Firewall Stormshield

Testé sur version 3.5.1 et 3.7.5 sur U30S, SN300 et SN700

- Première connexion et changement du mot de passe
- Créer un LAN et configurer le NAT
- Ouverture d'un port
- Configuration d'une passerelle de secours
- Configuration SNMP
- Configuration VPN SSL

Première connexion et changement du mot de passe

Introduction

Nous allons voir comment se connecter à la WEB UI et changer le mot de passe du compte administrateur.

Première connexion

L'adresse IP par défaut d'un pare-feu Stormshield est : https://10.0.0.254/admin

Passez le module de configuration rapide en cliquant sur le bouton "Accéder à l'interface d'administration"

La page de connexion doit s'afficher.

stormshield-login-1.png

En dépliant le menu OPTIONS, vous pouvez mettre l'interface en Français.

Les logins par défaut sont : admin/admin

Modification du mot de passe administrateur

Dans le menu de gauche, naviguez sur : Système > Administrateurs > Onglet compte admin

stormshield-login-2.png

Changez le mot de passe et cliquez sur "Appliquer" en bas de page.

Activer la synchronisation NTP

Naviguez dans : Système > Configuration > Configuration générale

Dans paramètre de date et d'heure, cochez maintenir le firewall à l'heure (NTP) puis validez.

stormshield-login-3.png

Créer un LAN et configurer le NAT

Etape 1 : Créer les interfaces WAN et LAN

Dans réseau > interfaces faites un cliquer/déposer de l'interface 'out' en dehors du Bridge

stormshield-lan-1.png

Indiquez l'adresse IP de l'interface WAN, dans l'exemple : 192.168.10.101/24

stormshield-lan-2.png

Faites la même chose avec l'interface 'in' puis indiquez l'adresse IP du LAN

stormshield-lan-3.png

Etape 2 : Créer un DHCP sur le LAN

Naviguez dans Réseau > DHCP > Plage d'adresses puis cliquez sur Ajouter

stormshield-lan-4.png

Au niveau de la nouvelle plage d'adresses, cliquez sur le bouton créer objet pour créer une plage d'adresses IP

stormshield-lan-5.png

Puis cliquez sur Créer

Dans le champs Passerelle, indiquez Firewall_in (correspond à la passerelle indiquée à l'étape 1 (192.168.1.1)). Enfin entrez les DNS primaire et secondaire, puis appliquez les changements.

Etape 3 : Configuration de la passerelle par défaut

Naviguez dans Réseau > Routage > Routes Statiques

Dans Passerelle par défaut (routeur), cliquez sur créer un objet.

stormshield-lan-6.png

Nom de l'objet : Saisissez un nom

Adresse IP : Saisissez l'adresse IP de la passerelle coté WAN

stormshield-lan-7.png

Cliquez sur Créer puis appliquez.

Etape 4 : Configuration du filtrage

Naviguez dans Politique de sécurité > Filtrage et NAT > Onglet Filtrage

Cliquez sur le Filtre 5 puis configurez les deux règles de base comme suit :

stormshield-lan-8.png

Règle 1 : Action : passer | Source : Network_in (LAN) | Destination : internet

Règle 2 : Action : bloquer | Source : Any | Destination : Any

Ces deux règles vont faire en sorte d'autoriser le LAN a sortir sur internet et bloquer le trafic venant du WAN.

Etape 5 : Configuration du NAT

Naviguez dans Politique de sécurité > Filtrage et NAT > Onglet NAT

configurez la règles comme suit :

stormshield-lan-9.png

A partir de ce moment, le LAN peut sortir sur internet.

Ouverture d'un port

Etape 1 : Autoriser le trafic via le port dans le filtrage

Politique de sécurité > Filtrage et NAT > Onglet Filtrage

Dans cet exemple, je vais autoriser le trafic entrant sur les ports HTTP(80) & HTTPS(443) vers une machine virtuelle. (Règle n°3)

stormshield-port-1.png

J'autorise internet à aller sur la machine 'wm_web' via les port http et https

Etape 2 : Configuration du NAT

Politique de sécurité > Filtrage et NAT > Onglet NAT

stormshield-port-2.png

Configuration d'une passerelle de secours

Introduction

Il est possible de configurer une 2e passerelle et un basculement automatique si la passerelle par défaut devient inaccessible.

Etape 1 : Créer un objet de type routeur

Chemin : Réseau > Routage > Routes statiques > Passerelle par défaut > Créer un objet

Type d'objet : Routeur

Dans l'onglet Liste des passerelles utilisées, indiquez votre gateway nominal et dans l'onglet Liste des passerelles de secours, indiquez la gateway de secours

Dans mon cas : Firewall_out_router (OUT) & Firewall_dmz1_router (DMZ1)

stormshield-gw-secours-1.png

stormshield-gw-secours-2.png

Une fois créer, vous devriez obtenir ceci :

stormshield-gw-secours-3.png

Etape 2 : Configuration du filtrage et du NAT

Configurez comme suit :

stormshield-gw-secours-4.png

stormshield-gw-secours-5.png

Il est impératif de créer les deux règles de NAT, une pour le NAT coté interface OUT (gateway nominal) et une autre pour l'interface DMZ1 (gateway de secours)

Appliquez les changements

Etape 3 : Test

stormshield-gw-secours-6.png

Configuration SNMP

Etape 1 : Activer l'agent SNMP

Naviguez dans : Configuration > Notifications > Agent SNMP

Puis cochez : Activer l'agent

stormshield-snmp-1.png

Etape 2 : Configurer l'agent SNMP

Nommez la communauté et ajoutez le serveur SNMP qui va recevoir les traps

stormshield-snmp-2.png

Appliquez

Etape 3 : Autoriser le serveur dans le filtrage

Dans Configuration > Politique de sécurité > Filtrage

Ajoutez la ligne suivante :

stormshield-snmp-3.png

Configuration VPN SSL

Etape 1 : Configuration d'un annuaire et création des utilisateurs

Chemin : Utilisateurs > Configuration des annuaires > Ajouter un annuaire

Créer un annuaire LDAP local

stormshield-vpn-1.png

Chemin : Utilisateurs > Utilisateurs > Créer un utilisateur

Créer un utilisateur dans l'annuaire LDAP

stormshield-vpn-2.png

Etape 2 : Vérification de la méthode d'authentification

Chemin : Utilisateurs > Authentification

Vérifier que LDAP est activé

stormshield-vpn-3.png

Etape 3 : Vérification du certificat

Chemin : Objets > Certificat et PKI

Vérifier la présence de : sslvpn-full-default-authority

stormshield-vpn-4.png

Etape 4 : Configuration des droits d'accès au VPN SSL

Chemin : Utilisateurs > Droits d'accès > Accès par défaut

Option 1 : Pour tous les utilisateurs

Mettre Politique VPN SSL sur Autoriser

stormshield-vpn-5.png

Option 2 : Par utilisateur

Onglet : Accès détaillé

stormshield-vpn-6.png

Etape 5 : Vérification des règles de filtrages implicite

Chemin : Politique de sécurité > Règles implicites

Vérifier que la ligne soit activé : Autoriser les clients à joindre le service VPN SSL du firewall par le port HTTPS

stormshield-vpn-7.png

Etape 6 : Configuration du VPN SSL

Chemin : VPN > VPN SSL

Paramètres généraux

Adresse IP de l'UTM utilisée	Votre @IP publique
Réseaux ou machines accessibles	Network_internals
Réseau assigné aux client UDP	Créer un LAN différent de votre LAN
Réseau assigné aux client TCP	Créer un LAN différent des LAN et LAN VPN
Max tunnels simultanés autorisés	Selon les modèles
Nom de domaine	Indiquer un nom de domaine local
Serveur DNS Primaire	IP DNS Primaire
Serveur DNS Secondaire	IP DNS Secondaire

stormshield-vpn-8.png

Configuration avancée

Adresse IP de L'UTM VPN SSL UDP	Firewall_out (votre interface wan)
Port UDP	udpvpn modifiable
Port TCP	sslvpn (443) modifiable
Délai avant renégociation des clés	14400
Utiliser les DNS fournis par le firewall	OUI
Interdire l'utilisation des serveurs DNS tiers	OUI

stormshield-vpn-9.png

Puis cliquer sur : Exporter le fichier de configuration pour télécharger le fichier .ovpn

Etape 7 : Configuration du filtrage

Chemin : Politique de sécurité > Filtrage et NAT > Filtrage

Créer la règle n°2 VPN

stormshield-vpn-10.png

Etape 8 : Connexion au VPN via OpenVPN

Télécharger le client Openvpn et utiliser le fichier téléchargé à l'étape 6 pour vous connecter.