Infrastructure à Clés Publiques (PKI) – Identité

STORMSHIELD

VALENTIN, THEO

BTS SIO 2024-2025

SNS GALWAY

Stormshield

Stormshield Network Security (SNS) est une solution de sécurité réseau de type pare-feu nouvelle génération (NGFW), développée par Stormshield (filiale d'Airbus Group). Elle est conçue pour protéger les infrastructures IT contre un large éventail de menaces tout en assurant un haut niveau de performance et de fiabilité.

Fonctions principales :

Filtrage de paquets
Analyse le trafic réseau entrant et sortant en fonction de règles de sécurité définies, pour autoriser ou bloquer les communications.

Contrôle applicatif
Permet d'identifier et de filtrer les applications utilisées sur le réseau (ex : Skype, BitTorrent, etc.), même si elles utilisent des ports non standards.

Inspection en profondeur (DPI)
Analyse les contenus des paquets réseau pour détecter des attaques complexes ou des comportements malveillants.

Prévention d'intrusion (IPS)
Intègre un moteur de détection et de prévention d'intrusion capable d'identifier et de bloquer des attaques en temps réel.

VPN IPsec / SSL
Permet la mise en place de connexions chiffrées sécurisées entre sites distants ou pour les télétravailleurs.

Gestion des identités & authentification
Supporte l'intégration avec des annuaires LDAP/Active Directory pour gérer les accès utilisateurs.

📊 Logs, alertes & reporting

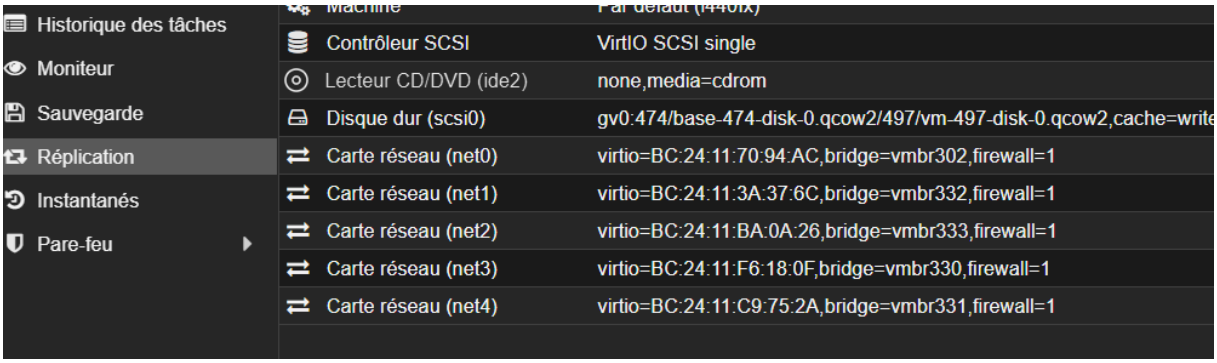
Fournit des outils de journalisation, de supervision et de génération de rapports pour suivre l’activité réseau et détecter les incidents.

Cas d’usage :

- **Protection d’un réseau d’entreprise contre les attaques extérieures.**
- **Mise en place de connexions sécurisées entre plusieurs sites distants (VPN).**
- **Application de politiques d’accès par utilisateur, par groupe, ou par zone réseau.**
- **Sécurisation d’un environnement industriel (OT/SCADA) grâce à des profils adaptés.**

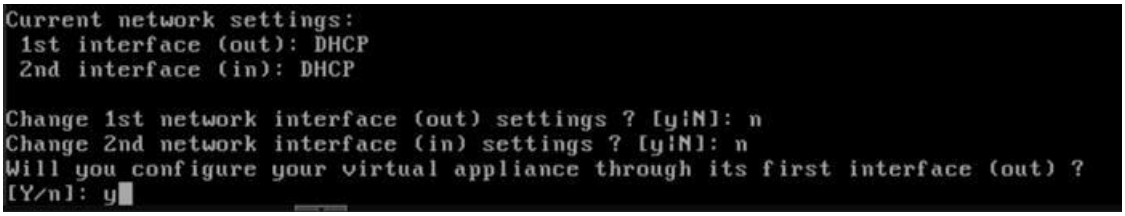
Configuration du clone de « Modele-SNS-4.3 » :

Il faut ajouter les cartes réseaux pour les différents réseaux de galway l'interface du SNS doit être dans le VLAN 302 qui est celui de CUB WAN

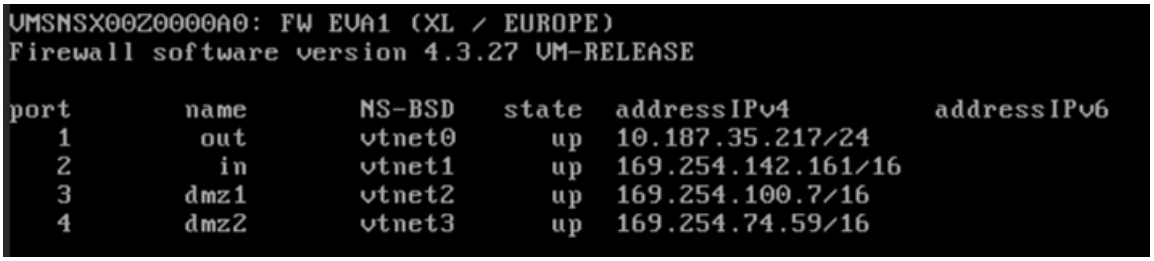


Répondre non pour changer les interfaces réseau out/in :

Répondre oui pour la configuration virtuel :



Connexion avec l'adresse Out 10.187.35.217 au site Stormshield qu'il faudra changer par la suite :



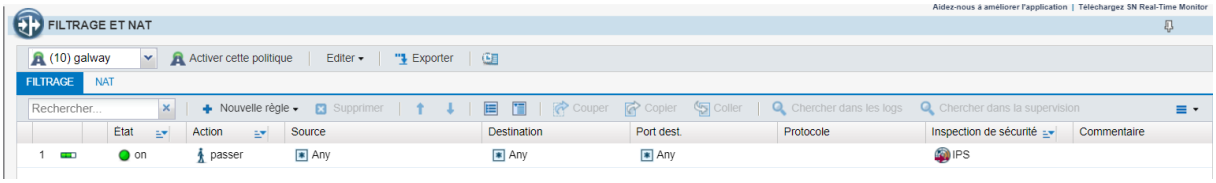
Configuration du pare feu virtuel

Une fois sur l'interface web nous devons ajouter comme passerelle le pare feu prof en 192.168.229.1

On donne accès au pare-feu via internet en donnant un IP fixe au WAN en 192.168.229.60

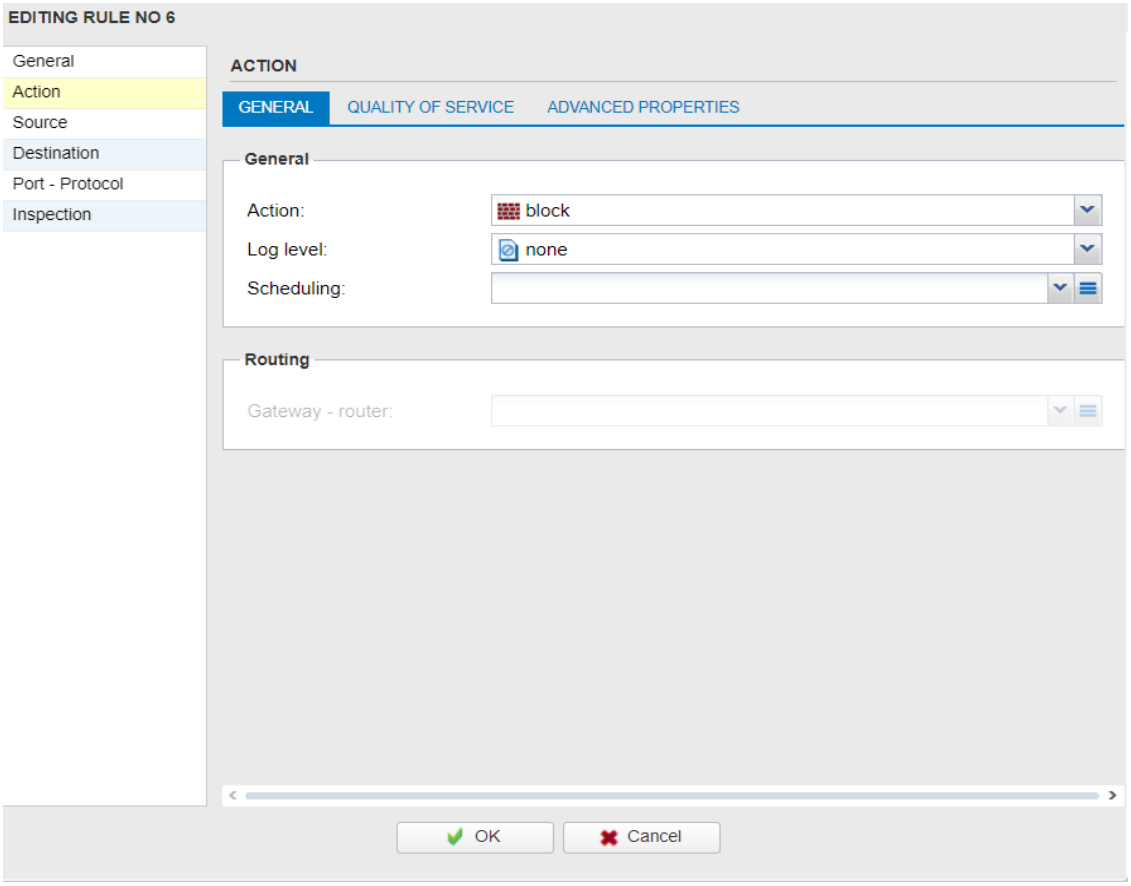
PHOTO ICI

On met le pare-feu en pass all pour avoir accès au pare-feu librement au début nous mettrons en place nos règles après :

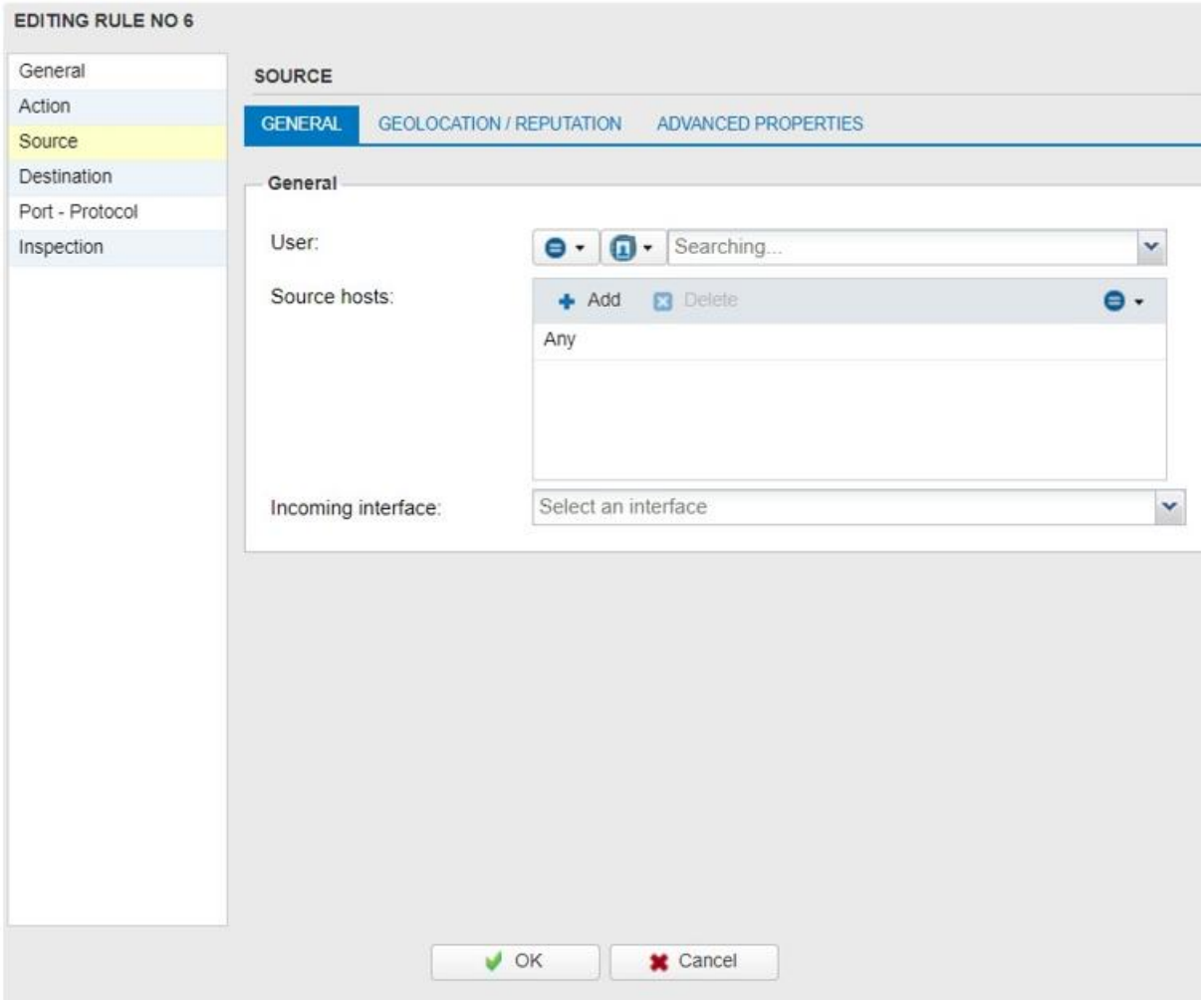


Dans la partie Security Policy - Filtrage et Nat nous créons différentes règles de sécurité de la manière suivante:

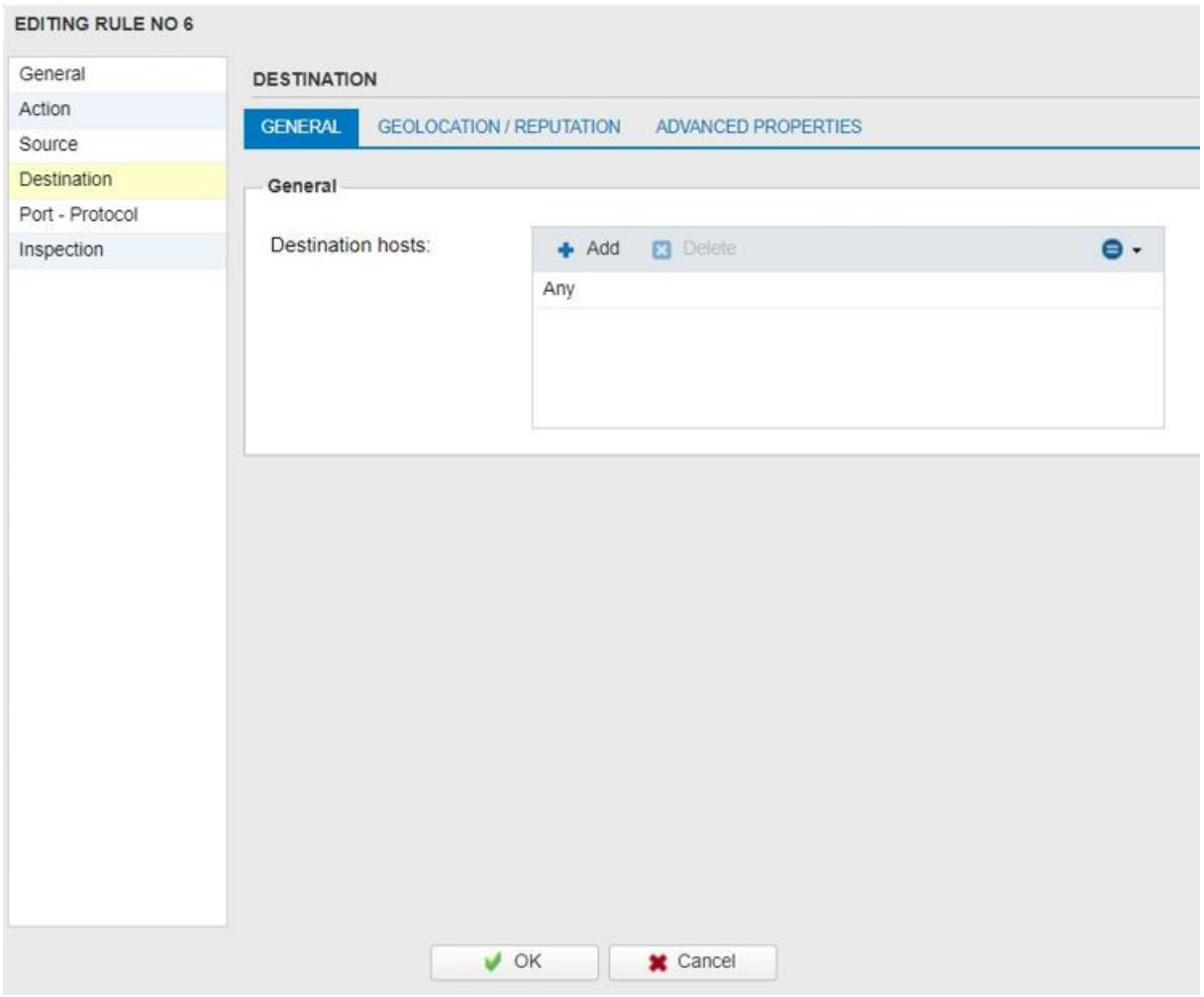
Création d'une nouvelle règle simple puis choisir son action



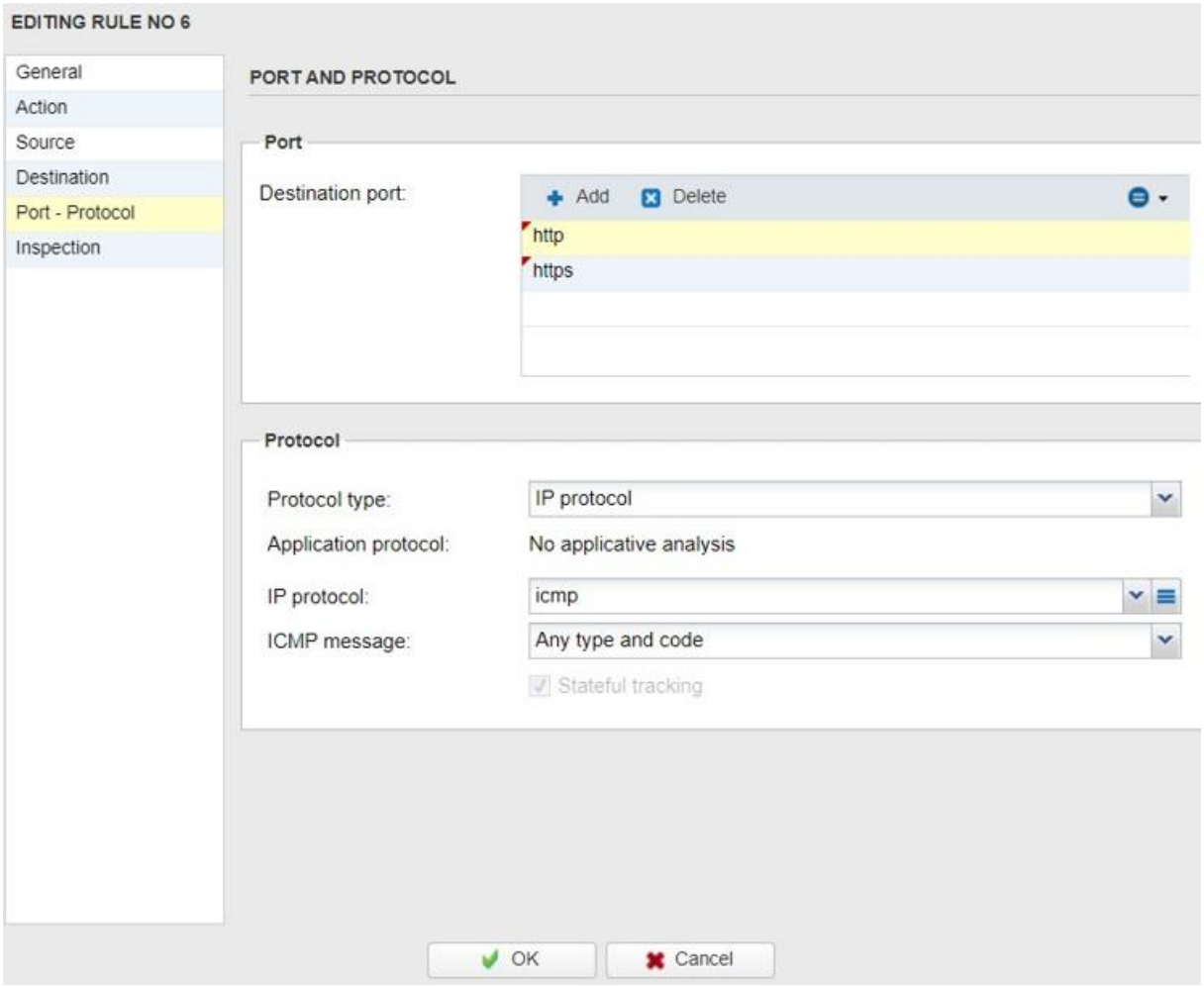
Ensuite choisir sa source :



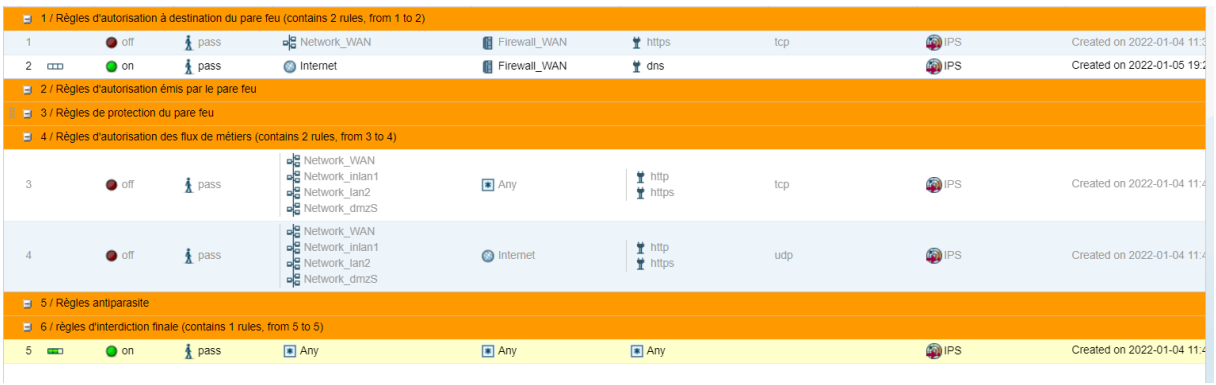
Choisir sa destination :



Choisir son port par exemple ici http/https et son protocole ici ICMP :

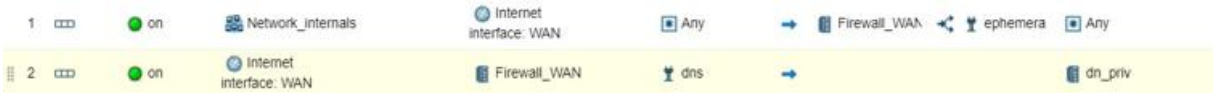


Une fois nos règles crée on les organise selon leurs utilisations :



1. **Permet au réseau WAN à destination du pare feu d'utiliser le port https sur le protocole TCP (inactif)**
2. **Permet à internet d'accéder à la destination du pare feu vers le port du DNS (actif)**
3. **Autorise l'accès pour le réseau WAN, le LAN 1, 2 et la DMZ serveur à n'importe quelle destination via le port http et https par le protocole TCP (inactif)**
4. **Autorise l'accès pour le réseau WAN, le LAN 1, 2 et la DMZ serveur internet via le port http et https par le protocole UDP (inactif)**
5. **Autorise tout (actif)**

Pour le filtrage Nat on crée deux règles :



1. **Les IP provenant d'un réseau interne destiné à Internet, passant par l'interface WAN par n'importe quelle protocol est autorisé à sortir vers l'interface WAN avec un mécanisme appelé "ephemeral ports". Cela signifie que les ports éphémères (temporairement utilisés pour des connexions sortantes) sont utilisés, et NAT est appliqué pour traduire les adresses internes.**
2. **Elle permet aux requêtes DNS externes (venant d'Internet) d'être redirigées vers notre adresse DNS privé (dn_priv),**