

## **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.

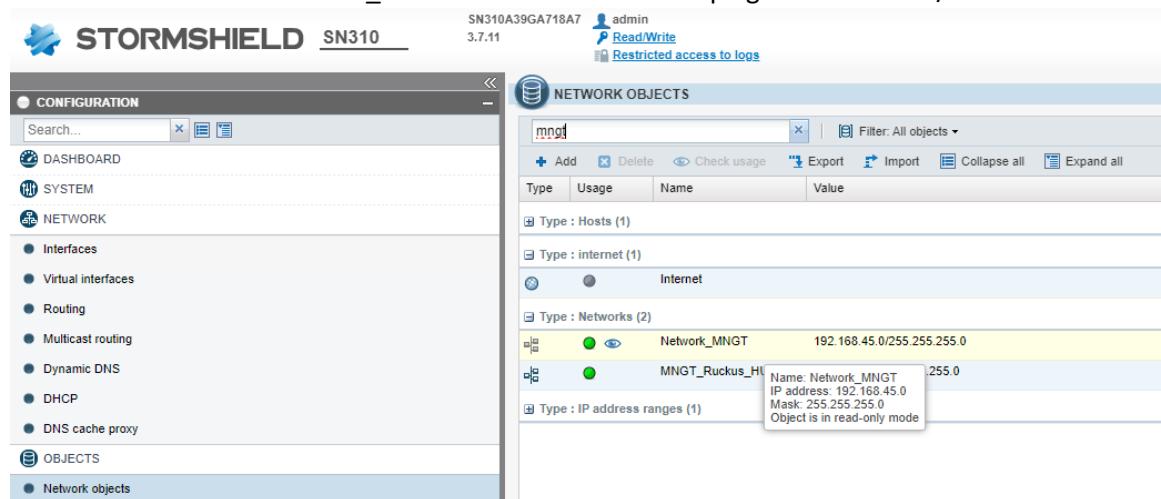
### Etape 1 :

Les APs Ruckus existant à l'HyperU communiquent 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



The screenshot shows the Stormshield SN310 management interface. On the left, the navigation menu includes 'CONFIGURATION', 'DASHBOARD', 'SYSTEM', 'NETWORK', 'Interfaces', 'Virtual interfaces', 'Routing', 'Multicast routing', 'Dynamic DNS', 'DHCP', 'DNS cache proxy', and 'OBJECTS'. Under 'OBJECTS', 'Network objects' is selected. On the right, the 'NETWORK OBJECTS' tab is active, showing a list of objects. A new object, 'Network\_MNGT', has been created and is highlighted in yellow. Its details are shown in a tooltip: Name: Network\_MNGT, IP address: 192.168.45.0, Mask: 255.255.255.0. Other objects listed include 'Internet' and 'MNGT\_Ruckus\_HL'.

## Mise en place du tunnel VPN entre les Arcs et le Network\_MNGT

The screenshot shows the STORMSHIELD SN310 configuration interface. The left sidebar is titled 'CONFIGURATION' and includes sections for DASHBOARD, SYSTEM, NETWORK (Interfaces, Virtual interfaces, Routing, Multicast routing, Dynamic DNS, DHCP, DNS cache proxy), OBJECTS (USERS, SECURITY POLICY, APPLICATION PROTECTION, VPN), and IPsec VPN. The main panel is titled 'IPSEC VPN' and shows the 'ENCRYPTION POLICY - TUNNELS' tab selected. It displays a table of tunnels:

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

A tooltip for the second tunnel (Line 2) provides details: 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

The screenshot shows the STORMSHIELD SN710 configuration interface. The left sidebar is titled 'CONFIGURATION' and includes sections for SYSTEM, NETWORK, OBJECTS, Network (URL, Certificates and PKI), USERS, SECURITY POLICY, APPLICATION PROTECTION, VPN, IPsec VPN, SSL VPN Portal, SSL VPN, PPTP Server, and NOTIFICATIONS. The main panel is titled 'OBJECTS / NETWORK' and shows a search results table for 'mngt':

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
		<b>NW_MNGT_STZAC</b>	<b>192.168.45.0/255.255.255.0</b>
Type : Address ranges (1)		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

The screenshot shows the STORMSHIELD SN710 configuration interface. The left sidebar is titled 'CONFIGURATION' and includes sections for SYSTEM, NETWORK, OBJECTS, USERS, SECURITY POLICY, APPLICATION PROTECTION, VPN, IPsec VPN, SSL VPN Portal, SSL VPN, PPTP Server, and NOTIFICATIONS. The main panel is titled 'VPN / IPSEC VPN' and shows the 'ENCRYPTION POLICY - TUNNELS' tab selected. It displays a table of tunnels:

Line	Status	Local network	Peer	Remote network	Encryption profile
1	off	Network_In	Gw_SOBI0	NW_SOBI0	GoodEncryption
2	on	Network_VIDEO	Gw_SOBI0	NW_SOBI0	GoodEncryption
3	on	Network_In	Gw_SOBI0	NW_SOBI0	GoodEncryption
4	off	Network_In	Gw_SOBI0	VOIP_SOBI0	GoodEncryption
5	on	Network_In	Site_GW_STZACH	NW_STZACH	GoodEncryption
<b>6</b>	<b>on</b>	<b>Network_In</b>	<b>Site_GW_STZACH</b>	<b>NW_MNGT_STZAC</b>	<b>GoodEncryption</b>
7	off	Network_VIDEO	Site_GW_STZACH	NW_VIDEO_S	

A tooltip for the sixth tunnel (Line 6) provides details: 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 screenshot shows two separate interface windows for the STORMSHIELD Network Security system.

**SN710 (Top Window):**

- Left Sidebar:** Configuration, Search, SYSTEM, NETWORK (Interfaces, Virtual interfaces, Routing, Multicast routing, Dynamic DNS, DHCP, DNS cache proxy), OBJECTS.
- Top Bar:** MONITORING, CONFIGURATION, SN710 SN710A59J6268A7.
- Central View:** SECURITY POLICY / FILTER - NAT. A table titled "mngt" lists NAT rules:
 

Index	Status	Action	Source	Destination	Dest. port	Protocol	Security
55	on	pass	Network_Ian	Network_MNGT	Any	IP5	
56	on	pass	Network_MNGT	Network_Ian	Any	IP5	
57	on	pass	Network_Ian	NW_STZACH	Any	IP5	
58	on	pass	NW_MNGT_STZAC	Network_Ian	Any	IP5	
59	off	pass	GLPI_10	Network_MNGT	Any	IP5	
60	off	pass	Network_MNGT	GLPI_10	Any	IP5	

**SN310 (Bottom Window):**

- Left Sidebar:** Configuration, Search, DASHBOARD, SYSTEM, NETWORK (Interfaces, Virtual interfaces, Routing, Multicast routing, Dynamic DNS, DHCP, DNS cache proxy), OBJECTS (Network objects, Web objects, Certificates and PKI), USERS, SECURITY POLICY, Filter - NAT.
- Top Bar:** SN310A39GA718A7, admin, Read/Write, Restricted access to logs.
- Central View:** FILTER - NAT. A table titled "mngt" lists NAT rules:
 

Index	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	
18	on	pass	Network_in	Network_MNGT	Any	IP5	Firewall	
19	on	pass	les-arcs	les-arcs	Name: Network_MNGT IP address: 192.168.45.0 Mask: 255.255.255.0 Object is in read-only mode	Any	IP5	Firewall

**Etape 4 :**

Création de l'interface WIFI\_TEST sur le SN310 avec l'adresse 192.168.46.254/24

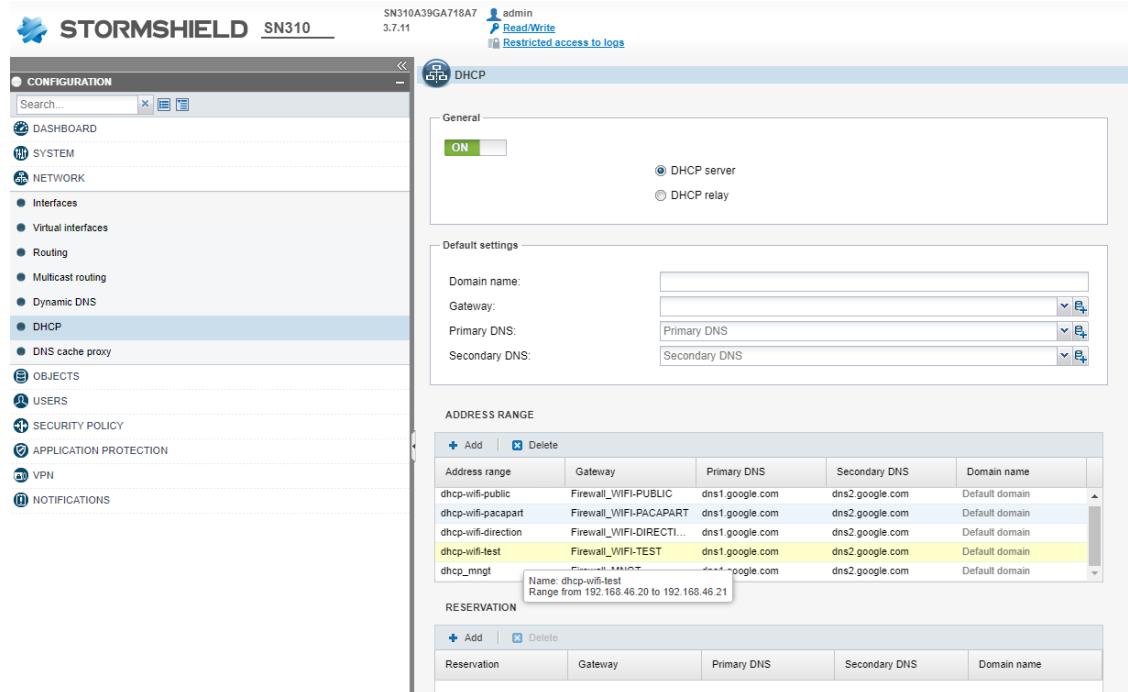
The screenshot shows the configuration interface for the SN310 device.

**Left Sidebar:** Configuration, Search, DASHBOARD, SYSTEM, NETWORK (Interfaces, Virtual interfaces, Routing, Multicast routing, Dynamic DNS, DHCP, DNS cache proxy), OBJECTS, USERS, SECURITY POLICY, APPLICATION PROTECTION, VPN (IPSec VPN, SSLVPN Portal, SSL VPN, PPTP Server), NOTIFICATIONS.

**Central View:**

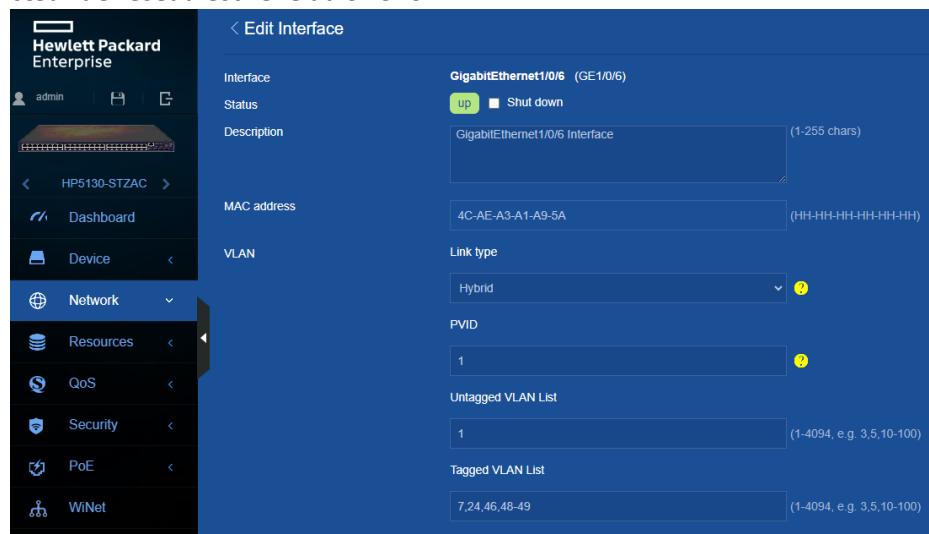
- Top Bar:** SN310A39GA718A7, admin, Read/Write, Restricted access to logs.
- Left Panel:** INTERFACES. A tree view shows available interfaces: out, in, WIFI-PCAPART, WIFI-PUBLIC, WIFI-DIRECTION, **WIFI-TEST** (selected), and MNGT.
- Right Panel:**
  - CONFIGURATION OF THE INTERFACE:** Advanced configuration tab is selected. Fields include:
    - Name: WIFI-TEST
    - Comments:
    - Parent interface: in
    - Color:
    - VLAN ID: 46
    - Priority (CoS): 0
    - This interface is: internal (protected)
  - Address range:** Fixed IP (static) is selected. IP address: 192.168.46.254, Network mask: 255.255.255.0, Comments:.

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.

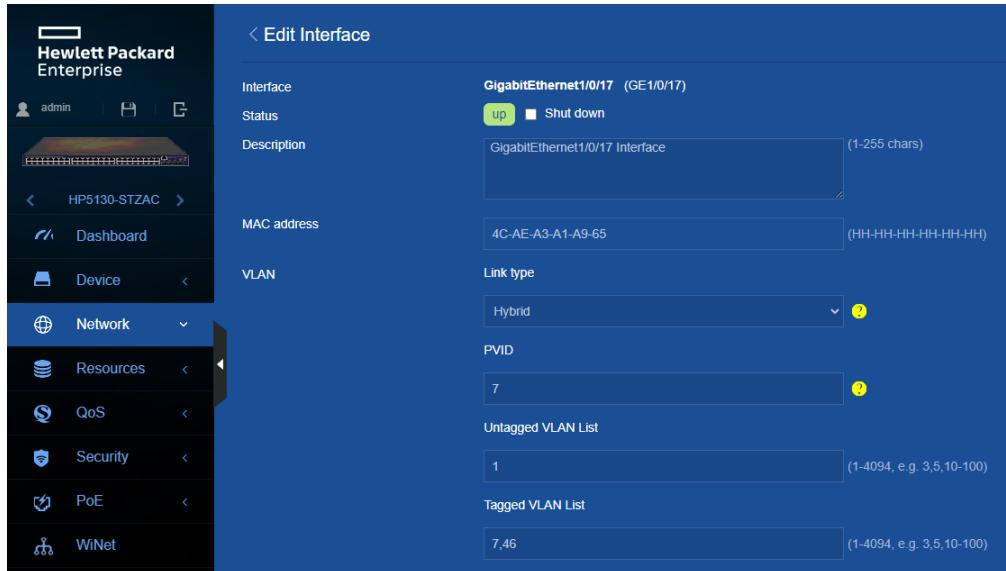


#### Etape 5 :

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.**



Branchements 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 taggés 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 :

Branchements 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.