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

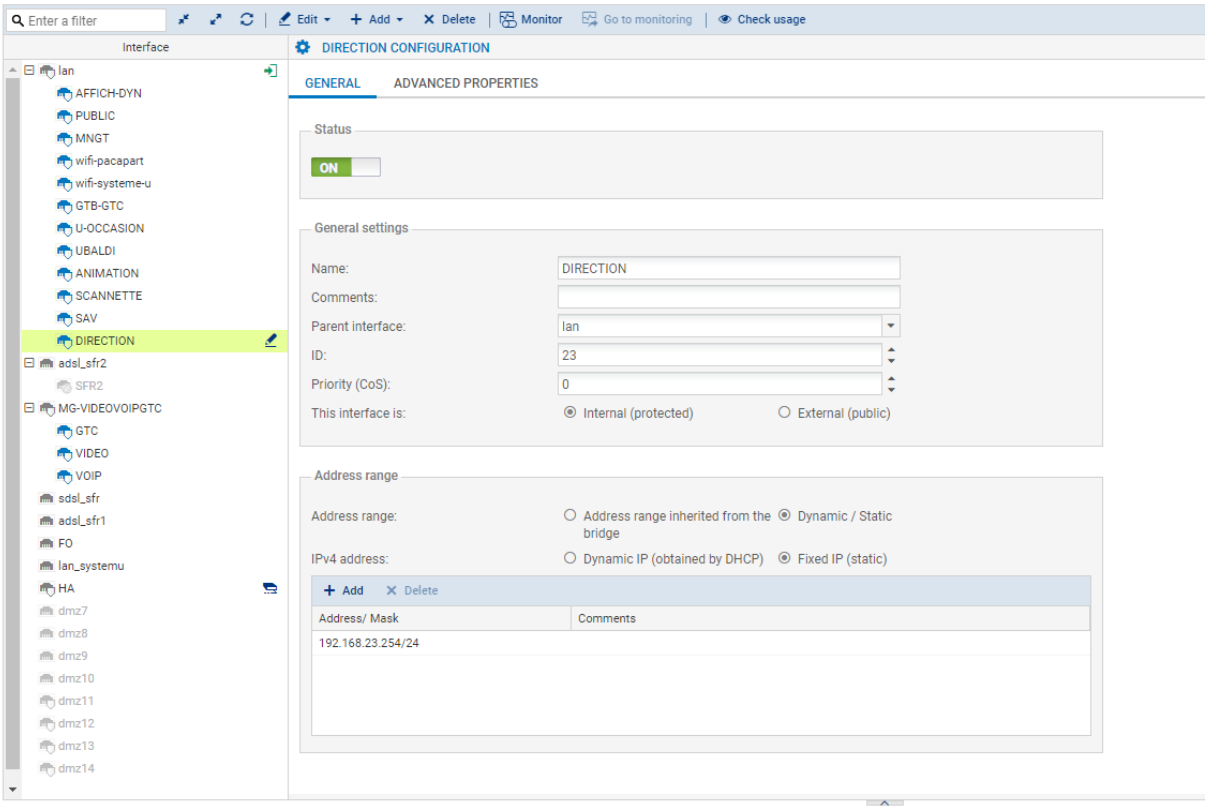
- **Objectif :** Créer un nouveau VLAN pour segmenter le réseau et améliorer la sécurité et la gestion du trafic.
- **Étapes :**
    1. Définir l'ID du VLAN (par exemple, VLAN 23).
    2. Créer le VLAN sur tous les switchs du réseau.
    3. Vérifier la propagation du VLAN sur l'ensemble des switchs.

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.).

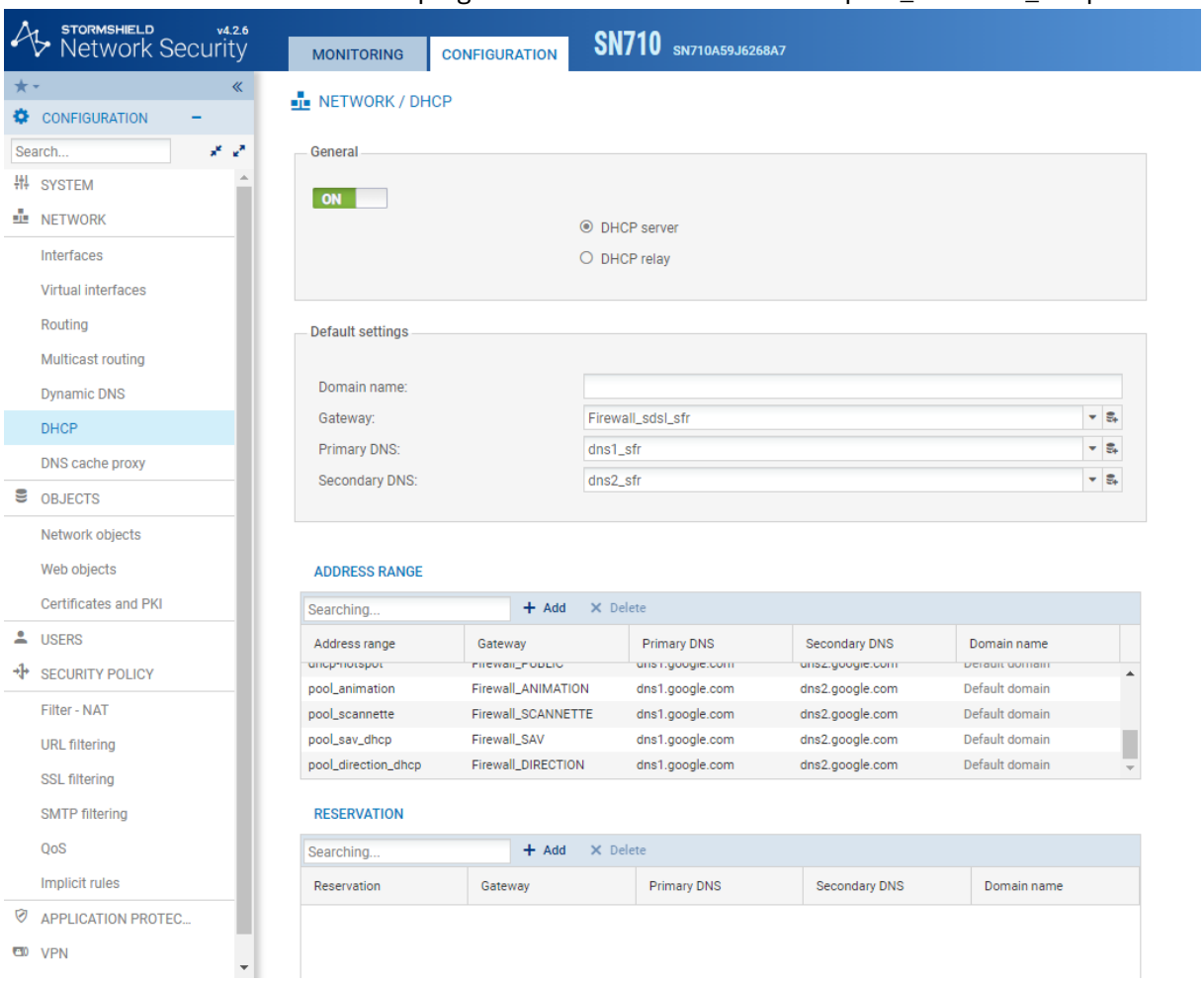
3. Configuration des règles sur le Stormshield

- **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.



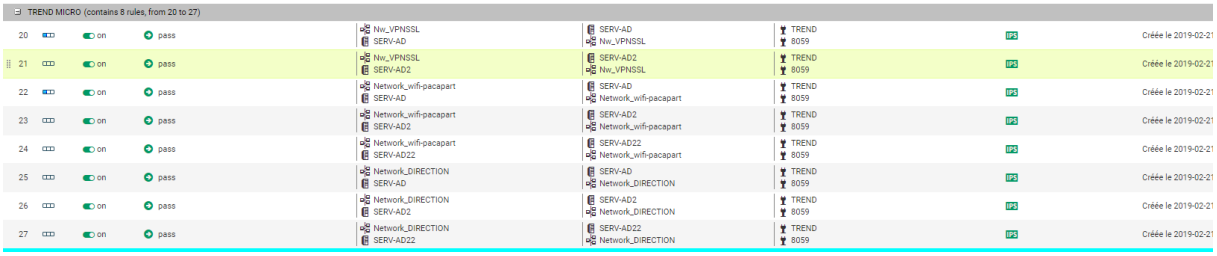
  2. **Création automatique d'objets réseau :**
     - Valider que le Stormshield crée automatiquement l'objet réseau "Network_DIRECTION".
     - Valider la création automatique de l'hôte "Firewall_Direction".

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



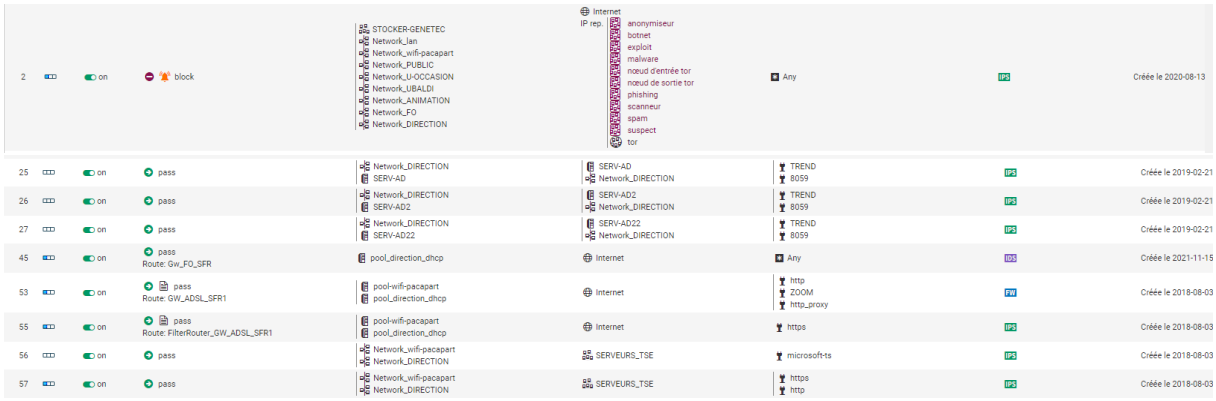
4. Règles de filtrage NAT

- **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.



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.



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.