Stormshield : UTM, zones et politiques de sécurité

Formation : BTS SIO — Option SISR

1. Rôle et fonctionnement

Un pare-feu stateful suit l'état des connexions. Une solution UTM regroupe plusieurs fonctions, comme le filtrage réseau, l'inspection applicative et la prévention d'intrusions. Les fonctions effectivement disponibles dépendent du modèle, de la version et des licences.

Dans le laboratoire, Stormshield sépare les zones réseau et réalise des traductions d'adresses. Le choix d'un produit français ne suffit pas à démontrer une conformité générale : une certification ou qualification porte sur un périmètre et une version précis.

2. Mise en œuvre

1. Identifier les interfaces WAN, LAN et DMZ à partir du schéma.
2. Configurer leur adressage et les routes nécessaires.
3. Créer des objets nommés pour les réseaux, machines et services.
4. Définir les flux autorisés, puis les règles NAT utiles.
5. Activer la politique prévue, vérifier les journaux et sauvegarder la configuration.

Une règle doit préciser sa source, sa destination, le service et son objectif. L'ordre des règles compte. Limiter les droits d'administration à la zone dédiée.

3. Filtrage et NAT

La traduction ne vaut pas autorisation. Une publication en DMZ nécessite un service actif, une règle NAT, le filtrage adapté et un chemin retour cohérent. Restreindre une règle de sortie à son périmètre évite de traduire involontairement des échanges internes.

La politique **Pass All** utilisée pendant la maquette facilite un diagnostic initial ; elle ne représente pas la politique finale de sécurité.

4. Vérification et dépannage

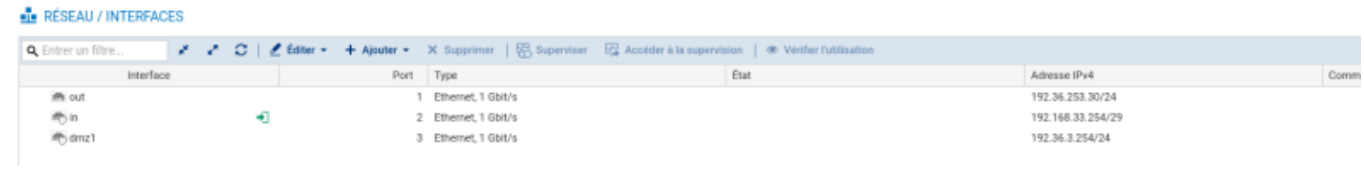
Tester un flux autorisé et un flux interdit depuis chaque zone pertinente. Examiner la politique active, les compteurs, les traces et les routes. Comparer les adresses avant et après traduction plutôt que d'attribuer systématiquement un blocage à l'IPS.

Les affectations réelles figurent dans les tables de routage et la table NAT.

5. Exemple : interfaces et routes

Interface / réseau	Adresse ou prochain saut
WAN	192.36.253.30/24
DMZ	192.36.3.254/24
Liaison vers le switch L3	192.168.33.254/29
Route vers 192.168.3.0/24	192.168.33.253
Route par défaut	192.36.253.254

Créer d'abord les objets réseau utilisés comme prochains sauts, puis les sélectionner dans la table de routage. Les sous-réseaux directement connectés n'ont pas besoin de routes statiques vers eux-mêmes.



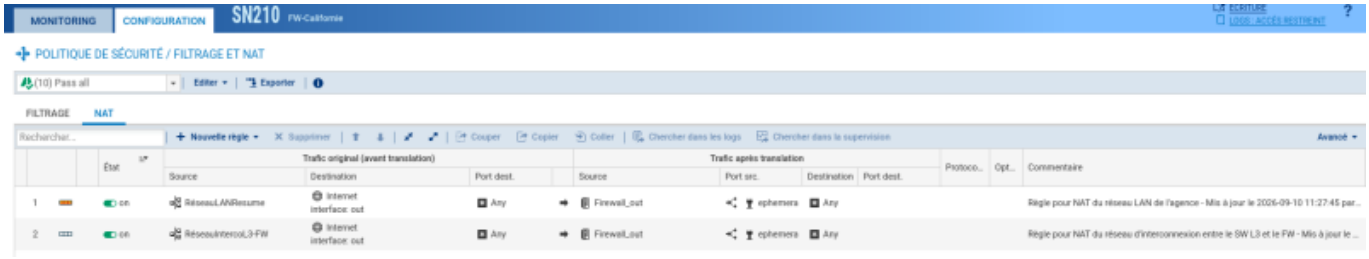
Interfaces réseau du pare-feu dans le laboratoire.



Route résumée vers le LAN et route par défaut.

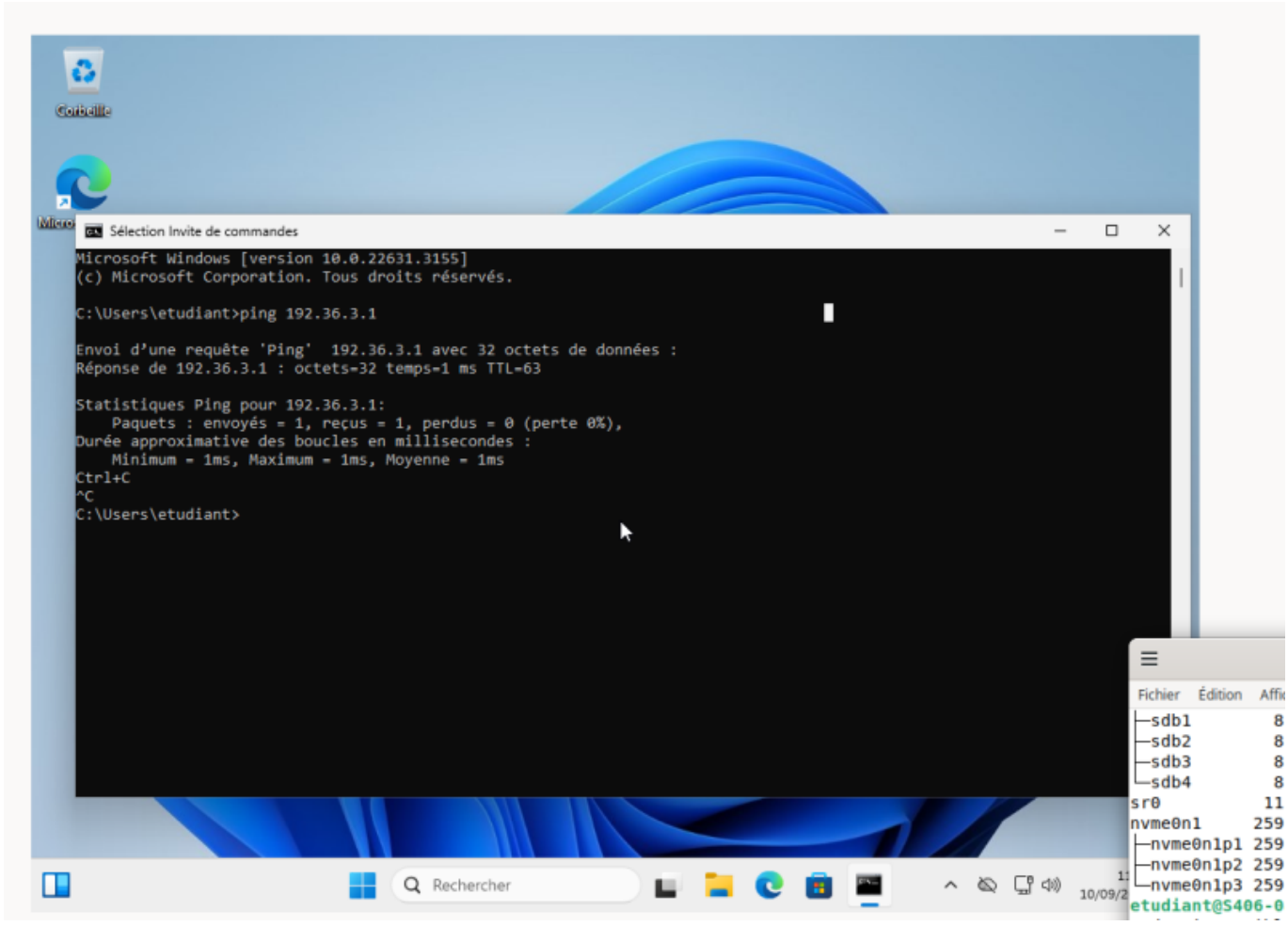
6. Traduction sortante

Les réseaux internes concernés utilisent l'adresse WAN 192.36.253.30 avec traduction de port. Décrire source et destination avant et après traduction permet de distinguer la règle NAT de la règle de filtrage.



Règles de traduction observées sur Stormshield.

Les essais de connectivité figurent dans les captures suivantes. Un ping réussi ne constitue pas une recette complète de publication Web ou FTP.



Test de connectivité depuis le laboratoire.

7. Paramètres d'exploitation

Le nom du pare-feu, ses comptes et son horloge facilitent l'administration et le rapprochement des journaux. Les réglages NTP sont détaillés dans Synchronisation horaire. La politique Pass All utilisée pendant les premiers essais est une étape de diagnostic, pas une politique finale à reproduire.

8. Références

- Stormshield — configuration du filtrage et du NAT

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
https://wiki.ewengadonnaud.xyz/doku.php?id=cyber:stormshield

Last update: **2026/10/18 01:23**