GOURMET&CO

Documentation Technique

Configuration du pare-feu UTM Stormshield

Projet	SIO2-AP3 — Atelier de Professionnalisation
Client	Gourmet&Co — Bordeaux
Équipement	UTM Stormshield (OVA VirtualBox)
Version du document	1.0
Date	Mars 2026
Auteur	Équipe Informatique Gourmet&Co

Sommaire

1. Contexte du projet

1.1 Présentation de Gourmet&Co

Gourmet&Co est une entreprise spécialisée dans la distribution de produits alimentaires haut de gamme à destination des restaurants et hôtels de luxe. Basée à Bordeaux, elle dispose d'un entrepôt logistique et de bureaux administratifs regroupant une quarantaine d'employés (commerciaux, gestionnaires de stock, comptables et service client).

Dans le cadre de son expansion, Gourmet&Co a engagé une modernisation de son infrastructure informatique, visant à :

- Améliorer la communication interne
- Sécuriser le réseau via un pare-feu UTM
- Assurer une supervision efficace des équipements
- Mettre en place des services partagés (Active Directory, OwnCloud, Centreon)

1.2 Architecture réseau générale

L'infrastructure repose sur les équipements et machines virtuelles suivants :

Nom de la VM	Rôle	OS	Adressage
UTM-STORMSHIELD	Pare-feu UTM	OVA Stormshield	Statique
SRV-OWNCLOUD	Serveur OwnCloud	Debian 12	Statique
SRV-CENTREON	Supervision Centreon	Debian 12	Statique
SRV-AD-DHCP	Active Directory / DHCP	Windows Server 2022	Statique
PC-CLIENT01	Poste client	Windows 11	DHCP

1.3 Plan d'adressage IP

Le Stormshield assure le routage inter-VLAN entre les trois réseaux internes et l'accès WAN :

Interface	VLAN ID	Adresse IPv4	Type	Description
datacenter	VLAN 10	192.168.1.254/24	Interne	Serveurs (AD, Centreon...)
Lan_Client	VLAN 20	192.168.2.254/24	Interne	Postes clients
DMZ	VLAN 30	192.168.3.254/24	Interne	Serveur OwnCloud
wan	—	192.168.147.77/24 (DHCP)	Externe	Accès Internet / réseau lycée

2. Configuration des interfaces réseau

Le Stormshield dispose de quatre interfaces réseau configurées depuis le menu Réseau > Interfaces. Les trois interfaces internes sont des sous-interfaces VLAN rattachées au port physique « port », tandis que l'interface WAN est directement connectée au réseau externe.

2.1 Vue d'ensemble des interfaces

La capture ci-dessous présente la liste complète des interfaces configurées sur le Stormshield :

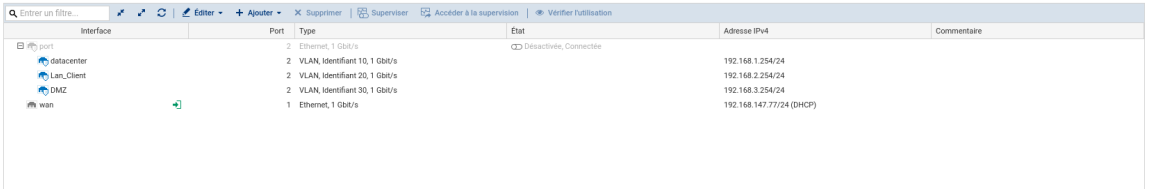

Figure 1 — Vue d'ensemble des interfaces Stormshield

2.2 Interface datacenter (VLAN 10)

Cette interface est dédiée au segment réseau hébergeant les serveurs internes (SRV-AD-DHCP, SRV-CENTREON).

Nom	datacenter
Interface parente	port
Identifiant VLAN	10
Adresse IPv4	192.168.1.254/24
Type	Interne (protégée)
Adressage	IP fixe (statique)

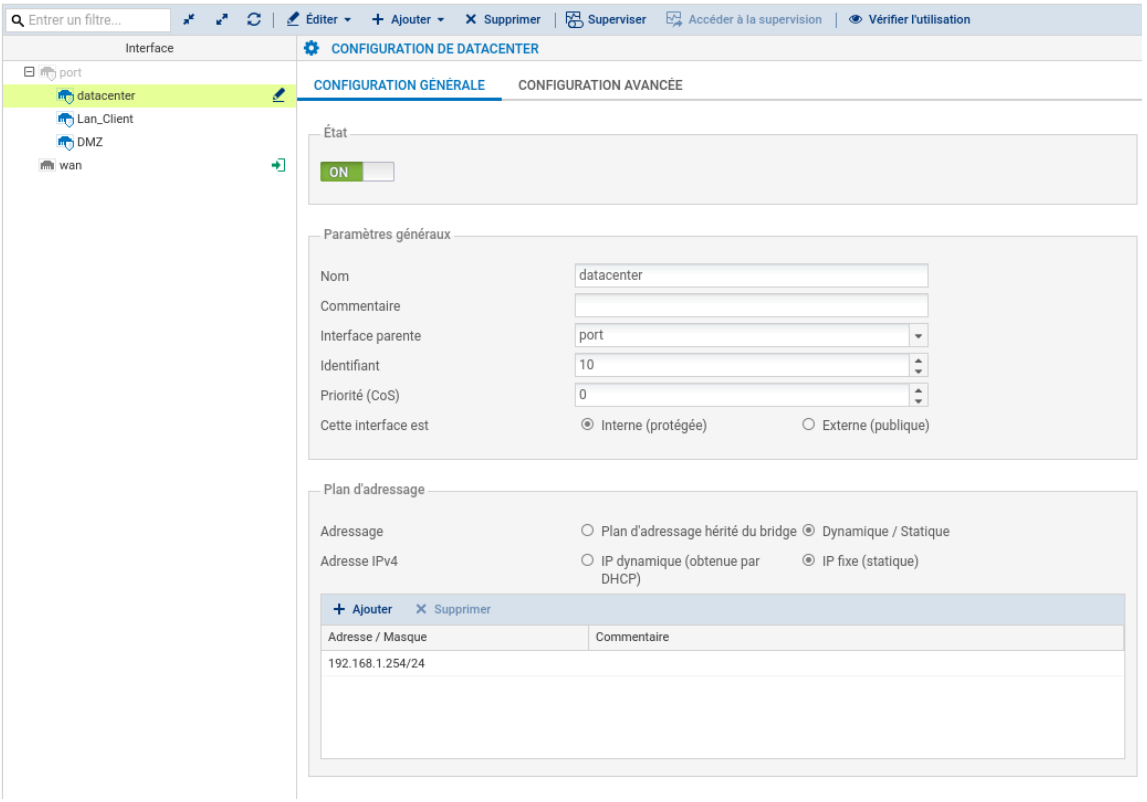

Figure 2 — Configuration de l'interface datacenter

2.3 Interface Lan_Client (VLAN 20)

Cette interface dessert le réseau des postes utilisateurs. Les adresses IP y sont distribuées par relai DHCP vers le serveur SRV-AD-DHCP.

Nom	Lan_Client
Interface parente	port
Identifiant VLAN	20
Adresse IPv4	192.168.2.254/24
Type	Interne (protégée)
Adressage	IP fixe (statique)

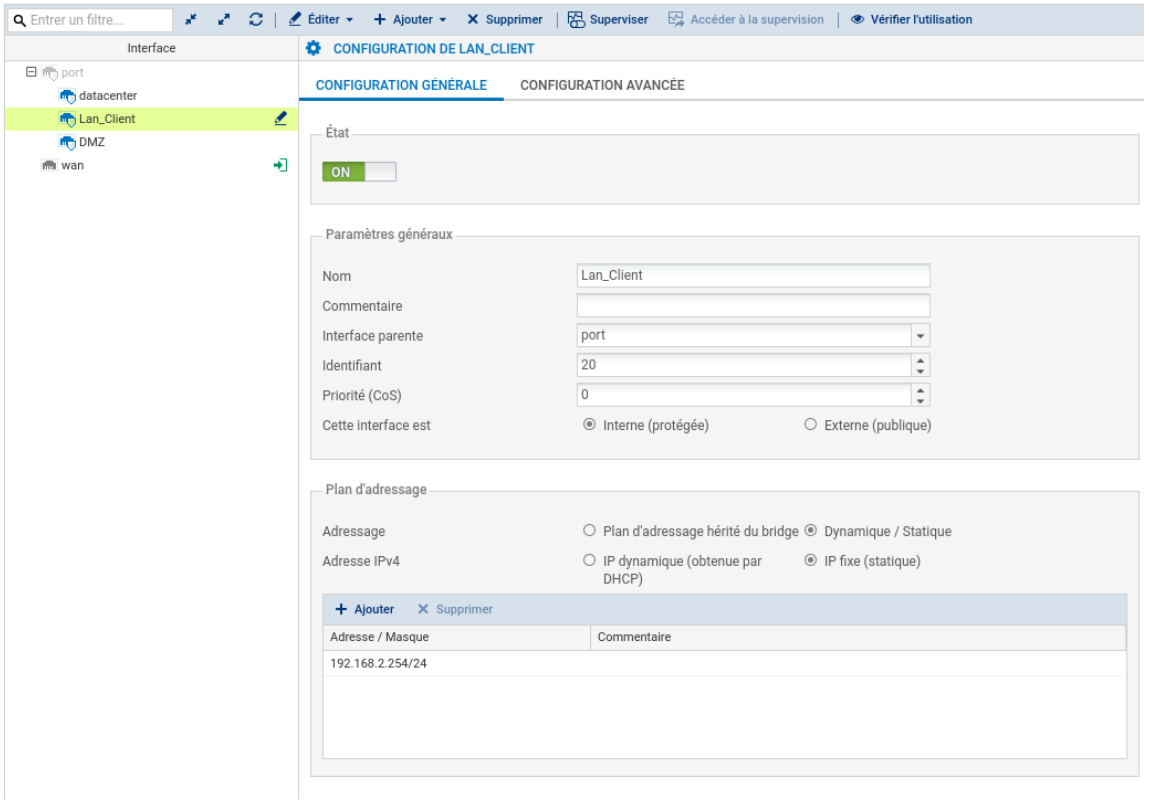

Figure 3 — Configuration de l'interface Lan_Client

2.4 Interface DMZ (VLAN 30)

La DMZ (Zone DéMilitarisée) héberge le serveur OwnCloud, accessible depuis internet (réseau lycée) via les règles NAT. Elle est isolée des autres segments internes.

Nom	DMZ
Interface parente	port
Identifiant VLAN	30
Adresse IPv4	192.168.3.254/24
Type	Interne (protégée)
Adressage	IP fixe (statique)

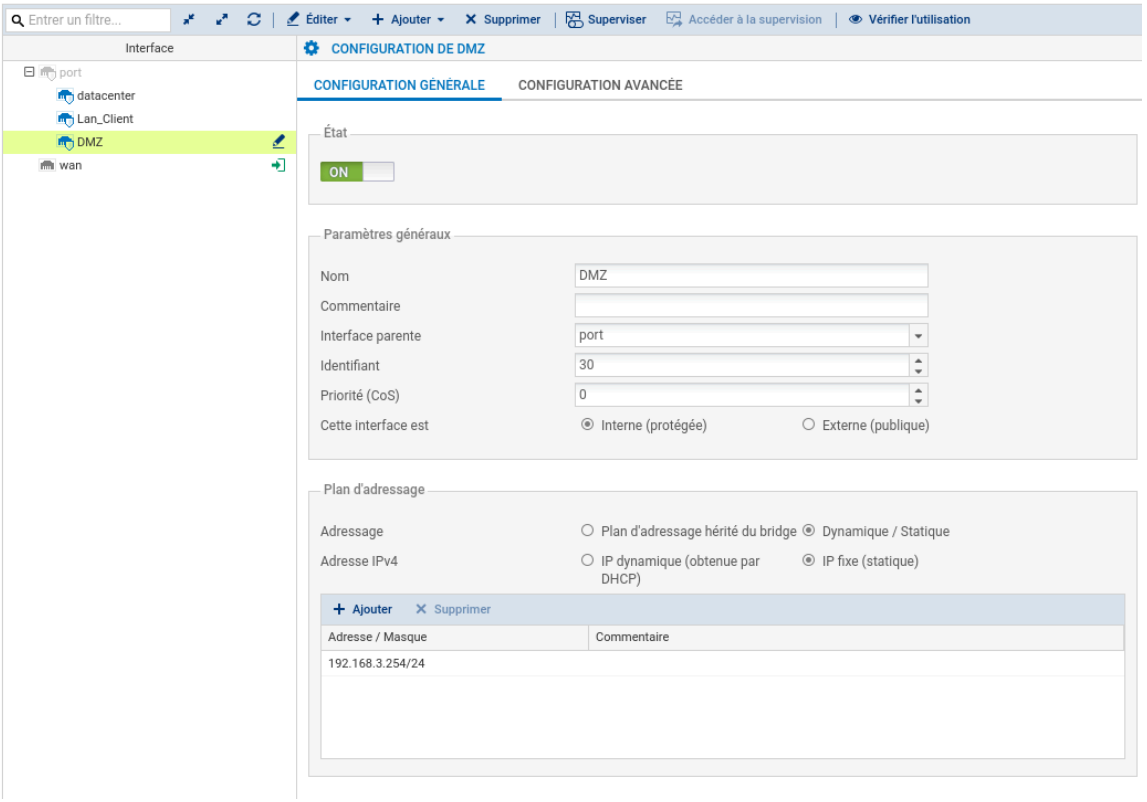

Figure 4 — Configuration de l'interface DMZ

2.5 Interface WAN

L'interface WAN connecte le Stormshield au réseau externe (réseau lycée simulant internet). Elle est configurée en DHCP pour obtenir son adresse automatiquement depuis le réseau pédagogique.

Nom	wan
Type	Externe (publique)
Adressage IPv4	IP dynamique (DHCP)
Adresse obtenue	192.168.147.77/24

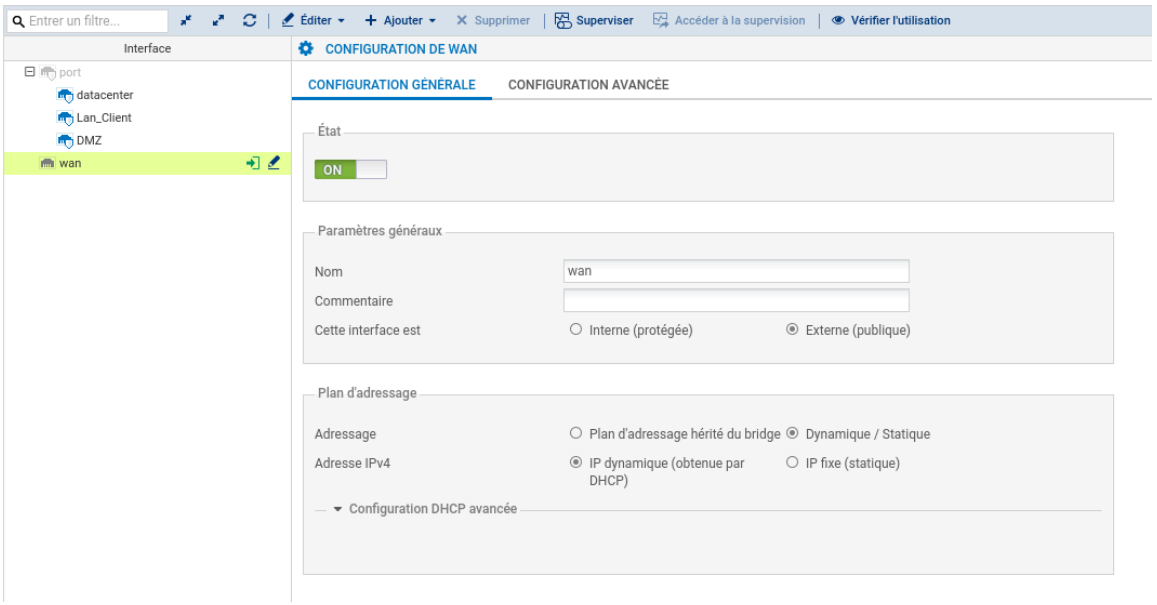

Figure 5 — Configuration de l'interface WAN

3. Configuration du relai DHCP

Le Stormshield est configuré en tant que relai DHCP (et non serveur DHCP). Il transmets les requêtes DHCP émises par les clients vers le serveur SRV-AD-DHCP situé dans le VLAN datacenter.

3.1 Paramètres du relai

Mode DHCP	Relai DHCP (relay)
Serveur DHCP cible	srvdhcp (SRV-AD-DHCP)
Interfaces écoutées	Lan_Client, datacenter

Ce choix architectural permet de centraliser la gestion des baux DHCP sur le serveur Windows Active Directory, ce qui facilite l'intégration avec le service DNS et la gestion des postes du domaine.

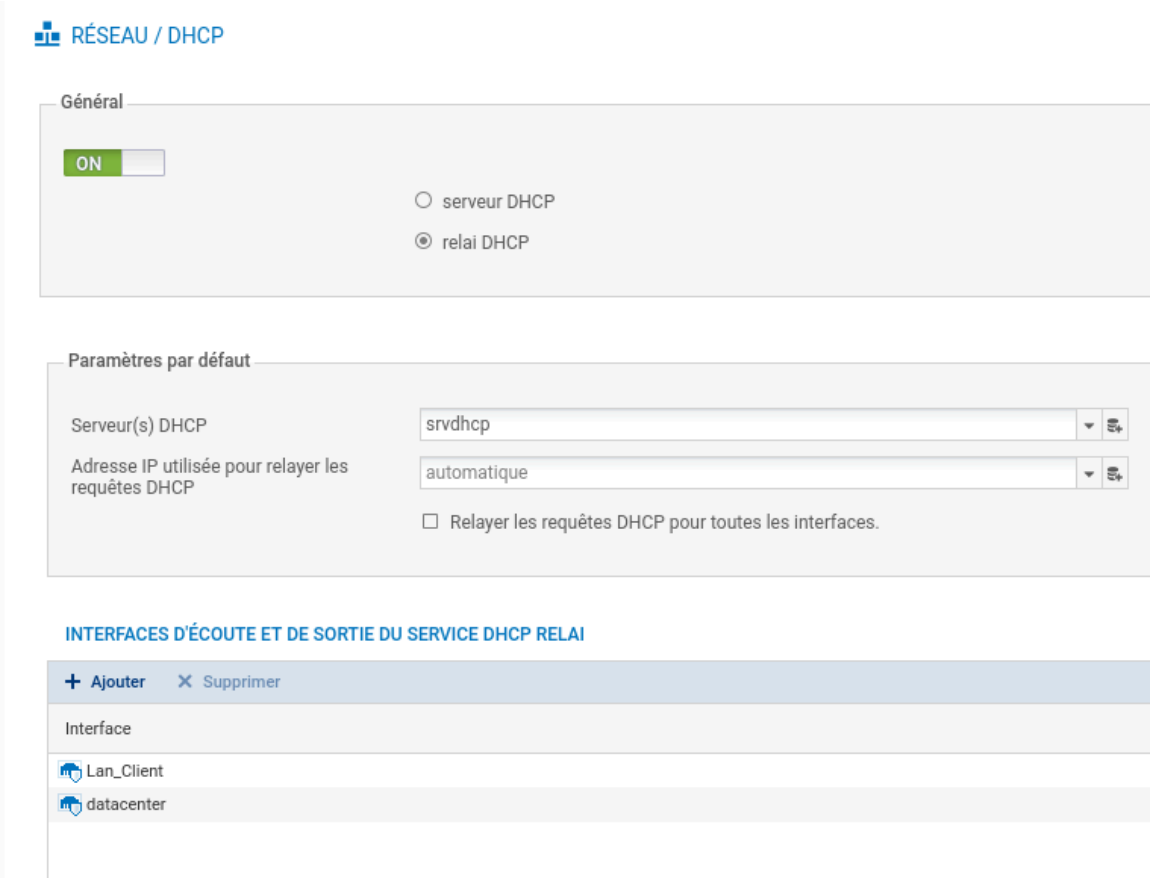

Figure 6 — Configuration du relai DHCP sur le Stormshield

4. Règles de filtrage (Politique de sécurité)

La politique de filtrage du Stormshield est nommée « Pass all » (règle n°10). Elle définit les flux autorisés entre les différentes zones réseau. Les règles sont évaluées de haut en bas, la première correspondance étant appliquée.

4.1 Vue d'ensemble des règles de filtrage

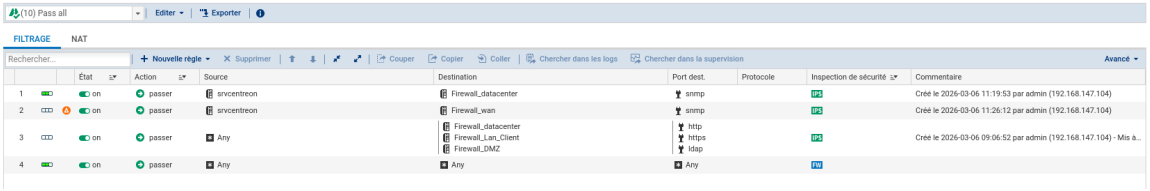

Figure 7 — Règles de filtrage de la politique « Pass all »

4.2 Détail des règles

N°	Source	Destination	Port dest.	Protocole	Inspection	Commentaire
1	srvcentreon	Firewall_datacenter	SNMP	—	IPS	Supervision SNMP datacenter (créée le 2026-03-06)
2	srvcentreon	Firewall_wan	SNMP	—	IPS	Supervision SNMP WAN (créée le 2026-03-06)
3	Any	Firewall_datacenterFirewall_Lan_ClientFirewall_DMZ	HTTP, HTTPS, LDAP	—	IPS	Accès aux interfaces de gestion et services
4	Any	Any	Any	—	FW	Règle permissive finale (pass all)

4.3 Analyse des règles

Règle 1 — Supervision SNMP datacenter

Autorise le serveur Centreon (srvcentreon) à interroger le Stormshield via SNMP sur l'interface datacenter. L'inspection IPS est activée pour surveiller ce trafic.

Règle 2 — Supervision SNMP WAN

Autorise le serveur Centreon à interroger l'interface WAN du firewall via SNMP. Utile pour surveiller la connectivité externe. L'état « orange » indique une alerte ou avertissement sur cette règle.

Règle 3 — Accès services HTTP/HTTPS/LDAP

Autorise tout le trafic HTTP, HTTPS et LDAP à destination des interfaces internes du Stormshield. Cette règle permet notamment l'authentification LDAP via Active Directory depuis les différentes zones.

Règle 4 — Pass all (règle permissive)

Règle de dernier recours autorisant tout le trafic restant. Elle est positionnée en fin de liste et utilise l'inspection FW (firewall simple sans IPS). À restreindre progressivement en production.

5. Règles NAT (Translation d'adresses)

Les règles NAT permettent d'exposer les services internes (Centreon, OwnCloud) sur le réseau externe et d'assurer la traduction pour les accès sortants des machines internes.

5.1 Vue d'ensemble des règles NAT

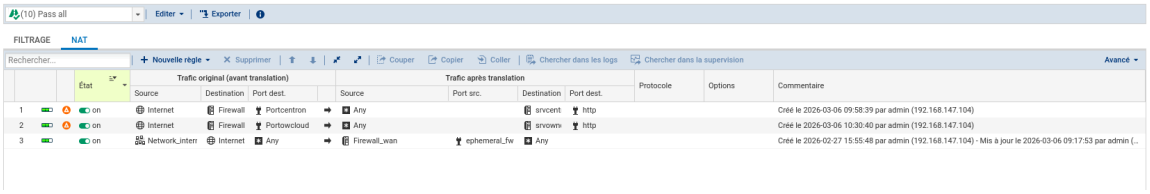

Figure 8 — Règles NAT configurées sur le Stormshield

5.2 Détail des règles NAT

N°	Source orig.	Destination orig.	Port orig.	Source trad.	Destination trad.	Port trad.
1	Internet	Firewall (Portcentron)	—	Any	srvcent	HTTP
2	Internet	Firewall (Portowcloud)	—	Any	srvown	HTTP
3	Network_interne	Internet	Any	Firewall_wan (éphémère)	Any	Any

5.3 Explication des règles NAT

Règle 1 — Publication du serveur Centreon

Redirige les connexions entrantes depuis internet sur le port « Portcentron » vers l'adresse HTTP du serveur Centreon (srvcent). Permet l'accès à l'interface web de supervision Centreon depuis le réseau externe.

Règle 2 — Publication du serveur OwnCloud

Redirige les connexions entrantes depuis internet sur le port « Portowcloud » vers le serveur OwnCloud (srvown) sur le port HTTP. Permet aux employés d'accéder à OwnCloud depuis internet (réseau lycée).

Règle 3 — Masquerade (sortant)

Règle de masquerade NAT pour le trafic sortant : traduit les adresses IP source du réseau interne en l'adresse éphémère du Stormshield WAN, permettant aux machines internes d'accéder à internet.

6. Configuration de l'agent SNMP

Le protocole SNMP (Simple Network Management Protocol) est activé sur le Stormshield afin de permettre sa supervision par le serveur Centreon. La version SNMPv1/v2c est utilisée dans cette maquette.

6.1 Paramètres de l'agent SNMP

État	Actif (ON)
Version	SNMPv1/v2c
sysLocation	VMSNSX09K0639A9
sysContact	who@where
Traps IPS (intrusion)	Alertes majeures et mineures
Traps événements système	Alertes majeures et mineures

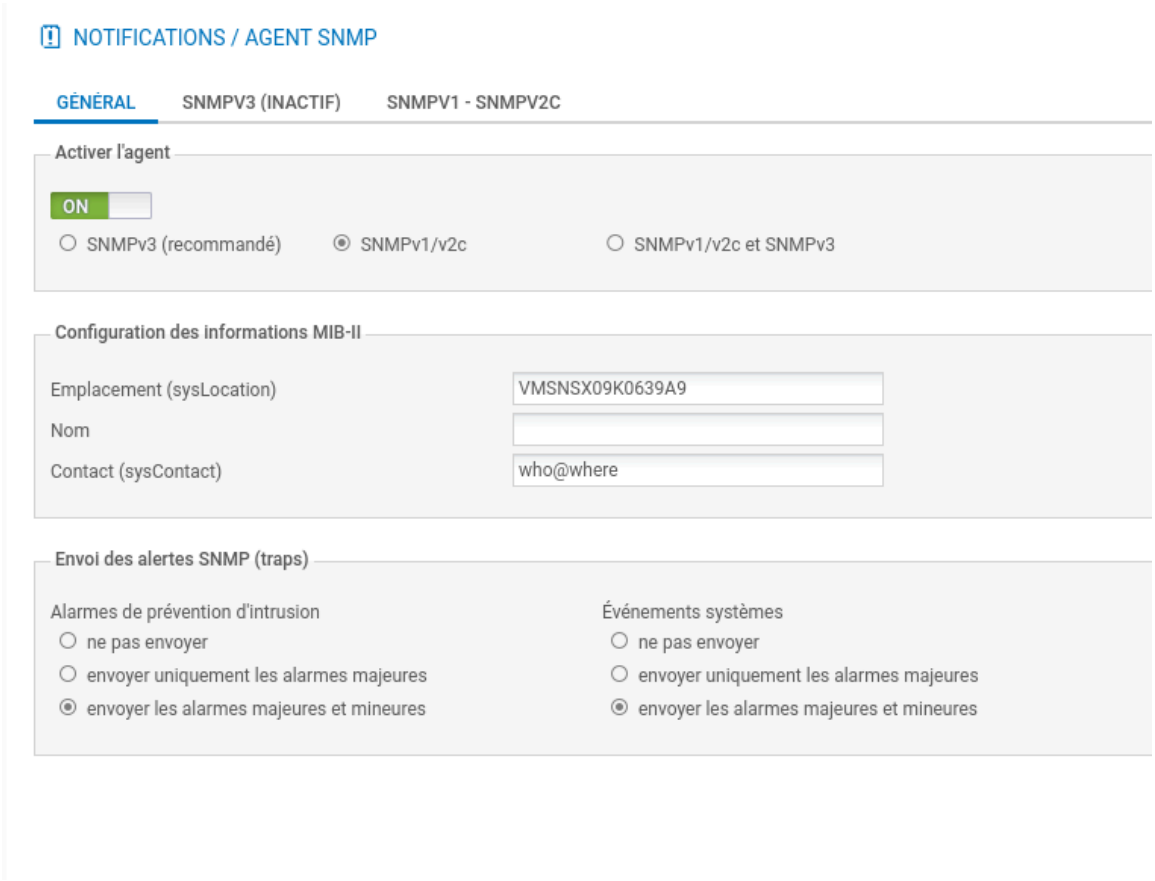

Figure 9 — Configuration de l'agent SNMP du Stormshield

6.2 Rôle dans l'architecture

L'agent SNMP permet au serveur Centreon de collecter des métriques sur le Stormshield : état des interfaces, charge CPU/mémoire, alertes d'intrusion IPS, événements système. Les règles de

filtrage n°1 et n°2 autorisent explicitement ce trafic SNMP depuis srvcentreon vers les interfaces datacenter et WAN du firewall.

7. Bilan et points de vigilance

7.1 Récapitulatif de la configuration

Le pare-feu UTM Stormshield est désormais entièrement configuré pour l'infrastructure Gourmet&Co :

- 4 interfaces réseau opérationnelles (datacenter VLAN10, Lan_Client VLAN20, DMZ VLAN30, WAN)
- Relai DHCP actif vers le serveur SRV-AD-DHCP
- 4 règles de filtrage couvrant la supervision SNMP, les accès services et le trafic général
- 3 règles NAT pour la publication de Centreon, OwnCloud et la sortie internet
- Agent SNMP actif en version SNMPv1/v2c avec envoi de traps vers Centreon

7.2 Points de vigilance

- La règle de filtrage n°4 « Pass all » est très permissive. En environnement de production, il conviendrait de la remplacer par des règles explicites.
- L'agent SNMP utilise SNMPv1/v2c qui ne chiffre pas les données. En production, préférer SNMPv3 avec authentification et chiffrement.
- La règle NAT n°2 (orange) sur le WAN mérite une vérification de son état dans les logs Stormshield.
- Régénérer l'adresse MAC de l'interface WAN lors de l'import VirtualBox est indispensable pour éviter les conflits réseau.