

Procédure de création d'un VLAN et son inclusion dans le Stormshield

Introduction

La gestion efficace des réseaux d'entreprise repose sur une segmentation claire et sécurisée, et la création de VLANs (Virtual Local Area Networks) est une solution incontournable pour répondre à ces besoins. Cette procédure détaille les étapes nécessaires pour configurer un nouveau VLAN, l'associer à un réseau Wi-Fi, et intégrer sa gestion dans le pare-feu Stormshield. L'objectif est de garantir un réseau segmenté, performant et sécurisé, tout en assurant une connectivité fluide et conforme aux meilleures pratiques de sécurité réseau.

1. Création du VLAN

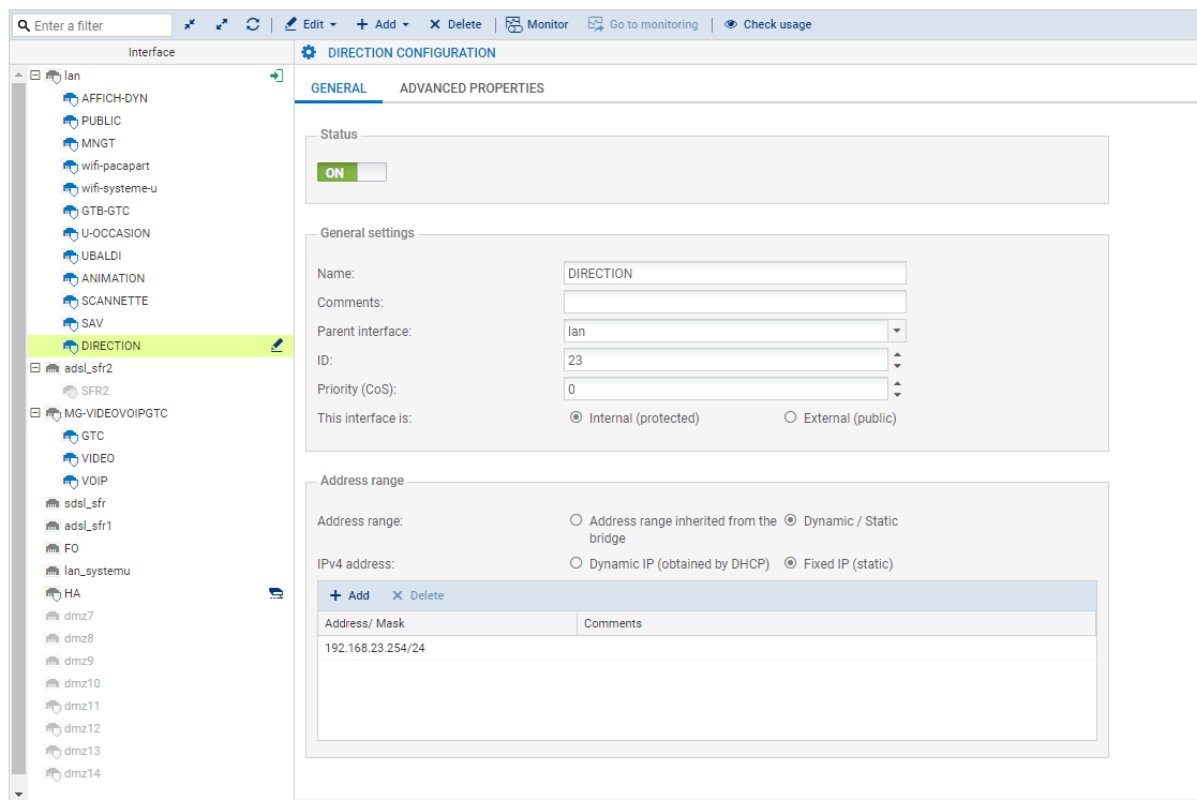
- **Objectif :** Créer un nouveau VLAN pour segmenter le réseau et améliorer la sécurité et la gestion du trafic.
- **Étapes :**
 1. Définir l'ID du VLAN (par exemple, VLAN 23).
 2. Créer le VLAN sur tous les switchs du réseau.
 3. Vérifier la propagation du VLAN sur l'ensemble des switchs.

2. Association du VLAN avec un SSID Wifi

- **Objectif :** Associer le nouveau VLAN à un SSID Wifi pour permettre une connexion sans fil sécurisée au nouveau segment de réseau.
- **Étapes :**
 1. Créer un nouveau SSID Wifi.
 2. Associer l'ID du VLAN créé (VLAN 23) au nouveau SSID.
 3. Configurer les paramètres de sécurité du SSID (WPA2, WPA3, etc.).

3. Configuration des règles sur le Stormshield

- **Objectif :** Définir des règles de sécurité pour gérer le trafic entrant et sortant du VLAN à travers le firewall Stormshield.
- **Étapes :**
 1. **Création de l'interface DIRECTION avec l'ID VLAN 23 :**
 - Accéder à la configuration des interfaces du Stormshield.
 - Créer une nouvelle interface nommée "DIRECTION" et associer l'ID VLAN 23.



The screenshot shows the Stormshield web interface for configuring a new interface. The left sidebar lists various interfaces, with 'DIRECTION' highlighted. The main panel is titled 'DIRECTION CONFIGURATION' and has two tabs: 'GENERAL' and 'ADVANCED PROPERTIES'. The 'GENERAL' tab is active, showing the following settings:

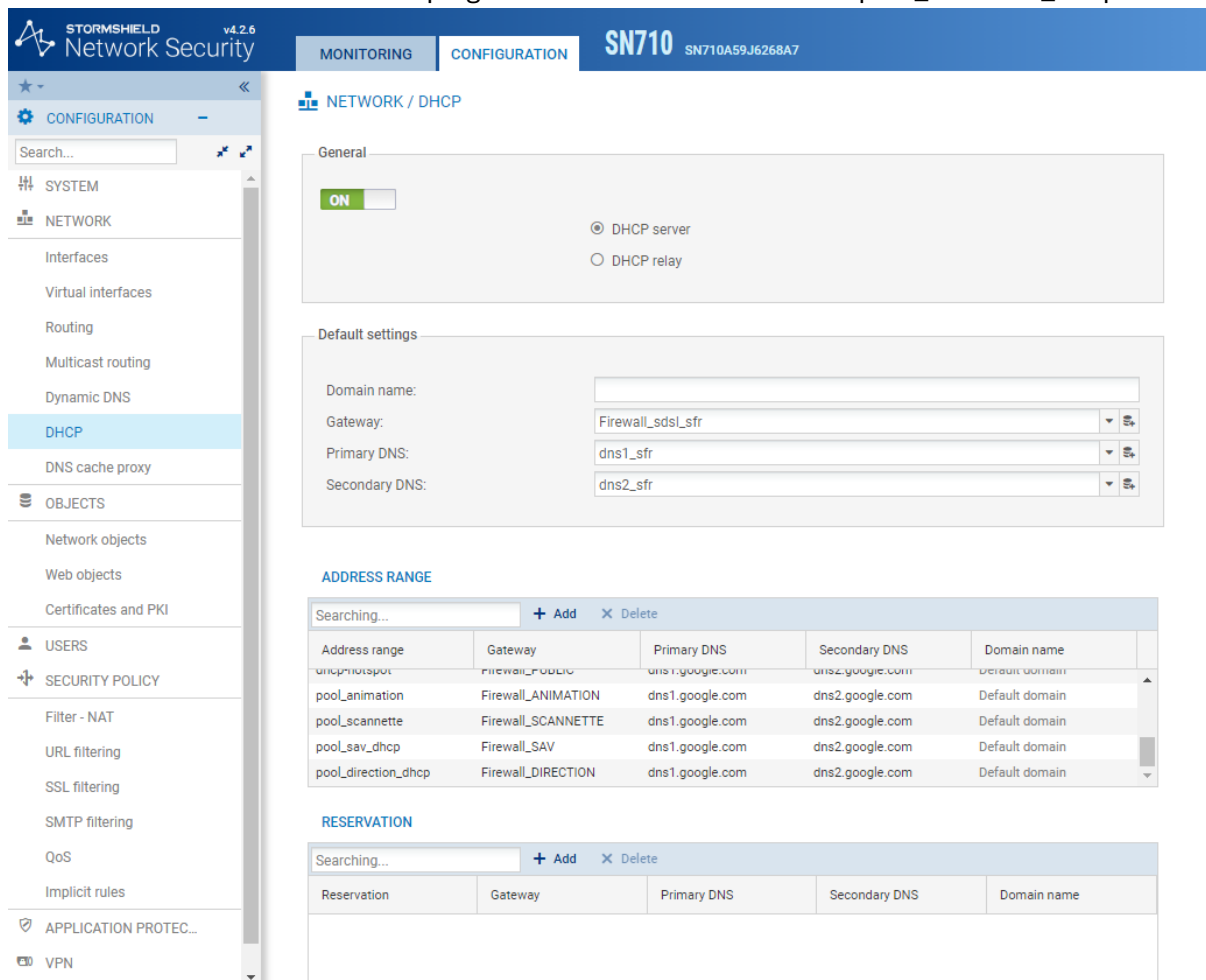
- Status:** A toggle switch set to 'ON'.
- General settings:**
 - Name:** DIRECTION
 - Comments:** (empty field)
 - Parent interface:** lan
 - ID:** 23
 - Priority (CoS):** 0
 - This interface is:** ☒ Internal (protected) ☐ External (public)
- Address range:**
 - Address range:** ☐ Address range inherited from the bridge ☒ Dynamic / Static bridge
 - IPv4 address:** ☐ Dynamic IP (obtained by DHCP) ☒ Fixed IP (static)
- Address range table:** A table with columns 'Address/ Mask' and 'Comments'. It contains one entry: '192.168.23.254/24'.

2. Création automatique d'objets réseau :

- Valider que le Stormshield crée automatiquement l'objet réseau "Network_DIRECTION".
- Valider la création automatique de l'hôte "Firewall_Direction".

3. Configuration du DHCP :

- Naviguer vers la section "Network" puis "DHCP" du Stormshield.
- Créer une plage d'adresses DHCP nommée "pool_direction_dhcp".



The screenshot shows the Stormshield Network Security v4.2.6 interface. The left sidebar contains a menu with sections: CONFIGURATION, SYSTEM, NETWORK, OBJECTS, USERS, and SECURITY POLICY. The NETWORK section is expanded, showing options like Interfaces, Virtual interfaces, Routing, Multicast routing, Dynamic DNS, and DHCP (which is selected). The main panel displays the DHCP configuration for SN710. It includes a 'General' section with a toggle switch set to 'ON' and radio buttons for 'DHCP server' (selected) and 'DHCP relay'. Below this is the 'Default settings' section with fields for Domain name, Gateway (Firewall_sdsl_sfr), Primary DNS (dns1_sfr), and Secondary DNS (dns2_sfr). The 'ADDRESS RANGE' section shows a table with columns: Address range, Gateway, Primary DNS, Secondary DNS, and Domain name. The table lists several ranges, including 'pool_animation', 'pool_scannette', 'pool_sav_dhcp', and 'pool_direction_dhcp'. The 'RESERVATION' section is also visible but empty.

4. Règles de filtrage NAT

- **Objectif :** Configurer des règles NAT pour permettre au VLAN d'accéder à des ressources spécifiques, comme les disques réseau via le serveur Active Directory.
- **Étapes :**
 1. Ajouter des règles NAT pour l'objet réseau "Network_DIRECTION" pour permettre l'accès au serveur Active Directory (serv-ad).
 2. Configurer l'accès aux disques réseau X: et I: sans nécessiter de réauthentification.

TREND MICRO (contains 8 rules, from 20 to 27)						
20	on	pass	Nw_VPNSSL SERV-AD	SERV-AD Nw_VPNSSL	TREND 8059	Crée le 2019-02-21
21	on	pass	Nw_VPNSSL SERV-AD2	SERV-AD2 Nw_VPNSSL	TREND 8059	Crée le 2019-02-21
22	on	pass	Network_wifi-pacart SERV-AD	SERV-AD Network_wifi-pacart	TREND 8059	Crée le 2019-02-21
23	on	pass	Network_wifi-pacart SERV-AD2	SERV-AD2 Network_wifi-pacart	TREND 8059	Crée le 2019-02-21
24	on	pass	Network_wifi-pacart SERV-AD22	SERV-AD22 Network_wifi-pacart	TREND 8059	Crée le 2019-02-21
25	on	pass	Network_DIRECTION SERV-AD	SERV-AD Network_DIRECTION	TREND 8059	Crée le 2019-02-21
26	on	pass	Network_DIRECTION SERV-AD2	SERV-AD2 Network_DIRECTION	TREND 8059	Crée le 2019-02-21
27	on	pass	Network_DIRECTION SERV-AD22	SERV-AD22 Network_DIRECTION	TREND 8059	Crée le 2019-02-21

5. Inclusion dans le filtrage IPS et autres règles de sécurité

- **Objectif :** Appliquer des règles de sécurité IPS, IDS et firewall pour le trafic HTTP et HTTPS associé au VLAN.
- **Étapes :**
 1. Inclure "Network_DIRECTION" dans le filtrage IPS.
 2. Appliquer des règles IPS, IDS et firewall pour "Network_DIRECTION" et "pool_direction_dhcp" pour différents accès HTTP et HTTPS.

2	on	block	STOCKER-GENETEC Network_lan Network_wifi-pacapart Network_PUBLIC Network_U-OCCASION Network_UBALDI Network_ANIMATION Network_FO Network_DIRECTION	Internet IP rep. anonymiseur botnet exploit malware nouveau d'entrée tor nouveau de sortie tor phishing scanneur spam suspect tor	Any	IP2	Crée le 2020-08-13
25	on	pass	Network_DIRECTION SERV-AD	SERV-AD Network_DIRECTION	TREND 8059	IP2	Crée le 2019-02-21
26	on	pass	Network_DIRECTION SERV-AD2	SERV-AD2 Network_DIRECTION	TREND 8059	IP2	Crée le 2019-02-21
27	on	pass	Network_DIRECTION SERV-AD22	SERV-AD22 Network_DIRECTION	TREND 8059	IP2	Crée le 2019-02-21
45	on	pass	Route: Gw_FO_SFR	pool_direction_dhcp	Internet	Any	Crée le 2021-11-15
53	on	pass	Route: GW_ADSL_SFR1	pool_wifi-pacapart pool_direction_dhcp	Internet	http ZOOM http_proxy	Crée le 2018-08-03
55	on	pass	Route: FiberRouter_GW_ADSL_SFR1	pool_wifi-pacapart pool_direction_dhcp	Internet	https	Crée le 2018-08-03
56	on	pass	Network_wifi-pacapart Network_DIRECTION	SERVEURS_TSE	microsofts	IP2	Crée le 2018-08-03
57	on	pass	Network_wifi-pacapart Network_DIRECTION	SERVEURS_TSE	https http	IP2	Crée le 2018-08-03

Conclusion

Cette procédure met en évidence l'importance d'une configuration réseau minutieuse pour garantir une sécurité optimale et une connectivité efficace. En intégrant un VLAN dans le pare-feu Stormshield, en associant ce dernier à un SSID Wi-Fi et en appliquant des règles de filtrage et de sécurité avancées, cette approche permet de gérer les ressources réseau de manière centralisée et sécurisée. Une telle configuration renforce la segmentation du réseau, améliore la gestion du trafic et garantit une protection accrue des données sensibles, tout en assurant un accès utilisateur simplifié et sécurisé.