

Configuration Stormshield d'un tunnel VPN entre le site des Arcs et celui de Saint-Zacharie et configuration du network WIFI Ruckus

Introduction :

Nous avons acheté XX Points d'accès RUCKUS R650 pour compléter le maillage des deux magasins (HyperU Les Arcs et SuperU Saint-Zacharie).

Nous avons déjà une VM vSZ (Virtual SmartZone, IP : 192.168.20.40) contrôleur Ruckus pour manager les bornes à l'HyperU.

Nous voulons intégrer les APs Ruckus de Saint-Zacharie avec le contrôleur situé aux Arcs.

Pour ce faire nous avons dû créer un tunnel VPN entre les 2 Stormshields présent sur les différents sites, créer les objets et les networks dans ces stormshield pour configurer et tester la solution.

Outils nécessaires :

Stormshield HyperU Les Arcs : SN710 manageable via un lien http.

Stormshield SuperU Saint-Zacharie : SN310 manageable via un lien http.

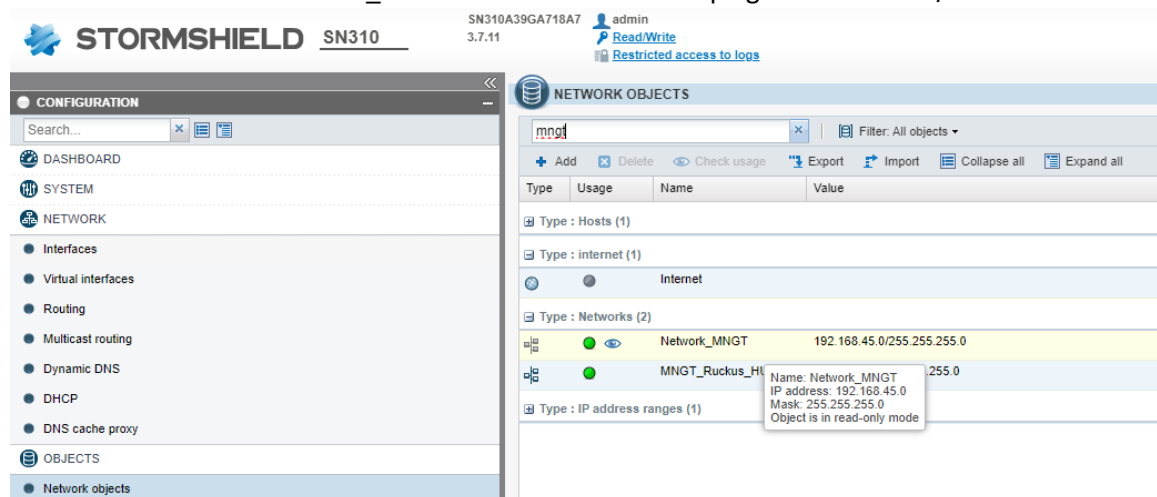
Contrôleur Ruckus : vSZ (Virtual SmartZone) est une virtual machine manageable via un lien http.

Etape 1 :

Les APs Ruckus existant à l'HyperU communique sur le VLAN 7 avec l'adressage IP suivant : 192.168.7.X/24

Création du VLAN 7 sur le SN310 de Saint-Zacharie et attribution de l'adressage IP 192.168.45.0/24
Cette plage IP doit être libre : non utilisée sur un site ou sur l'autre.

Création du network Network_MNGT dans le SN310 sur la plage 192.168.45.0/24



STORMSHIELD SN310 SN310A39GA718A7 3.7.11 admin Read/Write Restricted access to logs

CONFIGURATION

Search...

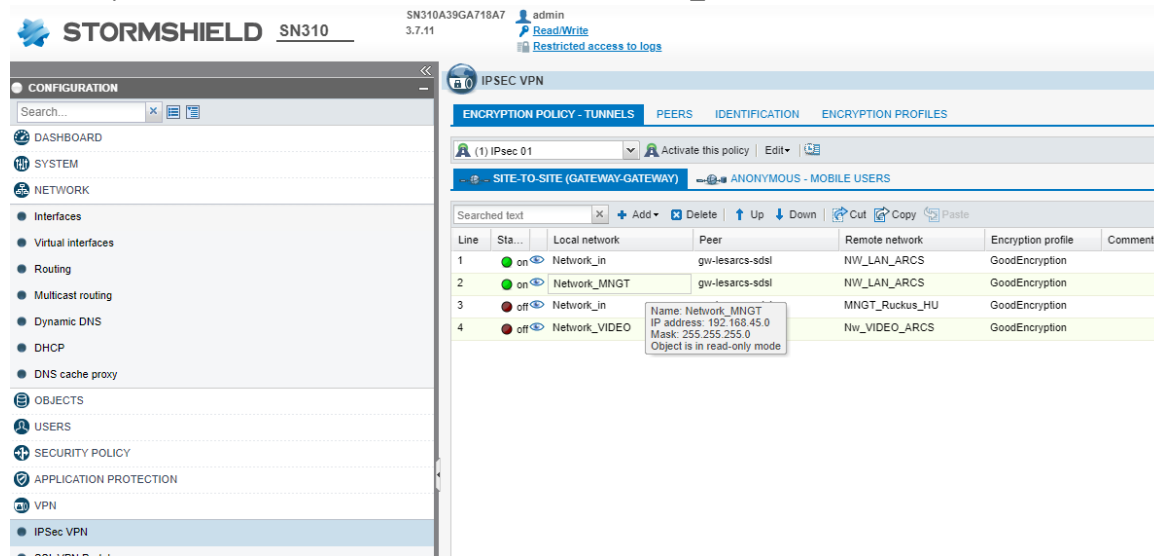
NETWORK OBJECTS

Filter: All objects

Type	Usage	Name	Value
Type : Hosts (1)			
Type : internet (1)			
		Internet	
Type : Networks (2)			
		Network_MNGT	192.168.45.0/255.255.255.0
		MNGT_Ruckus_HU	255.0
Type : IP address ranges (1)			

Name: Network_MNGT
 IP address: 192.168.45.0
 Mask: 255.255.255.0
 Object is in read-only mode

Mise en place du tunnel VPN entre les Arcs et le Network_MNGT



STORMSHIELD SN310 SN310A39GA718A7 3.7.11 admin Read/Write Restricted access to logs

IPsec VPN

ENCRYPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES

(1) IPsec 01 Activate this policy Edit

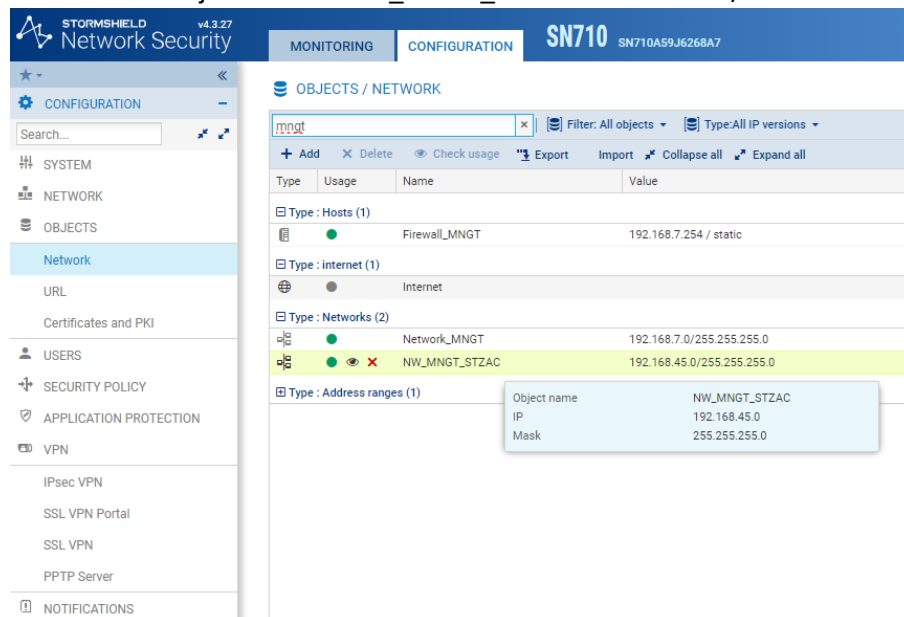
SITE-TO-SITE (GATEWAY-GATEWAY) ANONYMOUS - MOBILE USERS

Line	Sta...	Local network	Peer	Remote network	Encryption profile	Comment
1	on	Network_in	gw-lesarcs-sdsi	NW_LAN_ARCS	GoodEncryption	
2	on	Network_MNGT	gw-lesarcs-sdsi	NW_LAN_ARCS	GoodEncryption	
3	off	Network_in		MNGT_Ruckus_HU	GoodEncryption	
4	off	Network_VIDEO		Nw_VIDEO_ARCS	GoodEncryption	

Tooltip for Network_MNGT:
Name: Network_MNGT
IP address: 192.168.45.0
Mask: 255.255.255.0
Object is in read-only mode

Etape 2 :

Création de l'objet network NW_MNGT_STZAC 192.168.45.0/24 sur le SN710



STORMSHIELD Network Security v4.3.27 SN710 SN710A59J6268A7

MONITORING CONFIGURATION

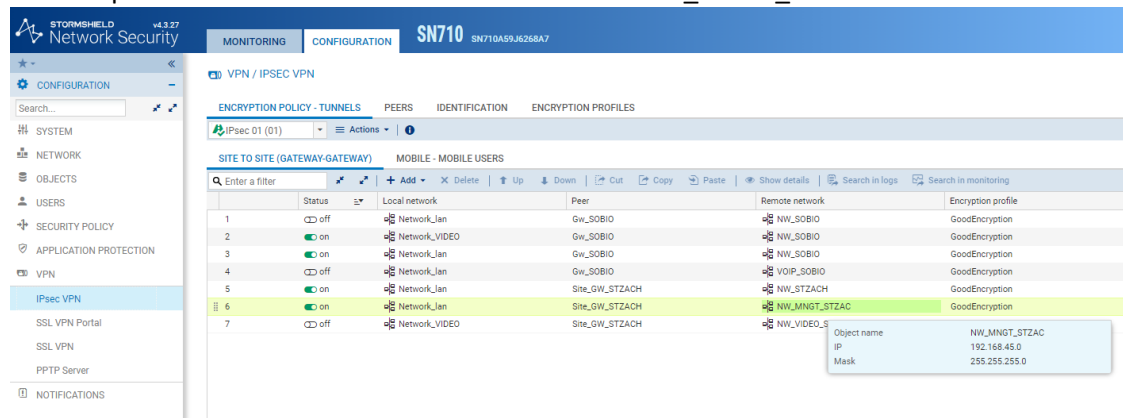
OBJECTS / NETWORK

Filter: All objects Type: All IP versions

Type	Usage	Name	Value
Type : Hosts (1)		Firewall_MNGT	192.168.7.254 / static
Type : internet (1)		Internet	
Type : Networks (2)		Network_MNGT	192.168.7.0/255.255.255.0
		NW_MNGT_STZAC	192.168.45.0/255.255.255.0
Type : Address ranges (1)			

Tooltip for NW_MNGT_STZAC:
Object name: NW_MNGT_STZAC
IP: 192.168.45.0
Mask: 255.255.255.0

Mise en place du tunnel VPN entre Saint-Zacharie et NW_MNGT_STZAC



STORMSHIELD Network Security v4.3.27 SN710 SN710A59J6268A7

MONITORING CONFIGURATION

VPN / IPsec VPN

ENCRYPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES

IPsec 01 (01) Actions

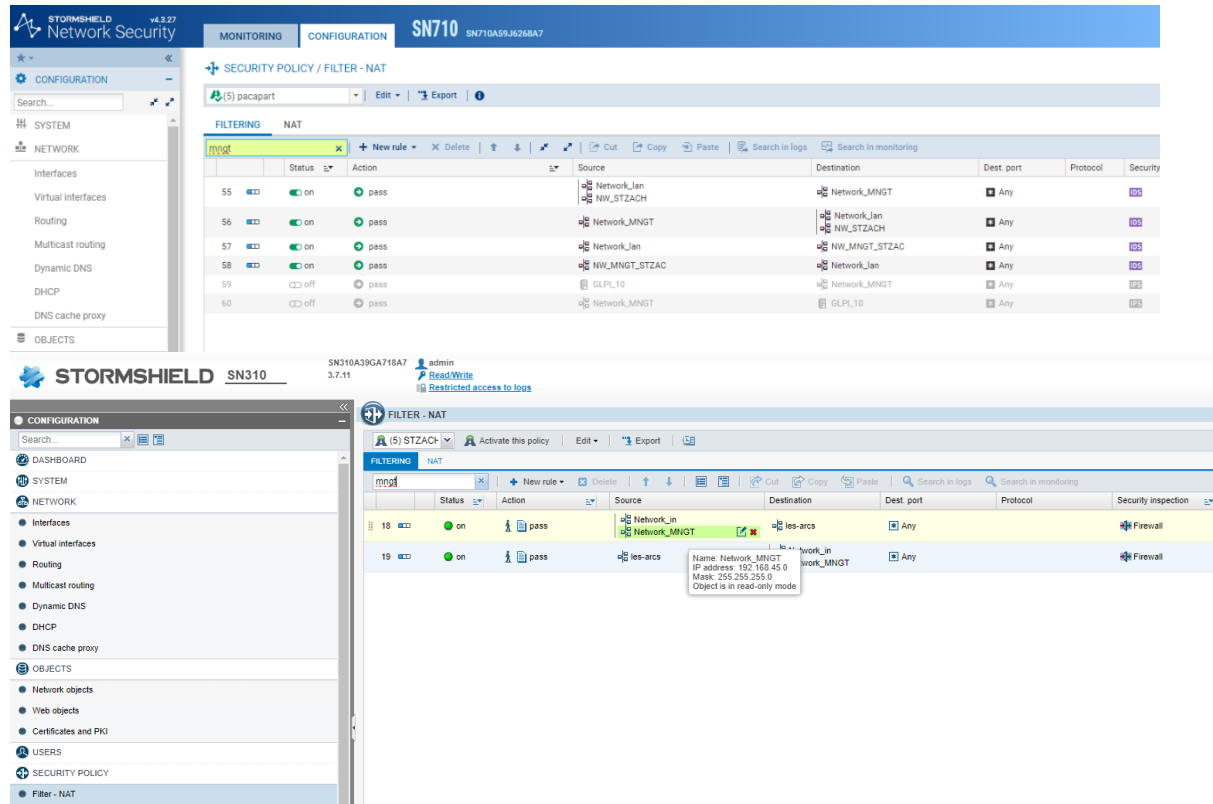
SITE TO SITE (GATEWAY-GATEWAY) MOBILE - MOBILE USERS

	Status	Local network	Peer	Remote network	Encryption profile
1	off	Network_Jan	Gw_SOBO	NW_SOBO	GoodEncryption
2	on	Network_VIDEO	Gw_SOBO	NW_SOBO	GoodEncryption
3	on	Network_Jan	Gw_SOBO	NW_SOBO	GoodEncryption
4	off	Network_Jan	Gw_SOBO	VOIP_SOBO	GoodEncryption
5	on	Network_Jan	Site_GW_STZACH	NW_STZACH	GoodEncryption
6	on	Network_Jan	Site_GW_STZACH	NW_MNGT_STZAC	GoodEncryption
7	off	Network_VIDEO	Site_GW_STZACH	NW_VIDEO_S	

Tooltip for NW_MNGT_STZAC:
Object name: NW_MNGT_STZAC
IP: 192.168.45.0
Mask: 255.255.255.0

Etape 3 :

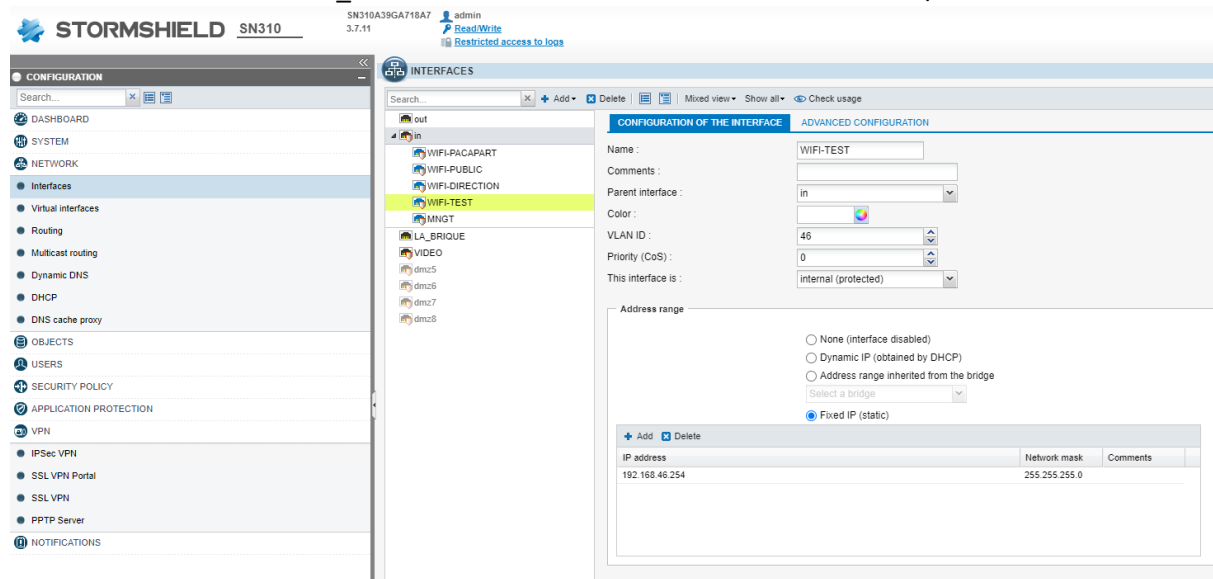
Création des règles de filtrage NAT permettant aux 2 networks de communiquer dans un sens et dans l'autre sur le SN710 et SN310



The image shows two screenshots of the Stormshield configuration interface. The top screenshot is for the SN710 device, showing the 'FILTER - NAT' configuration page. It displays a table of NAT rules with columns for Status, Action, Source, Destination, Dest. port, Protocol, and Security. Rules 55 through 60 are listed, showing various network-to-network and network-to-interface connections. The bottom screenshot is for the SN310 device, also showing the 'FILTER - NAT' configuration page. It displays a table of NAT rules with columns for Status, Action, Source, Destination, Dest. port, Protocol, and Security. Rules 10 and 19 are listed, showing connections between 'Network_in' and 'Network_MNGT' interfaces. A tooltip for rule 19 indicates that the 'Network_MNGT' object is in read-only mode.

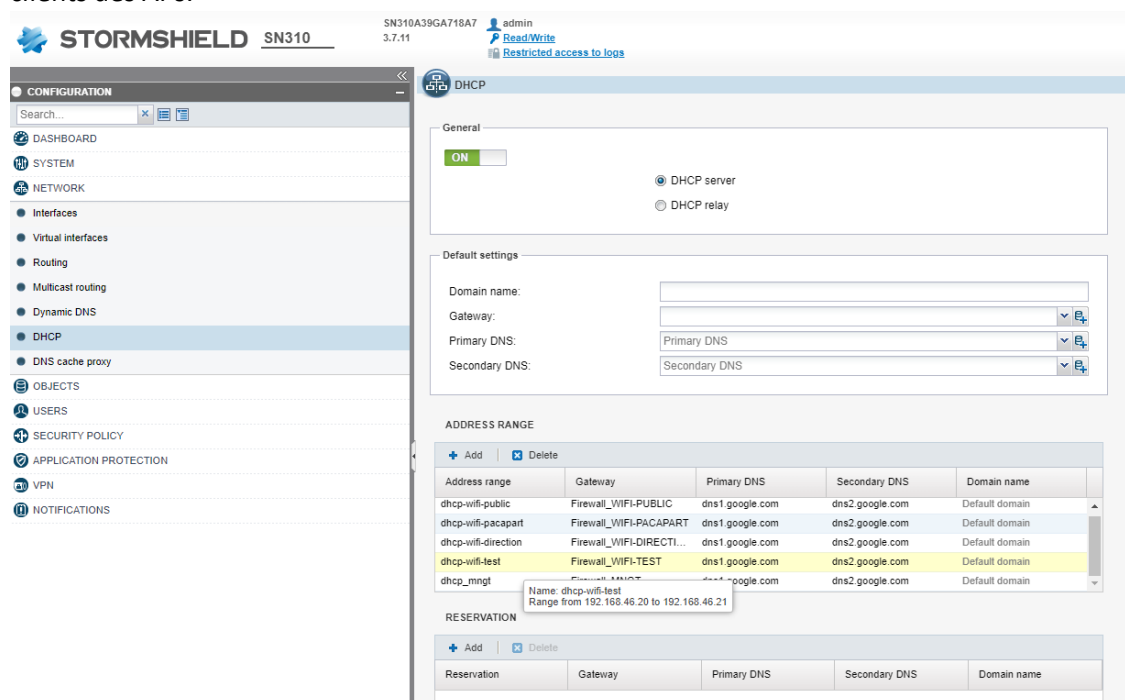
Etape 4 :

Création de l'interface WIFI_TEST sur le SN310 avec l'adresse 192.168.46.254/24



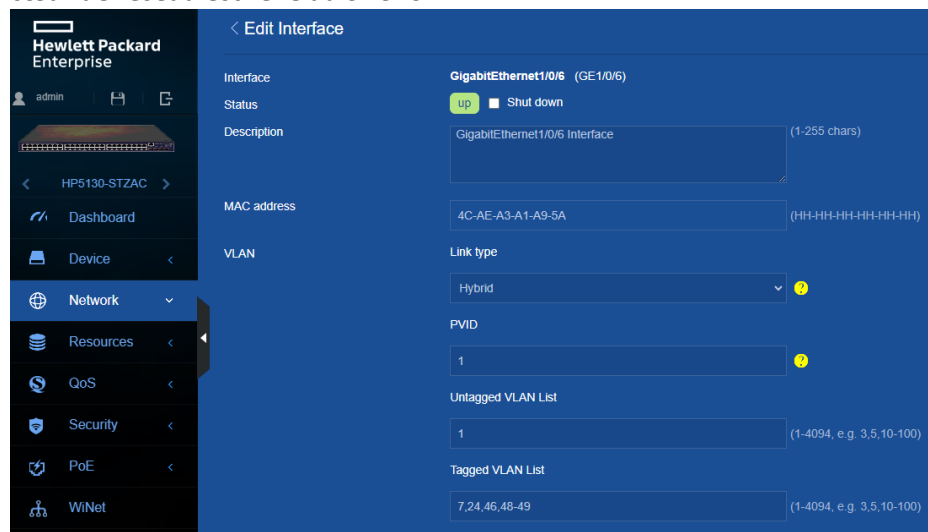
The image shows a screenshot of the Stormshield configuration interface for the SN310 device. The 'INTERFACES' section is selected, and the 'WIFI_TEST' interface is highlighted in the list. The 'CONFIGURATION OF THE INTERFACE' tab is active, showing the configuration details for the 'WIFI_TEST' interface. The configuration includes the Name (WIFI-TEST), Comments, Parent interface (in), Color, VLAN ID (46), Priority (CoS) (0), and This interface is (internal (protected)). The 'Address range' section shows the 'Fixed IP (static)' option selected, with the IP address 192.168.46.254 and Network mask 255.255.255.0.

Création d'une plage DHCP de 192.168.46.20 à 192.168.46.21 pour la distribution de baux pour les clients des APs.

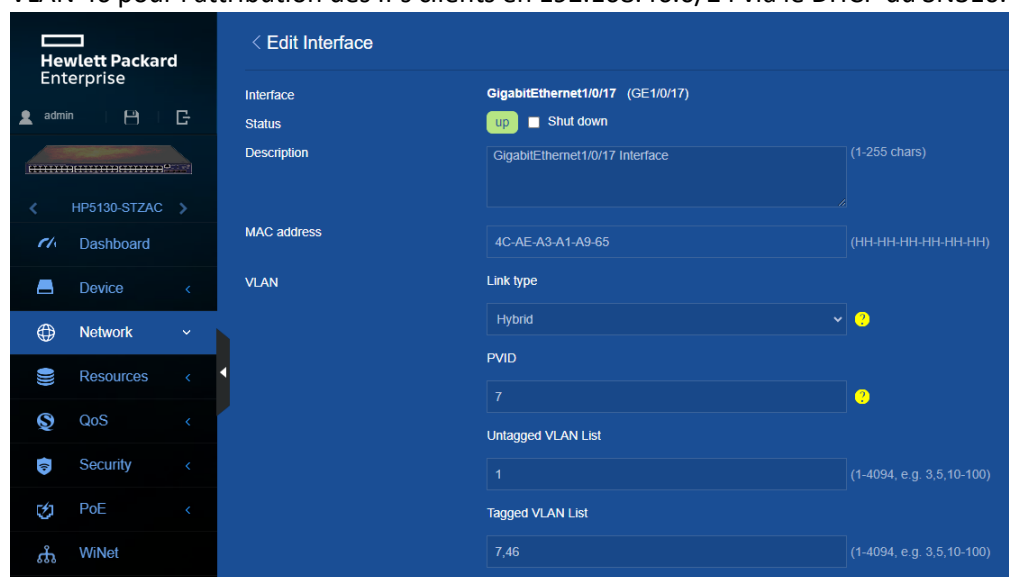


Etape 5 :

Déclaration des VLANs (dont le VLAN 46 diffusant les adresses IPs via le DHCP du SN310) sur le Port 6 du switch cœur de réseau de Saint-Zacharie, switch où est branché l'AP de test. **Le port 6 du switch cœur de réseau est relié au SN310.**



Branchement de l'AP Ruckus sur le port 17 du switch cœur de réseau de Saint-Zacharie.
Le port 17 est PoE (pour alimenter l'AP). Sur ce port sont tagged les VLANs 7 et 46.
VLAN 7 pour l'attribution d'une IP à l'AP sur le réseau 192.168.45.0/24.
VLAN 46 pour l'attribution des IPs clients en 192.168.46.0/24 via le DHCP du SN310.



Etape 6 :

Branchement de l'AP sur le port 17 du switch cœur de réseau et tests de connexions de la borne sur le vSZ des Arcs et tests wifi sur le SSID WIFI_test à Saint-Zacharie.



Conclusion de la procédure

La configuration du tunnel VPN entre les sites des Arcs et de Saint-Zacharie, combinée à l'intégration des points d'accès Ruckus dans le contrôleur vSZ des Arcs, démontre une solution réseau efficace et sécurisée pour la gestion centralisée des infrastructures Wi-Fi sur des sites distants. Cette procédure garantit une connectivité fluide et unifiée entre les deux sites tout en respectant les meilleures pratiques en matière de réseau.

La mise en place rigoureuse des VLANs, des plages IP, des règles de filtrage NAT et des interfaces DHCP sur les deux Stormshield a permis de connecter efficacement les APs et de distribuer les adresses IP aux clients via un réseau optimisé. Cette intégration assure une gestion simplifiée des réseaux sans fil et améliore la couverture et la performance des infrastructures Wi-Fi.

En conclusion, cette configuration offre une infrastructure réseau robuste et évolutive, tout en facilitant la maintenance et le support à distance grâce à une gestion centralisée. Elle représente une avancée significative pour garantir une expérience utilisateur homogène sur l'ensemble des sites, tout en sécurisant les communications intersites.