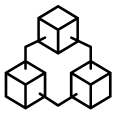
Mise en place d’un pare-feu Stormshield (SNS)



ES-SAIDI Naoufal

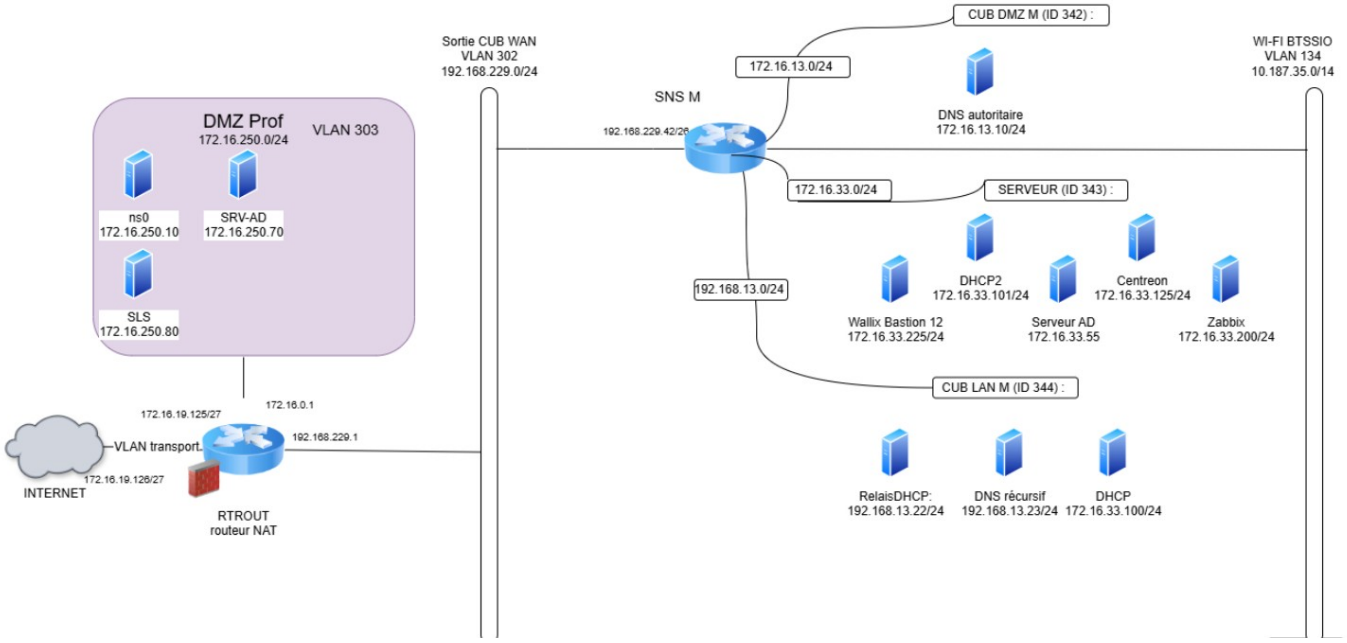
Sommaire

1. *Contexte :*

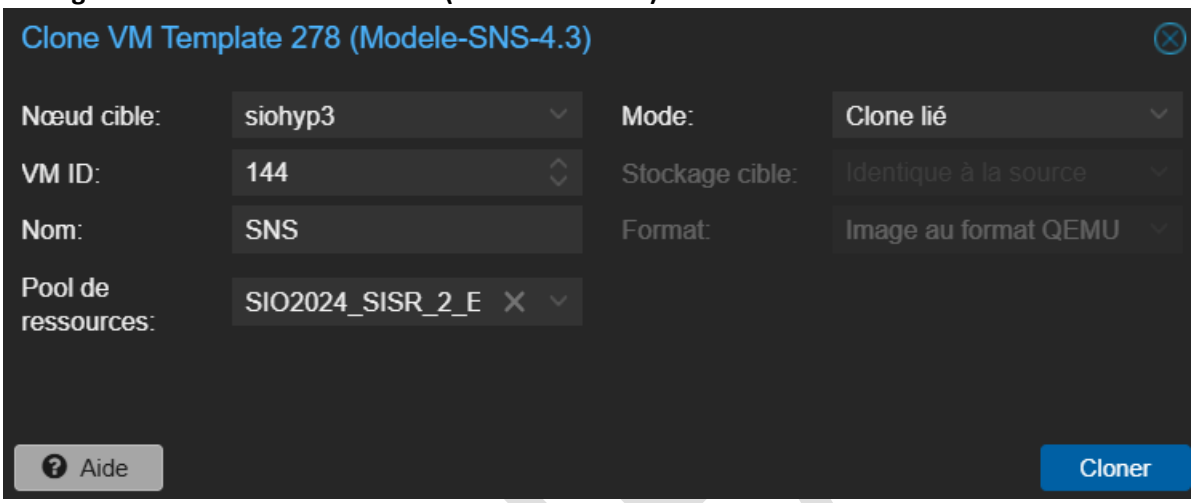
Agence Marrakech

Agence	ID VLAN	Adresses de sous-réseaux	Adresses IP de votre firewall Stormshield
M	342	**DMZ :** 172.16.13.0/24	**dmz :** 172.16.13.254
	343	**SERVEURS :** 172.16.33.0/24	**dmz :** 172.16.33.254
	344	**LAN :** 192.168.13.0/24	**in/lan :** 192.168.13.254
	302	**WAN :** 192.168.229.0/24	**out :** 192.168.229.42

Schéma logique du réseau de CUB



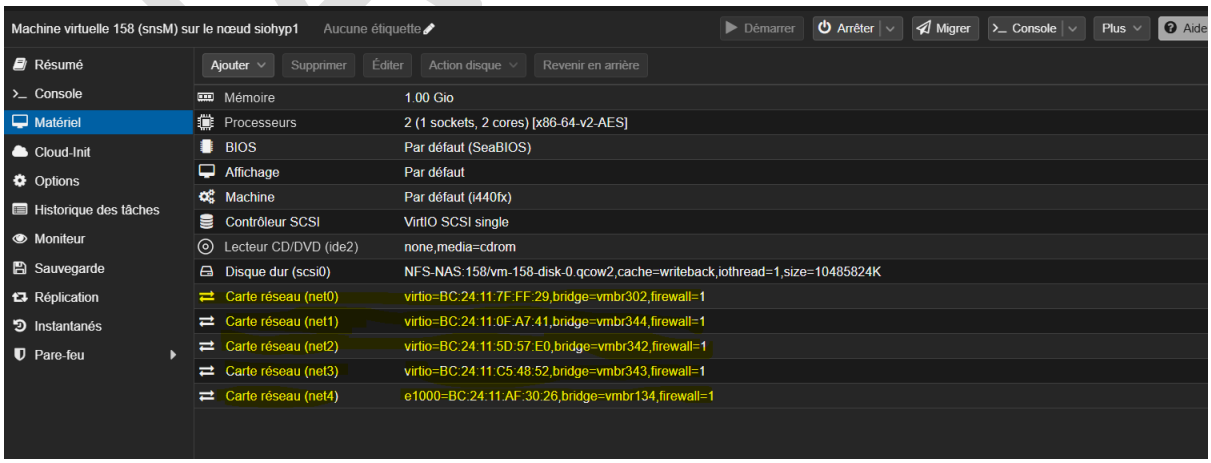
2. **Clonage de la Machine virtuelle 278 (Modele-SNS-4.3)**



3. **Ajout des VLANs sur l'interfaces :**

- **net0 (Out)** : VLAN `wifi-cub-wan` pour accéder à l'interface graphique du Stormshield via l'IP DHCP du pare-feu virtuel.

- **Autres interfaces** : VLAN internes (`LAN1`, `LAN2`, `DMZ`, `Serveur`).



Après avoir répondu aux questions :

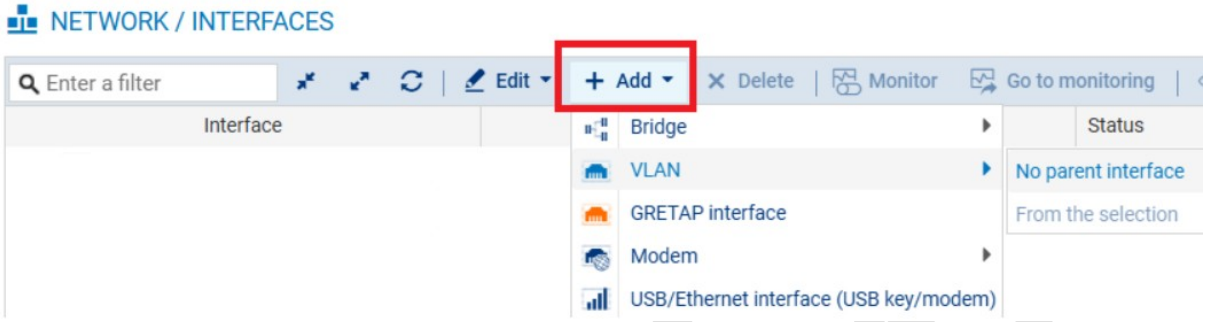
4. **Se connecter à l'interface Web du SNS**

On utilise l'URL suivant :

⇨ https://<adresse ip en DHCP>/admin
⇨ Puis mettre à jour le système

5. Configuration des interfaces réseaux :

Dans le menu **Configuration / Réseau / interfaces :**



- On ajoute les adresses Ip correspondant au plan d'adressage de l'agence MARRAKECH

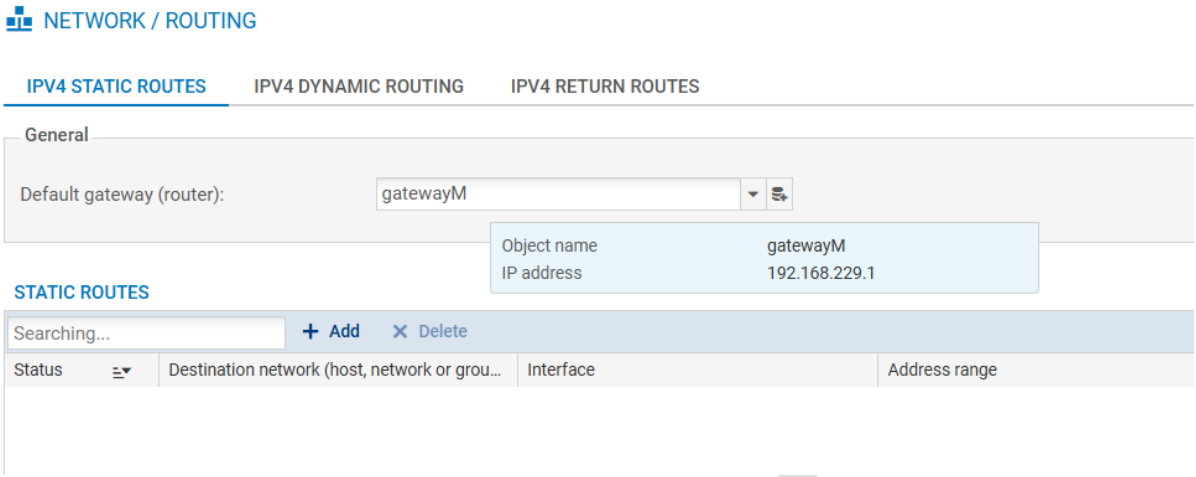
• **Résultat final :**

Interface	Port	Type	Status	IPv4 address
out/wan	1	Ethernet, 10 Gbit/s		192.168.229.42/24
in/lan	2	Ethernet, 10 Gbit/s		192.168.13.254/24
dmz1	3	Ethernet, 10 Gbit/s		172.16.13.254/24
server	4	Ethernet, 10 Gbit/s		172.16.33.254/24
admin	5	Ethernet, 10 Gbit/s		10.187.35.105/24 (DHCP)

6. Mettre en place la route par défaut :

- La passerelle par défaut du pare-feu SNS doit être configurée pour pointer vers l'adresse IP du pare-feu SNS enseignant : 192.168.229.1.

- Pour cela, accédez à : **Configuration → Réseau → Routage → onglet Routes statiques IPv4.**



7. **Mise en place des règles de translation NAT :**

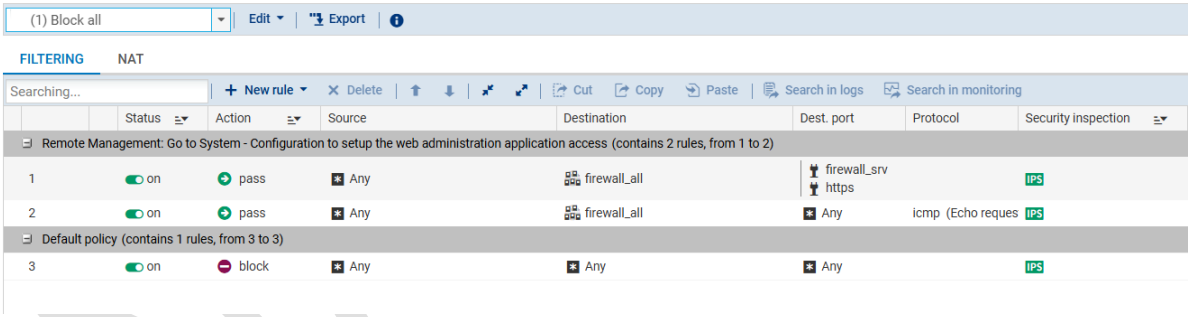
Accédez à **Configuration → Politique de sécurité → Filtrage et NAT.**

Créez une nouvelle politique de sécurité :

- Commencez par désactiver la règle de **filtrage Pass all.**
- Ajoutez ensuite les règles de filtrage conformément au cahier des charges.

Copie de la politique existante :

- Sélectionnez la politique **Block all** dans la liste déroulante des politiques de sécurité.
- Copiez-la vers une politique vide dans laquelle vous ajouterez ensuite **les règles NAT**.



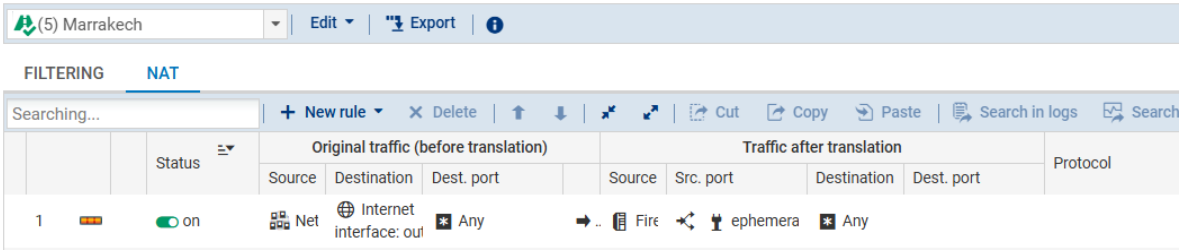
- **Copie de la politique** : Éditez la politique Block all et copiez-la vers une politique vide (Filter 05), puis sauvegardez.

- **Renommage et activation** : Sélectionnez la politique copiée (05 Block all), renommez-la en **Utilisateurs_Block all & NAT**, mettez à jour, puis appliquez et activez la politique.

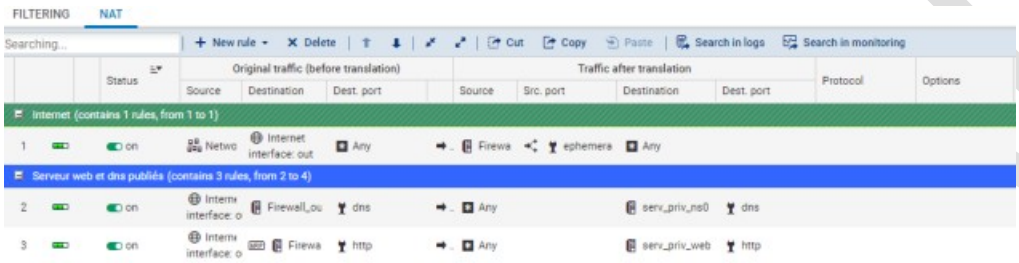
Transfert des règles NAT :

- Sélectionnez la politique précédente contenant les règles NAT, copiez-les.
- Collez-les dans l'onglet NAT de la politique **Utilisateurs_Block all & NAT**.

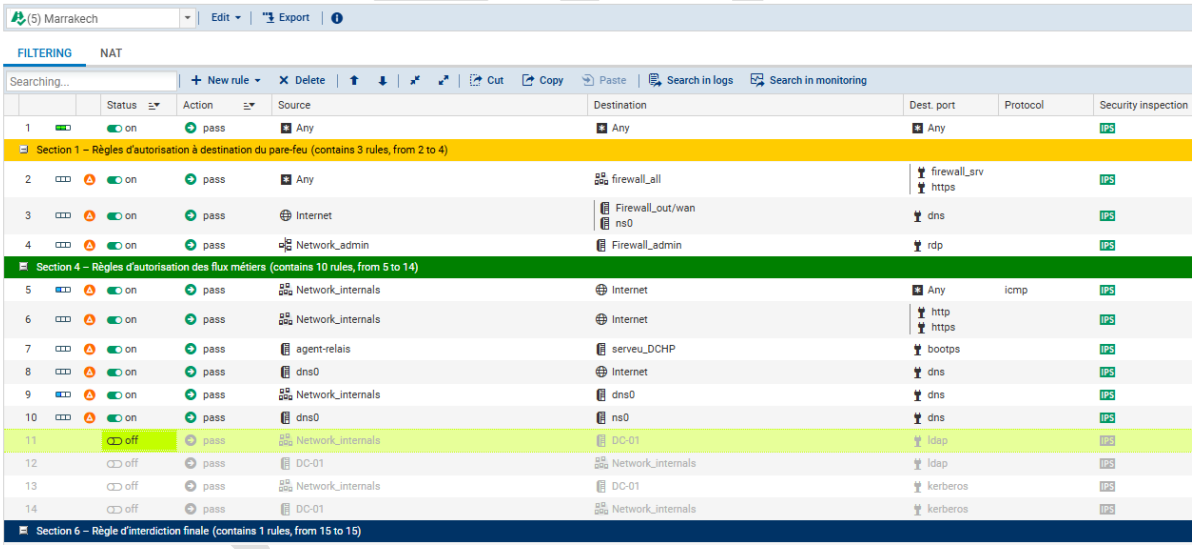
8. Mise en place de NAT dynamique :



9. Configuration de NAT pour publier le serveur Web interne et DNS autoritaire



10. Filtrage protocolaire pour le contexte cub :



11. **Explication des règles de filtrage :**

Règle 1

- **Action :** pass
- **Source :** Any
- **Destination :** Any
- **Port :** Any
- **Interprétation :** règle générale autorisant tout le trafic (généralement à désactiver ou limiter dans une politique stricte).

Règle 2

- **Action :** pass
- **Source :** Any
- **Destination :** firewall_all
- **Port :** HTTPS
- **Interprétation :** autorise l'accès HTTPS vers les services administratifs du firewall depuis toutes les sources.

Règle 3

- **Action :** pass
- **Source :** Internet (interface OUT)
- **Destination :** Firewall_out → ns0
- **Port :** DNS
- **Interprétation :** autorise les requêtes DNS venant d'Internet vers le service DNS exposé du firewall.

Règle 4

- **Action :** pass
- **Source :** Network_admin
- **Destination :** Firewall_admin
- **Port :** RDP
- **Interprétation :** permet à l'équipe de se connecter en RDP vers le firewall.

Règle 5

- **Action :** pass
- **Source :** Network_internals
- **Destination :** Internet
- **Port :** ICMP

- **Interprétation :** autorise les pings des machines internes vers Internet.

Règle 6

- **Action :** pass
- **Source :** Network_internals
- **Destination :** Internet
- **Port :** HTTP/HTTPS
- **Interprétation :** autorise la navigation web des machines internes vers Internet.

Règle 7

- **Action :** pass
- **Source :** agent-relais
- **Destination :** serveur_DHCP
- **Port :** BOOTP
- **Interprétation :** permet au relais DHCP d'acheminer les requêtes vers le serveur DHCP.

Règle 8

- **Action :** pass
- **Source :** dns0
- **Destination :** Internet
- **Port :** DNS
- **Interprétation :** permet au serveur DNS interne de faire des requêtes DNS vers Internet.

Règle 9

- **Action :** pass
- **Source :** Network_internals
- **Destination :** dns0
- **Port :** DNS
- **Interprétation :** autorise les machines internes à interroger le serveur DNS interne.

Règle 10

- **Action :** pass
- **Source :** dns0
- **Destination :** ns0
- **Port :** DNS
- **Interprétation :** autorise la communication entre les serveurs DNS internes.

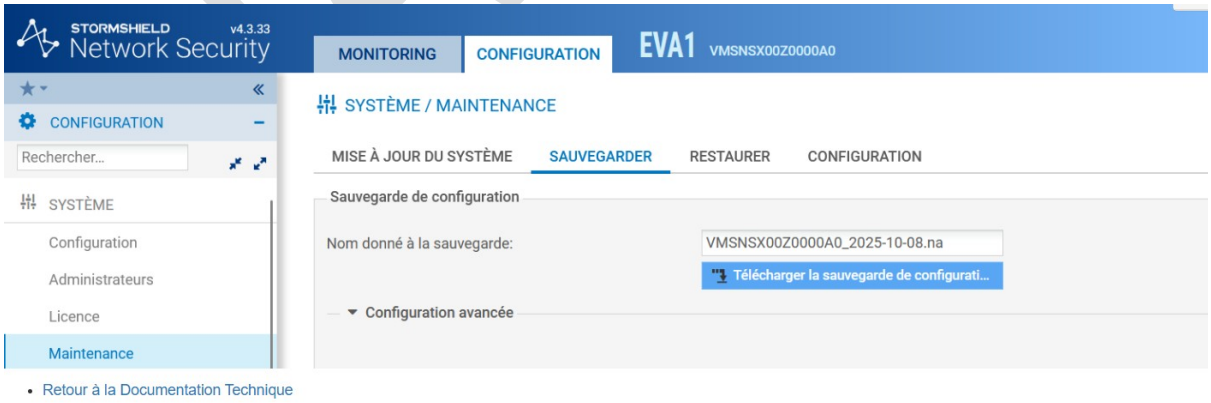
Règle 11

- **Action :** pass
- **Source :** Network_internals
- **Destination :** DC-01
- **Port :** LDAP
- **Interprétation :** autorise les machines internes à accéder au service LDAP du contrôleur de domaine.

12. Sauvegarde de la configuration

Pour sauvegarder la configuration de votre pare-feu Stormshield :

1. Accédez à **Configuration → Système → Maintenance**.
2. Ouvrez l'onglet **Sauvegarde**.
3. Téléchargez le fichier de sauvegarde.



Bonus Schéma de câblage réseau avec un pare-feu Stormshield et un switch Cisco :