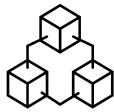


Mise en place d'un pare-feu Stormshield (SNS)



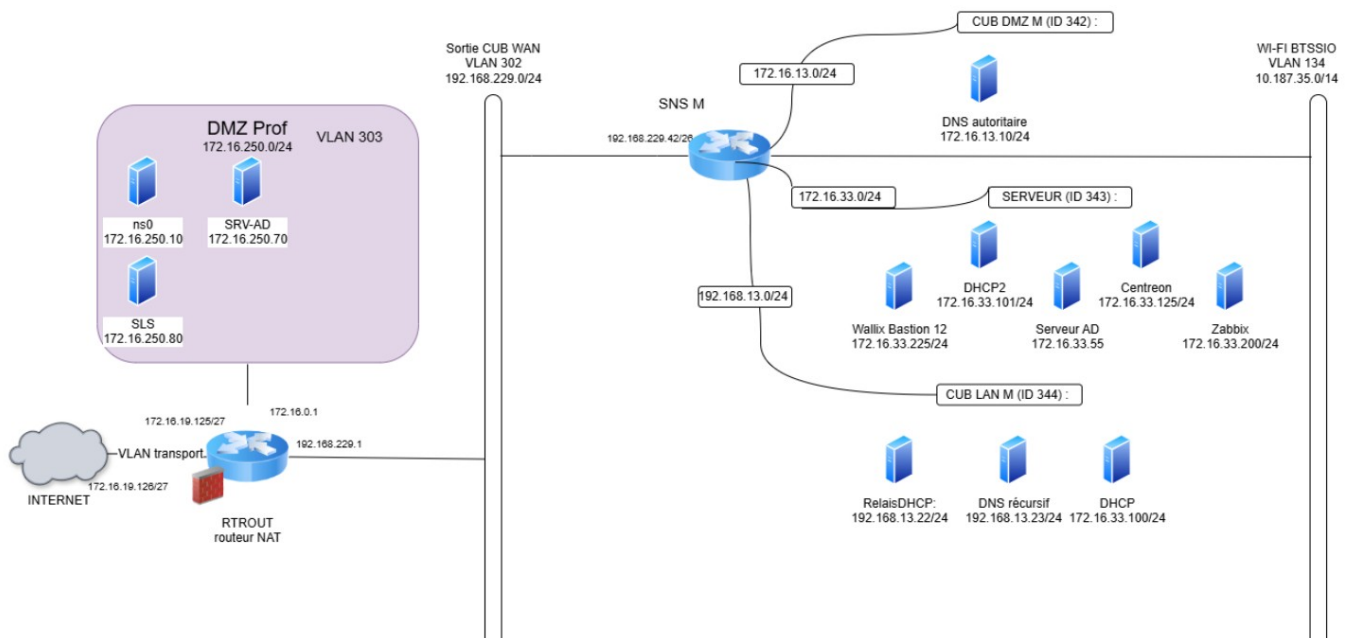
Sommaire

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)

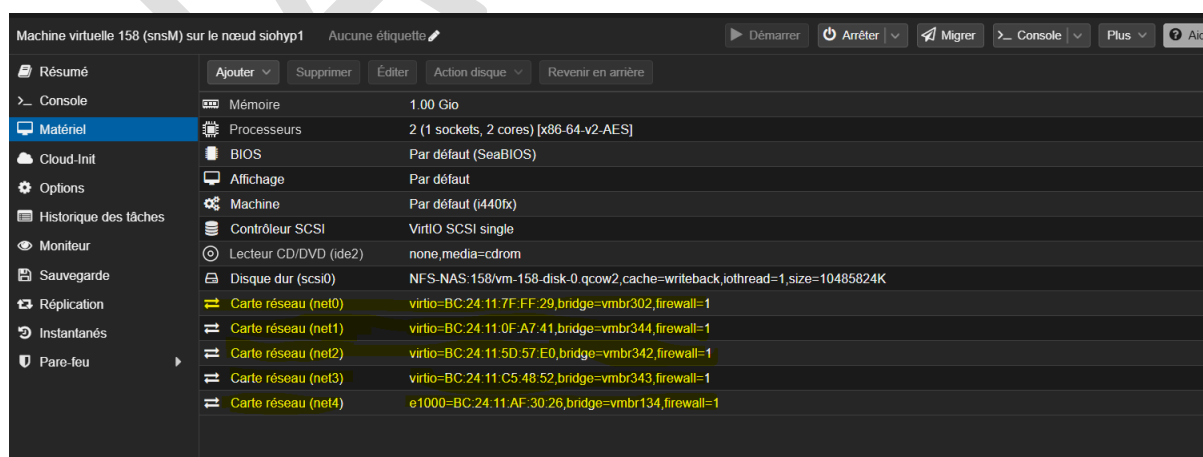
Clone VM Template 278 (Modele-SNS-4.3) ✕

Nœud cible:	<input type="text" value="siohyp3"/>	Mode:	<input type="text" value="Clone lié"/>
VM ID:	<input type="text" value="144"/>	Stockage cible:	<input type="text" value="Identique à la source"/>
Nom:	<input type="text" value="SNS"/>	Format:	<input type="text" value="Image au format QEMU"/>
Pool de ressources:	<input type="text" value="SIO2024_SISR_2_E"/>		

? Aide
Cloner

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 :

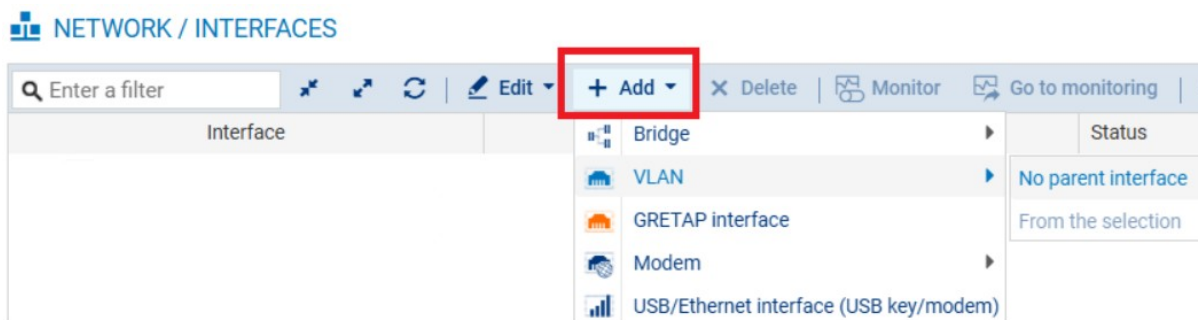
4. Se connecter à l'interface Web du SNS

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.**

NETWORK / ROUTING

IPV4 STATIC ROUTES IPV4 DYNAMIC ROUTING IPV4 RETURN ROUTES

General

Default gateway (router):

Object name: gatewayM
IP address: 192.168.229.1

STATIC ROUTES

Searching... + Add X Delete

Status	Destination network (host, network or grou...	Interface	Address range
--------	---	-----------	---------------

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**.

(1) Block all Edit Export

FILTERING NAT

Searching... + New rule X Delete ↑ ↓ ↻ ↺ Cut Copy Paste Search in logs Search in monitoring

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
Remote Management: Go to System - Configuration to setup the web administration application access (contains 2 rules, from 1 to 2)							
1	on	pass	Any	firewall_all	firewall_srv https		IPS
2	on	pass	Any	firewall_all	Any	icmp (Echo request)	IPS
Default policy (contains 1 rules, from 3 to 3)							
3	on	block	Any	Any	Any		IPS

- **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 :

(5) Marrakech										
FILTERING NAT										
Searching...										
+ New rule - X Delete ↑ ↓ Cut Copy Paste Search in logs Search										
	Status	Original traffic (before translation)			Traffic after translation				Protocol	
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port		
1	on	Net	Internet interface: out	Any	Fire	ephemera	Any			

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

(5) Marrakech										
FILTERING NAT										
Searching...										
+ New rule - X Delete ↑ ↓ Cut Copy Paste Search in logs Search in monitoring										
	Status	Action	Original traffic (before translation)			Traffic after translation			Protocol	Options
			Source	Destination	Dest. port	Source	Src. port	Destination		
Internet (contains 1 rules, from 1 to 1)										
1	on	pass	Netro	Internet interface: out	Any	Firewa	ephemera	Any		
Serveur web et dns publiés (contains 3 rules, from 2 to 4)										
2	on	pass	Intern interface: o	Firewall_lo	dns	Any	serv_priv_ns0	dns		
3	on	pass	Intern interface: o	Firewa	http	Any	serv_priv_web	http		

10. Filtrage protocolaire pour le contexte cub :

(5) Marrakech										
FILTERING NAT										
Searching...										
+ New rule - X Delete ↑ ↓ Cut Copy Paste Search in logs Search in monitoring										
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection			
								1	on	pass
Section 1 - Règles d'autorisation à destination du pare-feu (contains 3 rules, from 2 to 4)										
2	on	pass	Any	firewall_all	firewall_srv	https	IPS			
3	on	pass	Internet	Firewall_out/wan	ns0	dns	IPS			
4	on	pass	Network_admin	Firewall_admin	rdp		IPS			
Section 4 - Règles d'autorisation des flux métiers (contains 10 rules, from 5 to 14)										
5	on	pass	Network_internals	Internet	Any	icmp	IPS			
6	on	pass	Network_internals	Internet	http	https	IPS			
7	on	pass	agent-relais	serveu_DCHP	bootps		IPS			
8	on	pass	dns0	Internet	dns		IPS			
9	on	pass	Network_internals	dns0	dns		IPS			
10	on	pass	dns0	ns0	dns		IPS			
11	off	pass	Network_internals	DC-01	ldap		IPS			
12	off	pass	DC-01	Network_internals	ldap		IPS			
13	off	pass	Network_internals	DC-01	kerberos		IPS			
14	off	pass	DC-01	Network_internals	kerberos		IPS			
Section 6 - Règle d'interdiction finale (contains 1 rules, from 15 to 15)										

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.



The screenshot displays the Stormshield Network Security v4.3.33 interface. The top navigation bar includes 'MONITORING', 'CONFIGURATION', and 'EVA1 VMSNSX00Z0000A0'. The left sidebar shows a tree view with 'CONFIGURATION' selected, and sub-items like 'Rechercher...', 'SYSTÈME', 'Configuration', 'Administrateurs', 'Licence', and 'Maintenance'. The main content area is titled 'SYSTÈME / MAINTENANCE' and features tabs for 'MISE À JOUR DU SYSTÈME', 'SAUVEGARDER', 'RESTAURER', and 'CONFIGURATION'. The 'SAUVEGARDER' tab is active, showing a 'Sauvegarde de configuration' section with a text input field containing 'VMSNSX00Z0000A0_2025-10-08.na' and a 'Télécharger la sauvegarde de configurati...' button. A 'Configuration avancée' dropdown is also visible.

• Retour à la Documentation Technique

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

