

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

Historique des tâches	Machine	Par défaut (i440fx)
Moniteur	Contrôleur SCSI	VirtIO SCSI single
Sauvegarde	Lecteur CD/DVD (ide2)	none,media=cdrom
Réplication	Disque dur (scsi0)	gv0:474/base-474-disk-0.qcow2/497/vm-497-disk-0.qcow2,cache=write
Instantanés	Carte réseau (net0)	virtio=BC:24:11:70:94:AC,bridge=vmbr302,firewall=1
Pare-feu	Carte réseau (net1)	virtio=BC:24:11:3A:37:6C,bridge=vmbr332,firewall=1
	Carte réseau (net2)	virtio=BC:24:11:BA:0A:26,bridge=vmbr333,firewall=1
	Carte réseau (net3)	virtio=BC:24:11:F6:18:0F,bridge=vmbr330,firewall=1
	Carte réseau (net4)	virtio=BC:24:11:C9:75:2A,bridge=vmbr331,firewall=1

Répondre non pour changer les interfaces réseau out/in :

Répondre oui pour la configuration virtuel :

```
Current network settings:
1st interface (out): DHCP
2nd interface (in): DHCP

Change 1st network interface (out) settings ? [y|N]: n
Change 2nd network interface (in) settings ? [y|N]: n
Will you configure your virtual appliance through its first interface (out) ?
[Y/n]: y
```

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

```
UMSNSX00Z0000A0: FW EVA1 (XL / EUROPE)
Firewall software version 4.3.27 UM-RELEASE

port      name      NS-BSD   state  addressIPv4      addressIPv6
1         out      vtnet0   up     10.187.35.217/24
2         in       vtnet1   up     169.254.142.161/16
3         dmz1    vtnet2   up     169.254.100.7/16
4         dmz2    vtnet3   up     169.254.74.59/16
```

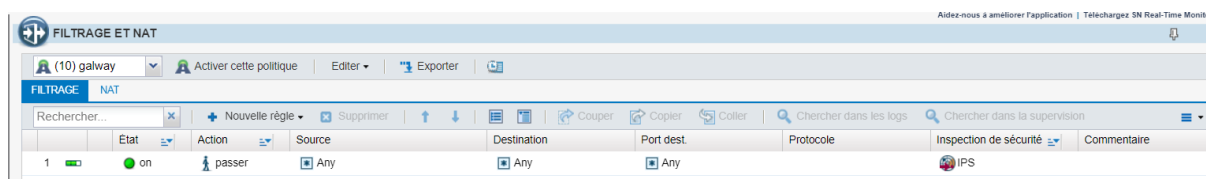
Configuration du pare feu virtuel

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

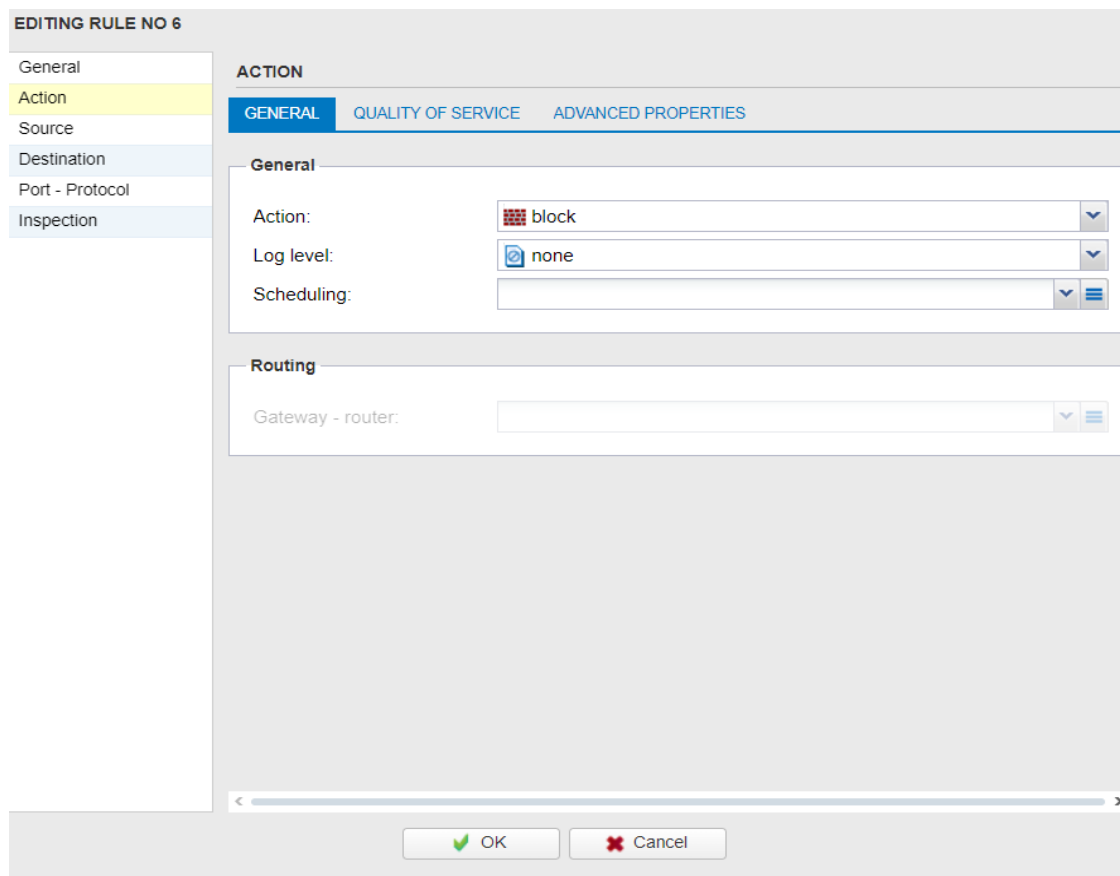
PHOTO ICI

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 :

EDITING RULE NO 6

General
Action
Source
Destination
Port - Protocol
Inspection

SOURCE

GENERAL GEOLOCATION / REPUTATION ADVANCED PROPERTIES

General

User:   Searching... 

Source hosts:  Add  Delete 

Any

Incoming interface: Select an interface 

 OK  Cancel

Choisir sa destination :

EDITING RULE NO 6

General

Action

Source

Destination

Port - Protocol

Inspection

DESTINATION

GENERAL

GEOLOCATION / REPUTATION

ADVANCED PROPERTIES

General

Destination hosts:

+ Add

✕ Delete

⌵

Any

✔ OK

✖ Cancel

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

EDITING RULE NO 6

General
Action
Source
Destination
Port - Protocol
Inspection

PORT AND PROTOCOL

Port

Destination port:

+ Add
Delete

http
https

Protocol

Protocol type: IP protocol

Application protocol: No applicative analysis

IP protocol: icmp

ICMP message: Any type and code

☒ Stateful tracking

OK
Cancel

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

1 / Règles d'autorisation à destination du pare feu (contains 2 rules, from 1 to 2)									
1	off	pass	Network_WAN	Firewall_WAN	https	tcp	IPS	Created on 2022-01-04 11:3	
2	on	pass	Internet	Firewall_WAN	dns		IPS	Created on 2022-01-05 19:2	
2 / Règles d'autorisation émis par le pare feu									
3 / Règles de protection du pare feu									
4 / Règles d'autorisation des flux de métiers (contains 2 rules, from 3 to 4)									
3	off	pass	Network_WAN Network_inlan1 Network_lan2 Network_dmzS	Any	http https	tcp	IPS	Created on 2022-01-04 11:4	
4	off	pass	Network_WAN Network_inlan1 Network_lan2 Network_dmzS	Internet	http https	udp	IPS	Created on 2022-01-04 11:4	
5 / Règles antiparasite									
6 / règles d'interdiction finale (contains 1 rules, from 5 to 5)									
5	on	pass	Any	Any	Any		IPS	Created on 2022-01-04 11:4	

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	on	Network_internals	Internet interface: WAN	Any	→	Firewall_WAN	←	ephemera	Any
2	on	Internet interface: WAN	Firewall_WAN	dns	→	dn_priv			

1. Les IP provenant d'un réseau interne destiné à Internet, passant par l'interface WAN par n'importe quelle protocole 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),