

STORMSHIELD CONFIGURATION DE BASE

*Procédure technique d'une configuration de base d'un routeur
stormshield.*

NYM-IT



Table des matières

Configuration de base d'un Stormshield.....	2
Connexion au Stormshield	2
Connexion à l'interface WEB.....	2
Configuration du système	3
Configuration des interfaces du Stormshield.....	4
Interface LAN.....	4
Interface WAN	5
Configuration de la route par défaut	5
.....	5
Création des règles de filtrage et NAT	6
Filtrage	6
NAT	7
Sauvegarde de la configuration.....	7
Conclusion.....	8

Configuration de base d'un Stormshield

Stormshield, un leader européen dans le domaine de la cybersécurité, offre une gamme de solutions de pare-feu et de sécurité réseau performantes.

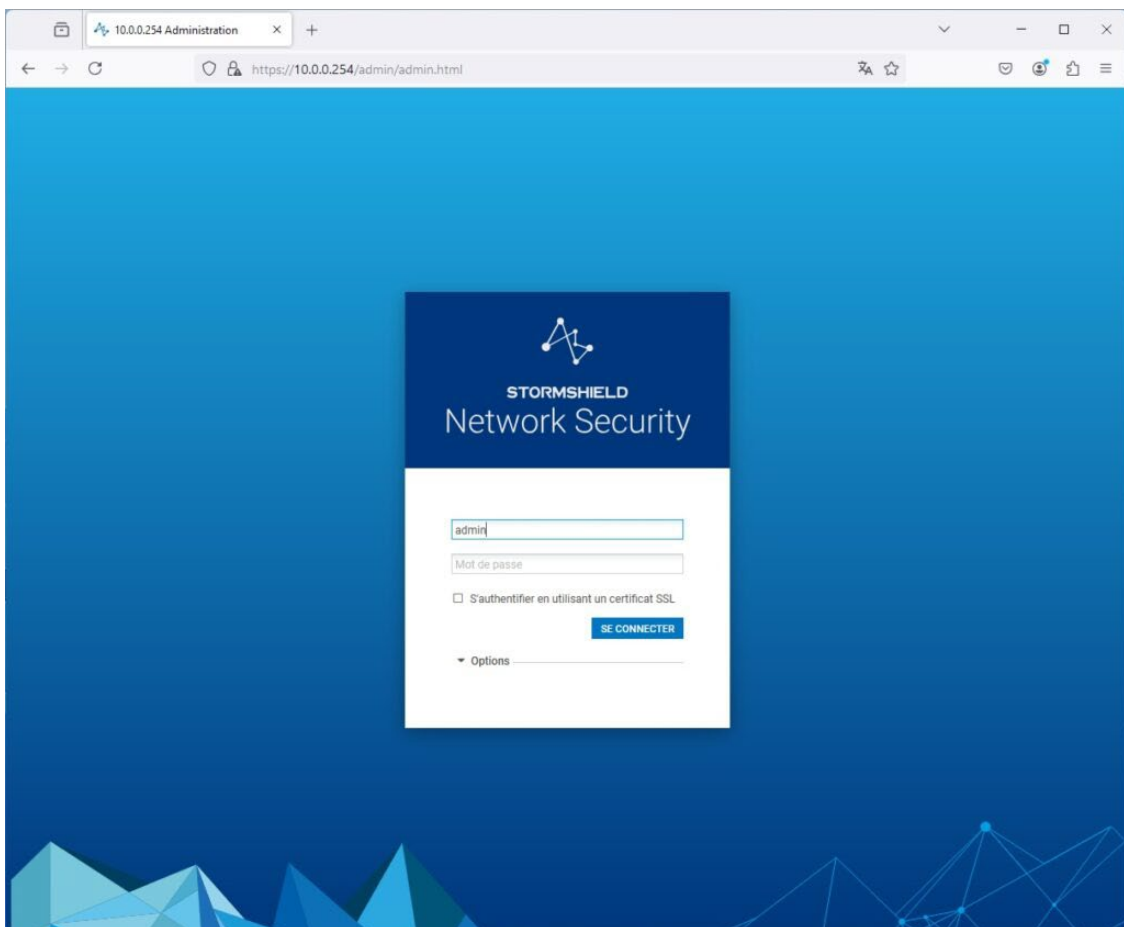
Connexion au Stormshield

- Relier un poste directement sur le **port LAN** du Stormshield.
- Configurer la carte réseau du poste afin qu'elle soit sur le même réseau que le Stormshield.
 - **10.0.0.10 255.255.255.0**

Connexion à l'interface WEB

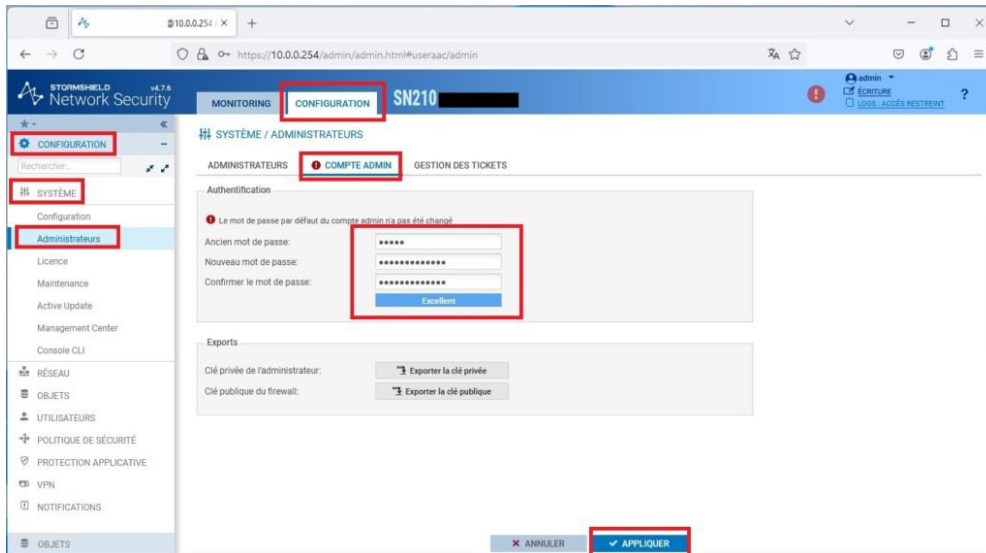
l'interface web est accessible en utilisant l'adresse IP par défaut :

- <https://10.0.0.254/admin/admin.html>
- Utilisateur: admin
- mot de passe: admin

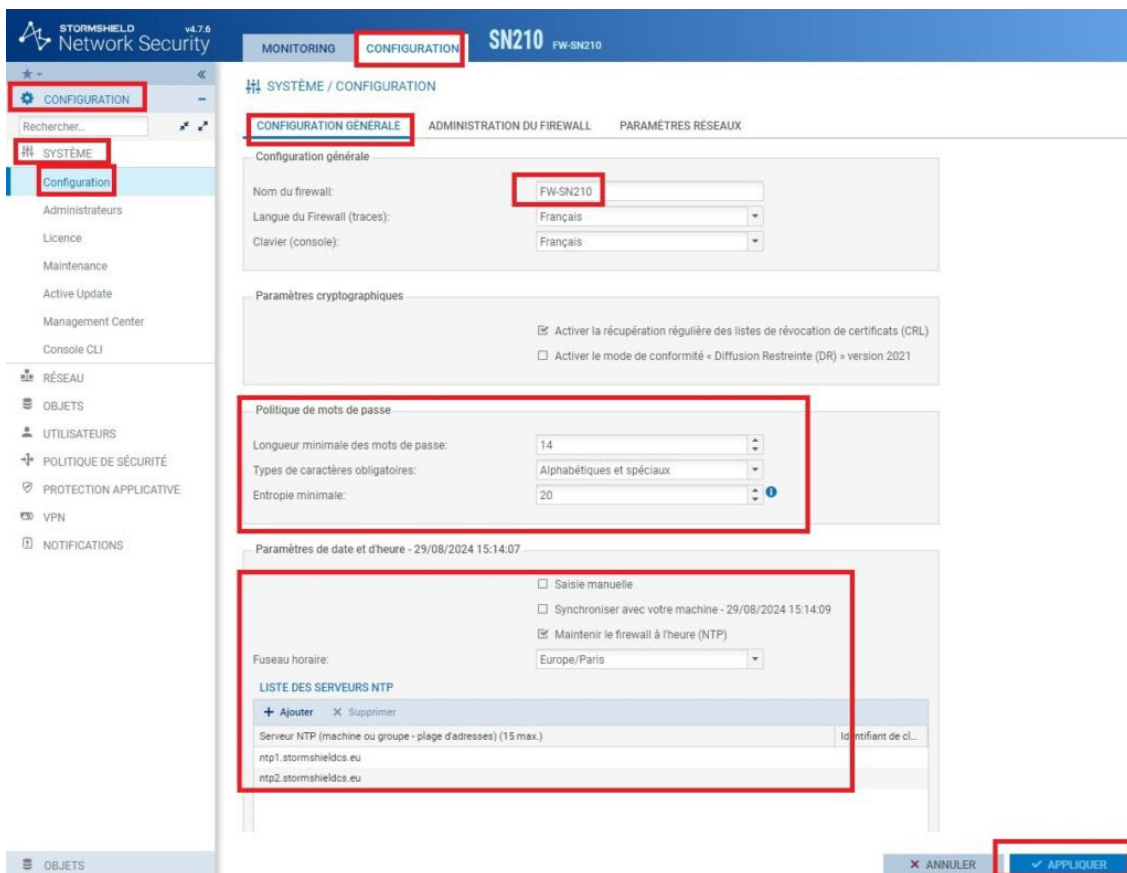


Configuration du système

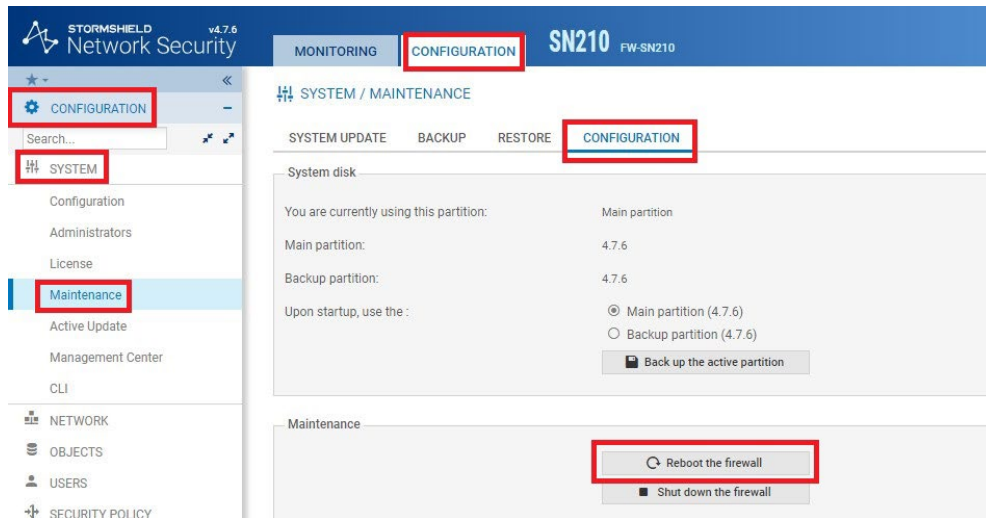
- Accéder à l'onglet « **CONFIGURATION** », puis à « **Configuration > Système > Administrateurs > Compte Admin** ». **Personnalisez le mot de passe** et cliquez sur « **Appliquer** » pour enregistrer les modifications.



- Se rendre dans l'onglet « **Configuration** » puis « **Configuration > Système > Configuration > Configuration Générale** ». Renseigner le nom de la machine, la politique de mots de passe et la configuration NTP.



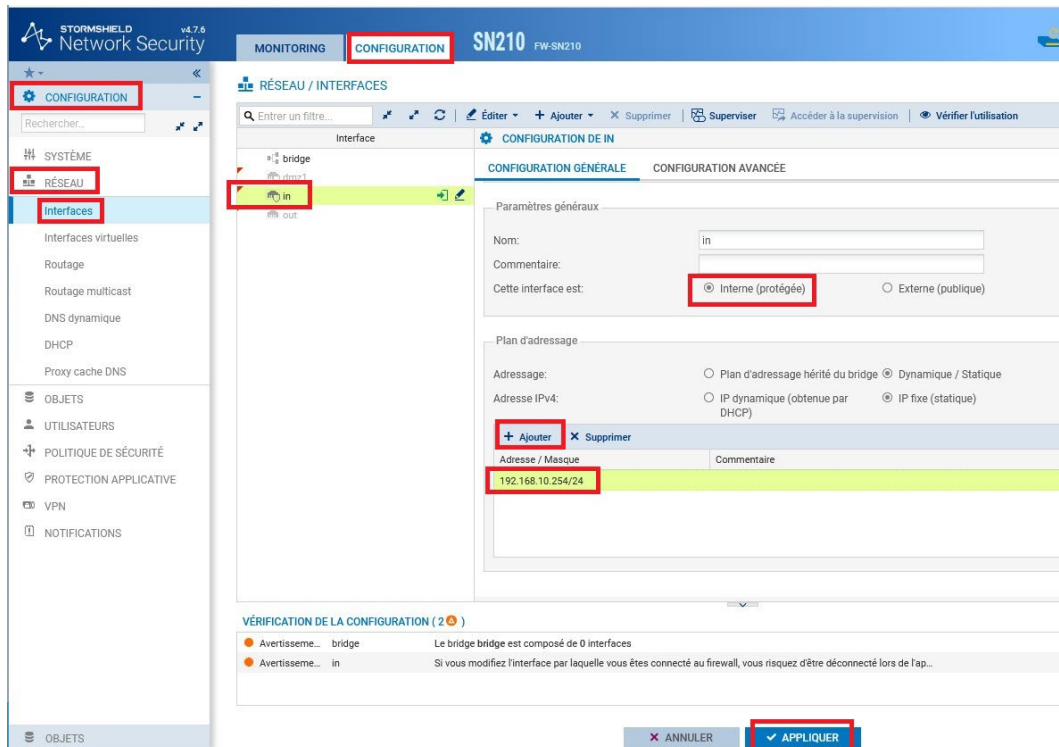
- Redémarrer le firewall, allez dans « **Configuration > Maintenance > Configuration** » et cliquer sur le bouton « **Redémarrer le firewall** ».



Configuration des interfaces du Stormshield

Interface LAN

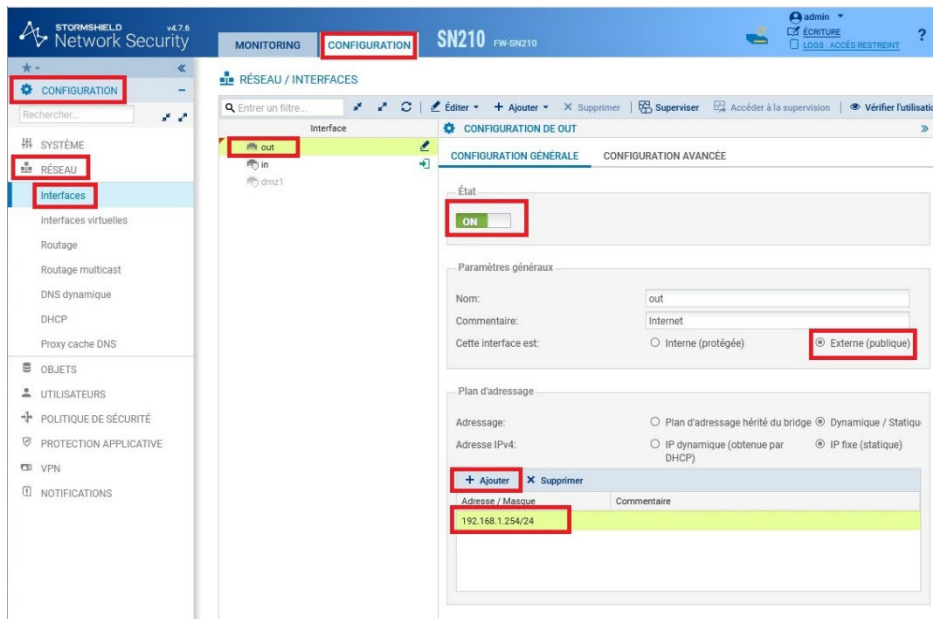
- Accéder à « **Réseau > Interface** ». **Par défaut**, tous les ports sont configurés en **mode Bridge**. Pour modifier cette configuration, **retirer les interfaces du bridge en les faisant glisser hors de celui-ci**.
- **Sélectionner** l'interface « **in** » **ajuster son adresse IP** en fonction de la plage IP souhaitée, puis cliquez sur « **Appliquer** ».



- la **connexion** au Stormshield sera perdue car le plan d'adressage a été modifié. Dans ce cas il faut reconfigurer la carte réseau du poste afin qu'elle soit sur le même réseau que l'interface « in ».
- Se reconnecter à l'interface WEB avec la nouvelle adresse IP.

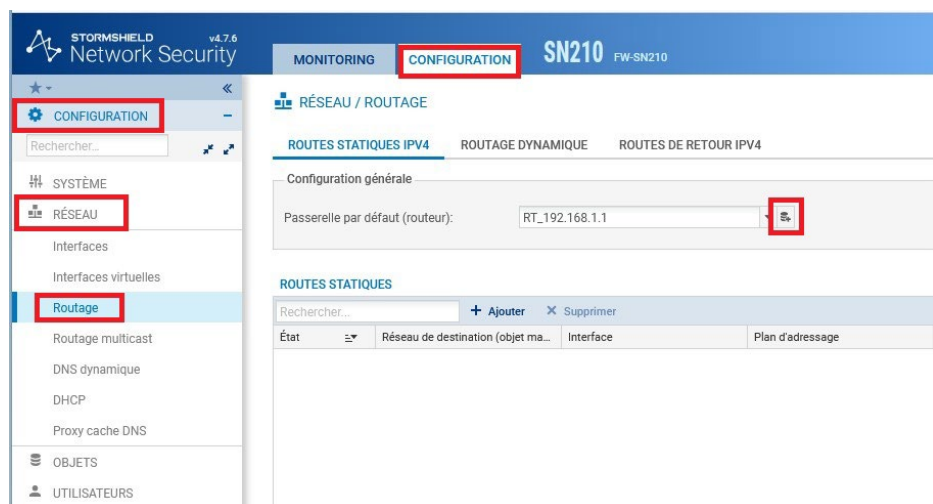
Interface WAN

- Retourner dans « **Configuration > Réseau > Interface** » et supprimer le **bridge**
- Configurer l'interface « **OUT** ». S'assurer que l'interface soit bien définie en « **externe** ».



Configuration de la route par défaut

- accéder à « **Configuration > Réseau > Routage** », dans la section « **Configuration générale** », créez un nouvel **objet** avec l'adresse IP qui servira de **passerelle par défaut**, en spécifiant cette adresse comme « **next-hop** ».

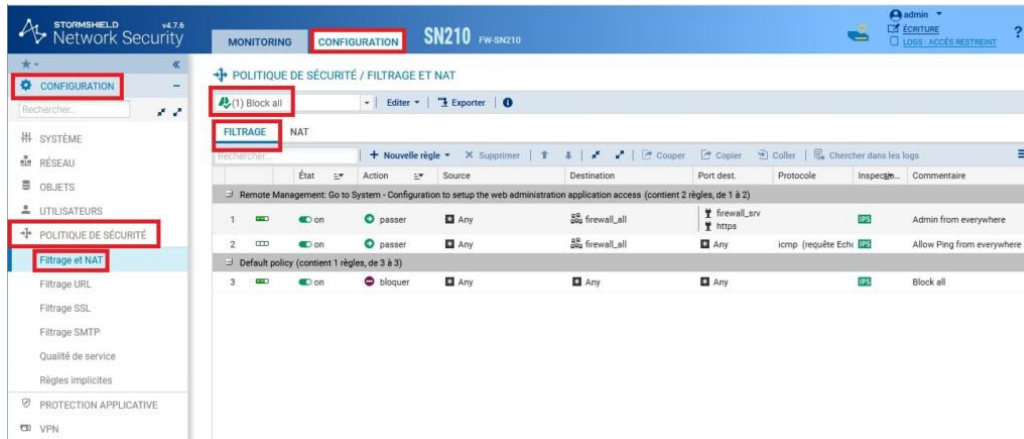


Création des règles de filtrage et NAT

Filtrage

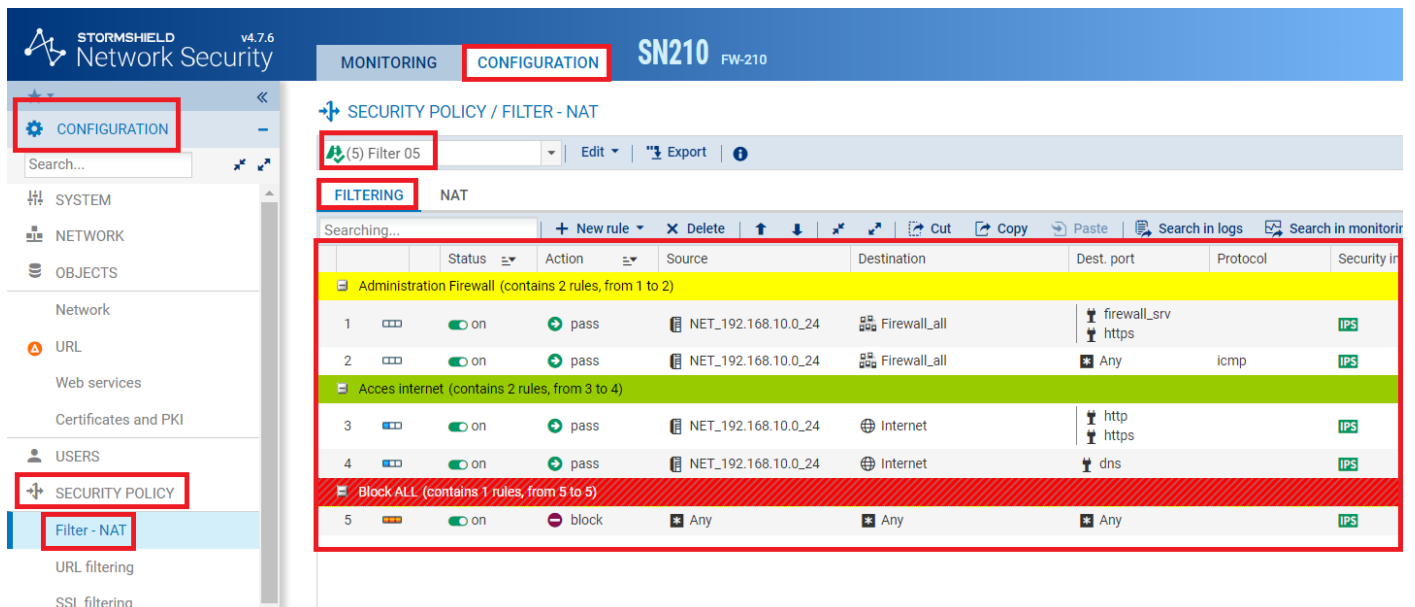
Il est maintenant nécessaire de **créer les règles d'accès à Internet** en accédant à « **Configuration > Politique de sécurité > Filtrage et NAT** ».

Par défaut, le profil est réglé sur « **Block all** ». Il est recommandé de **ne pas modifier les profils prédéfinis**, mais plutôt de **créer des règles spécifiques** pour autoriser l'accès selon vos besoins.



Sélectionner le profil « **Filter 05** », qui est actuellement vide. Ensuite, **créer de nouvelles règles** en cliquant sur « **Nouvelle règle** » puis en choisissant « **Règle simple** ».

Il est possible de **créer des séparateurs** pour vous organiser, il faut faire « **nouvelle règle > Séparateur – Regroupement de règle** ».



NAT

Dans l'onglet « **NAT** », il est nécessaire de **créer une règle de NAT** pour les flux sortants, afin que ces flux modifient leur adresse IP source pour utiliser celle du firewall.

Pour ce faire, cliquer sur « **Nouvelle règle** », puis sélectionnez « **Règle de partage d'adresse source** ».

S'assurer que le **port source après translation** est défini sur « **ephemeral_fw** », qui est configuré par défaut et indiquer en **Source** après translation l'adresse IP de votre **interface de sortie**.

Enfin, cliquer sur « **Appliquer** » pour sauvegarder les modifications.

The screenshot shows the Stormshield Network Security v4.7.6 interface. The 'CONFIGURATION' tab is selected. The left sidebar shows 'SECURITY POLICY' and 'Filter - NAT' highlighted. The main area displays 'SECURITY POLICY / FILTER - NAT' with a dropdown for '(5) Filter 05'. Below, the 'FILTERING' section is set to 'NAT'. A table shows a rule with the following details:

	Status	Original traffic (before translation)			Traffic after translation		
		Source	Destination	Dest. port	Source	Src. port	Destination
1	on	NET_192.168.10.0_24	Internet	Any	out_192.168.1.254		Any

Sauvegarde de la configuration

La configuration **minimale est maintenant terminée**. Pour **sauvegarder** la configuration, procéder à une sauvegarde sur la **partition de secours**.

Se rendre dans « **Configuration > Système > Maintenance > Configuration** » et cliquer sur le bouton « **Sauvegarder la partition active** ».

The screenshot shows the Stormshield Network Security v4.7.6 interface. The 'CONFIGURATION' tab is selected. The left sidebar shows 'CONFIGURATION', 'SYSTÈME', and 'Maintenance' highlighted. The main area displays 'SYSTÈME / MAINTENANCE' with buttons for 'MISE À JOUR DU SYSTÈME', 'SAUVEGARDER', 'RESTAURER', and 'CONFIGURATION'. The 'SAUVEGARDER' section shows the following information:

Disque système

Vous utilisez actuellement la partition: Partition principale

Partition principale: 4.7.6

Partition de secours: 4.7.6

Au démarrage, utiliser la partition:

Partition principale (4.7.6)

Partition de secours (4.7.6)

Sauvegarder la partition active

Une fois la **sauvegarde** sur la **partition de secours** effectuée, **télécharger le fichier de configuration** pour disposer d'une **sauvegarde externe**. Cela permet d'avoir une copie de sécurité supplémentaire en cas de besoin.

The screenshot shows the Stormshield Network Security v4.7.6 interface. The top navigation bar includes 'MONITORING', 'CONFIGURATION', and 'SN210 FW-SN210'. The left sidebar has 'CONFIGURATION', 'SYSTÈME', 'Maintenance', 'Active Update', 'Management Center', and 'Console CLI'. The main content area is titled 'SYSTÈME / MAINTENANCE' and contains a 'SAUVEGARDER' button. Below it, the 'Sauvegarde de configuration' section shows a backup name 'SN210AXXXXXXXXXX_2024-08-28_na' and a download button 'Télécharger la sauvegarde de configuati...'. The 'Configuration avancée' section includes fields for 'Mot de passe:', 'Confirmer:', and 'Mot de passe du TPM:', along with a 'Robustesse du mot de passe' indicator.

Conclusion

La configuration d'un Stormshield est une étape essentielle pour renforcer la sécurité d'un réseau contre les cybermenaces modernes. Comprendre et ajuster les différentes options de sécurité permet de protéger les données sensibles, mais aussi d'améliorer la résilience globale d'une infrastructure. Stormshield offre une interface intuitive et des fonctionnalités avancées qui répondent aux besoins variés des entreprises, quelle que soit leur taille.

The screenshot shows the Stormshield Network Security v4.3.21 interface. The top navigation bar includes 'MONITORING', 'CONFIGURATION', and 'SN160 SN160A31F9714A7'. The left sidebar has 'TABLEAU DE BORD', 'LOGS - JOURNAUX DAUDIT', and 'Rechercher...'. The main content area is titled 'TABLEAU DE BORD' and contains several sections: 'RÉSEAU' with traffic indicators, 'PROPRIÉTÉS' with system details (SN160, SN160A31F9714A7, 4.3.21, 28/01/2024), 'SERVICES' with icons for Management Center, Active Update, Sandboxing, Cloud Backup, Antivirus, Reports, Server Syslog, Agent SSO, and RADIUS, 'PROTECTIONS' with a list of security alerts (Certificate validity, DNS id spoofing, System was not properly halted, etc.), 'MESSAGES' with an authentication warning, and 'INDICATEURS DE SANTÉ' with icons for Link HA, Alimentation, Ventilateur, CPU, Mémoire, Disque, RAID, Température, Certificats, and SD-WAN.