Leyssene Loic 2022

AJOUT DE VLAN SUR L'interface PMX OPT1 du Pfsense

Se connecter à l'interface web du pfsense via vpn à l'adresse <u>https://172.27.27.254:9543</u> Dans l'onglet Interfaces, ouvrir Affectation, puis section vlans, cliquer sur ajouter.

DISENSE Système -	Interfaces -	Pare-feu 🔻	Services -	VPN -	État 🝷	Diagnost	ics -	Aide 🚽		G
Interfaces / VI ANS	Affectations									T IN O
Interfaces / VLANS	WAN									= ••• •
	LAN			1		0.05	015			
Assignations des interfaces	PMX	Sans-fil	VLANS	2 QinQs	PPPs	GRES	GIFs	Ponts	LAGGS	
Interfaces de récesules	PROXY21									
Interface	GUACA20		Priorité			Description			Actions	
om((opt1)	CLIENT1		Thomas			guacamolo				
enio (opti)	CLIENT2					guacamole			Ø Ш	
em0 (opt1)	CLIENT3	_				rproxy			Ø* 🔟	
em0 (opt1)	CLIENT4					client1			er 💼	
em0 (opt1)	CLOUD22					client2			er 🔟	
em0 (opt1)	103					client3			e 🖉 🗇	
em0 (opt1)	104					client4			e 🗇	
em0 (opt1)	22					nextcloud			Ø 🛅	
										Ajouter

Les vlans sont renseignés sous l'interfaces em0 (opt1). Donner un ID de vlan (balise) ici 105, puis un nom (description) ici client5

IEITALES / VLA	NS / MODIFIER	華岡
nfiguration VLAN		
Interface parente	em0 (68:05:ca:35:ed:6d) - opt1 Seules les interfaces compatibles VLAN seront affichées.	
Balise VLAN	105 Balise VLAN 802.1Q (entre 1 et 4094).	
Priorité du VLAN	0 Priorité VLAN 802.1Q (entre 0 et 7).	
Description	Client5 Une description du groupe est proposée ici pour aider l'administrateur (non pris en compte).	

Dans Interfaces, affectation, assignation des interfaces, ajouter l'interface vlan créé précédement

Système -	Interfaces 🗕 🛛	Pare-feu ▼	Services 🗸	VPN -	État 🕶	Diagnosti	cs *	Aide 🗕	
Interfaces / Assigna	ations des inter	faces							
Assignations des interfaces	Groupes d'interface	Sans-fil	VLANs	QinQs	PPPs	GREs	GIFs	Ponts	LAGGs
Interface	P	ort réseau							
WAN		bge1 (00:1e:c9:	:bb:96:6d)						*
LAN		bge0 (00:1e:c9:	:bb:96:6c)						Supprimer
РМХ		em0 (68:05:ca:	35:ed:6d)						Supprimer
proxy21		VLAN 21 March	ne em0 - opt1 (rproxy)					Supprimer
guaca20		VLAN 20 March	ne em0 - opt1 (guacamole)					Supprimer
client1		VLAN 101 Marc	che em0 - opt1	(client1)					Supprimer
client2		VLAN 102 Marc	che em0 - opt1	(client2)					Supprimer
client3		VLAN 103 Marc	che em0 - opt1	(client3)					Supprimer
client4		VLAN 104 Marc	che em0 - opt1	(client4)					Supprimer
CLOUD22		VLAN 22 March	ne em0 - opt1 (nextcloud)					Supprimer
Ports réseau disponibles	[ovpns1 (open v	pn pc2vpn)						✓ 🕂 Ajouter
Enregistrer		ovpns1 (open v ovpns2 (ovpn a VLAN 105 Marc	pn pc2vpn) ccés client tes <mark>che em0 - opt1</mark>	t vers v) (client5)					

Une fois créé cliquer sur son nom ici OPT9

guacazu	VLAN 20 Marche em0 - opt1 (guacamole)	~	Supprimer
client1	VLAN 101 Marche em0 - opt1 (client1)	~	Supprimer
client2	VLAN 102 Marche em0 - opt1 (client2)	~	Supprimer
client3	VLAN 103 Marche em0 - opt1 (client3)	~	Supprimer
client4	VLAN 104 Marche em0 - opt1 (client4)	~	Supprimer
CLOUD22	VLAN 22 Marche em0 - opt1 (nextcloud)	~	i Supprimer
OPT9	VLAN 105 Marche em0 - opt1 (client5)	~	i Supprimer
Ports réseau disponibles	ovpns1 (open vpn pc2vpn)	~	+ Ajouter

Dans la fenetre qui s'ouvre activer l'interface, renseigner sa description (nom) type de configuration, et son adresse ip v4 et masque de sous réseau ; enregistrer les changements en de page, puis appliquer les modifications

es modifications doivent publiez pas d'ajouter la p	être appliquées pour prendre effet. lage du serveur DHCP si besoin, après avoir appliqué.
<i>h i i</i>	
onfiguration genera	
Activer	
Description	
	Entrez loi une description (nom) pour cette interface.
ype de configuration	IPv4 statique
Type de configuration	Aucun
IPv6	
Adresse MAC	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	The MAC address of a VLAN interface must be set on its parent interface
MTU	
	Si ce champ est laissé vide, la valeur MTU par défaut de la carte réseau est utilisée. En général 1 500 octets, mais peut varier dans certaines circonstances.
MSS	
	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Vitesse et Duplex	Par défaut (aucune préférence, habituellement une auto-sélection) 🗸
	Forcer la vitesse et le mode duplex pour cette interface. ATTENTION: doit être défini sur autoselect (vitesse négociée automatiquement) à moins que la vitesse et duplex du port auquel cette interface e connectée soit aussi forcé.
onfiguration statiqu	ue IPv4
Adresse IPv4	192.168.105.1

Si on shouaite un service dhcp sur cette interface, se rendre dans service, serveur dhcp.

COMMUNITY EDITION	✓ Interfaces ✓ Pa	are-feu 👻	Services -	VPN -	État 👻	Diagnostics -		
Interfaces / client	t5 (em0.105)		DNS Dynamiq DNS Forwarde NTP	ue er				
Les modifications ont été a	opliquées avec succès.		Portail Captif Proxy IGMP					
Configuration généra Activer	le ✔ Activer interface		Relais DHCP Relais DHCPv Résolveur DN	6 S				
Description	client5 Entrez ici une description ((nom) pour c	Sauvegarde au Serveur DHCP	utomatique d	e la configui	ration		
Type de configuration IPv4	IPv4 statique		Serveur PPPol Serveurs et RA	E A DHCPv6				
Type de configuration IPv6	Aucun IPv6		SNMP UPnP & NAT-PMP					
Adresse MAC	xxxxxxxxxxxxx The MAC address of a VLA	AN interface r	nust be set on it	s parent inter	face			

Au besoin, activer le serveur dhcp, renseigner la plage d'adresse voulue, suivant le masque de sousréseau. (ainsi que les autres paramêtres éventuels, serveur dns ...)

Services / Serveu	IT DHCP / CLIENT5 C® 幸 Ш 🗏 🕑
WAN LAN PMX	PROXY21 GUACA20 CLIENT1 CLIENT2 CLIENT3 CLIENT4 CLOUD22 CLIENT5
Options générales	
Activer	Activer le serveur DHCP sur l'interface CLIENT5
BOOTP	□ Ignorer les requêtes BOOTP
Rejeter les clients	Allow all clients
inconnus	When set to Allow all clients , any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.
Ignorer les clients inconnus	Les clients refusés seront ignorés plutôt que rejetés Cette option n'est pas compatible avec le failover et ne peut pas être activée lorsqu'une adresse Failover Peer IP est configurée.
Ignorer les identifiants clients	Si un client inclue un identifiant unique dans sa requête DHCP, cet UID ne sera pas enregistré dans son bail. Cette option peut être utile lorsqu'un client peut dual boot en utilisant différents identifiants client, mais avec la même adresse matérielle (MAC). Notez que ce comportement du serveur est contraire aux spécifications officielles de DHCP.
Sous-réseau	192.168.105.0
Masque de sous-réseau	255.255.248
Plage disponible	192.168.105.1 - 192.168.105.6
Plage	De À
Pools additionnels	

LES REGLES DU PARE FEU PEUVENT ETRE REGLES COMME SUR L'EXEMPLE SUIVANT :

Pa	are-	feu /	Règles /	CLIENT4								≢ Ш 🗏 (
Flo	ottant oenVF	(e) PN	WAN L	AN PMX	PRO	XY21 GUA	CA20 CLIEN	T1 CLIE	NT2 CLIENT3	CLIENT4	CLOUD22	CLIENT5
Rè	gles	(Faire États	glisser po Protocole	ur changer l'o Source	ordre) Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
	~	0 /0 B	IPv4 UDP	CLIENT4 net	*	*	53 (DNS)	*	aucun			₺₡₽०₫
	~	0 /0 B	IPv4 UDP	CLIENT4 net	*	*	123 <mark>(</mark> NTP)	*	aucun			÷∥⊡⊙i
		0 /0 B	IPv4 TCP	CLIENT4 net	*	*	443 (HTTPS)	*	aucun			₺∥□०₫
	~							*	aucun			₺∥₽०₫
	 	0 /0 B	IPv4 TCP	CLIENT4 net	*	*	00 (IIIIF)		adoun			
	✓ ✓ ×	0 /0 B	IPv4 TCP IPv4 TCP	CLIENT4 net CLIENT4 net	*	* CLIENT1 net	*	*	aucun			₺∥₽०₫
	✓ ✓ × ×	0 /0 B 0 /0 B 0 /0 B	IPv4 TCP IPv4 TCP IPv4 TCP	CLIENT4 net CLIENT4 net CLIENT4 net	* * *	* CLIENT1 net CLIENT2 net	*	*	aucun			₺/00i ₺/00i
	✓ ✓ × × ×	0 /0 B 0 /0 B 0 /0 B 0 /0 B	IPv4 TCP IPv4 TCP IPv4 TCP IPv4 TCP IPv4 TCP	CLIENT4 net CLIENT4 net CLIENT4 net CLIENT4 net	* * * *	* CLIENT1 net CLIENT2 net CLIENT3 net	* * * *	* * *	aucun aucun aucun aucun			\$ 1 ⊂ 0 i \$ 1 ⊂ 0 i \$ 1 ⊂ 0 i

Seuls les ports en vert sont autorisés en sortie, en rouge, blocage vers les autres vlan.

On peut durcir les rêgles en renseignant comme passerelle WAN sur les ports autorisés.

AJOUT VLAN DANS LE SWITCH ALLIED

Sur place ou a distance, Se connecter à un PC physique ayant un accès Bureau distant (mstsc ou vnc) configuré, Ainsi qu'un câble console connecté au switch . Via Vpn, se connecter au switch via ssh si configuré sur le switch.

Avec un cable console, relever le num de port com, et avec putty :

com3

speed 115200



sinon en ssh (172.27.27.253)... avec putty. Configuration ssh sur le switch :

crypto key generate rsa

ip ssh server

Administration login/user name : afrbr



AJOUT VLAN CREE DANS LE PFSENSE, passer en mode configuration

console# conf

console(config)# vlan database

console(config-vlan)# vlan 105

console(config-vlan)# exit

console(config)# interface vlan 105

console(config-if)# name client5

console(config-if)# end

AJOUT DU VLAN A L'INTERFACE (ici 1/g47) TRUNK vers OPT1 du pfsense

console# conf

console(config)# interface ethernet 1/g47

console(config-if)# switchport trunk allowed vlan add 105

console(config-if)# end

Enregristrer les modifications :

console# copy running-config startup-config

Overwrite file [startup-config] ?[Yes/press any key for no]....

<mark>Y</mark> pour yes.

TAGGUER LES VLAN SUR LES INTERFACES DU SWITCH VIA INTERFACE WEB

C A Non sécurisé 172.27.27353/confrig/authentication_page.htm	9	Authentica	tion	×		
AT-8000GS System Name: MAC Addr. ec.cd 6d.0b.98:78		\rightarrow G	仚	A Non sécurise	é 172.27.27.253/config/authentication_page.htm	
User Name Password				AT-8000GS	Log In System Name: MACA date: ec:rdf 6d 0b:98:78	
Sign in Clear					MAC AOU. EC.Co.60.00.98/78	User Name Password Sign in Clear

Dans l'onglet Layer2, sélectionner VLAN, puis l'ID du vlan a taggué dans les ports souhaités, puis cliquer sur modify en bas de page

😏 Home	× +			
	on sécurisé 172.27	7.27.253/home.htm		
8-TA**	000GS/48**			
C	onfig	uratio	n	
	M	System Name: IAC Addr: ec:cd:6d:0	b:98:78	
System	MAC Address			
Layer 1				
Layer 2	VLAN			
Mgmt. Security	Interface			
	GVRP			
Mamt Protocole	Spanning Tree			
Network Security	RSTP			
DHCP Snooping				
Services	MSTP			
Multicast	MAC Based Groups			
Utilities				_
Statistics		-	VLAN Type	
Save Config	VLAN ID		Static	
Help	105 🗸	3	802.1x Authentication	
Logout	VLAN Nam	ie	Enable 🗸	
	client5		Delete VLAN	
		Add	Apply	_
	Ports	O Trunks		
	#	Interface	Interface Status	7
	4 💿 1	1/g1	Excluded	
	<u> </u>	1/g2	Excluded	
	<u> </u>	1/g3	Excluded	
	0 4	1/g4	Excluded	_
	0 5	1/g5	Excluded	_
	06	1/g6	Excluded	_
	0 7	1/g7	Excluded	_
		1/g8	Excluded	
	0 g	1/g9	Excluded	
Allied Telesis Copyright	t © 2009 Allied Telesis In	c. All rights reserved.		

0	41	1/g41		Excluded
0	42	1/g42		Excluded
0	43	1/g43		Excluded
0	44	1/g44		Excluded
0	45	1/g45		Excluded
0	46	1/g46		Excluded
0	47	1/g47		Tagged
0	48	1/g48		Excluded
			Mod	lify 5

Dans la fenêtre qui s'ouvre sélectionner tagged, pour tagguer le vlan dans le port.

🕄 v	/LAN Config	uration - Google Chrom	e	-		×
▲	Non sécu	risé 172.27.27.253 /	/Vmember/b	ridg_v	lan_m	<u>s</u> e
te e	VL	AN Configuration				_
		VLAN ID VLAN Name Interface Interface Status Apply	105 client5 1/g1 Excluded Forbidden Tagged Untagged			-
-						

Faire ceci dans tous les ports ou l'on souhaite tagguer les vlan.

Déclarer Vlan créer dans le pfsense sur une interface réseau d'une machine virtuelle

Ne Pas oublier de Cocher vlan aware

VLAN SUR BONDO



Sur la VM :

Rechercher								
Vue Serveur V	Machine Virtuelle 101 (WindowsTestclientvlan100) sur le nœud dell							
✓ ■ Datacenter (brglange) > ■ bull1	🛢 Résumé	Ajouter v Supprimer Édite	r Atimensionner le disque Déplacer le disque Revenir en arrière					
> 🛃 bull2	>_ Console	🚥 Mémoire	4.00 GiB					
∽ 🛃 dell	🖵 Matériel 👩	Processeurs	4 (1 sockets, 4 cores)					
 100 (Supervision) 101 (Windows Testclientvlan 101) 102 (win10admin) 106 (Debian-cloud-vlan22) 120 (Guacamole-vlan20) 121 (ReverseProxy-vlan21) 104 (debian-base-lamp) brglangebckup (dell) local (dell) local-lvm (dell) 	Cloud-Init	BIOS	OVMF (UEFI)					
	Options	🖵 Affichage	Défaut					
	 Historique des tâches Moniteur 	😋 Machine	pc-q35-6.1					
		Contrôleur SCSI	LSI 53C895A					
		 Lecteur CD/DVD (ide2) 	none,media=cdrom					
	🖺 Sauvegarde	🗇 Disque Dur (sata0)	local-lvm:vm-101-disk-1.size=60G					
	ta Réplication 3		e1000=02:BB:E9:6B:22:9B,bridge=vmbr0,tag=101					
	Snapshots	🖨 Disque EFI	local-lvm:vm-101-disk-0,efitype=4m,pre-enrolled-keys=1,size=4M					
	D Parefeu	TPM State local-lvm:vm-101-disk-2,size=4M,version=v2.0						
mx-samba-iso (dell)	0 Descriptions							
e la pmx-samba-vm (dell)	■' Permissions							

EXEMPLE POUR vlan 101 (client1) sur la vm Windows10 du client 1.

Èditer: Carte r	éseau				\otimes
Bridge:	vmbr0	\sim	Modèle:	Intel E1000	\sim
Tag VLAN:	101	$\hat{}$	Adresse MAC:	02:BB:E9:6B:22:9B	
Parefeu:	vlan 10	1 pour	le vlan 101	(client1) dans	le pfs
Aide			Avancé	G OK F	Reset