TP DMZ et wifi publique

BTS SIO2

 \times

Lebeau

Mathéo

Intro :

Bonjour, aujourd'hui nous allons créer une DMZ ainsi qu'une zone pour le wifi publique qui viendront compléter notre wan et lan créer tout au long de notre contexte.

Pour commencer nous allons créer deux nouveaux commutateurs virtuels un DMZ et un wifi publique.



Et sur nos deux pfsense on va les ajouter.

💼 Paramètres pour SRV-Pfsense sur SRV-P-HV-ML



Ensuite on va se rendre sur l'interface web du pfsense pour ajouter nos deux nouvelles zones fraichement créer.

COMMUNITY EDITION	Interfaces 🕶	Firewall 👻	Services 🗸	VPN -	- Stat	us -	Diagnostics	▪ Help ▪		
Interfaces / Interfac	Assignments									
	WAN	-								
Interface Assignments In	LAN CARP1	eless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges	LAG	Gs
Interface			Network po	rt						
WAN			hn1 (00:1	5:5d:10:36:0)c)				*	
LAN			hn0 (00:1	5:5d:10:36:0)b)				*	Delete
Carp1			hn2 (00:1	5:5d:10:36:1	2)				*	Delete
Available network ports:			hn3 (00:1	5:5d:10:36:1	9)				*	+ Add

Pour les deux zones on sera en ip fixe pour la DMZ:

Static IPv4 Configurat	ion		
IPv4 Address	192.168.31.1	/ 24	~

Pour le wifi public :

	Statia IBv4 Configurat	ion
	IPv4 Address	192.168.32.1
Vo	oilà le résultat	
1	nterface	
	WAN	
	LAN	
	Carp1	
	DMZ	
	Wifipublique	

On va ensuite créer un serveur debian avec une nouvelle VM et on le mettra bien sur la carte réseau DMZ

Chaque nouv utiliser un cor Connexion :	el ordinateur virtuel inclut une carte réseau. Vous pouvez configurer celle-ci nmutateur virtuel ou la laisser déconnectée. DMZ	de faço
du même r	éseau en /24	
L'adresse I * quatre n * des blocs « deux-p	P est propre à une machine et peut être constituée de : ombres séparés par des points (IPv4) ; 6 de caractères hexadécimaux séparés par le caractère pints » (IPv6).	
Il est égale	ment possible d'ajouter un masque de sous-réseau au format	CIDR (par exemple « /24 »).

Si vous ne savez pas quoi indiquer, veuillez consulter l'administrateur de votre réseau. Adresse IP :

192.168.31.2

Г	
	La passerelle est une adresse IP (quatre nombres séparés pa aussi appelée le routeur par défaut. Tout le trafic qui sort du circonstances, vous n'avez pas besoin de routeur. Si c'est le connaissez pas la réponse correcte à cette question.
	Passerelle :

Pour compléter l'installation on va devoir créer une règle de pare-feu pour accepter les connexion internet vers la DMZ

DMZ	WIFIPUBLIQUE	OpenVPI	N
Port	Destination	Port	Gateway
e blocked u	ntil pass rules are ad	ded. Click th	e button to add a
			Add

Puis on va faire en sorte que toute las connexions vers la DMZ puissent accéder à internet.

Ensuite une fois bien avancé dans l'installation de debian on va ajouter le rôle serveur web.

Sélection o	les logiciels
Actuellem ensemble	ent, seul le système de base s prédéfinis de logiciels.
Logiciels à	installer :
✓ enviro	nnement de bureau Debian
🗹 GNC	OME
🗌 Xfce	e
🗆 bur	eau GNOME Flashback
🗌 КDE	Plasma
🗌 Cini	namon
🗆 MAT	ſE
🗆 LXD	E
🗆 LXQ	t
✓ serveu	ır web
🗌 serveu	IT SSH
	res usuels du système

Edit Redirect Entry							
Disabled	Disable this rule						
		<i>(</i>					
No KDK (NUT)	Disable redirection for tra	Dop't use this without therew	ah knowladaa of tha impli	iontions			
	This option is fallely needed.	. Don't use this without thorou	gir knowledge of the impli	ications			
Interface	WAN		~				
	Choose which interface this	rule applies to. In most cases	"WAN" is specified.				
Address Family	IPvA						
	Select the Internet Protocol	version this rule applies to.					
Protocol	TCP		~				
	Choose which protocol this	rule should match. In most ca	ses "TCP" is specified.				
Source	Hide Advanced						
Source	 Invert match. 	Any		~		1	~
	<u> </u>	Туре			Address/mask		
Source port range	Other 🗸	0	Other	~	0		
	From port	Custom	To port		Custom		
	Specify the source port or p 'any'). The 'to' field may be le	ort range for this rule. This is u ft empty if only filtering a sing	usually random and almos le port.	st never	equal to the destination port range	(and should u	isually be
Destination	Invert match	WAN address		~		/	~
Destination		Туре			Address/mask		
Destination and server	HTTP		НТТР	~			
Destination port range	From port	Custom	To port		Custom		
	Specify the port or port rang	e for the destination of the pa	cket for this mapping. The	e 'to' fiel	d may be left empty if only mappin	a a single port	
	opeoing the port of port ang		enerrer ane mapping.			g a enigie peri	
Redirect target IP		Address or Alias		~	192.168.31.2		
	Enter the internal ID - Jar-	Type	- the perto a p. 100 160	1 10 6	Autress		
	In case of IPv6 addresses, ir	s of the server on which to ma n must be from the same "sco	p the ports. e.g.: 192.108. pe",	1.12 for	IPV4		
	i.e. it is not possible to redire	ect from link-local addresses	scope (fe80:*) to local sco	ope (::1)			
Redirect target port	HTTP		~				
iteaneer target port							

Une fois l'installation terminée on va créer une règle de redirection :

On peut alors tester d'accéder au serveur debian via un navigateur on accède donc bien au debian en passant par le réseau WAN

▲ Non sécurisé 172.16.16.67		
	debian	Apache2 Debian Default Page

Voilà qui conclut la partie DMZ

nous allons maintenant passer au wifi publique pour que de l'extérieur on n'a uniquement accès à internet et pas aux serveurs.

. 1

0

En ce sens on va déjà faire en sorte que la vm sur la carte réseau wifi publique ai accès à internet avec un adressage ip correspondant.

Obtenir une adresse IP automatiq	uement
Otiliser l'adresse IP suivante :	
Adresse IP :	192 . 168 . 32 . 2
Masque de sous-réseau :	255 . 255 . 255 . 0
Passerelle par défaut :	192.168.32.1
Obtenir les adresses des serveurs	DNS automatiquement
O Utiliser l'adresse de serveur DNS s	suivante :

Ouliser radresse de serveur DNS s	uivante		
Serveur DNS préféré :	192 .	168.	32
	_	_	_
Convolut DMC publication (- W	

On a désormais accès à internet sur le réseau wifi publique.

Pour cela on va créer un serveur sur un client windows en installer le controleur de la borne wifi que l'on va utiliser dans notre cas et qui est une ubiquiti.

Après avoir téléchargé le logiciel on va le lancer sur le windows



Ensuite il faudra attendre que la borne se configure



Une fois l'installation terminée on aura un bouton qui permet de manager la borne



On arrive et on va devoir faire quelques paramétrages.

Set Local Access Credentials

Use these credentials to locally access your Network Server. Learn More

Username		
WIFIML		
Password		
Azerty.2	0	
Confirm Password		
Azerty.2	0	
Email		
wifi@wifi.fr		C

Création d'admin local

Ensuite dans le menu devices il faudra suivre les indications et reset la borne pour pouvoir ensuite faire l'adoption.

Q Search		All (2)	Switches (0) APs (2)				U6 Lite ×			
_	Гуре	Name	Application	Status	IP Address	Uplink	Parent Device	Ch. 2.4 G	O U6 Lite		
•		U6 Lite	Network	Click to Adopt	192.168.1.20						
•		U6 Lite	Network	Click to Learn More	192.168.1.20	-	-	-		Adopt Device	

On va ensuite créer le réseau.

÷	☆ WiFi	Name	WIFI ML	
\sim	🚓 Networks	Password		Ø
9	Internet		Must have at least 8 characters.	~
<u>-</u> 6)	O VPN	Broadcasting APs (i)	● All ○ Specific ○ Groups	
O	Security	Advanced	Auto Manual	
02	속 Routing	Private Pre-Shared Keys ()		
	Ba Profiles	Hotspot 🕕	• Off Captive Portal	
<u></u>	🗃 System	Enhanced IoT Connectivity ()		
	Network 9.1.120	WiFi Band 🕕	🕑 2.4 GHz 🛛 🥑 5 GHz 🗌 6 GHz	
ΥŢ	Submit Support Ticket	Band Steering ()		
		Hide WiFi Name		
		Client Device Isolation (i)		
		Add WiFi Network Cancel		
		BSS Transition (i)		Puis la borne WIFI se

connecte après avoir reçu une ip une fois terminé on verra apparaître le wifi



Ensuite je me suis connecté sur le wifi de la borne à l'aide de mon téléphone et dans le menu devices on peut voir tous les appareils connectés.

	Name	Vendor	Connection	Network	WiFi	Experie	Technol	Channel	IP Addr	Activity	Download	Upload	24H
•	📫 21081111RG	-	U6 Lite	-	WIFI M	Excellent	2x2, WiFi 6	48 (5 GHz, 80 MHz)	192.168.32.54	12.8 Kbps	↓ 7.07 Kbps	1 5.74 Kbps	ş -
•	Mouton-eveill	-	U6 Lite	-	WIFI M	Excellent	2x2, WiFi 6	48 (5 GHz, 80 MHz)	192.168.32.55	0 bps	↓ 0 bps	1 0 bps	-

Ensuite on peut également utiliser un portail captif uniquement si le serveur wifi quant à lui est lancé.



Voilà qui conclut notre tp et nous avons maintenant accès à un wifi public mangeable via le serveur wifi pour des clients éventuels. Et nous avons également appris à créer une zone démilitarisée pour que de l'extérieur on accède uniquement au serveur web par exemple. Elle sert donc à isoler. Ces solutions permettent une meilleure sécurisation et gestions des accès extérieurs vers le parc informatique.