VLAN

Document d'exploitation Kim LAUGAUDIN

NOM Prénom

Table des matières

1.	Définition2
2.	Configuration sur le commutateur
3.	Configuration dans le Proxmox Virtual Environment

1. Définition

Un VLAN, pour Virtual Local Area Network, décrit un type de réseau local. On le traduit en français par réseau local virtuel.

Le VLAN regroupe, de façon logique et indépendante, un ensemble de machines informatiques. On peut en retrouver plusieurs coexistant simultanément sur un même commutateur réseau.

Le VLAN améliore la gestion du réseau en apportant plus de souplesse dans son administration. Il apporte davantage de sécurité en imposant, par exemple, le passage par un routeur pour la communication entre deux machines. Il optimise la bande passante, sépare les flux et réduit la diffusion du trafic.

Il existe trois différents types de réseau local virtuel : de niveau 1 (aussi appelé VLAN par port), de niveau 2 (VLAN par adresse MAC) et de niveau 3 (VLAN par adresse IP).

2. Configuration sur le commutateur

Pour notre infrastructure réseau nous possédons un commutateur Cisco SG300-28 28 ports.



Afin de pouvoir le configurer, une première fois, nous devons modifier notre adresse IP afin de nous connecter une première fois dessus.

Vous trouverez ci dessous les paramètres à rentrer dans la carte réseau :

Propriétés de : Protocole Internet ver	sion 4 (TCP/IPv4) ×
Général	
Les paramètres IP peuvent être déter réseau le permet. Sinon, vous devez appropriés à votre administrateur rés	minés automatiquement si votre demander les paramètres IP eau.
Obtenir une adresse IP automati	quement
• Utiliser l'adresse IP suivante :	
Adresse IP :	192.168.1.1
Masque de sous-réseau :	255 . 255 . 255 . 0
Passerelle par défaut :	192.168.1.254
Obtenir les adresses des serveu	rs DNS automatiquement
Utiliser l'adresse de serveur DNS	suivante :
Serveur DNS préféré :	· · · ·
Serveur DNS auxiliaire :	· · ·
🗌 Valider les paramètres en quitta	nt Avancé
	OK Annuler

Une fois ces paramètres enregistrés, il faut alors se connecter à l'aide d'un câble RJ45 au commutateur Cisco.

Il faut alors ouvrir un navigateur Web et se connecter à l'adresse suivante : <u>http://192.168.1.254</u>

Ce lien nous redirige vers l'interface Web du commutateur, où nous pourrons alors modifier son mot de passe administrateur dans un premier temps.

Please change your passwo	rd from the default settings for better protection of your network
The minimum requirements a • Cannot be the same as the • Cannot be the same as the • Minimum length is 8. • Minimum number of charac	are as follows: user name. current password. :ter classes is 3. Character classes are upper case, lower case, numeric, and special characters.
New Password Configuration	n
Old Password:	
New Password:	
Confirm Password:	
Password Strength Meter:	Below Minimum

Par la suite, nous avons changé son adresse IP fixe.

Nous pouvons dès lors passer à la création de nos VLANs par ports, car son avantage principal est qu'il permet une étanchéité maximale des VLANs. Une attaque extérieure ne pourra se faire qu'en branchant le PC pirate sur un port tagué. Le pirate a donc besoin d'avoir accès au commutateur pour pénétrer le VLAN. Nous avons tout d'abord créé des agrégations de liens pour nos Proxmox Virtual Environment et Proxmox Backup Server, pour se faire, nous avons créé des Linux Bond sur nos Proxmox et avons créé des LAGs sur notre commutateur :

LAG:	1 🗸	
LAG Name:	LAG_PVE	(7/64 Characters Used)
LACP:	Enable	
Port List:	LAG Members:	
GE5	▲ GE1 ▲	
GE6	GE2	
GE7	GE3	
GE8	GE4	
GE9		
GE10		
GE11		
GE12		
		<i>.</i>
<u></u>		
Apply	Close	

LAG 1 pour le Proxmox VE sur le commutateur

Name:	bond0	Autostart:	
IPv4/CIDR:		Slaves:	eno1 eno2 eno3 eno4
Gateway (IPv4):		Mode:	LACP (802.3ad)
IPv6/CIDR:		Hash policy:	~
Gateway (IPv6):		bond-primary:	
		Comment:	

Linux Bond dans Proxmox VE

Nous avons alors répété l'opération pour Proxmox BS.

```
NOM Prénom
```

Nous avons alors défini l'état de nos ports : s'ils sont en Access ou en Trunk :

nte	rface Se	ttings					
Inte	rface Settin	g Table					Showing 1-28 of 28 All 💙 pe
Filte	er: Interface	Type equal	is to Port 🗸	Go			
	Entry No.	Interface	Interface VLAN Mode	Administrative PVID	Frame Type	Ingress Filtering	
0	1	GE1	Trunk	1	Admit All	Enabled	
0	2	GE2	Trunk	1	Admit All	Enabled	
0	3	GE3	Trunk	1	Admit All	Enabled	
0	4	GE4	Trunk	1	Admit All	Enabled	
0	5	GE5	Access	10	Admit All	Enabled	
0	6	GE6	Access	10	Admit All	Enabled	
0	7	GE7	Trunk	1	Admit All	Enabled	
0	8	GE8	Trunk	1	Admit All	Enabled	
0	9	GE9	Trunk	1	Admit All	Enabled	
0	10	GE10	Trunk	1	Admit All	Enabled	
0	11	GE11	Access	20	Admit All	Enabled	
0	12	GE12	Access	20	Admit All	Enabled	
0	13	GE13	Access	40	Admit All	Enabled	
0	14	GE14	Access	40	Admit All	Enabled	
0	15	GE15	Access	40	Admit All	Enabled	
0	16	GE16	Trunk	1	Admit All	Enabled	
0	17	GE17	Trunk	1	Admit All	Enabled	
0	18	GE18	Truck	1	Admit All	Enabled	

Les ports Trunk vont envoyer les paquets taggés destinés aux ports en mode Access.

Un port en mode Access a accès à un VLAN ce qui veut dire qu'il ne recevra que les paquets qui lui sont destinés.

Nous devons alors nous rendre dans l'onglet "Gestion des VLAN" puis "Créer un VLAN" :

Cr	éer un VLA	AN	
Та	ble VLAN		
	ID de VLAN	Nom du VLAN	Туре
C	1		Par défaut
	10	VLAN_MZ	Statique
	20	VLAN_DMZ	Statique
	32	VLAN_INFO	Statique
	40	VLAN_SLAM	Statique
	99	VLAN_WAN	Statique
	Ajouter	Modifier	Suppr.

NOM Prénom

BTS SIO SISR

6

Le VLAN 1 est le VLAN administratif et il est fortement déconseillé de le modifier.

Nous avons alors créé 5 VLANs :

- VLAN 10 : VLAN_MZ pour notre Proxmox Virtual Environment
- VLAN 20 : VLAN_DMZ pour notre Proxmox Backup Server
- VLAN 32 : VLAN_INFO pour un accès total à l'infrastructure
- VLAN 40 : VLAN_SLAM pour un accès à leur site hébergé ainsi qu'à internet
- VLAN 99 : VLAN_WAN pour l'accès internet

Une fois créés, nous devons attribuer nos VLANs à nos ports.

Pour ce faire, nous devons nous rendre dans l'interface "Ports vers VLAN" et y sélectionner le VLAN que l'on souhaite attribuer aux ports

Small Business							_	_	_							ci	sco L	angue:	Franç	ais	~	Se déc	onnecter	À propo	os de	Aide
cisco SG300-28 Con	nmutateur admi	nistr	able	e 28	por	ts G	igat	oit																		
Mise en route	Port vers VI AN																									1
 État et statistiques 																										
 Administration 					-					- 6																
 Gestion des ports 	Filtre: ID de VLAN e	stegal		V EI	iype o	interta	ce est	egal a	Port)K															
 Port intelligent 	Interface	GE1	G 10	iE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10	GE11	GE12	GE13	GE14	GE15	GE16	GE17	GE18	GE19	GE20	GE21	GE22	GE23 GE	=24	
 Gestion des VLAN 	Accès		20																							
Paramètres VLAN par défaut	Liaison		30					ŏ		ŏ									ŏ		õ					
Créer un VLAN	Général		40	6																						
Paramètres d'interface	Client			0																						
Port vers VLAN	Interdit	Õ	Õ	0	Õ	0	Õ	Õ	0	Õ	0	Õ	0	Õ	Õ	Õ	Õ	Õ	Õ	0	Õ	Õ	Õ	0		
Appartenance VLAN des ports Paramètres GVPP	Exclu																									
Groupes VLAN	Balisé	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 (
VLAN voix	Non balisé																							•		
 Accès VLAN TV port multidiffusion 	VLAN TV multidiffusion																									
 VLAN TV port client multidiffusion 	PVID																									
 Protocole STP 	Interface	0505	0500	0507	0500																					
 Tables d'adresses MAC 	Interiace Accès	GE25	GE20	GEZI	GE28																					
 Multidiffusion 	Acces																									
 Configuration IP 	Cápáral																									
Sécurité	Client																									
 Contrôle d'accès 	Interdit	0	0	õ	0																					
 Qualité de service 	Exclu	0	0	0	ŏ																					
▶ SNMP	Balisé	ŏ	0	0	õ																					
	Non balisé																									
	VLAN TV multidiffusion	ő	ő	ő	õ																					
																										•
© 2010-2013 Cisco Systems, Inc. Tous dr	oits réservés.																									

NOM Prénom

Ci-dessous, l'attribution du VLAN_MZ pour les ports du commutateur :

	quais	to 10	✓ AN	ID Inter	face Ty	pe equ	als to	Port V	G	0														
Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10	GE11	GE12	GE13	GE14	GE15	GE16	GE17	GE18	GE19	GE20	GE21	GE22	GE23	GE24
Access					10							10	10		101/					10				
Trunk			۲	00			(6)			(1)						10	۲					۲		<u>(i)</u>
General																								
Customer																								
Forbidden	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Excluded	۲	۲	۲	۲	0	0	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲
Tagged	0	0	0	0			0	0	0	0						0	0	0	0			0	0	0
Untagged	0	0	0	0	۲	۲	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Multicast TV VLAN					0	0					0	0	0	0	0					0	0			
PVID					53	12																		
Interface	GE25	GE26	GE27	GE28																				
Access																								
Trunk	۲		۲	(0)																				
General																								
Customer																								
Forbidden	0	0	0	0																				
Excluded	۲	۲	۲	۲																				
Tagged	0		0	0																				
Untagged	0	0	0	0																				
Multicast TV VLAN		0																						

Configuration pour les ports

Filter: VLAN ID e	quals t	0 10	• AN	ID Inte	rface T)	pe equ	als to	LAG 🗸
Interface	1	2	3	4	5	6	7	8
Access								
Trunk	(8)	(6)	(8)	100	(10)	(0)	100	۲
General								
Customer								
Forbidden	0	0	0	0	0	0	0	0
Excluded	0	۲	۲	۲	۲	۲	۲	۲
Tagged	۲	0	0	0	0	0	0	Ö
Untagged	0	0	0	0	0	0	0	0
Multicast TV VLAN								
PVID								

Configuration pour les LAG

Nous avons alors effectué cette opération pour chaque VLAN respectivement avec des accès limités.

Nous avons alors effectué cette opération pour chaque VLANs créés précédemment.

Les VLANs du commutateur étant maintenant configurés, passons à la configuration dans le Proxmox Virtual Environment.

3. Configuration dans le Proxmox Virtual Environment

Vient alors la configuration dans Proxmox Virtual Environment, nous allons alors créer des Linux Bridge (VMBR), qui sont des cartes réseaux virtuelles fonctionnant comme des commutateurs.

Nous avons donc créé 5 VMBRs :

Create: Linux B	ridge		\otimes
Name: IPv4/CIDR: Gateway (IPv4): IPv6/CIDR: Gateway (IPv6):	vmbr10	Autostart: VLAN aware: Bridge ports: Comment:	bond0.10 VLAN_MZ
Help			Advanced Create

L'option "Bridge ports" est assignée au bond0, qui est notre agrégation de lien, et ".10" permet de taguer les paquets dans le VLAN 10.

Pour le VLAN_INFO, nous avons attribué une adresse afin de se connecter au Proxmox dans le bon VLAN, ainsi qu'une adresse de routage afin que Proxmox ait accès à internet pour les mises à jour :

Create: Linux B	ridge		\otimes
Name: IPv4/CIDR: Gateway (IPv4): IPv6/CIDR: Gateway (IPv6):	vmbr32 192.168.32.50/24 192.168.32.1	Autostart: VLAN aware: Bridge ports: Comment:	bond0.32 VLAN_INFO
Help			Advanced Create

Voici alors notre configuration réseau pour le Proxmox VE :

Create \lor	Revert Edit	Remove	Apply C	onfiguration				
Name ↑	Туре	Active	Autos	VLAN aware	Ports/Slaves	Bond Mode	CIDR	Gatev
bond0	Linux Bond	Yes	Yes	No	eno1 eno2	LACP (802.3		
eno1	Network De	Yes	Yes	No				
eno2	Network De	Yes	Yes	No				
eno3	Network De	Yes	Yes	No				
eno4	Network De	Yes	Yes	No				
vmbr10	Linux Bridge	Yes	Yes	No	bond0.10			
vmbr20	Linux Bridge	Yes	Yes	No	bond0.20			
vmbr32	Linux Bridge	Yes	Yes	No	bond0.32		192.168.32.50/	192.1
vmbr40	Linux Bridge	Yes	Yes	No	bond0.40		192.168.40.50/	
vmbr99	Linux Bridge	Yes	Yes	No	bond0.99			

Nous devons alors créer une machine virtuelle pfSense et une machine maître afin de servir de pare-feu et gérer les routages de nos VMBRs.

Pour ce faire, nous devons attribuer chaques VMBRs créés précédemment à notre machine :

Summary	Add V Remove Edit	Disk Action \lor Revert	
Console	Memory	4.00 GiB	
Hardware	Processors	2 (1 sockets, 2 cores)	
Cloud-Init	BIOS	Default (SeaBIOS)	
Options	Display	Default	
Task History	S Machine	Default (i440fx)	
	SCSI Controller	Default (LSI 53C895A)	
Monitor	O CD/DVD Drive (ide2)	none,media=cdrom	
🖺 Backup	Hard Disk (virtio0)	datastorage:vm-119-disk-0,size=32G	
Replication	Retwork Device (net0)	virtio=52:55:20:F5:E0:4E,bridge=vmbr99	
Snapshots	➡ Network Device (net1)	virtio=0E:4B:45:B9:F5:8A,bridge=vmbr10	
♥ Firewall ▶	Retwork Device (net2)	virtio=1E:8F:E5:86:D7:09,bridge=vmbr20	
Permissions	Retwork Device (net3)	virtio=76:4B:B8:4C:7E:7C,bridge=vmbr32	
		virtio=EA:4A:01:20:16:FA,bridge=vmbr40	

Pour la machine maître :

rtual Machine 115 (DebianMaster) on node 'M2L'		Start	🖒 Shutdown 🗸	>_ Console $ $ \vee	More \lor	Hel
Summary	Add ~ Remove Edit	Disk Action V Revert					
Console	m Memory	4.00 GiB					
Hardware	Processors	2 (1 sockets, 2 cores)					
Cloud-Init	BIOS	Default (SeaBIOS)					
Options	🖵 Display	Default					
Tack History	✿ Machine	Default (i440fx)					
i lask i listory	SCSI Controller	VirtIO SCSI					
Monitor	Hard Disk (virtio0)	datastorage:vm-115-disk-0,size=30G					
Backup	Retwork Device (net0)	virtio=46:CA:14:D0:0C:3E,bridge=vmbr10					
Replication	Retwork Device (net1)	virtio=BE:ED:1F:51:85:96,bridge=vmbr20					
Snapshots		virtio=5E:6E:16:FB:99:31,bridge=vmbr32					
Firewall >	Retwork Device (net3)	virtio=CA:81:5F:AD:24:CE,bridge=vmbr40					
Permissions							

Une fois notre pfSense installé et prêt à configurer, nous nous connectons via la machine maître et commençons par ajouter les interfaces de nos VMBRs :

Interfaces / Inte	erface Assignments	Lut. 😮
Interface Assignments	Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs	
Interface	Network port	
WAN	vtnet0 (52:55:20:f5:e0:4e)	
VLAN_MZ	vtnet1 (0e:4b:45:b9:f5:8a)	
VLAN_DMZ	vtnet2 (1e:8f:e5:86:d7:09)	
VLAN_INF0	vtnet3 (76:4b:b8:4c:7e:7c)	
VLAN SLAM	vtnet4 (ea:4a:01:20:16:fa)	

Nous devons alors, pour chaque interfaces, les autoriser à fonctionner avec le bouton "Enable interface", les renommer, leur donner un adresse IPv4 ainsi qu'une ip de routage pour le WAN afin que la connexion à Internet soit établie :

General Configur	ation
Enable	Enable interface
Description	WAN Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4 v
IPv6 Configuration Type	None 🗸

ici, pour l'interface du WAN

Chaque interfaces possédant sa propre adresse, nous avons fait comme suit :

- VLAN_MZ : 192.168.10.1
- VLAN_DMZ : 192.168.20.1
- VLAN_INFO : 192.168.32.1

```
NOM Prénom
```

• VLAN_SLAM : 192.168.40.1

Nous reste alors l'interconnexion entre nos VLANs et le WAN pour donner accès à Internet, pour ce faire nous allons dans "Firewall", "NAT" et "Outbound" puis nous passons en mode manuel :

d 1:1	Outbound NPt			
d NAT M	lode			
Mode	0	0	0	0
	Automatic outbound	Hybrid Outbound	Manual Outbound	Disable Outbound
	NAT rule generation.	NAT rule generation.	NAT rule generation.	NAT rule generation.
	(IPsec passthrough	(Automatic	(AON - Advanced	(No Outbound NAT
	included)	Outbound NAT +	Outbound NAT)	rules)

Puis nous avons créé nos règles de transitions d'IPv4 propre à chaque VLANs :

М	Mappings										
		Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
	~	WAN	192.168.10.0/24	*	*	*	WAN address	*	*	VLAN_MZ to WAN	
	~	WAN	192.168.20.0/24	*	*	*	WAN address	*	*	VLAN_DMZ to WAN	∥ □
	~	WAN	192.168.32.0/24	*	*	*	WAN address	*	*	VLAN_INFO to WAN	
	~	WAN	192.168.40.0/24	*	*	*	WAN address	*	*	VLAN_SLAM to WAN	
									1 Add	1 Add 🛅 Delete	Save

Il nous reste une dernière étape qui est la création de règles dans le pare-feu, il faut se rendre dans "Firewall" et "Rules" :

Firewall / Rules / WAN										<u>Lui</u> ([]	0	
Floating WAN VLAN_MZ VLAN_INFO VLAN_SLAM												
Rules	(Drag to	o Change	Order)									
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
	States 0 /0 B	Protocol IPv4+6 *	Source WAN address	Port *	Destination	Port *	Gateway *	Queue none	Schedule	Description	Actions) 11

ici une règle sur le réseau WAN permettant de tout autoriser en IPv4 et IPv6 afin de tester que le réseau sort bien

Plusieurs options sont disponibles lors de la création d'une règle :

Edit Firewall Rule	•								
Action	Pass	~							
	Choose what to do with p	Choose what to do with packets that match the criteria specified below.							
	returned to the sender, 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.						
Interface	WAN	~							
	Choose the interface from	n which packets must come to ma	tch this rule.						
Address Family	IPv4+IPv6	~							
	Select the Internet Protoc	ol version this rule applies to.							
Protocol	Any	~							
	Choose which IP protoco	I this rule should match.							
Source									
Source	Invert match	WAN address	~	Source Address	/ ~				
Destination									
Destination	Invert match	any	~	Destination Address	/ ~				

- Action : permet de choisir entre autoriser ou bloquer
- Disabled : permet de désactiver la règle
- **Interface :** choix de l'interface sur laquelle la règle va s'appliquer
- Adress Family : IPv4, IPv6 ou les 2
- Protocol : choix du protocol, tel que UDP ou TCP
- Source : adresse ou réseau de provenance de notre règle
- **Destination :** adresse ou réseau de destination de notre règle

Les règles étant maintenant créées selon nos besoins, le réseau des VLANs est configuré. Il faut cependant noter qu'il faut créer des règles et les adapter à chaque besoin, l'exemple de règle pour le WAN vu précédemment n'était que pour tester le bon transit des paquets vers Internet.

NOM Prénom