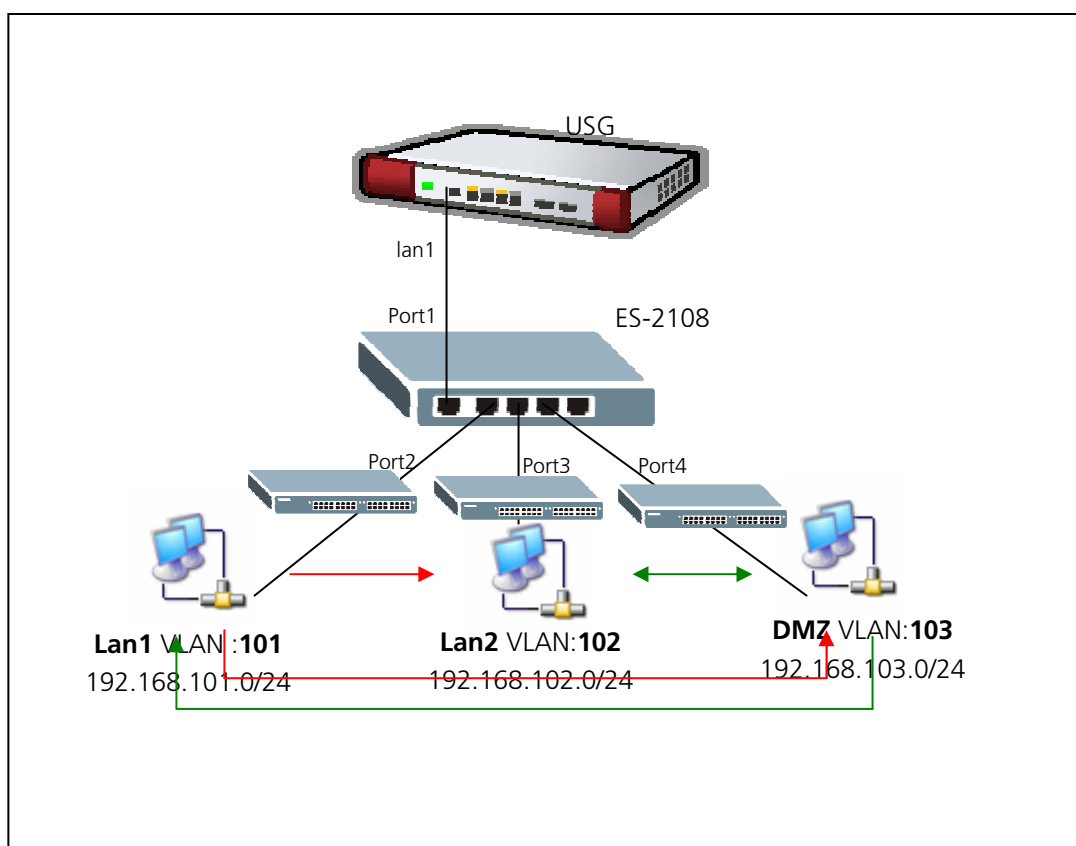


### Configuration du Virtual LAN et des zones avec le ZyWALL USG

Un VLAN est un sous réseau de niveau 2, qui peut partager le même réseau avec d'autres VLANs. Les commutateurs sont chargés d'isoler chaque VLAN, ce qui est utile pour sécuriser les échanges. Le protocole 802.1q est utilisé pour marquer les trames Ethernet et indiquer le VLAN auxquels elles appartiennent.

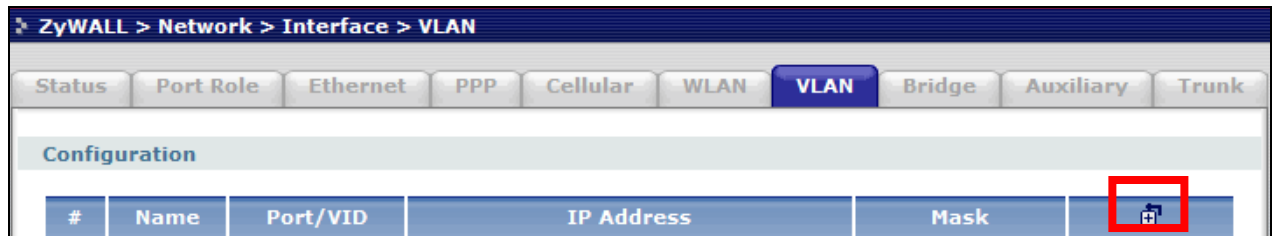
Cet exemple démontre comment utiliser la fonction "Virtual LAN" avec un commutateur ZyXEL (comme par exemple le ES-2108) et un ZyXEL USG. Chaque département appartient à une zone unique, ces zones sont au moyen de règles placées sur Firewall USG ouvertes ou fermées entre elle. Pour chaque zone une configuration d'une Policy route est nécessaire afin que les vlan ont un accès Internet sortant.



Ligne rouge = le trafic du réseau est bloqué avec des règles Firewall

## Configuration de l'USG

Ajouter un **VLAN** avec **Add**.

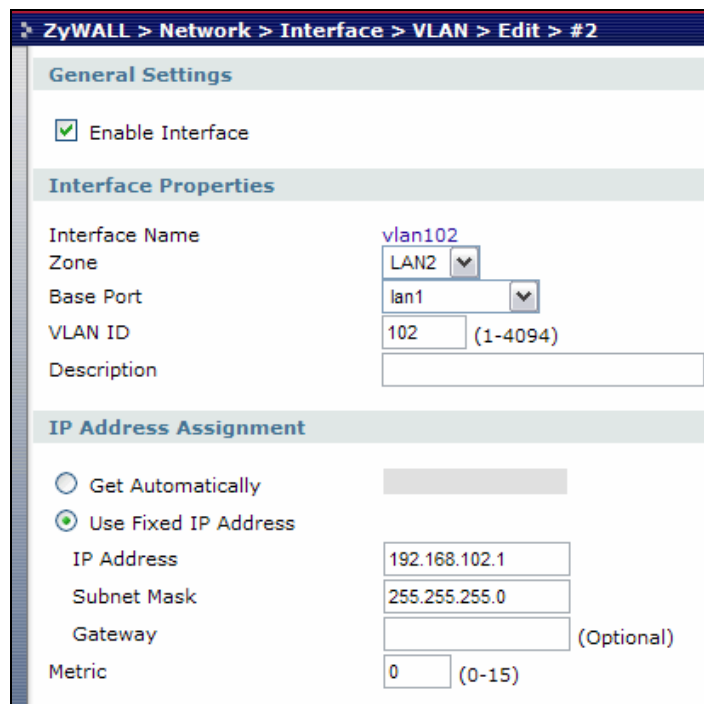


Ajout du premier VLAN:

Nom de l'Interface **vlan101**, Zone = **LAN1**, Based Port = **lan1**, VLAN ID = **101**. L'Interface reçoit l'adresse IP **192.168.101.1** avec le Masque **255.255.255.0**.

Ajout du deuxième VLAN:

Nom de l'Interface **vlan102**, Zone = **LAN2**, Based Port = **lan1**, VLAN ID = **102**. L'Interface reçoit l'adresse IP **192.168.102.1** avec le Masque **255.255.255.0**.



**ZyWALL > Network > Interface > VLAN > Edit > #2**

**General Settings**

☒ Enable Interface

**Interface Properties**

Interface Name: **vlan102**  
Zone: **LAN2**  
Base Port: **lan1**  
VLAN ID: **102** (1-4094)  
Description:

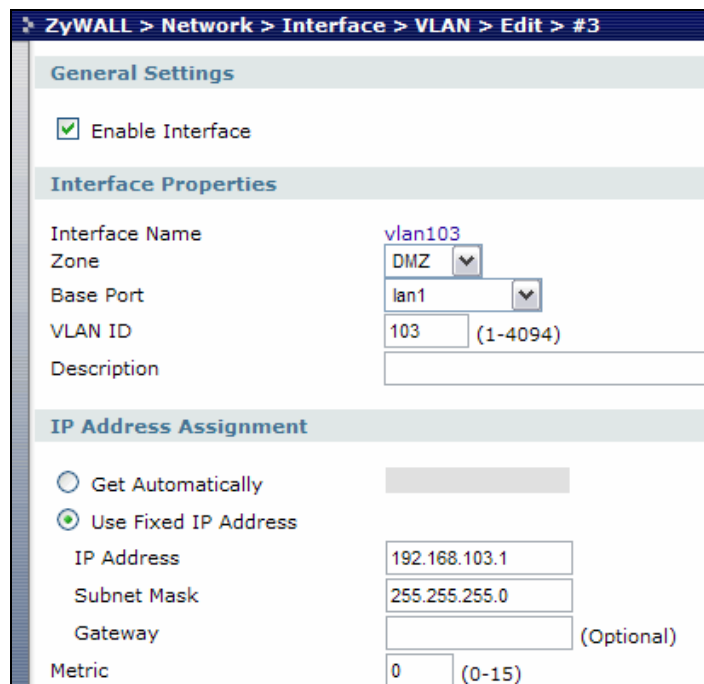
**IP Address Assignment**

☐ Get Automatically  
☒ Use Fixed IP Address

IP Address: **192.168.102.1**  
Subnet Mask: **255.255.255.0**  
Gateway: (Optional)  
Metric: **0** (0-15)

Ajout du troisième VLAN:

Nom de l'Interface **vlan103**, Zone = **DMZ**, Based Port = **lan1**, VLAN ID = **103**. L'Interface reçoit l'adresse IP **192.168.103.1** avec le Masque **255.255.255.0**.



**ZyWALL > Network > Interface > VLAN > Edit > #3**

**General Settings**

☒ Enable Interface

**Interface Properties**

Interface Name: **vlan103**  
Zone: **DMZ**  
Base Port: **lan1**  
VLAN ID: **103** (1-4094)  
Description:

**IP Address Assignment**

☐ Get Automatically  
☒ Use Fixed IP Address

IP Address: **192.168.103.1**  
Subnet Mask: **255.255.255.0**  
Gateway: (Optional)  
Metric: **0** (0-15)

Ajouter des objets pour les réseaux vlan afin de vous faciliter la tâche pour les règles de Policy et du Firewall

**ZyWALL > Object > Address > Address > Edit > #1**

**Configuration**

Name	<input type="text" value="vlan101_Netz"/>
Address Type	<input type="text" value="SUBNET"/> ▼
Network	<input type="text" value="192.168.101.0"/>
Netmask	<input type="text" value="255.255.255.0"/>

.....

**ZyWALL > Object > Address > Address > Edit > #1**

**Configuration**

Name	<input type="text" value="vlan102_Netz"/>
Address Type	<input type="text" value="SUBNET"/> ▼
Network	<input type="text" value="192.168.102.0"/>
Netmask	<input type="text" value="255.255.255.0"/>

.....

**ZyWALL > Object > Address > Address > Edit > #1**

**Configuration**

Name	<input type="text" value="vlan103_Netz"/>
Address Type	<input type="text" value="SUBNET"/> ▼
Network	<input type="text" value="192.168.103.0"/>
Netmask	<input type="text" value="255.255.255.0"/>

.....

Le trafic Internet est impossible (pour toutes les interfaces VLAN) sans l'ajout de règles Policy Routing  
Important: La coche **Enable BWM** doit être activé afin de conduire le trafic de la bande passante  
(seulement pour le trafic de données sortant Upstream).

Règle vlan101:

**Activer** la règle (avec Enable), donner un **Nom** à cette règle. Pour l'Interface **Incoming** choisir **vlan101**.  
Avec l'objet du réseau du vlan101 Changer le **Next-Hop** avec le Type **Trunk**, **Trunk** avec **WAN\_TRUNK**  
et SNAT sur **outgoing-interface**.

**ZyWALL > Network > Routing > Policy Route > Edit > #1**

---

**Configuration**

☒ Enable

Description  (Optional)

---

**Criteria**

User

Incoming  [Change...](#)

Source Address

Destination Address

Schedule

Service

---

**Next-Hop**

Type

Trunk

---

**Address Translation**

Source Network Address Translation

Port Triggering

#	Incoming Service	Trigger Service

---

**Bandwidth Shaping**

Maximum Bandwidth  Kbps

Bandwidth Priority  (1-7, 1 is highest priority)

☐ Maximize Bandwidth Usage

.....

Règle vlan102:

**Activer** la règle (avec Enable), donner un **Nom** à cette règle. Pour l'Interface **Incoming** choisir **vlan102**. Avec l'objet du réseau du vlan102 Changer le **Next-Hop** avec le Type **Trunk**, **Trunk** avec **WAN\_TRUNK** et SNAT sur **outgoing-interface**.

**ZyWALL > Network > Routing > Policy Route > Edit > #2**

---

**Configuration**

☒ Enable

Description  (Optional)

---

**Criteria**

User

Incoming  [Change...](#)

Source Address

Destination Address

Schedule

Service

---

**Next-Hop**

Type

Trunk

---

**Address Translation**

Source Network Address Translation

Port Triggering

#	Incoming Service	Trigger Service

---

**Bandwidth Shaping**

Maximum Bandwidth  Kbps

Bandwidth Priority  (1-7, 1 is highest priority)

☐ Maximize Bandwidth Usage

.....

Règle vlan103:

**Activer** la règle (avec Enable), donner un **Nom** à cette règle. Pour l'Interface **Incoming** choisir **vlan103**. Avec l'objet du réseau du vlan103 Changer le **Next-Hop** avec le Type **Trunk**, **Trunk** avec **WAN\_TRUNK** et SNAT sur **outgoing-interface**.

**ZyWALL > Network > Routing > Policy Route > Edit > #3**

---

**Configuration**

☒ Enable

Description  (Optional)

---

**Criteria**

User

Incoming  [Change...](#)

Source Address

Destination Address

Schedule

Service

---

**Next-Hop**

Type

Trunk

---

**Address Translation**

Source Network Address Translation

Port Triggering

#	Incoming Service	Trigger Service

---

**Bandwidth Shaping**

Maximum Bandwidth  Kbps

Bandwidth Priority  (1-7, 1 is highest priority)

☐ Maximize Bandwidth Usage

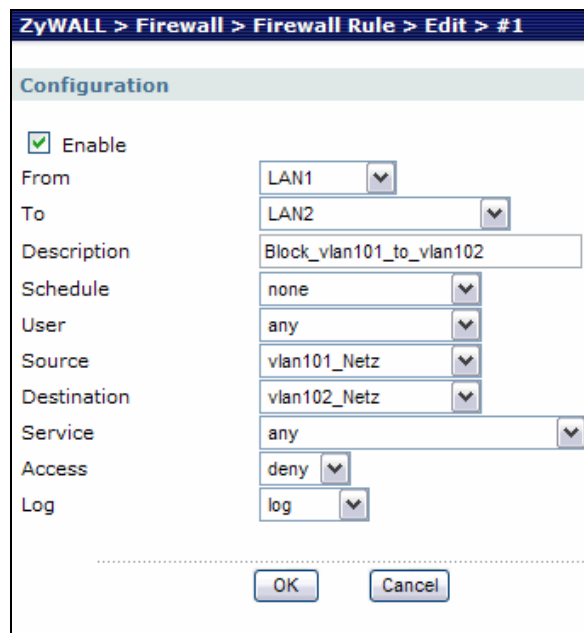
.....

Maintenant à l'aide de plusieurs règles Pare-feu vous pouvez contrôler l'accès entre les zones.  
Important : le transport des données est toujours permis si vous n'ajoutez pas de règle avec l'accès deny.

L'ordre des règles est très important, la règle **allow** (permis) doit **toujours se situer avant** les règles **deny** (fermé), sinon cette règle (permis) ne sera pas prise en considération par le Pare-feu.  
Ceci est aussi valable pour les règles de la Policy Route.

### Menu Firewall (Par-feu)

Les données entre le vlan101 et le vlan103 seront bloquées (**deny**) et enregistré dans le journal (avec **log**).



ZyWALL > Firewall > Firewall Rule > Edit > #1

**Configuration**

☒ Enable

From: LAN1

To: LAN2

Description: Block\_vlan101\_to\_vlan102

Schedule: none

User: any

Source: vlan101\_Netz

Destination: vlan102\_Netz

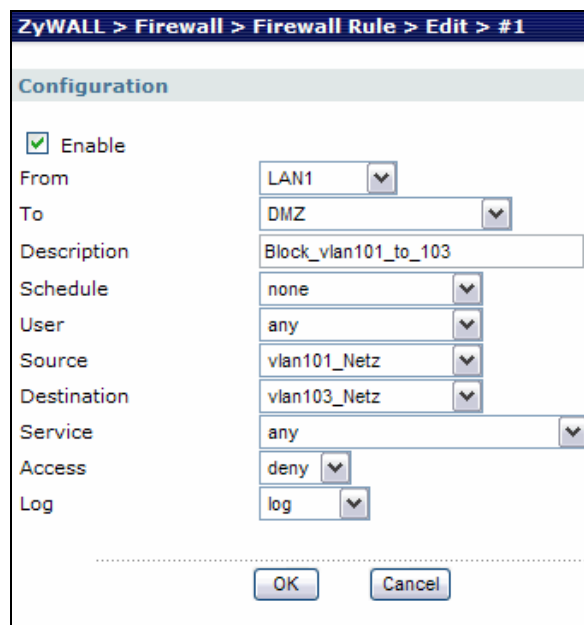
Service: any

Access: deny

Log: log

OK Cancel

Le transport des données entre le vlan101 et le vlan103 sera aussi fermé (**deny**).



ZyWALL > Firewall > Firewall Rule > Edit > #1

**Configuration**

☒ Enable

From: LAN1

To: DMZ

Description: Block\_vlan101\_to\_103

Schedule: none

User: any

Source: vlan101\_Netz

Destination: vlan103\_Netz

Service: any

Access: deny

Log: log

OK Cancel



**Configuration du ZyXEL commutateur**

Dans notre exemple de configuration le Port 1 du commutateur est branché sur le ge1 (Port1 LAN) de l'USG.

**VLAN 101:**

Ajouter dans le menu VLAN / Static VLAN: le VLAN Group ID **101** pour le réseau Sales. Le **Port 1** est placé sur **fixed** et il est marqué avec le **TX Tagging**. Le **Port 2** pour la zone lan1 est changé sur **fixed** sans marquage de TX Tagging. Tous les autres Ports sont placés sur **Forbidden** (interdiction).

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
1	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
3	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
4	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
5	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
6	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
7	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
8	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
9	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

Add Cancel Clear

VLAN 102:

Ajouter dans le menu VLAN / Static VLAN: le VLAN Group ID **102** pour le réseau Sales. Le **Port 1** est placé sur **fixed** et il est marqué avec le **TX Tagging**. Le **Port 3** pour la zone lan2 est changé sur **fixed** sans marquage de TX Tagging. Tous les autres Ports sont placés sur **Forbidden** (interdiction).

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Fixed	<input checked="" type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
3	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
4	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
5	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
6	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
7	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
8	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
9	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

VLAN 103:

Ajouter dans le menu VLAN / Static VLAN: le VLAN Group ID **103** pour le réseau Sales. Le **Port 1** est placé sur **fixed** et il est marqué avec le **TX Tagging**. Le **Port 4** pour la zone DMZ est changé sur **fixed** sans marquage de TX Tagging. Tous les autres Ports sont placés sur **Forbidden** (interdiction).

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Fixed	<input checked="" type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
3	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
4	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
5	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
6	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
7	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
8	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
9	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

Menu **VLAN Port Setting**. Attribution des VLAN ID aux Ports. Port2 avec PVID101, Port3 avec PVID102 et Port4 avec PVID103, le Port1 reste sur le PVID1.

VLAN Port Setting

VLAN Status

GVRP☐

Port isolation☐

Ingress Check☐

Port	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
*		<input type="checkbox"/>	All	<input type="checkbox"/>
1	1	<input type="checkbox"/>	All	<input type="checkbox"/>
2	101	<input type="checkbox"/>	All	<input type="checkbox"/>
3	102	<input type="checkbox"/>	All	<input type="checkbox"/>
4	103	<input type="checkbox"/>	All	<input type="checkbox"/>
5	1	<input type="checkbox"/>	All	<input type="checkbox"/>
6	1	<input type="checkbox"/>	All	<input type="checkbox"/>
7	1	<input type="checkbox"/>	All	<input type="checkbox"/>
8	1	<input type="checkbox"/>	All	<input type="checkbox"/>
9	1	<input type="checkbox"/>	All	<input type="checkbox"/>

Apply

Cancel