Dans le cadre de mes missions d'administration réseau, il m'est parfois demandé de mettre en place une DMZ (Demilitarized Zone) pour rendre des services disponibles depuis l'extérieur du réseau de manière sécurisée.

Étape 1 : Accéder à l'interface d'administration

J'ouvre mon navigateur et je saisis l'adresse. Je me connecte avec mon compte administrateur.

ZYXEL	Entrer nom d'utilisateur et mot de norte et cliquer tur	
030210	Connexion	
	nom d'utilisateur.	
	Mot de passe:	
	Mot de passe OTP:	
\bigcirc	(Uptionnel)	
	for oniciality unsuited on a state offenda.	
	Connexion	
	Note:	
	Activer les Cookies et le Javascript dans votre navigateur. Activer les Cookies et le Javascript dans votre navigateur.	
	3. Activer le Java Runtime Environment (JRE) sur votre navigateur.	
	4. Autorisez Gears is vous unilizez Google Chrome	

Étape 2 : Créer l'interface VLAN pour la DMZ

Je vais dans Configuration > **Réseau** > Interface, onglet VLAN. Je clique sur Ajouter et je configure :

- Zone : Je choisis d'intégrer ce VLAN à la Zone LAN1
- VLAN ID : 50
- Description : dmz
- Addresse IP : 192.168.50.1 /24
- DHCP : Je séléctionne DHCP Server et je définie l'adresse de début ainsi que la taille du pool d'adresse disponible. Je choisis également les serveurs DNS attribué et la durée du bail

MISE EN PLACE DE DMZ

1150210	Modifier le VLAN		2 × Berrye
036210	Afficher les paramètres avancés		
ATION	Nom de l'interface:	van50	^
infiguration rapide	Zone:	LANI 🛩 🖬	
	Port de la base:	ESC_LAN Y	
	VLAN ID:	50 (1-4094)	
000	💌 Avancé		
200 C	Description:	dmz (Optionnel)	
ection de service	Antibution d'adresses in		-
	Adresse IP:	1/2/16.50.1	
n P/MAC	Masque de sous-réseau:	255 255 205.0	
nent Couche 2	Activer le support lumP		
entrant LB	USMP Upstream		
ncation web	 IGMP downstream 		
sécurité	Paramètres de l'interface		
NM	Bande passe de sortie:	1048576 Kbps	
	💌 Avancé		
A	▼ Avancé		
sponibilité			
	Paramètre DHCP		· 1 -
teur/Groupe	DHCP:	DHCPServer v	
AP MON	Adresse de début du pool IP:	192.168.50.10 Talle ou 40 poot	
ZyMesh	Premier serveur DNS (Option):	zywall ~	
cation	Second serveur DNS (Option):	Custom Defined 🛛 88.8.8	
28 July 360 IP	3ème serveur DNS (optionnel):	None v	
Ication	Premier serveur WINS (Option):		
ur AAA Mathada	Second serveur WINS (Option):		
leat	Routeur par défaut:	VanS0 P 👻	
ote FAI	Durée du bail:	© Infrai	
noort		2 jours 0 heures (Option) 0 minutes (option)	
	💌 Avancé		+
		OK Case	

• Je sauvegarde et j'applique les changements.

Étape 3 : Définir les objets réseau

Je vais dans Configuration > Objet > Addresse/Geo IP. Je crée l'objet suivant :

- Nom : Vlan50
- Type d'adresse : SUBNET
- Réseau : 192.168.50.0 /24

	Adresse	Groupe d'adresse	Geo IP					
	Cont	Modifier une règle d'Ac	tresses VLan50				? ×	
	Te.							
		Nom:	VLan50					D.W.
		Type d'adresse:	SUBNET	~				Keterence
		Réseau:	192.168.50.0					
		Masque réseau:	255.255.255.0					
								0
								0
								1
								0
								0
								0
								0
								8
								Affichage 1 - 14 dr
						0×	Canad	
						OK.	Concor	
Adresse/Geo IP								

Étape 4 : Configurer la règle NAT (Virtual Server)

J'ai ensuite créé une règle qui permet d'accéder en HTTP à un serveur qui se trouve sur le VLAN

Je vais dans Configuration > **Réseau** > NAT et je clique sur Ajouter. Je configure :

- Interface d'entrée : FO
- IP Source : any
- IP Externe : Mon IP publique
- IP Interne : L'IP sur serveur sur le VLAN50
- Service : HTTP
- Type de mappage de port : Service

Je coche Activer la boucle avec retour NAT et je valide.

7VXFL USG210		📝 Edit NAT		2 X	🕞 🖬 🖧 💯 👔 👔 Bienwenue Jadmin <u>Disconnexion</u>
	_	🛅 Créer un nouvel objet -			
CONTRACTOR CONTRACTO	Active Configuration Configuration	ter MA Toronkies Clearance Toronkies Clearance Toronkies Clearance Monte Clearance Monte Clearance Monte Ange Non da la rège: Nye de mapoga de port Classification: Placeme: Plac	accompletity Image: show where Image: show where <th>Protocole</th> <th>Image: The second se</th>	Protocole	Image: The second se
		fransher stockt		Cancel	
			Applquer Réinitialiser		

Étape 5 : Créer la règle de pare-feu

Je vais dans Configuration > **Règle de sécurité** > Politique de contrôle. Je clique sur Ajouter et je configure :

- Depuis : WAN → Vers : LAN1
- Source : any
- Destination : VLan50
- Service : HTTP

- Action : Allow
- Trafic log correspondant : Je choisis log afin de journaliser connections

	Stratégie										
NHGURATION	Afficher le fitre	_	_	_		_	_	_	_		
	Modifier règle1										?
	Créer un nouvel objet •										
	Activer										
	Nom:	WAN_IN_HTTP]								
	Description:		(Optionn	el)							
	Depuis:	WAN ¥									
	À:	LAN1 ~									
	Source:	any 👻									
	Destination:	VLan50 ¥									
	Service:	HTTP									
Politique de contrôle	Utilisateur:	any 👻									
• ADP	Hanification:	none	1								
Cloud CNM	Trafic los comercondant:	diow •	1								
	indicitog conceptionalit.	~ ~									
	Profil UTM										
	Application Patrol:	none Y	log:	by profile	~						
	Filtrage de contenu:	none	log:								
	- DP:	none	100:	by profile	•						
	Anti-wros:	none	log:		*						
	Inspection SSI:	none	log								
											OY Cased
			_								UK Cancel
	24 🥥 SSL VPN to	Device #SSL	VPN	ZyWALL	any	any	any	any	none	allow no	

Je déplace la règle au-dessus des règles par défaut et j'applique.

Étape 6 : Tester l'accès externe

Depuis une connexion extérieure j'accède à mon IP public et je vérifie que le service est bien affiché.



Conclusion

Dans cette procédure, j'ai pu mettre en place une DMZ sur VLAN, en assurant la publication sécurisée d'un service depuis l'extérieur. J'ai ainsi validé plusieurs compétences importantes.

Compétences validées

- Mettre à disposition des utilisateurs un service informatique
- Gérer le patrimoine informatique
- Répondre aux incidents et aux demandes d'assistance