DOCUMENTATION TECHNIQUE

Firewall Stormshield SNS

GourmetAndCo

Configuration couverte **Réseau, DHCP, NAT, Filtrage**

Sommaire

1. Configuration générale du Firewall

1.1 Identité du Firewall

Nom du Firewall	GourmetAndCo
Langue du Firewall (traces)	Français
Clavier (console)	Français

1.2 Paramètres cryptographiques

✔ Récupération régulière des listes de révocation de certificats (CRL) activée
✘ Mode de conformité « Diffusion Restreinte (DR) » version 2021 — désactivé

1.3 Politique de mots de passe

Longueur minimale des mots de passe	8 caractères
Types de caractères obligatoires	Aucun
Entropie minimale	20

1.4 Date, heure et fuseau horaire

Fuseau horaire	GMT
Paramètres au moment de la capture	27/02/2026 15:36:32
Synchronisation NTP	Non activée
Synchronisation avec la machine locale	Non activée

2. Interfaces réseau et VLANs

2.1 Vue d'ensemble des interfaces

Le firewall GourmetAndCo dispose d'un port physique (Port) sur lequel sont déclarés plusieurs VLANs et interfaces logiques. Voici le récapitulatif des interfaces configurées :

Interface	Port	Type	État	Adresse IPv4
Datacenter	2	VLAN, Identifiant 10, 1 Gbit/s	—	192.168.10.254/24
LAN	2	VLAN, Identifiant 20, 1 Gbit/s	—	192.168.20.254/24
DMZ	2	VLAN, Identifiant 30, 1 Gbit/s	—	192.168.30.254/24
WAN	1	Ethernet, 1 Gbit/s	Désactivée, Connectée	192.168.147.17/24 (DHCP)

2.2 Détail de l'interface Datacenter

Nom	Datacenter
Interface parente	Port
Identifiant VLAN	10
Priorité (CoS)	0
Type	Interne (protégée)
Mode d'adressage	Dynamique / Statique — IP fixe (statique)
Adresse IPv4	192.168.10.254/24
État	Activé (ON)

> **i** Les interfaces LAN et DMZ suivent le même schéma de configuration que Datacenter, avec respectivement les identifiants VLAN 20 et 30 et les adresses gateway .254.

3. Relai DHCP

3.1 Mode de fonctionnement DHCP

Le service DHCP est activé et configuré en mode Relai DHCP (et non en mode serveur DHCP local).

État du service DHCP	Activé (ON)
Mode sélectionné	Relai DHCP
Serveur(s) DHCP cible	WindowsServer
Adresse IP pour relayer les requêtes	automatique
Relayer sur toutes les interfaces	Non (désactivé)

3.2 Interfaces d'écoute et de sortie

Les interfaces sur lesquelles le service DHCP Relai écoute et fait transiter les requêtes sont les suivantes :

Interface activée pour le relai DHCP
LAN
Datacenter

i Le relai DHCP transmet les requêtes des clients des segments LAN et Datacenter vers le serveur Windows nommé « WindowsServer ». Cela évite la nécessité d'un serveur DHCP distinct sur chaque VLAN.

4. NAT — Politique de sécurité

4.1 Vue d'ensemble des règles NAT

La politique NAT (Network Address Translation) est configurée sous Politique de Sécurité > Filtrage et NAT, onglet NAT. Cinq règles sont définies :

#	État	Source (avant)	Dest. (avant)	Port dest.	Source (après)	Destination (après)
1	ON	Network_Internals	Internet	Any	Firewall_WAN + ephemeral_fw	Any
2	ON	Internet	Firewall_WAN	http	Any	OwnCloud (http)
3	ON	Internet	Firewall_WAN	SSH-ownCloud	Any	OwnCloud (ssh)
4	ON	Internet	Firewall_WAN	PortCommon	Any	Commun (http)
5	ON	Internet	Firewall_WAN	SSH-Commun	Any	Commun (ssh)

4.2 Détail des règles NAT

Règle 1 — NAT sortant (masquerade)

Tout le trafic issu des réseaux internes (Network_Internals) à destination d'Internet est translaté. L'adresse source est remplacée par l'IP WAN du firewall (Firewall_WAN) avec un port source éphémère. C'est la règle de masquerade standard permettant l'accès Internet à tous les postes internes.

> Commentaire (capture) : Créé le 2026-02-27 15:14:44.99 — adresses (192.168.141.17x)

Règle 2 — Publication OwnCloud (HTTP)

Le trafic entrant depuis Internet à destination du Firewall_WAN sur le port HTTP (80) est redirigé vers le serveur OwnCloud sur le même port HTTP. Cela permet l'accès public au service OwnCloud en HTTP.

> Commentaire (capture) : Créé le 2026-02-27 15:17:25 — adresses (192.168.141.145)

Règle 3 — Publication OwnCloud (SSH)

Le trafic entrant depuis Internet sur le port SSH-ownCloud est redirigé vers le serveur OwnCloud sur le port SSH standard. Cela permet une administration distante sécurisée du serveur OwnCloud.

> Commentaire : Uniquement pour la configuration

Règle 4 — Publication serveur Commun (HTTP)

Le trafic entrant depuis Internet à destination du Firewall_WAN sur le port PortCommon est redirigé vers le serveur Commun sur le port HTTP. Permet l'accès HTTP public à un second serveur hébergé.

> Commentaire : Uniquement pour la configuration — mis à jour le 2026-07-13 10:19 par adm

Règle 5 — Publication serveur Commun (SSH)

Le trafic entrant depuis Internet sur le port SSH-Commun est redirigé vers le serveur Commun sur le port SSH. Cela permet une administration distante sécurisée du serveur Commun.

4.3 Récapitulatif des flux NAT

> Sortant → Network_Internals → Internet via Firewall_WAN (masquerade ephemeral)
> Entrant → HTTP : Internet → Firewall_WAN → OwnCloud
> Entrant → SSH : Internet → Firewall_WAN → OwnCloud
> Entrant → HTTP : Internet → Firewall_WAN → Commun
> Entrant → SSH : Internet → Firewall_WAN → Commun