yin]? 📕

Starting syslog...done. Starting CRON... done. pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021 Bootup complete FreeBSD/amd64 (pfSense.home.arpa) (ttyv0) KVM Guest - Netgate Device ID: Obf2f3b50d2Ob29a7294 *** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense *** WAN (wan) -> v4/DHCP4: 192.168.20.137/24 -> vtnet0 LAN (lan) -> vtnet1 $-> \lor4: 192.168.1.1/24$ 0) Logout (SSH only) 9) pfTop 1) Assign Interfaces 10) Filter Logs 2) Set interface(s) IP address 11) Restart webConfigurator 3) Reset webConfigurator password 12) PHP shell + pfSense tools 4) Reset to factory defaults 13) Update from console 5) Reboot system 14) Enable Secure Shell (sshd) 6) Halt system 15) Restore recent configuration 7) Ping host 16) Restart PHP-FPM 8) Shell

| Éditer: Carte ré | seau | | | |
|------------------|------------|--------------|-------------------|----|
| Pont (bridge): | vmbr1 | Modèle: | Intel E1000 | |
| Étiquette de | aucun VLAN | Adresse MAC: | BC:24:11:C0:93:EC | |
| Pare-feu: | | | | |
| O Aide | | | Avancé 🗌 | ОК |

| The province - Login A | Apache2 Debian Default Page: It v × + |
|-----------------------------|---------------------------------------|
| 🔶 🔿 🙆 🔕 Non sécurisé http | s://192.168.1.1/index.php |
| pf sense | |
| ₩ | |
| | |
| | |
| | SIGN IN |
| | |
| | Username |
| | Username Password |

Test du Pfsense

Pour tester le Pfsense, mettre une VM cliente avec une interface graphique dans le LAN, c'est comme la VM Pfsense au début, on connecte l'interface LAN que l'on a crée dans proxmox à la VM sur sa carte réseau, mais il n'y a pas besoin d'ajouter une carte réseau.

Normalement une @IP devrait remonter sur la VM, ensuite ouvrir un navigateur web, puis tapper 192.168.1.1 pour accéder à l'interface web d'administration de Pfsense, le login par défaut est **admin** et le mot de passe est **pfsense**

Suite de la configuration de Pfsense depuis la page web d'administration

1^{ère} étape choisir le nom host, le domaine et les DNS

2^{ème} étape choix du fuseau horaire

| : E |) 🗾 pfSense.home.arpa - Wiz | and: pfSc × + | | - | Ø | \times | 2° E | 🕽 🗾 pfSens | e.home.arpa - Wizard | pfSe x + | | | | | | | - | ōΧ |
|--------------|-----------------------------|--|--|-----------------------------------|-----|----------|--------------|------------|-----------------------------|--|-------------------------|------------------|------------------|------------------------|---------|-----|--------------|-------|
| \leftarrow | C 🛛 😣 Non sécurisé 🛛 🕴 | https://192.168.1.1/wizard.php?xml=setup_wizard.xml | as A 🟠 🗘 🖆 | <u>ک</u> ہ | | 4 | \leftarrow | C ON | on sécurisé http | s://192.168.1.1/wiza | rd.php?xml=set | up_wizard.xml | | | as A° ☆ | ወ 🕼 | <u>ک</u> ہ ش | ··· 📀 |
| | Wizard / pfSense | Setup / General Information | | 0 | | ^ | | | e System - on | Interfaces - | Firewall - | Services - | VPN - | Status - Diagnostics - | Help 🕶 | | G | • |
| | Step 2 of 9 | | | | | | | WARNING: | The 'admin' accour | nt password is set to | the default valu | Je. Change the p | assword in the U | ser Manager. | | | | |
| | General Information | On this screen the general pfSense parameters will be set. | | | | 1 | | Wizard | / pfSense S | etup / Time | Server Inf | ormation | | | | | 0 | |
| | | EXAMPLE: myserver | | | | | | Time Ser | Step 3 o | n | | | | | | | | |
| | Domain | pfsense.local EXAMPLE: mydomain.com | | | | | | | | Please enter the tim | e, date and time | zone. | | | | | | |
| | | The default behavior of the DNS Resolver will ignore manually configured DNS servers for o manually configured DNS servers below for client queries, visit Services > DNS Resolver an | ient queries and query root DNS servers direc I enable DNS Query Forwarding after complet | ctly. To use th ting the wizar | rd. | | | Time ser | ver hostname | 2.pfsense.pool.ntp Enter the hostname | org (FQDN) of the ti | me server. | | | | | | |
| | Primary DNS Server | 8.8.8.8 | | | | | | | Timezone | Europe/Paris | | | | ¥ | | | | |
| | Secondary DNS Server | 1.1.1.1 | | | | | | | | >> Next | | | | | | | | |
| | Override DNS | Allow DNS servers to be overridden by DHCP/PPP on WAN | | | | | | | | | | | | | | | | |
| | | » Next | Activer Windows | | | | | | | | | | | | | | | |

| C O Non sécurisé | https://192.1 | 68.1.1/inter | faces.php? | lif=wan | | | | | đđ | A3 | \sim | m | 4 | G | 82 | | 1 |
|-------------------------|--|---|--|---|---|---|---|--|-----------------------|-------------------|-----------------------------------|---------------------------------|---------------------|------------------------|---------------------|---|---|
| | | | area of property of the | | | | | | | 12 | 1-4 | 42 | P- | -w | | | |
| DHCPv6 Prefix | 64 | | | | | | ~ | | | | | | | | | | |
| Delegation size | The value | in this field i | is the dele | gated pref | fix length pro | wided by the [| HCPv6 server. | Normally specifie | ed by the | e ISP. | | | | | | | |
| Send IPv6 prefix hint | 🗌 Send a | n IPv6 prefi | x hint to in | dicate the | desired pref | fix size for del | egation | | | | | | | | | | |
| Debug | 🗌 Start D | HCP6 client | t in debug | mode | | | | | | | | | | | | | |
| Do not wait for a RA | C Require | d by some | ISPs, espe | ecially thos | se not using | PPPoE | | | | | | | | | | | |
| Do not allow PD/Address | C dhop60 | will send a | release to | the ISP or | n exit, some | ISPs then rele | ase the allocate | d address or pre | efix. Thir | s optic | n prever | nts that | signal | ever be | ing | | |
| Reserved Networks | | | | | | | | | | | | | | | - | 1 | |
| Block private networks | 0 | | | | - | | | | | | | | | | | | |
| and loopback addresses | Diselse trai | fic from IP | addresses | s that are re copback as | eserved for ; ddresses (12 | private networ 27/8). This op | ks per RFC 191 iion should gen | 3 (10/8, 172.16/ erally be turned o | 12, 192. on, unles | 168/1 ss this | 6) and ur network | nique lo interfa | cal ado ce resid | dresses des in s | per uch a | | |
| | RFC 4193 private add | (fc00::/7) a dress space | s well as lo , too. | | | | | | | | | | | | | | |
| Block bogon networks | RFC 4193 private ad | (fc00::/7) a dress space | s well as lo , too. | | | | | | | | | | | | | | |
| Block bogon networks | RFC 4193 private add Blocks tra | (fc00::/7) a dress space | s well as lo a, too. served IP a | addresses | (but not RFC | : 1918) or not | yet assigned by | IANA. Bogons a | re prefo | xes tha | at should | Inever | appear | in the l | nternet | | |
| Block bogon networks | Blocks trai RFC 4193 private add Blocks trai routing tab | (fc00::/7) a dress space fic from res | s well as lo , too. served IP a ihould not | addresses i appear as | (but not RFC | 1918) or not address in any | yet assigned by packets receiv | IANA. Bogons a | re prefo | xes tha | it should | I never i | appear | in the l | nternet | | |
| Block bogon networks | Blocks tra RFC 4193 private add Blocks trai routing tab This option Note: The | (fc00::/7) a dress space lfsc from res sle, and so s n should on update freq | s well as fo , too. served IP a should not ly be used uency can | addresses appear as on externa be change | (but not RFC the source al interfaces ed under Sys | 2 1918) or not address in any (WANs), it is stem > Advan | yet assigned by packets receiv not necessary c red, Firewall & N | IANA. Bogons a ed. n local interface AT settings. | ire prefo s and it | xes tha can po | at should | l never i v block i | appear required | in the li d local 1 | nternet traffic. | | |
| Block bogon networks | Blocks trai routing tab This option Note: The | (fc00::/7) at dress space ffic from res ile, and so s in should on update freq | s well as k a, too. served IP a should not ly be used uency can | addresses appear as l on externa i be change | (but not RFC the source a al Interfaces ed under Sys | C 1918) or not address in an i (WANs), it is stem ≻ Advani | yet assigned by packets receiv not necessary c xed, Firewall & N | IANA. Bogons a ed. n local interface AT settings. | ire prefu s and it | xes tha | at should | l never i v block i | appear require | in the l | nternet traffic. | | |
| Block bogon networks | Blocks trai RFC 4193 private add Blocks trai routing tak This option Note: The Save | (fc00::/7) a dress space fisc from res ole, and so s in should on update freq | s well as k n, too. aerved IP a ihould not ly be used uency can | addresses appear as on externa be change | (but not RFC the source a al interfaces ed under Sys | (1918) or not address in an (WANs), it is stem > Advani | yet assigned by , packets receiv not necessary c xed, Firewall & N | IANA. Bogons a ed. n local interface AT settings. | ire prefu s and it | can po | at should otentially er Win | I never i v block i idows | appear required | in the l | nternet traffic. | | |

Suite de la configuration

DANS LES INTERFACES, SUR LE WAN DÉSACTIVER LE BLOCAGE DES @IP PRIVÉES

Mise en place de la DMZ

| | ent 8 | | | | | | | | | | | Documentati | on 📮 Créer un |
|---|-------|---------------------------------|--------------|------------------------------|-------|---------|---------|-------------|------------|-------------------|----------------|-------------|---------------|
| Vue serveur | | Nasud 'proxmax2' | | | | | | | | | | Redemarrer | O Arrêter >. |
| Centre de données | | | | | | | | | | | | | |
| 103 (WIN-SRV-FLORENTIN) | | Q Rechercher | Nom † | Туре | Actif | Démarr. | Gère le | Ports/escla | Mode d'agr | CIDR | Passerelle | Commen | taire |
| 104 (WIN-SERV-SAM) | | D Notes | eno1 | Carte réseau | | Non | Non | | | | | | |
| 106 (windows florentin) | | >_ Shell | eno2 | Carte réseau | Non | Non | Non | | | | | | |
| 107 (pfsensegatien) 108 (Pfsense florentin) | | o¢ Système | eno3 eno4 | Carte reseau Carte réseau | Non | Non | Non | | | | | | |
| 109 (WIN-SRV-Flo-Supervision) | | ≓ Réseau | vmbe0 | Linux Bridge | Oui | Oui | Non | eno1 | | 192 168 20 202/24 | 192.168.20.254 | | |
| 110 (W10-82-Florentin) | | Certificats | vmbr1 | Linux Bridge | Oui | Oul | Non | | | | | LAN B2 F | lorentin |
| III (phsensegatiendoleau) 201 (WinServ-Nicolas) 202 (Win10-Nicolas) 203 (Zabbic-Nicolas) | | DNS Hötes Options | vmbr2 | Linux Bridge | Oui | Oul | Non | <u> </u> | | | | DMZ B2 | Florentin |

| | nent 8.2.2 | Rechercher | 1 | | |
|---|------------|--|---------------------|---|--|
| Vue serveur 🗸 🖓 | Mac | chine virtuelle 108 (Pfsense | e.flore | ntin) sur le nœud proxmox2 | Aucune étiquette d |
| Centre de données prozmoz2 103 (WN-SRV-FLORENTIN) 104 (WIN-SERV-SAM) 105 (windows samael) 105 (windows samael) 107 (prisensegatien) 108 (Pfeares florentin) 109 (WN-SRV-FLO-Supervision) 101 (WIO-B2-Florentin) 101 (WIO-B2-Florentin) 201 (WnServ-Nicolas) 202 (Wn10-Nicolas) 202 (Wn10-Nicolas) 202 (Wn10-Nicolas) 203 (Zabbia-Nicolas) 100 (debian) 101 (Windows 10) 102 (Wndows -server-2019) 102 (Wndows -server-2019) 102 (Undows -server-2019) 102 (Undows -lerver-2019) 101 (Undows -lerver-2019) 102 (Undows -lerver-2019) 101 (Undows -lerver-2019) 101 (Undows -lerver-2019) 101 (Undows -lerver | | Rósumé Console Matériel Cloud-Init Options Historique des tâches Moniteur Sauvegarde Réplication Instantanés Pare-fou ↓ Permissions | 11 11 12 00 8 10 00 | youter V Supplmer Edi Processors BIOS Affichage Machine Controlleur SCSI Controlleur SCSI Disque dur (scsi0) Carte réseau (net1) Carte réseau (net2) | Action disque v Revenir en arrière 2.00 Gio 1 (1 sockets, 1 cores) [x86-64-v2-AES] Par doffaut (SeaBIOS) Par doffaut (SeaBIOS) Par doffaut (Molox) Virilo SCS single local iso/plSense-CE-2.5 2-RELEASE-amd64 iso,media=cdrom,size=636490K Jocal-wm vm-108-disk.0 jothread=1, size=32G virilo=BC-24.11.3E A2-5 Erbridge=vmbr0,firewall=1 virilo=BC-24.11.5B 68 B0,bidge=vmbr2,firewall=1 |

Création de l'interface DMZ dans proxmox

Il faut créer une nouvelle interface dans proxmox (bridge linux) qui va nous servir de DMZ, dans mon cas l'interface que je vais ajouter va être vmbr2. Pour résumer, il y a 3 interfaces vmbr0 qui est le WAN (réseau de la salle), vmbr1 qui est le LAN derrière le pare feu et enfin vmbr2 qui est la DMZ

Ensuite, il faut se rendre dans les paramètres matériels de la VM Pfsense pour ajouter une carte réseau et y connecter vmbr2



routing table, and so should not appear as the source address in any packets received.

ofSense is developed and ma

Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings

This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic

by Netgate. © ESF 2004 - 2024 View license

Configuration de vmbr2 en DMZ

Dans un premier temps depuis l'interface web d'administration, dans les interfaces penser à activer la nouvelle interface connectée à la VM, aller ensuite sur la configuration de l'interface, donner un nom, donner une adresse IPv4 statique et enfin cliquer sur save pour enregistrer

Configuration du serveur DHCP pour la DMZ

Pour mettre en place un DHCP dans la DMZ, cliquer sur Services, DHCP puis DMZ, cliquer sur Enable DHCP server on DMZ interface, dans Range définir le pool d'@IP et enfin dans DNS servers mettre l'@IP de l'interface DMZ

| | and a li | | | | | | | | | | | | |
|--|---|---|--|--|---|--|--|-----------------------------------|-----------|----------|-------------|---------|---|
| 🗟 🤨 Non sécu | risé https://192.168.1. | 1/services_dhcp | o.php?if=opt1 | | | | äð | Ag | 슈 | Φ | ¢ @ | ~ | 2 |
| Sense System | • Interfaces • | Firewall + | Services - | VPN - | Status 🕶 | Diagnostics - | Help | * | | | | G | • |
| Services / DHCP | Server / DMZ | | | | | | | | | C |) 幸 🖻 | • • | |
| LAN DMZ | | | | | | | | | | | | | |
| General Options | | | | | | | | | | | | | l |
| Enable | Enable DHCP serve | er on DMZ inter | face | | | | | _ | | | | | |
| BOOTP | 📋 Ignore BOOTP que | ries | - | | | | | | | | | | |
| Deny unknown clients | Allow all clients | | | | ~ | | | | | | | | |
| | Miner ant to Allen all | clients, any DH | CP client will get | an IP addre | s within this s | cope/range on this | interface | . If set | to Allow | known | clients fro | m any | |
| | interface, only MAC at | ddresses listed | below (i.e. for the | is interface) | will get an IP a | ddress within this s | ress. If s cope/rai | et to Ange. | now kno | | nts from of | ny tras | |
| Ignore denied clients | interface, any DHCP c interface, only MAC as Denied clients will | dresses listed | below (i.e. for the for the formation of | is interface) | will get an IP a | s) will get an IP add ddress within this s | ress. If s cope/rai | et to A nge. | now kno | | nts from o | ny très | |
| Ignore denied clients | interface, any DHCP c interface, only MAC a Denied clients will This option is not corr | ddresses listed be ignored rath spatible with fai | below (i.e. for the than rejected lover and cannot be the than rejected lover and cannot be the the the the the the the the the th | the enabled | will get an IP a | s) will get an IP add ddress within this s r Peer IP address is | ress. If s cope/rai | et to A nge. red. | now kno | | nts from o | ny tris | |
| Ignore denied clients Ignore client identifiers | interface, any DHCP o interface, any DHCP o interface, only MAC at Denied clients will This option is not corr If a client includes | ddresses listed be ignored rath spatible with fai a unique identi | below (i.e. for the than rejected lover and cannot be the than rejected lover and cannot be in its DHCP (| t be enabled | will get an IP a when a Failow | s) will get an IP add ddress within this s ir Peer IP address it recorded in its lease | ress. If s cope/rai configu e. | et to A nge. red. | BOW KNO | | nts from o | ny mis | |
| Ignore denied clients Ignore client identifiers | interface, any DHCP of interface, any DHCP of Denied clients will This option is not com I if a client includes This option may be us server behavior violate | ient with a MA ddresses listed be ignored rath apatible with fai a unique identii ieful when a clin es the official D | below (i.e. for the formation of the for | t be enabled equest, that t using differ | will get an IP a when a Failow UID will not be ent client ident | s) will get an iP add ddress within this s rr Peer IP address is recorded in its lease ifiers but the same | ress. If s cope/rai configu e. hardwar | et to Ange. red. e (MAC | () addres | is. Note | that the re | sulting | |
| Ignore denied clients Ignore client identifiers Subnet | Interface, any DHCP of Interface, only MAC at Denied clients will This option is not corr If a client includes This option may be us server behavior violate 192.168.2.0 | eent with a MAA ddresses listed be ignored rath apatible with fai a unique identii eful when a clis the official D | o dures instea below (i.e. for the er than rejected lover and canno foer in its DHCP in int can dual boo HCP specificatio | t be enabled equest, that t using differ | (a)/interace(will get an IP a when a Failow UID will not be ent client ident | s) will get an IP add ddress within this s Ir Peer IP address is recorded in its leas ifiers but the same | ress. If s cope/rai configu e. hardwar | et to A nge. red. e (MAC | c) addree | 16. Note | that the re | sulting | |

| | server behavior violates the official DHCP specification. | |
|-----------------|---|---------------|
| Subnet | 192.168.2.0 | |
| Subnet mask | 255.255.255.0 | |
| Available range | 192.168.2.1 - 192.168.2.254 | |
| Range | 192.168.2.100 | 192.168.2.200 |
| | From | То |





Permettre l'accès à internet dans la DMZ

Pour permettre l'accès à internet dans la DMZ, il faut créer une règle dans le Firewall, créer une nouvelle règle. Dans **Action** mettre **Pass**, pour **Interface** mettre **DMZ**, pour **Protocol** mettre **Any**, dans **Source** choisir **DMZ net** et pour **Destination** choisir **Any**, puis cliquer sur **save** et appliquer la configuration

Enfin créer une VM debian avec un Lamp installé dessus (apache 2) et connecter la carte réseau de la VM sur vmbr2 (DMZ), une @IP devrait remonter grâce au serveur DHCP en 192.168.2.x et il devrait être possible d'accéder à internet grâce à la règle qui vient d'être ajoutée (ping 8.8.8.8), récupérer l'@IP attribuée avec la commande ip a

Source : https://www.youtube.com/watch?v=2YZ_C8Ze0CM

| dit Redirect Entry Disable Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications. Interface 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 applies to. Source Otisplay Advanced Destination Invert match. Type | newait/ INAT/ | Fortroiward / Edit | | | | U |
|--|--------------------|---|--|-----------------------------------|-----------------|---|
| Disable this rule No RDR (NOT) Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications. Interface 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 applies to. Source Display Advanced Destination Invert match. Type Address / TCP' is specified. | dit Redirect Entry | | | | | |
| No RDR (NOT) Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications. Interface 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 Advecced Destination Invert match, Type Address/mask | Disabled | Disable this rule | | | | |
| Interface 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 about most cases "TCP" is specified. Source Choose which protocol this rule should match. In most cases "TCP" is specified. Source Chopsely Advected Destination Invert match. Type Address/mask | No RDR (NOT) | Disable redirection for tra This option is rarely needed | affic matching this rul . Don't use this withou | le it thorough knowledge of th | e implications. | |
| 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. Type Address/mask | Interface | WAN Choose which interface this | rule applies to. In mo | st cases "WAN" is specified | | |
| Protocol TCP V Choose which protocol this rule should match. In most cases "TCP" is specified. Very State of the specified. Source Display Advanced Van address Very State of the specified. Destination Invert match. WAN address Very State of the specified. | Address Family | IPv4 Select the Internet Protocol | version this rule appli | ► to. | | |
| Source Display Advanced Destination Invert match. WAN address / Type Address/mask | Protocol | TCP Choose which protocol this | rule should match. In | w most cases "TCP" is specifi | ed. | |
| Destination Invert match. WAN address / / / / / / / / / / / / / / / / / / | Source | Display Advanced | | | | |
| | Destination | Invert match. | WAN address | | | ask i i i i i i i i i i i i i i i i i i i |

| Redirect target iP | | Single host | ~ | 192.168.2.100 |
|--|---|--|---|--|
| | | Туре | | Address |
| | Enter the internal IP addre In case of IPv6 addresses i.e. it is not possible to re- | ess of the server on which to map s, in must be from the same "scop direct from link-local addresses s | the ports. e.g.: 192.168.1.12 fo be", cope (fe80:*) to local scope (::1 |) |
| Redirect target port | HTTP | | | |
| | Port | | Custom | |
| | Specify the port on the m calculated automatically) This is usually identical to | achine with the IP address entere). o the "From port" above. | d above. In case of a port range | e, specify the beginning port of the range (the end port will be |
| Description | | | | |
| | A description may be ente | ered here for administrative refer | ence (not parsed). | |
| No XMLRPC Sync | Do not automatically a provide the second | sync to other CARP members | | |
| | | | | de la NOT esta de la ferra la la compañía de la la compañía de la compañía de la compañía de la compañía de la |
| | This prevents the rule on | Master from automatically synci | ng to other CARP members. Thi | s does NUT prevent the rule from being overwritten on Slave. |
| NAT reflection | This prevents the rule on Use system default | Master from automatically synci | ng to other CARP members. Thi | s does NUT prevent the rule from being overwritten on Slave. |
| NAT reflection | This prevents the rule on Use system default Rule NAT | Master from automatically synci | ng to other CARP members. Thi | s does NUT prevent the rule from being overwritten on Slave. |
| NAT reflection | This prevents the rule on Use system default Rule NAT View the filter rule | Master from automatically synci | ng to other CARP members. Thi | s does NU1 prevent the rule from being overwritten on slave. |
| NAT reflection Filter rule association ule Information | This prevents the rule on Use system default Rule NAT View the filter rule | Master from automatically synci | ig to other CARP members. Thi | s does NUT prevent the rule from being overwritten on Slave. |
| NAT reflection Filter rule association ule Information Created | This prevents the rule on Use system default Rule NAT View the filter rule 9/25/24 09:15:12 by adm | Master from automatically syncii sin⊚192.168.1.124 (Local Databa | ig to other CARP members. Thi | s does NUT prevent the rule from being overwritten on slave. |
| NAT reflection Filter rule association ule Information Created Updated | This prevents the rule on Use system default Rule NAT View the filter rule 9/25/24 09:15:12 by adm 9/25/24 09:15:12 by adm | Master from automatically synci in@192.168.1.124 (Local Databa in@192.168.1.124 (Local Databa | se) | a does NUT prevent the rule from being overwritten on Slave. Activer Windows Activer windows |

Mise en place de la redirection de ports

Le but est de rendre accessible le site web qui est sur le serveur lamp dans la DMZ sur le WAN avec l'@IP publique.

Pour cela il faut se rendre dans **Firewall** pour créer une nouvelle règle **NAT**, dans **Interface** mettre **WAN**, pour **Destination** mettre **WAN** address, dans **Destination port range**, mettre **HTTP** (port 80), puis dans **Redirect target IP**, choisir **Single host** et entrer l'@IP du serveur lamp, pour **Redirect target port** mettre HTTP, cliquer ensuite sur **save**

Source : <u>https://www.youtube.com/watch?v=98jrJjCn1M0</u>

Test de la DMZ

Pour tester la DMZ taper l'@IP publique dans un navigateur web depuis internet (réseau de la salle)

