STORMSHIELD

MANUEL D'UTILISATION ET DE CONFIGURATION
STORMSHIELD NETWORK SECURITY

REAL-TIME MONITOR - MANUEL D'UTILISATION ET DE CONFIGURATION

Date	Version	Détails
Juin 2015	V2.1	Création
Septembre 2015	V2.2	Mise à jour
Décembre 2015	V2.3	Mise à jour
Avril 2016	V2.4	Mise à jour

Référence : snfrgde_snrmonitor-v2

AVANT-PROPOS

Licence

Produits concernés

U30, U70, U120, U250, U450, U1100, U1500, U6000,

NG1000-A, NG5000-A,

U30S, U70S, U150S, U250S, U500S, U800S,

SN150, SN200, SN300,

SN500, SN510, SN700, SN710, SN900, SN910

SN2000, SN3000, SN6000,

SNi40,

VS5, VS10, V50, V100, V200, V500 et VU.

Copyright © Stormshield 2016. Tous droits réservés.

Responsabilités

Ce manuel a fait l'objet de plusieurs relectures et révisions afin d'assurer l'exactitude des informations qui y sont contenues. Les descriptions et procédures qu'il comporte sont correctes pour les firewalls Stormshield Network. Stormshield n'accepte aucune responsabilité pour des dommages liés directement ou indirectement à des erreurs, des omissions ou des incohérences entre le produit et le manuel.

Avertissement

Directive DEEE

Tous les produits Stormshield soumis à la directive DEEE qui ont été livrés dans l'Union européenne après le 13 août 2005 sont signalés par le pictogramme représentant une poubelle sur roues barrée d'une croix. Ce marquage stipule que le produit répond aux exigences imposées par la directive DEEE en termes de destruction et de réutilisation des DEEE. Pour plus de détails, veuillez consulter le site Web à l'adresse suivante :
https://www.stormshield.eu/fr/about/recycling/

1. Table des matières

1. INTRODUCTION

1.1 NOTIONS DE BASE

1.1.1 A QUI S'ADRESSE CE MANUEL D'UTILISATION ?

Ce manuel s'adresse à un administrateur réseau ou tout au moins à un utilisateur possédant un minimum de connaissances sur IP.

Pour configurer efficacement votre Firewall Stormshield Network, vous devez connaître le fonctionnement d'IP, de ses protocoles et de leurs particularités :

- ICMP (Internet Control Message Protocol).
- IP (Internet Protocol).
- TCP (Transmission Control Protocol).
- UDP (User Datagram Protocol).

La connaissance du fonctionnement général des principaux services TCP/IP est appréciable :

- HTTP.
- FTP.
- Messagerie (SMTP, POP3, IMAP).
- Telnet.
- DNS.
- DHCP.
- SNMP.
- NTP.

Si vous ne possédez pas ces connaissances, ne vous inquiétez pas : l'acquisition d'un ouvrage généraliste sur TCP/IP vous les apportera.

1.1.2 CONVENTIONS TYPOGRAPHIQUES

Abréviations

Pour la clarté, les abréviations usuelles ont été conservées. Par exemple, **VPN** (*Virtual Private Network/Réseau Privé Virtuel*).

Affichage

Les noms de fenêtres, les menus et sous menus et les boutons de l'application sont représentés en utilisant la police ci-dessous :

Exemple : menu **Interfaces**

Indications

Les indications présentés dans ce manuel fournissent des informations importantes et sont destinés à attirer votre attention sur un point important. Les différentes indications que vous pourrez trouver sont :

NOTE/REMARQUE

Ces messages vous donnent une explication plus détaillée sur un point particulier.

AVERTISSEMENT

Ces messages vous mettent en garde contre une manipulation ou une utilisation incorrecte de votre produit.

ASTUCE

Ce message vous fournit des procédés ingénieux pour utiliser les options de votre produit.

DEFINITION

Description de termes techniques liés à Stormshield Network ou langage réseau. Ces termes seront repris dans le glossaire.

Messages

Les messages au sein de l'application sont indiqués entre ""

Exemple: "Voulez-vous vraiment supprimer cette entrée ?"

Exemples

Exemple : cette présentation vous permet d'avoir un exemple de ce qui a été expliqué au préalable.

Lignes de commandes

Lignes de commandes

```
Indication de lignes de commandes (par exemple, une saisie dans la fenêtre de commandes dos).
```

Rappels

Les rappels sont indiqués de la manière suivante :

Texte de rappel.

Accès

Les accès à une fonction sont indiqués de la manière suivante :

Accédez au menu Fichier\Firewall.

1.1.3 VOCABULAIRE UTILISÉ DANS LE MANUEL

Dialup	Interface sur laquelle est branché le modem.
Firewall	Equipement/produit multifonction Stormshield Network.
Slot (de configuration)	(Ou Politique.). Mais slot ou politique (de filtrage, de NAT…) sont utilisés.
Traces/Logs	Indifféremment utilisés.

1.1.4 OBTENIR DE L'AIDE

Pour obtenir de l'aide au sujet de votre produit et des différentes applications qui le composent :

- Site web : https://mystormshield.eu/. Votre espace privé vous permet d'accéder à un certain nombre de documentations et d'informations diverses.
- Manuels de l'utilisateur : Stormshield Network Global Administration, Stormshield Network Real-Time Monitor et Stormshield Network Event Reporter.

1.1.5 CENTRE D'ASSISTANCE TECHNIQUE

Stormshield Network met à votre disposition différents moyens et outils pour la résolution d'un problème technique sur votre firewall.

- Une base de connaissances.
- Un réseau de distribution certifié. Vous pouvez ainsi faire appel à votre revendeur.
- Des documents : accessible sur votre espace clients ou partenaires. Vous devez posséder un compte client pour pouvoir accéder à ces documents.

Pour plus d'informations au sujet de l'assistance technique, veuillez-vous référer au document « Charte du support ».

1.2 INSTALLATION LOGICIELLE

Cette partie vous donne des éléments pour installer la suite logicielle vous permettant d'administrer votre produit. *Si vous souhaitez des informations sur les boîtiers et leur installation, veuillez vous référer au guide d'installation produit.*

Vous devez posséder le fichier d'installation de l'interface graphique sur le site Web (https://mystormshield.eu/). Le fichier d'installation est bilingue. Vous devez connaître l'adresse IP interne de votre firewall, ainsi que son numéro de série.

1.2.1 PRÉREQUIS

La bibliothèque de base correspond à l'ensemble des modules nécessaires aux autres programmes. L'espace disque nécessaire est de 15,3 MB.

L'installation minimale regroupe :

- Stormshield Network Unified Manager : Interface graphique d'administration des Firewalls Stormshield Network
- Stormshield Network Real-Time Monitor : Visualisation de votre Firewall Stormshield Network en temps réel (2,58 MB)
- Stormshield Network Event Reporter : Consultation et gestion des traces de votre Firewall (140 MB)

L'installation constitue l'ensemble des outils de configuration graphique des suites Stormshield Network servant d'interface entre l'utilisateur et l'appliance. Ces outils sont à installer sur une station d'administration.

La configuration complète du Firewall Stormshield Network se fait par un logiciel développé par la société NETASQ: Stormshield Network Global Administration. A partir de ce logiciel vous pourrez configurer entièrement votre Firewall depuis un poste Windows.

L'installation de ce logiciel requiert les éléments suivants :

- CPU à 2Ghz minimum
- 2 Go de RAM minimum (Windows 7) pour les logiciels clients, 2 Go pour les logiciels serveurs.
- La place occupée sur le disque dur après installation est d'environ 300 Mo. Pensez à réserver plusieurs giga-octets d'espace pour la base de données (selon l'activité du/des Firewall(s) connecté(s))
- Carte réseau Ethernet 100 ou 1000 Mbps

Stormshield Network supporte l'exécution des logiciels Stormshield Network Administration suite V1 à partir des environnements suivants :

- Microsoft Windows 7 et 8,
- Microsoft Windows Serveur 2008 et 2012.

1.2.2 INSTALLATION VIA VOTRE ESPACE

Téléchargez les fichiers nécessaires à partir du site Web Stormshield Network et exécutez le programme .EXE correspondant à la suite d'administration. Les informations d'installation apparaissent dans la langue de la version Windows.

Procédure de vérification

Procédure de vérification de la signature

Lorsque vous téléchargez un applicatif à partir de votre espace clients ou partenaires depuis le site https://mystormshield.eu/, un message vous demande : « Voulez-vous ouvrir un fichier ou l'enregistrer sur votre ordinateur ? ».

- Si vous choisissez l'option « Ouvrir », votre explorateur Web réalisera automatiquement la vérification de la signature et vous en avisera.
- Si vous choisissez l'option « Enregistrer » (option recommandée), vous devrez réaliser la vérification manuellement.

Vérification manuelle

Pour effectuer la vérification manuelle de la signature de l'application, effectuez la procédure suivante avant d'installer l'applicatif :

1 Effectuez un clic-droit sur l'application Stormshield Network dont vous voulez vérifier la signature puis sélectionnez le menu **Propriétés** dans le menu contextuel qui s'affiche.

2 Sélectionnez l'onglet *Signatures numériques* puis le nom du signataire (NETASQ).

3 Cliquez sur le bouton **Détails** : la validité de la signature numérique est indiquée dans cette fenêtre.

Enregistrement

Lors de l'installation, un enregistrement de votre produit vous est proposé. Cet enregistrement est obligatoire pour obtenir la licence de votre produit, pour télécharger les mises à jour et pour accéder au support technique.

2. SN REAL-TIME MONITOR

Stormshield Network **Real-Time Monitor** vous permet de visualiser simplement l'activité de votre firewall en temps réel. Il vous donne les informations suivantes :

- Utilisation des ressources internes du firewall (mémoire, CPU ...),
- Liste des remontées d'alertes en cas de vulnérabilités,
- Liste des machines et utilisateurs connectés,
- Alarmes remontées en temps réel,
- Nombre de connexions, utilisation de la bande passante, débit,
- Liste et état des passerelles utilisées par le firewall,
- Informations sur l'état des interfaces et des tunnels VPN,
- Dernières traces remontées,
- L'utilisation de l'espace disque alloué aux logs.

Vous pouvez, avec cet outil, vous connecter sur plusieurs firewalls et ainsi surveiller l'ensemble de votre parc.

Stormshield Network **Real-Time Monitor** vous permet de visualiser simplement les connexions transitant par le firewall et les alarmes qu'il a déclenchées.

Par défaut, le Monitor ne peut être exécuté que sur une machine connectée au réseau interne et doit être lancé en permanence pour ne pas perdre d'alarmes.

SN Real-Time Monitor se connecte aux firewalls en utilisant leur port d'administration Web (TCP/443 – HTTPS par défaut). Cela permet ainsi de bénéficier des méthodes et politiques d'authentification définies sur les firewalls supervisés. Lorsque ce port a été modifié (onglet Administration du firewall du module Configuration), la connexion peut être effectuée en indiquant l'adresse IP du firewall et le port d'administration personnalisé, séparés par deux points (« : »).

2.1 LANCEMENT

2.1.1 ACCÈS

2 exécutions sont possibles pour accéder à l'application Stormshield Network **Real-Time Monitor** :

A partir du raccourci **Applications\Lancer Stormshield Network Real-Time-Monitor** dans la barre de menus des autres applications de la Suite d'Administration.

A partir du menu **Démarrer\Stormshield\Administration Suite 2.1\Stormshield Network Real-Time Monitor**.

Si vous vous connectez pour la première fois à votre produit, un message vous demande de confirmer le n° de série (visible sous le boîtier).

L'écran principal **Vue d'ensemble** s'affiche après la connexion :

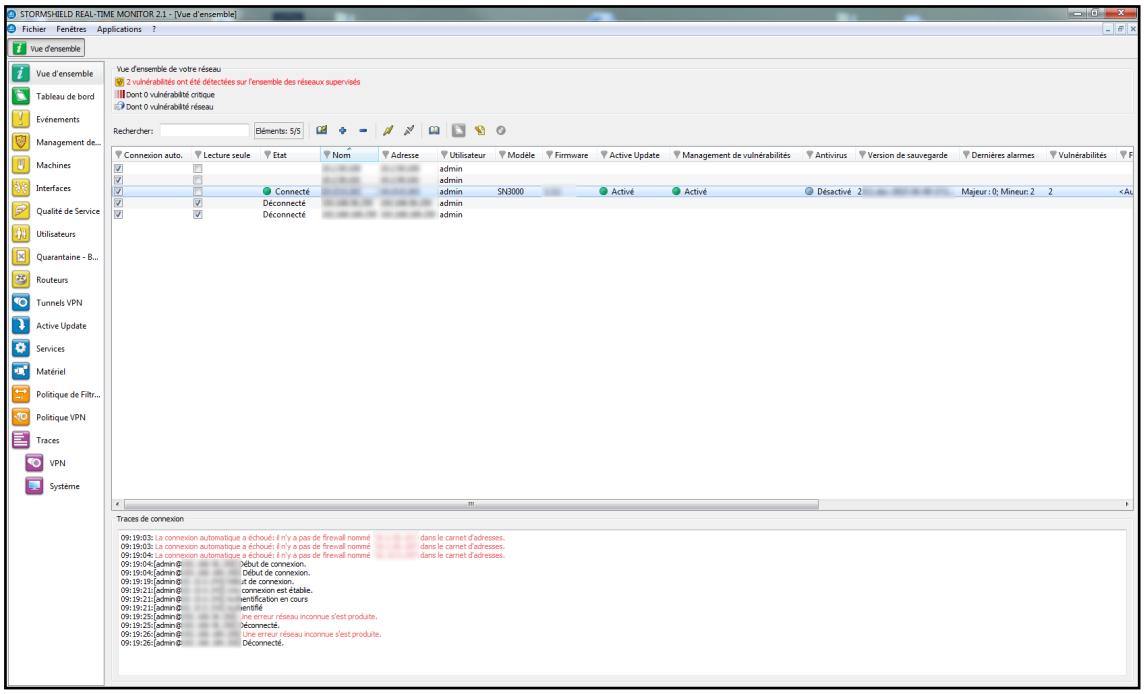


Figure 1 : Vue d'ensemble

2.1.2 CONNEXION

L'ouverture de **Stormshield Network Real-Time Monitor** s'effectue différemment, selon l'option choisie dans l'onglet *Comportement au démarrage* du menu **Paramètres de l'application** (cf. Voir le chapitre Comportement au démarrage).

Les options possibles sont :

- Connexion directe.
- Se connecter automatiquement aux sources de données.
- Aucun.

Connexion directe à un équipement multifonction Stormshield Network

La connexion directe permet l'entrée des informations de connexion à un firewall donné.

Pour établir une connexion directe, accédez au menu **Fichier\Connexion directe**. Ou, si le Moniteur a été configuré pour que la connexion directe soit effectuée au moment du démarrage de l'application, la fenêtre suivante s'affiche :

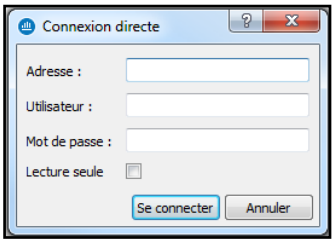


Figure 2 : Connexion directe

NOTE

Pour plus d'informations au sujet de la connexion, lisez la section Comportement au démarrage.

1 Indiquez l'adresse IP du firewall dans le champ **Adresse**. Si le port d'administration Web du firewall a été modifié, indiquez l'adresse IP suivie du caractère « : » puis du port d'administration. Exemple : *192.168.0.1:3333*.

2 Indiquez le nom d'utilisateur dans le champ **Utilisateur**.

3 Indiquez le mot de passe de l'utilisateur dans le champ **Mot de passe**.

REMARQUE

Cocher l'option **Lecture seule** permet de se connecter au firewall en lecture uniquement.

4 Cliquez sur le bouton **Se connecter**.

5 Un message proposant d'accepter le certificat du firewall est alors présenté. Cliquez sur le bouton **Faire confiance à ce certificat et se connecter** afin de finaliser la connexion au firewall.

Ouvrir le carnet d'adresses

Pour ouvrir le carnet d'adresses, accédez au menu **Fichier\Carnet d'adresses**. Ou, si le Monitor a été configuré pour que le carnet d'adresses soit ouvert au moment du démarrage de l'application, la fenêtre "Carnet d'adresses" s'affiche.

NOTE

Pour plus d'informations au sujet du carnet d'adresses, lisez la section Carnet d'adresses).

Se connecter automatiquement aux sources de données

Si cette option est cochée dans **Paramètres de l'application\Comportement au démarrage**, le Monitor ouvre directement la fenêtre principale "Vue d'ensemble" et l'application se connecte automatiquement aux firewalls existants. (cf. Pour plus d'informations au sujet de la connexion, lisez la section Comportement au démarrage).

Aucun

Si cette option est cochée dans **Paramètres de l'application\Comportement au démarrage**, le Monitor ouvre directement la fenêtre principale "Vue d'ensemble" mais aucune application n'est connectée au firewall. Seul le menu **Vue d'ensemble** est actif. Les autres menus de l'arborescence sont grisés. (cf. Pour plus d'informations au sujet de la connexion, lisez la section Comportement au démarrage).

2.1.3 CARNET D'ADRESSES

Vous accédez au carnet d'adresses par le menu **Fichier\Carnet d'adresses…**

REMARQUE

Le carnet d'adresses peut également être ouvert de manière automatique au démarrage de l'application si vous en avez coché l'option dans **Paramètres de l'application\ Comportement au démarrage**. (cf. Chapitre Comportement au démarrage).

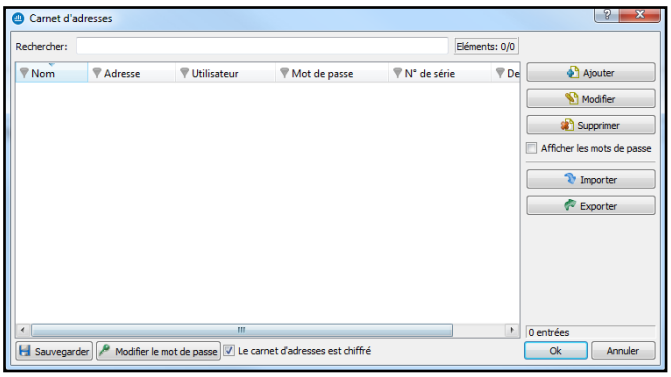


Figure 3 : Carnet d'adresses

Vous avez la possibilité de mémoriser les informations de connexion sur vos différents firewalls. Ces informations sont stockées sur le poste client où est installée l'interface. Elles peuvent être chiffrées si vous cochez l'option **Le carnet d'adresses est chiffré**. Dans ce cas, une clé de chiffrement vous est demandée. Les informations mémorisées pour chaque firewall sont l'adresse IP, le login, le mot de passe de connexion et le numéro de série du firewall auquel vous souhaitez vous connecter. Le mot de passe est celui d'un utilisateur autorisé.

En spécifiant un numéro de série vous vous prévenez contre les attaques de type "man in the middle". En effet, si vous tentez une connexion sur un équipement qui ne répond pas au critère "Numéro de série" indiqué dans le carnet d'adresses, le monitor vous indique que vous êtes en train de tenter une connexion sur un équipement inconnu. Il vous demande si vous désirez rajouter ce numéro dans la liste autorisée. Vérifiez bien les informations affichées par le monitor avant d'accepter une telle requête.

Une fois les informations entrées, vous pouvez les sauvegarder avec le bouton **Sauvegarder**. Pour ouvrir une session sur un des firewalls du carnet d'adresses, cliquez sur le nom de ce dernier puis sur le bouton **OK** ou double-cliquez sur ce même nom.

AVERTISSEMENT

Si vous modifiez l'option **Le carnet d'adresses est chiffré**, il faut enregistrer à nouveau le carnet pour prendre en compte les modifications.

Cochez l'option **Afficher les mots de passe** pour vérifier les mots de passe utilisés pour chacun des firewalls enregistrés dans le carnet d'adresses (les mots de passe sont affichés en clair).

Ajouter une adresse

Pour ajouter une adresse au carnet, cliquez sur le bouton **Ajouter**. Les indications à ajouter sont les suivantes :

Nom	Indication du nom du firewall.
Adresse	Indication de l'adresse IP du firewall. Si le port d'administration Web du firewall a été modifié, indiquez l'adresse IP suivie du caractère « : » puis du port d'administration. Exemple : *192.168.0.1:3333*.
Utilisateur	Indication du compte de l'utilisateur.

Mot de passe	Indication du mot de passe de l'utilisateur.
Confirmer	Confirmation du mot de passe.
Description	Description ou commentaire au sujet du firewall créé.

Modifier une adresse

Pour modifier une adresse dans le carnet d'adresses, suivez la procédure ci-dessous :

1. Sélectionnez le firewall à modifier.
2. Cliquez sur le bouton **Modifier**. La fenêtre suivante s'affiche :

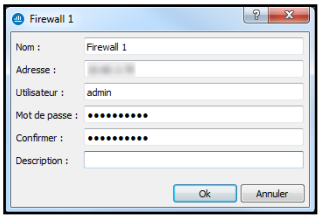


Figure 4 : Modifier une adresse

3. Effectuez les modifications nécessaires.
4. Cliquez sur **OK** pour valider les modifications.

Supprimer une adresse

Pour supprimer un firewall du carnet d'adresses, suivez la procédure ci-dessous :

1. Sélectionnez le firewall à supprimer.
2. Cliquez sur le bouton **Supprimer** Le message suivant s'affiche :
"Voulez-vous vraiment supprimer cette entrée ?"
3. Cliquez sur **Oui** ou **Non** selon votre choix.

Importer un carnet d'adresses

Pour importer un carnet d'adresses existant, suivez la procédure suivante :

1. Cliquez sur **Importer**. La fenêtre suivante s'affiche :

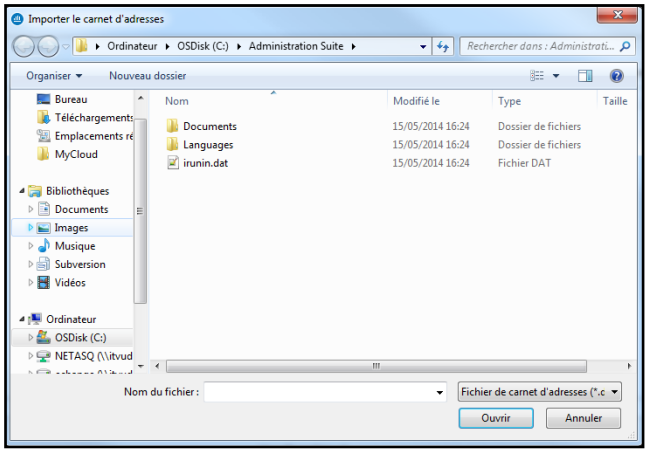


Figure 5 : Importer le carnet d'adresses

2 Sélectionnez le fichier d'importation.

REMARQUE

Le fichier d'importation est un fichier au format .dat.

3 Cliquez sur **Ouvrir**.

Exporter un carnet d'adresses

Pour exporter un carnet d'adresses existant, suivez la procédure suivante :

1 Cliquez sur Exporter. La fenêtre suivante s'affiche :

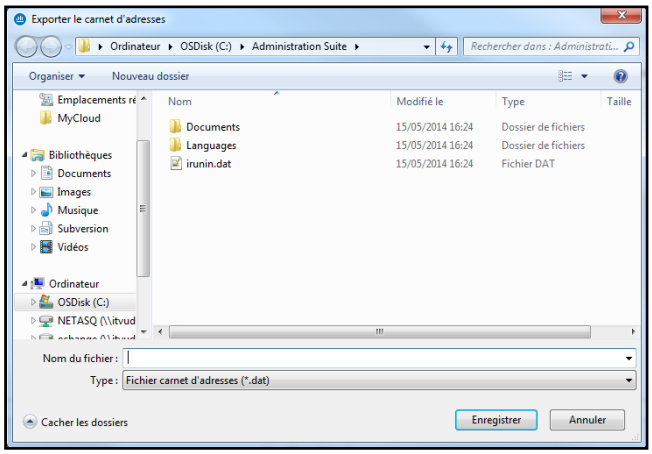


Figure 6 : Exporter le carnet d'adresses

2 Sélectionnez le fichier d'exportation.

REMARQUE

Le fichier d'exportation sera un fichier au format .dat.

3 Cliquez sur Enregistrer.

Rechercher

La recherche porte sur n'importe quelle information se trouvant dans les colonnes.

Il est possible de filtrer l'information sur une colonne puis d'affiner la recherche ensuite.

Exemples :

- Filtre sur la colonne « Adresse » qui contient 129 : une liste de résultats s'affiche ; puis, recherche globale en affinant l'adresse.
- Filtre sur la colonne « Adresse » commençant par « 10.2 » puis recherche, parmi les adresses affichées, des machines dont l'adresse commence par « 10.2.14 » en saisissant uniquement « 14 » dans le champ « Recherche ».

2.2 PRISE EN MAIN

2.2.1 PRESENTATION DE L'INTERFACE

Fenêtre principale

Vous pouvez, à partir de cette fenêtre, ouvrir plusieurs fenêtres connectées chacune sur différents firewalls.

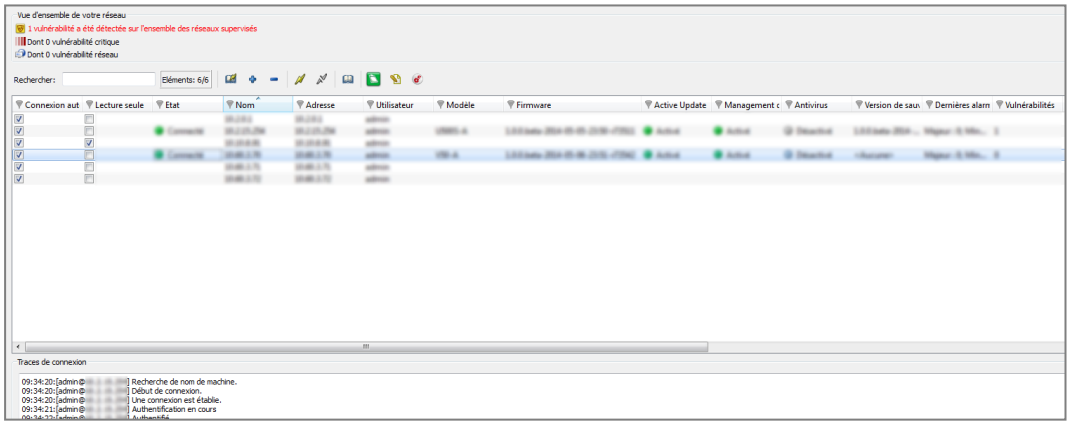


Figure 7 : Vue d'ensemble

Une fois connecté, le moniteur ouvre une fenêtre d'accueil (Menu Vue d'ensemble) qui vous apporte un certain nombre d'informations sur l'activité du firewall.

Elle est composée de cinq parties :

- Une barre de menus ;
- Une barre horizontale contenant des icônes liées à la connexion et une zone de recherche ;
- Une barre verticale contenant l'arborescence des menus et permettant la visualisation et le paramétrage des options de **Stormshield Network Real-Time Monitor** ;
- Une zone d'affichage des résultats ;
- Une barre d'état.

REMARQUE

Les autres fenêtres des menus de l'arborescence peuvent contenir une barre de boutons :

- Actualiser
- Afficher l'aide/Cacher l'aide
- Firewall
- Dupliquer

Descriptif des icônes

	Connexion depuis le carnet d'adresses.
	Connexion directe à un firewall.
	Déconnexion et suppression d'une connexion.
	Connexion au firewall sélectionné.
	Déconnexion du firewall sélectionné.
	Edition du carnet d'adresses.
	Affichage du Tableau de bord du firewall sélectionné.
	Génération d'un rapport Web pour le firewall sélectionné : • Résumé système, mémoire, CPU. • Liste des machines connectées (adresse IP, interface à laquelle est rattaché l'utilisateur, quantité de données transférées, nombre de connexions, débit utilisé ...). • Liste des utilisateurs authentifiés (nom de l'utilisateur, IP, temps d'authentification restant...). • Liste des alarmes remontées (majeures et mineures). • Liste des tunnels VPN actifs. • Liste des services actifs. • Etat de l'Active Update. • Statistiques. • Management de vulnérabilités…
	Connexion à l'administration Web du firewall sélectionné.

Les onglets

La fenêtre principale contient les menus suivants : **Fichier**, **Fenêtres**, **Applications**, et **? (Aide)**.

Fichier	Permet de vous connecter aux firewalls et d'accéder aux options générales de l'application.
Fenêtres	Permet d'organiser les fenêtres de connexion sur l'écran.
Applications	Permet de lancer directement les deux autres applications composant la Suite d'Administration Stormshield Network, **Global Administration** et **Event Reporter**.
? (Aide)	Permet d'accéder au présent fichier d'aide et de connaître la version du moniteur.

L'arborescence des menus

Vue d'ensemble	Cet écran liste les firewalls. Le Monitor s'ouvre sur cet écran une fois la connexion effectuée. • Le sous menu **Console** : En cochant l'option Activé du menu **Paramètres de l'application\Divers**, zone console, vous pouvez accéder aux équipements en mode console (commandes CLI). En validant cet écran, un menu **Console** vient se rajouter sous le menu de l'arborescence **Vue d'ensemble**.
Tableau de bord	Cet écran vous permet d'avoir une vue synthétique des principales informations liées à l'activité de votre produit.
Evénements	Cet écran liste des événements déclenchés par le firewall.
Management des vulnérabilités	Cet écran permet de visionner la remontée des alertes et d'obtenir une aide en cas de vulnérabilité.
Machines	Liste des machines de votre réseau.
Interfaces	Cet écran permet d'obtenir des statistiques concernant la bande passante, les connexions et le débit.
Qualité de service	A décrire.
Utilisateurs	Cet écran permet d'obtenir des informations au sujet des utilisateurs et des droits de session au moment de l'authentification.
Quarantaine- Bypass ASQ	Cet écran présente la liste des machines mises en quarantaine dynamique.
Tunnels VPN	Cet écran affiche les informations statiques sur le fonctionnement des tunnels VPN et les informations sources et destinations.
Active Update	Cet écran présente l'état de l'Active Update sur le firewall pour chaque type de mise à jour disponible.
Services	Cet écran présente les services actifs et non actifs présents sur le firewall et depuis combien de temps ils ont été activés/désactivés.
Matériel	Cet écran présente les informations au sujet de l'initialisation de la Haute Disponibilité et du RAID.
Politique de Filtrage	Cet écran affiche la politique de filtrage active en regroupant les règles implicites et les règles locales.
Politique VPN	Cet écran permet de visualiser la configuration des différentes politiques de tunnels VPN.
Traces	Cet écran permet de visualiser en temps réel la taille du fichier de logs. • Le sous-menu VPN donne des informations sur les traces VPN. • Le sous-menu Système donne des informations au sujet du système.

Zone d'affichage des résultats

Dans cette zone apparaissent les données et options des menus sélectionnés dans la barre horizontale. Le détail de ces écrans est traité dans les sections correspondantes.

Menu contextuel sur les colonnes

Un clic droit sur un nom de colonne affiche les options suivantes :

Filtrer sur cette colonne	Isole un ensemble d'évènements selon des critères donnés. Par exemple, pouvoir filtrer les évènements dont le protocole est « mineur ». Lorsqu'un filtre est appliqué à une colonne, l'icône s'affiche en bleu dans le libellé de la colonne.
Effacer le filtre de la colonne	Efface le filtre qui avait été mis au préalable sur la colonne.

Effacer tous les filtres	Efface les filtres mis sur toutes les colonnes.
Effacer tous les filtres sauf celui-ci	Efface les filtres mis sur les colonnes sauf celui de la colonne sélectionnée.
Cacher la colonne	Cache la colonne sélectionnée.
Colonnes	Permet de sélectionner les colonnes à afficher.
Ajuster les colonnes au contenu	Les colonnes sont redimensionnées en fonction du contenu.

En sélectionnant le menu **Filtrer sur cette colonne**, l'écran suivant s'affiche :

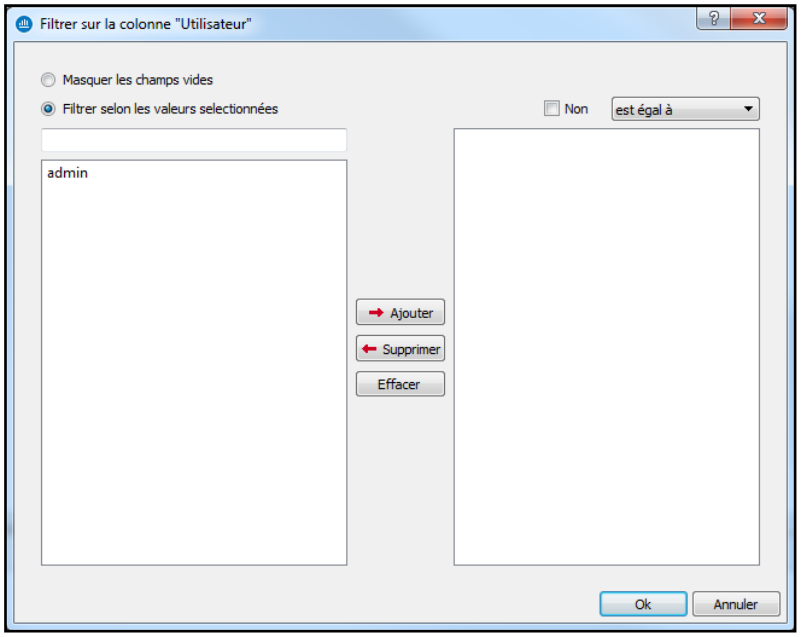


Figure 8 : Filtrer sur cette colonne

L'écran se rapporte à la colonne sélectionnée au préalable (Exemple : *Filtrer sur la colonne « Modèle »*).

- Option **Masquer les champs vides** : permet de n'afficher que les champs qui contiennent des données.
- Option **Filtrer selon les valeurs sélectionnées** : il est possible de saisir une valeur manuellement ou alors de la sélectionner dans la liste proposée.

Pour réaliser un filtre, il suffit juste de sélectionner une ou plusieurs valeur(s) dans la liste proposée et de les ajouter pour qu'ils apparaissent à droite du tableau.

Vous pouvez utiliser les opérateurs :

- **Est égal à** : les valeurs trouvées doivent être égales à celles sélectionnées.
- **Contient** : recherche d'un mot dans une phrase
- **Commence par** : recherche d'une phrase commençant par une chaîne
- **Se termine par** : recherche d'une phrase se terminant par une chaîne.
- **Joker (Wildcard)** : Voir le tableau ci-dessous.
- **Expression régulière** : cf. http://qt-project.org/doc/qt-4.8/qregexp.html

c	Par exemple, en saisissant « c », « c » est recherché.
?	Permet de rechercher sur un caractère unique
*	Permet de rechercher sur un ou plusieurs caractères.
[...]	Permet la saisie de plusieurs caractères entre crochets. Par exemple, en saisissant [ABCD], la recherche porte sur A ou B ou C ou D. En saisissant [A-D], recherche ABCD, en saisissant [A-Z], la recherche porte sur toutes les lettres majuscules de l'alphabet français.

Il est donc possible de filtrer les événements selon une ou plusieurs valeurs. Par exemple, afficher les événements dont le protocole est HTTP ou HTTPS.

Il est possible également de donner une négation à un critère en cochant l'option **Non**. Par exemple, afficher toutes les entrées sauf si le protocole est http.

- Les colonnes peuvent être redimensionnées en fonction de leur contenu (option **Ajuster les colonnes au contenu**).

En outre, l'administrateur peut trier la grille en cliquant sur la colonne qu'il désire classer.

Menu contextuel sur les lignes

Un clic-droit sur une ligne affiche un menu contextuel permettant diverses manipulations. Les options proposées varient selon la grille dans laquelle on se trouve.

Vue d'ensemble

3 menus contextuels peuvent être ouverts dans cet écran :

- En effectuant un clic-droit sur un firewall
- En effectuant un clic-droit sur une zone vide de la liste des firewalls
- En effectuant un clic-droit dans la vue "Traces de connexion"

Menu contextuel lié à un firewall

Afficher le tableau de bord...	Affiche le menu Tableau de bord du produit sélectionné.
Générer un rapport web...	En cliquant sur ce bouton, vous générez un rapport au format HTML. Ce rapport contient les informations suivantes, à un instant t : les informations système, la mémoire, les utilisateurs connectés, les services, le statut de l'Active Update, les statistiques de bande passante, les statistiques de connexion, les vulnérabilités, le nombre de machines, les utilisateurs authentifiés, le nombre d'alarmes majeures et mineures, la quarantaine, le nombre de tunnels VPN, Les règles de filtrage et les tunnels IP Sec configurés.
Lancer l'interface d'Administration Web	Permet de se connecter à l'interface d'administration Web du Firewall sélectionné
Déconnecter	Permet de se déconnecter du produit sélectionné.
Supprimer ce firewall de la liste des connexions...	Permet de se déconnecter et de supprimer l'entrée correspondant à cette connexion.
Ajouter un nouveau firewall à la liste des connexions et s'y connecter	Affiche la fenêtre de connexion directe afin de se connecter à un firewall.

Ajouter un firewall du carnet d'adresses à la liste des connexions	Affiche la fenêtre du Carnet d'adresses afin de choisir un produit enregistré.
Ajouter ce firewall dans le carnet d'adresses	Affiche une fenêtre qui permet d'enregistrer le firewall sélectionné dans le carnet d'adresses.
Editer le carnet d'adresses	Affiche la fenêtre du Carnet d'adresses afin de l'éditer.

Menu contextuel lié à une zone vide

Ajouter un nouveau firewall à la liste des connexions et s'y connecter	Affiche la fenêtre de connexion directe afin de se connecter à un firewall.
Ajouter un firewall du carnet d'adresses à la liste des connexions	Affiche la fenêtre du Carnet d'adresses afin de choisir un produit enregistré.
Editer le carnet d'adresses	En sélectionnant cette option, l'écran du carnet d'adresses s'affiche.

Menu contextuel lié aux traces de connexion

Copier	Copie la/les ligne(s) de traces sélectionnée(s).
Copier le lien	Copie la localisation du lien.
Tout sélectionner	Sélectionne toutes les lignes de traces.
Effacer les traces	Efface toutes les lignes de traces.

Evénements

En effectuant un clic-droit sur une ligne d'événement, vous avez accès à un menu contextuel qui vous permet de :

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur la priorité « Majeur », l'administrateur obtient toutes les lignes contenant la priorité « Majeur ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Voir la machine source…	Indication du nom de la machine source. En sélectionnant cette option, le menu Machines s'affiche.
Voir la machine de destination…	indication du nom de la machine de destination.

Ajouter la machine source à la base Objets

Cette option permet :

- De créer directement un objet correspondant à l'adresse IP source sélectionnée, dans la base objets du Firewall depuis Stormshield Network Real Time Monitor.
- D'ajouter cet objet à un groupe existant du Firewall.

Pour de plus amples informations concernant cette option, reportez-vous à la Note Technique « Stormshield Network Sécurité collaborative ».

Ajouter la machine de destination à la base Objets

Cette option permet :

- De créer directement un objet correspondant à l'adresse IP destination sélectionnée, dans la base objets du Firewall depuis Stormshield Network Real Time Monitor.
- D'ajouter cet objet à un groupe existant du Firewall.

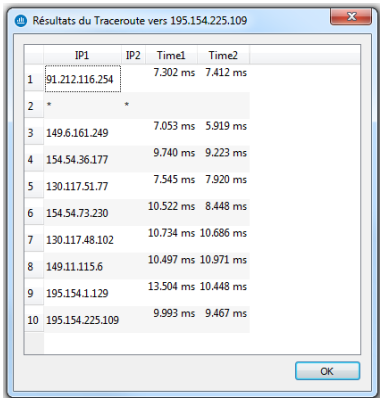
Pour de plus amples informations concernant cette option, reportez-vous à la Note Technique « Stormshield Network Sécurité collaborative »

Ping de la machine source

Permet de réaliser un test de disponibilité (ping) de la machine source depuis le firewall et indique en retour le temps de réponse de celle-ci.

Traceroute vers la machine source

Deux commandes `Traceroute` sont utilisées pour déterminer et tester l'ensemble des équipements traversés pour joindre la machine source depuis le firewall. Le résultat se présente sous la forme d'un tableau à quatre colonnes :



- Adresse IP n°1 : adresse IP nominale des machines rencontrées.
- Adresse IP n°2 : adresse IP alternative des machines rencontrées (cas d'équipements en partage de charge par exemple).
- Délai n°1 : temps de réponse de chaque équipement lors du premier Traceroute.
- Délai n°2 : temps de réponse de chaque équipement lors du second Traceroute.

REMARQUE

Lorsqu'un équipement présent sur la route ne répond pas aux requêtes de Traceroute, SN Real-Time Monitor attend le délai d'expiration du paquet de test. Le délai d'affichage de la fenêtre de résultat peut alors être plus élevé.

Ping de la machine destination	Permet de réaliser un test de disponibilité (`Ping`) de la machine destination depuis le firewall et indique en retour le temps de réponse de celle-ci.
Traceroute vers la machine destination	Permet de tester et de lister (`Traceroute`) l'ensemble des équipements traversés pour joindre la machine destination sélectionnée depuis le firewall. Le fonctionnement de cette action est identique à celle d'un **Traceroute vers la machine source**.
Envoyer la source en quarantaine	permet de mettre la machine source en quarantaine pour une durée déterminée à 1 minute, 5 minutes, 30 minutes ou 3 heures.
Voir le paquet...	Permet d'ouvrir l'outil qui vous permettra de visionner les paquets malicieux.
Purger les alarmes	Vide la liste des alarmes affichées.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier.

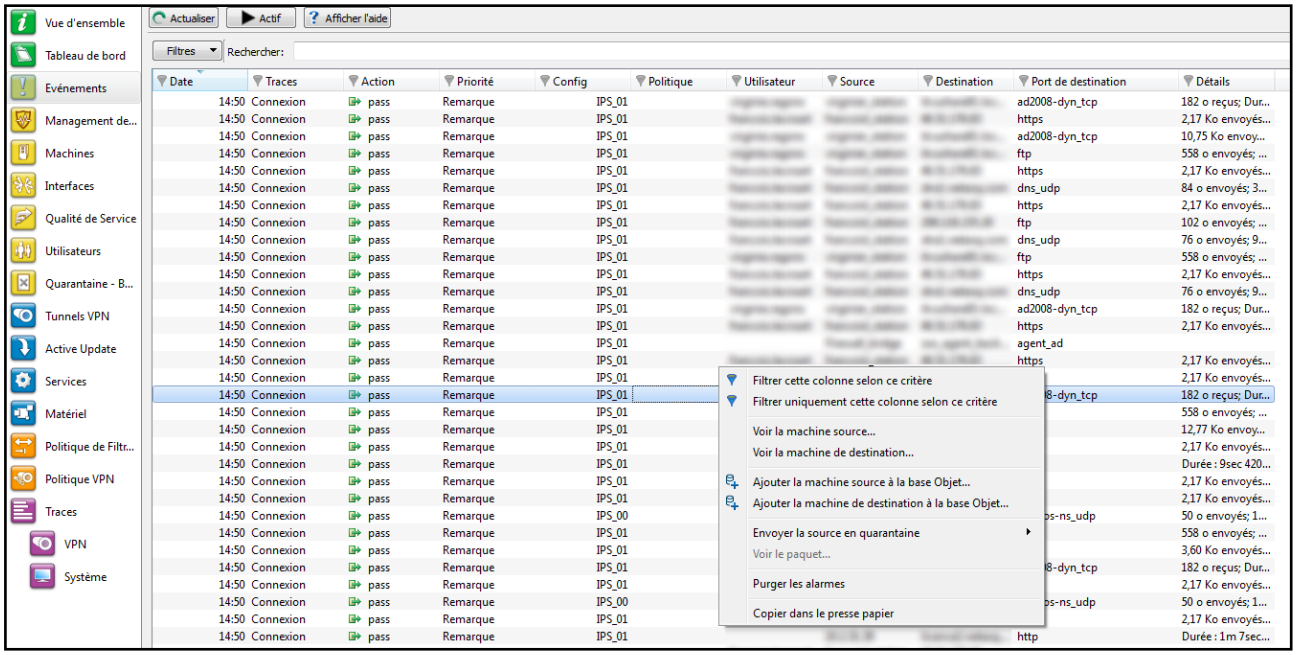


Figure 9 : Menu contextuel

Management de vulnérabilités

Au niveau de l'onglet Vulnérabilité, 3 menus contextuels peuvent être ouverts dans cet écran :

- En effectuant un clic-droit sur une ligne de vulnérabilité
- En effectuant un clic-droit sur une ligne de machine
- En effectuant un clic-droit dans la zone d'aide

Menu contextuel sur une ligne de vulnérabilité

En effectuant un clic-droit sur une ligne de vulnérabilité, vous avez accès à un menu contextuel qui vous permet de :

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur la priorité « Critique », l'administrateur obtient toutes les lignes contenant la priorité « Critique ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier.

Menu contextuel sur une ligne de machine

En effectuant un clic-droit sur une ligne de machine, vous avez accès à un menu contextuel qui vous permet de :

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur le type « Client », l'administrateur obtient toutes les lignes contenant le type de machine « Client ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Voir la machine	Le menu de l'arborescence **Machines** s'affiche afin d'obtenir des informations supplémentaires sur la machine détectée. En « pré-filtrage », la machine concernée est sélectionnée. Le filtrage s'effectue avec le nom de la machine s'il est disponible ou avec son adresse.
Ajouter la machine à la base Objets	Cette option permet : • De créer directement un objet correspondant à l'adresse IP sélectionnée, dans la base objet du Firewall depuis Real Time Monitor. • D'ajouter cet objet à un groupe existant du Firewall. Pour de plus amples informations concernant cette option, reportez-vous à la Note Technique « Stormshield Network Sécurité collaborative ».
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier. La copie de données peut agir de deux manières différentes : 1. Une seule ligne d'application est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. 2. Plusieurs lignes d'application sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Au niveau de l'onglet *applications*, 2 menus contextuels peuvent être ouverts dans cet écran :

- En effectuant un clic droit sur une ligne d'application
- En effectuant un clic droit sur une ligne de machine

Menu contextuel sur une ligne d'application

En effectuant un clic-droit sur une ligne d'application, vous avez accès à un menu contextuel qui vous permet de :

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur la famille « Web Serveur », l'administrateur obtient toutes les lignes contenant la famille « Web Serveur ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier. La copie de données peut agir de deux manières différentes : 1. Une seule ligne d'application est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. 2. Plusieurs lignes d'application sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Menu contextuel sur une ligne de machine

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur le système d'exploitation « Linux OS », l'administrateur obtient toutes les lignes contenant le système d'exploitation « Linux OS ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Voir la machine	Le menu de l'arborescence Machines s'affiche afin d'obtenir des informations supplémentaires sur la machine détectée. En « pré-filtrage », la machine concernée est sélectionnée. Le filtrage s'effectue avec le nom de la machine s'il est disponible ou avec son adresse.

Ajouter la machine à la base Objets	Cette option permet : • De créer directement un objet correspondant à l'adresse IP sélectionnée, dans la base objet du Firewall depuis Stormshield Network Real Time Monitor. • D'ajouter cet objet à un groupe existant du Firewall. Pour de plus amples informations concernant cette option, reportez-vous à la Note Technique « Stormshield Network Sécurité collaborative ».

Au niveau de l'onglet *informations*, 3 menus contextuels peuvent être ouverts dans cet écran :

- En effectuant un clic-droit sur une ligne d'informations
- En effectuant un clic-droit sur une ligne de machine
- En effectuant un clic-droit dans la zone d'aide

Menu contextuel sur une ligne d'informations

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur la famille « Web Serveur », l'administrateur obtient toutes les lignes contenant la famille « Web Serveur ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier. . La copie de données peut agir de deux manières différentes : 1. Une seule ligne d'application est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. 2. Plusieurs lignes d'application sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Menu contextuel sur une ligne de machines

En effectuant un clic-droit sur une ligne d'événement, vous avez accès à un menu contextuel qui vous permet de :

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur le système d'exploitation « Linux OS », l'administrateur obtient toutes les lignes contenant le système d'exploitation « Linux OS ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.

Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Voir la machine	Le menu de l'arborescence **Machines** s'affiche afin d'obtenir des informations supplémentaires sur la machine détectée. En « pré-filtrage », la machine concernée est sélectionnée. Le filtrage s'effectue avec le nom de la machine s'il est disponible ou avec son adresse.
Ajouter la machine à la base Objets	Cette option permet : • De créer directement un objet correspondant à l'adresse IP sélectionnée, dans la base objet du Firewall depuis Stormshield Network Real Time Monitor. • D'ajouter cet objet à un groupe existant du Firewall. Pour de plus amples informations concernant cette option, reportez-vous à la Note Technique « Stormshield Network Sécurité collaborative ».
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier. La copie de données peut agir de deux manières différentes : 1. Une seule ligne est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. 2. Plusieurs lignes sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Machines

De nombreux menus contextuels peuvent être ouverts dans cet écran :

- En effectuant un clic-droit sur une machine,
- En effectuant un clic-droit dans l'onglet « Vulnérabilités »,
- En effectuant un clic-droit dans l'onglet « Applications »,
- En effectuant un clic-droit dans l'onglet « Informations »,
- En effectuant un clic-droit dans l'onglet « Connexions »,
- En effectuant un clic-droit dans l'onglet « Evénements »,
- En effectuant un clic-droit dans la zone d'aide,
- En effectuant un clic-droit sur un bail DHCP.

Menu contextuel sur une machine

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur le système d'exploitation « Linux OS », l'administrateur obtient toutes les lignes contenant le système d'exploitation « Linux OS ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.

Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Supprimer la machine de l'ASQ…	Permet d'effacer les informations ASQ de la machine. Cela peut être utile notamment si une machine est touchée par une attaque. Le droit « Monitor modify » est nécessaire. Un message vous demande de confirmer l'action.
Réinitialiser les informations Vulnerability Manager	Effectue une réinitialisation des données Vulnerability Manager de la machine sélectionnée. Le droit « Monitor MODIFY » est nécessaire. Un message vous demande de confirmer l'action. Lorsque vous faites cette réinitialisation, la machine est effacée de la base Vulnerability Manager ainsi que les compteurs de données (vulnérabilités détectées, softwares…).
Envoyer en quarantaine	Blocage dynamique de la machine mise en quarantaine pour une durée à spécifier. (Cette durée peut être d'1 minute, de 5 minutes, de 30 minutes et de 3 heures). Le droit « Modify monitor » est nécessaire. Il n'existe pas de message pour confirmer l'action.

Cette option permet de préciser le système d'exploitation d'une machine lorsque Stormshield Network Vulnerability Manager n'a pu le détecter automatiquement. La fenêtre présente alors plusieurs champs :

Système d'exploitation courant : OS que Stormshield Network Vulnerability Manager utilise afin de trouver les vulnérabilités sur une machine. Il se peut que l'OS d'une machine ne soit pas détecté.

Système d'exploitation détecté : OS que Stormshield Network Vulnerability Manager utilise après analyse du trafic sur la machine. Le bouton Restaurer permet de retirer l'OS donné par l'utilisateur et de revenir à l'OS détecté par Stormshield Network Vulnerability Manager.

Nouveau nom d'OS : Dans le cas où l'OS de la machine n'est pas détecté par Stormshield Network Vulnerability Manager, il est possible de le forcer en le sélectionnant dans la liste proposée. Deux cas peuvent alors se présenter :

Modifier l'OS de la machine

1. Vous ne pouvez pas préciser la version exacte (exemples : *Android*, *Blackberry*,...), dans ce cas, le champ « Version » reste grisé. Cliquez sur OK pour forcer la valeur à cet OS.
2. Vous pouvez préciser la version (exemple : Linux). Dans ce cas, le champ « Version » s'affiche en clair et vous pouvez saisir un numéro de version (exemple : 2.6). Cliquez ensuite sur le bouton Valider. Si Stormshield Network Vulnerability Manager détecte la version, un nom est affiché (exemple, *Linux 2.6.14*). Cliquez, pour terminer, sur OK, afin de valider votre choix.

Forcer l'OS de la machine lorsque celui-ci n'est pas détecté, permet, notamment, de visualiser, selon un système donné, les vulnérabilités des services ou des produits.

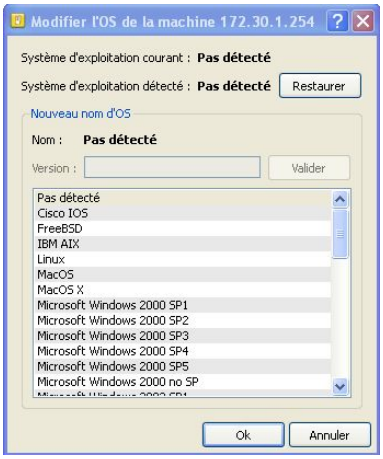


Figure 10: Modifier l'OS de la machine

Ajouter la machine à la base Objets

Cette option permet :

- De créer directement un objet correspondant à l'adresse IP sélectionnée, dans la base objet du Firewall depuis Stormshield Network Real Time Monitor.
- D'ajouter cet objet à un groupe existant du Firewall.

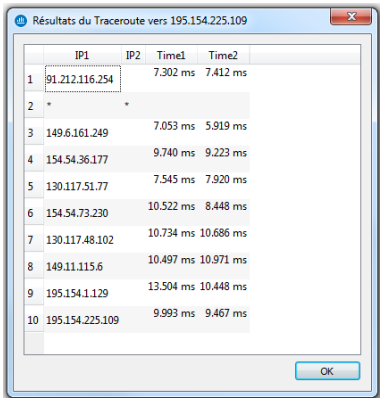
Pour de plus amples informations concernant cette option, reportez-vous à la Note Technique « *Stormshield Network Sécurité collaborative* ».

Ping de la machine

Permet de réaliser un test de disponibilité (`Ping`) de la machine depuis le firewall et indique en retour le temps de réponse de celle-ci.

Traceroute vers la machine

Deux commandes `Traceroute` sont utilisées pour déterminer et tester l'ensemble des équipements traversés pour joindre la machine sélectionnée depuis le firewall. Le résultat se présente sous la forme d'un tableau à quatre colonnes :



- Adresse IP n°1 : adresse IP nominale des machines rencontrées.
- Adresse IP n°2 : adresse IP alternative des machines rencontrées (cas d'équipements en partage de charge par exemple).
- Délai n°1 : temps de réponse de chaque équipement lors du premier `Traceroute`.
- Délai n°2 : temps de réponse de chaque équipement lors du second `Traceroute`.

REMARQUE
Lorsqu'un équipement présent sur la route ne répond pas aux requêtes de `Traceroute`, SN Real-Time Monitor attend le délai d'expiration du paquet de test. Le délai d'affichage de la fenêtre de résultat peut alors être plus élevé.

Copier dans le presse-papier

Copie de la ligne sélectionnée dans le presse-papier. La copie de données peut agir de deux manières différentes :

1. Une seule ligne d'application est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails.
2. Plusieurs lignes d'application sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Menu contextuel dans l'onglet « Vulnérabilités »

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur la sévérité « Critique », l'administrateur obtient toutes les lignes contenant la sévérité « Critique ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Lister les machines ayant la même vulnérabilité	Permet de n'afficher que les machines ayant une vulnérabilité similaire.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier. . La copie de données peut agir de deux manières différentes : 1. Une seule ligne est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. 2. Plusieurs lignes sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Menu contextuel dans l'onglet « Applications»

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur le système d'exploitation « Unix », l'administrateur obtient toutes les lignes contenant le système d'exploitation « Unix ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Lister toutes les machines qui utilisent cette application	Le menu Stormshield Network Vulnerability Manager s'affiche avec en pré-filtrage le nom du soft concerné.
Lister les vulnérabilités de cette application	L'onglet détail "Vulnérabilités" est sélectionné, avec, en pré-filtrage le nom du software concerné.
Forcer l'application du serveur	Le droit "Monitor modify" est nécessaire. Seuls les logiciels de type serveur sont modifiables/

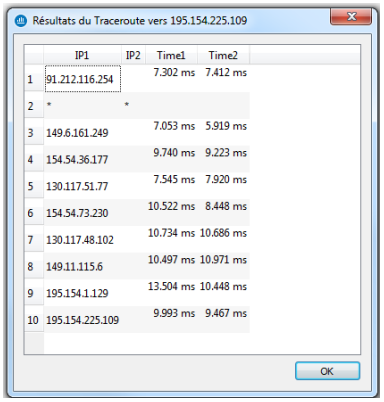
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier. . La copie de données peut agir de deux manières différentes : 1. Une seule ligne est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. 2. Plusieurs lignes sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Menu contextuel dans l'onglet « Informations »

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur le système d'exploitation « Unix », l'administrateur obtient toutes les lignes contenant le système d'exploitation « Unix ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Lister toutes les machines partageant la même information	Le menu Stormshield Network Vulnerability Manager s'affiche avec en pré-filtrage le nom du soft concerné.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier. . La copie de données peut agir de deux manières différentes : • Une seule ligne est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. • Plusieurs lignes sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Menu contextuel dans l'onglet « Connexions »

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur le système d'exploitation « Unix », l'administrateur obtient toutes les lignes contenant le système d'exploitation « Unix ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.

Ping de la machine source	Permet de réaliser un test de disponibilité (ping) de la machine source depuis le firewall et indique en retour le temps de réponse de celle-ci.
Traceroute vers la machine source	Deux commandes `Traceroute` sont utilisées pour déterminer et tester l'ensemble des équipements traversés pour joindre la machine source depuis le firewall. Le résultat se présente sous la forme d'un tableau à quatre colonnes :  • Adresse IP n°1 : adresse IP nominale des machines rencontrées. • Adresse IP n°2 : adresse IP alternative des machines rencontrées (cas d'équipements en partage de charge par exemple). • Délai n°1 : temps de réponse de chaque équipement lors du premier `Traceroute`. • Délai n°2 : temps de réponse de chaque équipement lors du second `Traceroute`. **REMARQUE** Lorsqu'un équipement présent sur la route ne répond pas aux requêtes de `Traceroute`, SN Real-Time Monitor attend le délai d'expiration du paquet de test. Le délai d'affichage de la fenêtre de résultat peut alors être plus élevé.
Ping de la machine destination	Permet de réaliser un test de disponibilité (ping) de la machine destination depuis le firewall et indique en retour le temps de réponse de celle-ci.
Traceroute vers la machine destination	Permet de tester et de lister (Traceroute) l'ensemble des équipements traversés pour joindre la machine destination depuis le firewall. Le fonctionnement de cette action est identique à celle d'un **Traceroute vers la machine source**.
Mettre la connexion en quarantaine	Permet de mettre la connexion en quarantaine pour une durée déterminée à 1 minute, 5 minutes, 30 minutes ou 3 heures. Cela permet, par exemple, d'empêcher un téléchargement particulier.

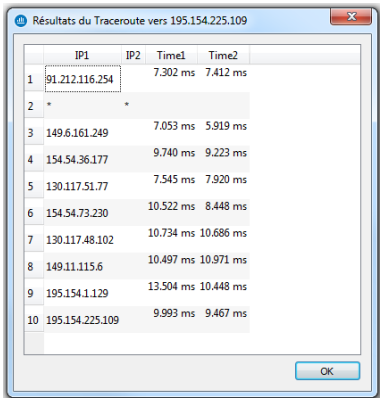
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier. . La copie de données peut agir de deux manières différentes : 1. Une seule ligne est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. 2. Plusieurs lignes sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Menu contextuel dans l'onglet « Evénements »

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur le système d'exploitation « Unix », l'administrateur obtient toutes les lignes contenant le système d'exploitation « Unix ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Voir le paquet qui a déclenché l'alarme	Permet d'ouvrir l'outil qui vous permettra de visionner les paquets malicieux.
Ping de la machine source	Permet de réaliser un test de disponibilité (ping) de la machine source depuis le firewall et indique en retour le temps de réponse de celle-ci.

Traceroute vers la machine source

Deux commandes `Traceroute` sont utilisées pour déterminer et tester l'ensemble des équipements traversés pour joindre la machine source depuis le firewall. Le résultat se présente sous la forme d'un tableau à quatre colonnes :



- Adresse IP n°1 : adresse IP nominale des machines rencontrées.
- Adresse IP n°2 : adresse IP alternative des machines rencontrées (cas d'équipements en partage de charge par exemple).
- Délai n°1 : temps de réponse de chaque équipement lors du premier Traceroute.
- Délai n°2 : temps de réponse de chaque équipement lors du second Traceroute.

REMARQUE
Lorsqu'un équipement présent sur la route ne répond pas aux requêtes de `Traceroute`, SN Real-Time Monitor attend le délai d'expiration du paquet de test. Le délai d'affichage de la fenêtre de résultat peut alors être plus élevé.

Ping de la machine destination

Permet de réaliser un test de disponibilité (ping) de la machine destination depuis le firewall et indique en retour le temps de réponse de celle-ci.

Traceroute vers la machine destination

Permet de tester et de lister (Traceroute) l'ensemble des équipements traversés pour joindre la machine destination depuis le firewall. Le fonctionnement de cette action est identique à celle d'un **Traceroute vers la machine source**.

Copier dans le presse-papier

Copie la ligne sélectionnée dans le presse-papier. . La copie de données peut agir de deux manières différentes

1. Une seule ligne est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails.
2. Plusieurs lignes sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Menu contextuel sur un bail DHCP

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur le système d'exploitation « Linux OS », l'administrateur obtient toutes les lignes contenant le système d'exploitation « Linux OS ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Afficher la machine…	Permet d'afficher le détail de la machine sélectionnée.
Ping de la machine	Permet de réaliser un test de disponibilité (ping) de la machine depuis le firewall et indique en retour le temps de réponse de celle-ci.
Traceroute vers la machine	Permet de tester et de lister (Traceroute) l'ensemble des équipements traversées pour joindre la machine depuis le firewall.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier. . La copie de données peut agir de deux manières différentes 1. Une seule ligne est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. 2. Plusieurs lignes sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Interfaces

Plusieurs menus contextuels peuvent être ouverts dans cet écran :

- En effectuant un clic-droit sur une interface
- En effectuant un clic-droit dans l'onglet « Connexions entrantes »
- En effectuant un clic-droit dans l'onglet « Connexions sortantes »

Menu contextuel sur une interface

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur le système d'exploitation « Unix », l'administrateur obtient toutes les lignes contenant le système d'exploitation « Unix ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Afficher les machines associées à cette interface	Cette option permet d'afficher la liste des machines qui ont une interface identique.

Menu contextuel dans l'onglet « Connexions entrantes »

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur le système d'exploitation « Unix », l'administrateur obtient toutes les lignes contenant le système d'exploitation « Unix ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Voir la machine source…	Indication du nom de la machine source. En sélectionnant cette option, le menu **Machines** s'affiche.
Voir la machine de destination…	Indication du nom de la machine de destination.
Mettre la connexion en quarantaine	Permet de mettre la connexion en quarantaine pour une durée déterminée à 1 minute, 5 minutes, 30 minutes ou 3 heures. Cela permet, par exemple, d'empêcher un téléchargement particulier.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier. . La copie de données peut agir de deux manières différentes 1. Une seule ligne est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. 2. Plusieurs lignes sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Menu contextuel dans l'onglet « Connexions sortantes »

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur le système d'exploitation « Unix », l'administrateur obtient toutes les lignes contenant le système d'exploitation « Unix ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Voir la machine source…	Indication du nom de la machine source. En sélectionnant cette option, le menu **Machines** s'affiche.
Voir la machine de destination…	Indication du nom de la machine de destination.
Mettre la connexion en quarantaine	Permet de mettre la connexion en quarantaine pour une durée déterminée à 1 minute, 5 minutes, 30 minutes ou 3 heures. Cela permet, par exemple, d'empêcher un téléchargement particulier.

Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier. . La copie de données peut agir de deux manières différentes 1. Une seule ligne est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. 2. Plusieurs lignes sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Qualité de service

Reportez-vous au chapitre Qualité de service (QoS).

Utilisateurs

2 menus contextuels peuvent être ouverts dans cet écran :

- En effectuant un clic-droit sur la zone « utilisateurs »
- En effectuant un clic-droit sur une zone « sessions d'administration »

Menu contextuel dans la zone utilisateurs

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur une adresse de firewall précise, l'administrateur obtient toutes les lignes contenant cette machine. **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Supprimer l'utilisateur de l'ASQ	Permet d'effacer les informations ASQ de l'utilisateur. Cela peut être utile notamment si un utilisateur est touchée par une attaque. Le droit « Monitor modify » est nécessaire. Un message vous demande de confirmer l'action.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier. La copie de données peut agir de deux manières différentes : 1. Une seule ligne est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. 2. Plusieurs lignes sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Menu contextuel dans la zone « Sessions d'administration »

Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier. La copie de données peut agir de deux manières différentes : 1. Une seule ligne d'application est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. 2. Plusieurs lignes d'application sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Quarantaine-Bypass ASQ

2 menus contextuels peuvent être ouverts dans cet écran :

- En effectuant un clic-droit sur la zone « Quarantaine »
- En effectuant un clic-droit sur une zone « Bypass-ASQ »

Menu contextuel dans la zone « Quarantaine »

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur une adresse de firewall précise, l'administrateur obtient toutes les lignes en rapport. **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier.

Menu contextuel dans la zone « Bypass-ASQ »

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur une adresse de firewall précise, l'administrateur obtient toutes les lignes en rapport. **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier.

Tunnels VPN

Ce module présente désormais les tunnels montés via VPN IPSec et via VPN SSL dans deux onglets distincts.

Onglet « Tunnels VPN SSl »

En effectuant un clic-droit sur une ligne de tunnels VPN SSL, vous avez accès à un menu contextuel qui vous permet de :

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe le nom d'un utilisateur, la liste affichée ne présentera que les éléments contenant cet utilisateur
Voir la machine	Cette option permet d'afficher, au sein du module Machines de Stormshield Network Real Time Monitor, l'ensemble des caractéristiques de la machine correspondant aux adresses IP (Vulnérabilités, Applications, Connexions, etc.).
Supprimer ce tunnel	Cette option permet de mettre fin instantanément au tunnel VPN SSL sélectionné.

Onglet « Tunnels VPN IPSec »

En effectuant un clic-droit sur une ligne de tunnels VPN, vous avez accès à un menu contextuel qui vous permet de :

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur l'état « mature », l'administrateur obtient toutes les lignes contenant l'état « mature ».
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. Exemple Si votre curseur pointe une adresse source, la liste affichée ne présentera que les éléments contenant cette adresse source.
Voir les traces des SPI sortants	Cette option permet d'afficher les SPI de la SA sortante négociée.
Voir les traces des SPI entrants	Cette option permet d'afficher les SPI de la SA entrante négociée.
Voir la politique sortante	Lien hypertexte permettant d'afficher la politique sortante visible dans le menu Politique VPN.
Voir la politique entrante	Lien hypertexte permettant d'afficher la politique entrante visible dans le menu Politique VPN.
Réinitialiser ce tunnel	Le tunnel sélectionné est supprimé, la configuration sur les firewalls est toujours active. Les SA correspondant au tunnel sélectionné sont purgées ; de nouvelles SA devront être renégociées pour que le tunnel soit à nouveau utilisable.
Réinitialiser tous les tunnels	Tous les tunnels sont supprimés.

Active Update

En effectuant un clic droit sur une ligne Active update, vous avez accès à un menu contextuel qui vous permet de :

Copier dans le presse-papier	La copie de données peut agir de deux manières différentes : 1. Une seule ligne d'application est sélectionnée : dans ce cas, cette ligne est copiée ainsi que les lignes de détails. 2. Plusieurs lignes d'application sont sélectionnées : dans ce cas, seules ces lignes sont copiées dans le presse-papier.

Services

En effectuant un clic-droit sur une ligne de services, vous avez accès à un menu contextuel qui vous permet de :

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, Par exemple, en filtrant sur l'état « Activé », l'administrateur obtient toutes les lignes contenant l'état « Activé ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe l'état « Activé », la liste affichée ne présentera que les éléments correspondant à cet état.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier.

Matériel

Il s'agit du menu dédié à la Haute Disponibilité. Reportez-vous à la section Matériel.

Politique de filtrage

Ce menu permet de visualiser différents types de règles :

- Règles implicites
- Règles de filtrage globales
- Règles de filtrage locales
- Règles de NAT locales

Reportez-vous à la section Politique de filtrage.

Politique VPN

En effectuant un clic-droit sur une ligne de politique VPN, vous avez accès à un menu contextuel qui vous permet de :

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur le routeur destination « Firewall_bridge », l'administrateur obtient toutes les lignes contenant le routeur destination « Firewall_bridge ».
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur.
Voir les tunnels correspondants	Accès au menu Tunnels VPN avec un filtre.

Traces

VPN

En effectuant un clic-droit sur une ligne de politique VPN, vous avez accès à un menu contextuel qui vous permet de :

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, Par exemple, en filtrant sur le message « Phase established », l'administrateur obtient toutes les lignes contenant le message « Phase established ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur. **Exemple** Si votre curseur pointe la destination/le site web consulté, la liste affichée ne présentera que les éléments contenant cette destination/ce site web.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier.

Système

En effectuant un clic-droit sur une ligne de Système, vous avez accès à un menu contextuel qui vous permet de :

Filtrer cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats selon le champ sélectionné. Par exemple, en filtrant sur la priorité « Majeur », l'administrateur obtient toutes les lignes contenant la priorité « Majeur ». **NOTE** Utiliser cette option a pour effet de remplacer tous les filtres en cours sur les colonnes.
Filtrer uniquement cette colonne selon ce critère	Cette option permet de restreindre la liste des résultats au critère pointé par votre curseur.
Copier dans le presse-papier	Copie la ligne sélectionnée dans le presse-papier.

Barre d'état

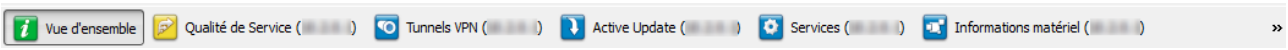


Figure 11 : Barre d'état

La barre d'état contient les menus de l'arborescence qui ont pu éventuellement être ouverts au cours d'une session. Cette possibilité est particulièrement utile lorsque vous supervisez plusieurs firewalls à la fois. Vous pouvez récupérer la même fenêtre d'informations pour chaque firewall et ainsi effectuer des comparaisons de manière simultanée.

Barre de boutons

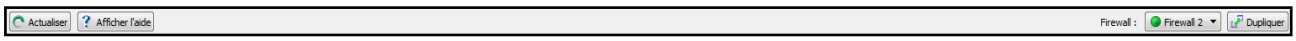


Figure 12 : Barre de boutons

Cette barre s'affiche dans la plupart des menus du Monitor.

Actualiser

Ce bouton permet de réinitialiser la liste affichée (menus Alarmes, VULNERABILITY MANAGER, Machines, Interfaces, Qualité de Service, Utilisateurs, Quarantaine, Tunnels VPN, Active Update, Services, Matériel, Politique de Filtrage, VPN, Traces).

Afficher l'aide/Cacher l'aide

Ce bouton permet d'afficher ou de cacher un écran d'aide. Il suffit ensuite de cliquer sur la ligne sélectionnée pour obtenir une aide éventuelle.

Firewall

Ce menu déroulant permet de filtrer la liste des alarmes sur un firewall choisi.

Dupliquer

Ce bouton permet de dupliquer la fenêtre dans laquelle se trouve ce bouton. Cela est particulièrement utile lorsque l'on veut changer de cible (firewall ou <all>) et de vue.

La zone de recherche

La zone de recherche se présente sous 2 formes différentes :

1ère forme : la barre affichée ci-dessous est visible sur tous les écrans hormis sur l'écran « Evènements »

Figure 13 : Zone de recherche

2ème forme : la barre ci-dessous s'affiche dans le menu Evénements

Figure 14 : Zone de recherche - Événements

Le bouton **Filtres** contient des filtres définis par l'application et permet d'obtenir uniquement les lignes suivantes :

- Alarme
- Virus

- Connexion
- Web
- Mail
- FTP
- Filtrage
- SSL
- VPN SSL
- Authentification
- Applications (alarme)
- Protections (alarme)
- Malwares (alarme)

Rechercher

Cette zone permet d'effectuer des recherches au niveau des éléments de la liste. Les éléments de la liste sont filtrés au fur-et-à-mesure de la saisie.

2.2.2 PRÉSENTATION DES MENUS

Fichier

Le menu **Fichier** concerne la connexion aux firewalls et les options générales de l'application

Carnet d'adresses...	Ce menu permet de configurer le carnet d'adresses des firewalls.
Connexion directe...	Ce menu ouvre une nouvelle fenêtre de connexion à un firewall. Entrez l'adresse IP du firewall et le mot de passe de l'utilisateur.
Paramètres de l'application...	Ce menu permet de déterminer le comportement que doit adopter le Monitor au moment de son démarrage, de récupérer un outil d'analyse de paquets, de déterminer un répertoire de destination pour le rapport, et le langage utilisé pour l'interface graphique.
Paramètres par défaut du monitoring...	Ce menu permet de configurer la fréquence d'actualisation de différents paramètres, la mémoire, et le temps pour le timeout de connexion.
Quitter	Ce menu permet de déconnecter les moniteurs et de quitter l'application.

Fenêtres

Le menu **Fenêtres** permet de gérer les fenêtres d'affichage des différents firewalls connectés :

Maximiser	Ouvre la fenêtre sélectionnée.
Cascade	Organise les différentes fenêtres connectées en cascade dans l'application.
Titre	Permet d'avoir une visualisation globale des principaux services proposés par le Monitor.
Dupliquer la fenêtre courante	Duplique la fenêtre sur laquelle vous vous trouvez selon le firewall que vous avez préalablement sélectionné.
Vue d'ensemble	Adresse IP du/des firewall(s) connectés.
Adresse du firewall	Le menu déroulant indique les derniers écrans visités et distingue celui sur lequel on se trouve par une coche.

Applications

Le menu **Applications** permet une connexion aux autres applications de la Suite d'Administration Stormshield Network. Utiliser les deux raccourcis procurent l'avantage de ne pas devoir se ré-authentifier sur ces deux applications.

Lancement de l'application de configuration	Permet d'accéder à l'interface Web d'administration du Firewall sélectionné.
Exécuter Stormshield Network Event Reporter…	Permet l'ouverture du **Stormshield Network Event Reporter** de la Suite d'Administration.

? (Aide)

Aide	Ouvre une page permettant d'avoir accès à votre espace privé, ceci afin d'avoir accès aux documentations.
A propos…	Donne des informations sur le moniteur utilisé (numéro de version, crédit).

2.2.3 PARAMÈTRES DE L'APPLICATION

Il est possible de configurer certains paramètres de l'application **Stormshield Network Real-Time Monitor**.

➲ Sélectionnez le menu **Fichier\Paramètres de l'application**... : l'écran des paramètres s'affiche.

Comportement au démarrage

Cet onglet propose différentes options permettant de configurer le comportement au démarrage de l'application.

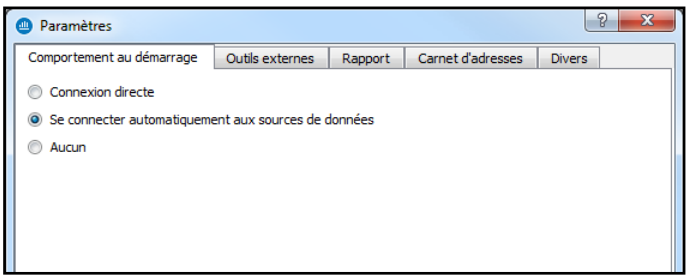


Figure 15 : Comportement au démarrage

Connexion directe	En cochant cette option, la fenêtre de connexion directe s'affiche au démarrage de Monitor. Elle vous permet de saisir l'adresse IP du firewall désiré et le mot de passe de l'utilisateur.
Se connecter automatiquement aux sources de données	En cochant cette option, la connexion est effectuée automatiquement sur les différents firewalls du carnet d'adresses.
Aucun	L'écran **Vue d'ensemble** s'affiche mais le Monitor ne se connecte à aucun firewall.

Outils externes

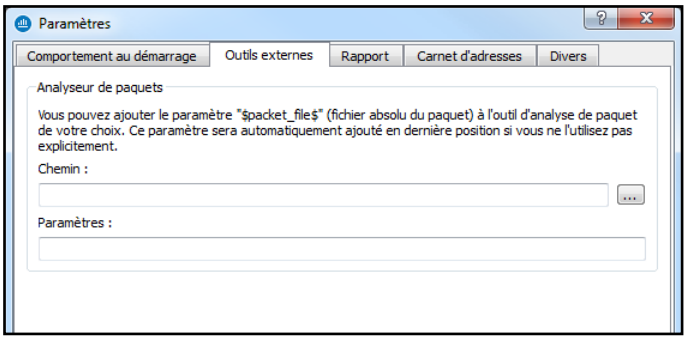


Figure 16 : Paramètres - Outils externes

Analyseur de paquets	Lorsqu'une alarme se déclenche sur un Firewall Stormshield Network, il est possible de visualiser le paquet responsable du déclenchement de cette alarme. Pour cela il faut vous munir d'un outil de visualisation de paquets comme **Ethereal** ou **Packetyzer**… Spécifiez l'outil choisi dans le champ "Analyseur de paquets", celui-ci sera utilisé par le Monitor pour afficher les paquets malicieux.
Chemin	Indication de la localisation du répertoire où se trouve l'application permettant d'analyser les paquets.
Paramètres	Possibilité d'ajouter le paramètre "$paquet_file$" à l'outil d'analyse du paquet.

Rapport

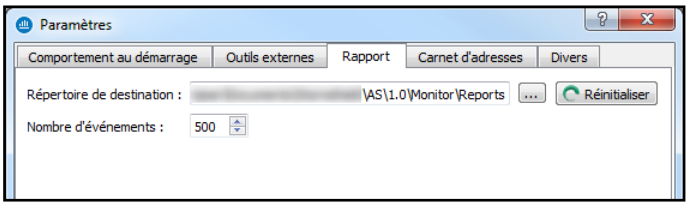


Figure 17 : Paramètres - Rapport

Répertoire de destination	Permet de choisir l'emplacement du répertoire de destination du rapport. Le bouton **Réinitialiser** vous permet de réinitialiser le répertoire de stockage des rapports.
Nombre d'événements	Permet de définir le nombre d'évènements souhaités dans la génération du rapport. Par défaut, la valeur est portée à 500 lignes.

REMARQUE

Le rapport pourra être généré en effectuant un clic-droit sur une ligne dans le menu **Vue d'ensemble** et en sélectionnant **Générer un rapport web...**

Le rapport comporte les informations suivantes:

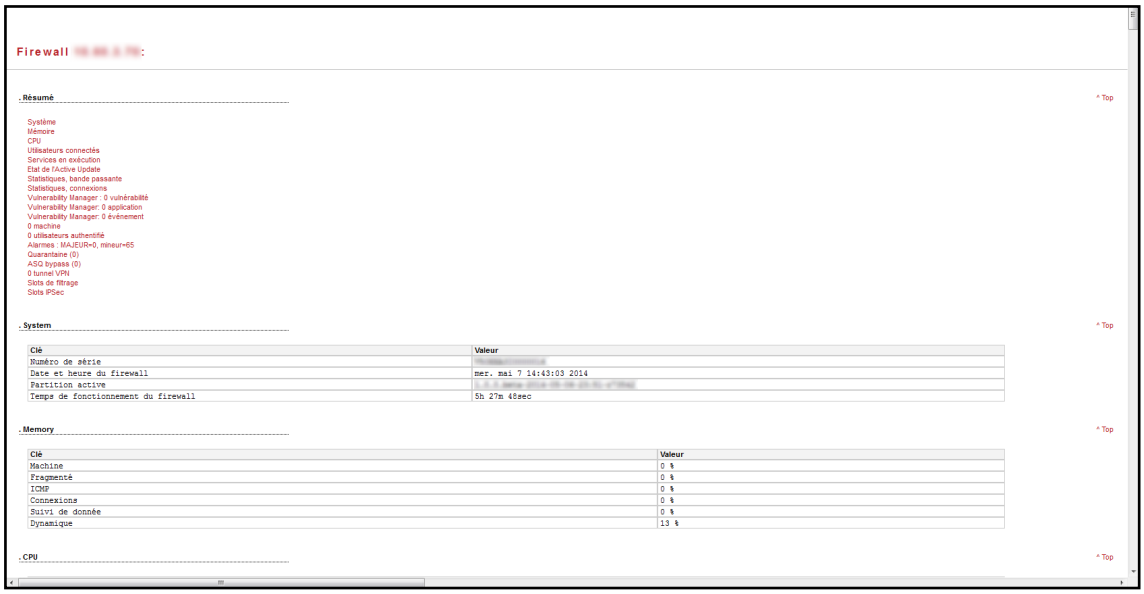


Figure 18 : rapport de synthèse

Il affiche des informations diverses au sujet du firewall pour lequel vous avez souhaité générer un rapport. En cliquant sur un lien dans la liste, les informations s'affichent sous forme de tableaux ou de graphiques.

Par exemple, ci-dessous, les informations concernant la mémoire sont indiquées.

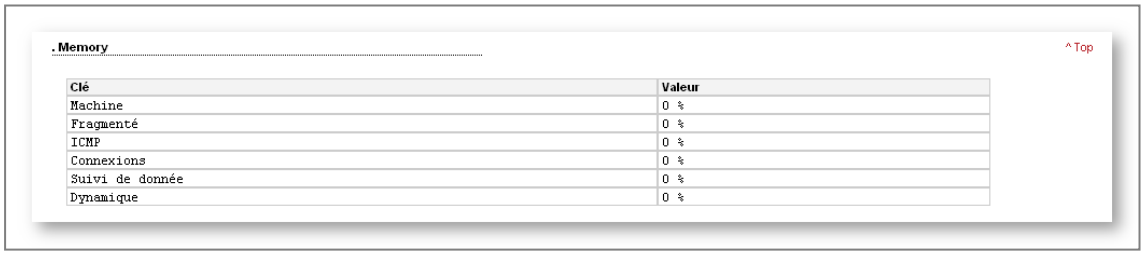


Figure 19 : Informations mémoire

Carnet d'adresses

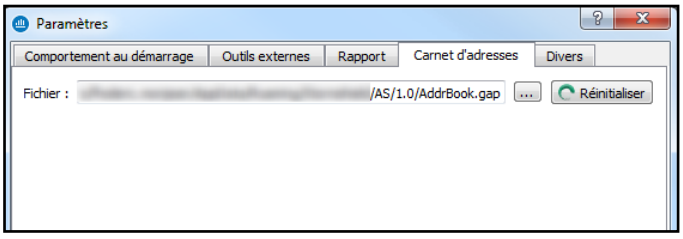


Figure 20 : Paramètres - Carnet d'adresses

Les applications Stormshield Network Global Administration, Stormshield Network Real-Time Monitor ET Stormshield Network Event Reporter utilisent le même carnet d'adresses et donc le même fichier de carnet d'adresses.

Pour récupérer un fichier .gap (fichier de projet Stormshield Network), il suffit de cliquer sur le bouton **Parcourir**.

Divers

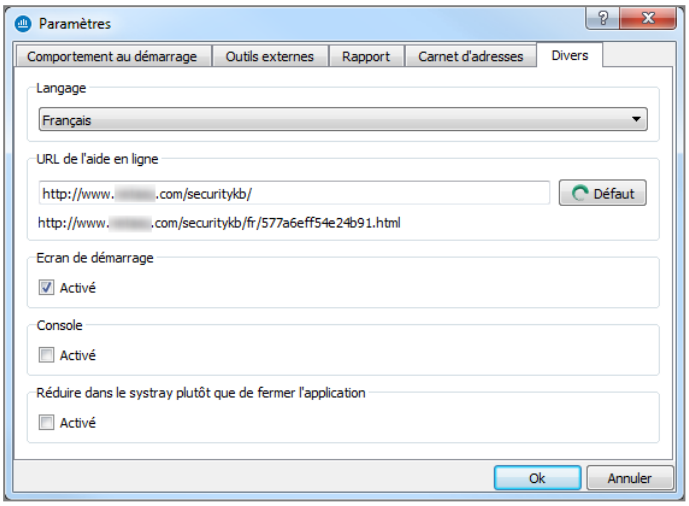


Figure 21 : Paramètres – Divers

Langage	Vous pouvez choisir entre trois langues pour les menus de l'interface : Anglais, Français, et désormais, Polonais. La sélection automatique prendra la langue de la version de Windows installée sur le poste. Après modification du choix, il faut redémarrer l'application pour activer le nouveau choix de langue.
URL de l'aide en ligne	Cette option vous permet à tout moment d'accéder à la base de connaissances Stormshield Network.
Ecran de démarrage	En cochant cette option, la première fenêtre qui apparaît au démarrage est celle qui contient le nom, le logo, la version et l'état de chargement du logiciel. En décochant cette option, la fenêtre de démarrage ne sera plus affichée.
Console	En cochant l'option **Activé**, vous pouvez accéder aux équipements en mode console (commandes CLI). En validant cet écran, un menu **Console** vient se rajouter sous le menu de l'arborescence **Vue d'ensemble**.
Réduire dans le systray plutôt que de fermer l'application	En cochant cette option, l'application est réduite dans le Systray au lieu d'être fermée.

2.2.4 PARAMÈTRES PAR DÉFAUT DU MONITORING

Ce menu permet de configurer les temps de rafraîchissement de l'ensemble des informations contenues dans le Monitor. Il existe 6 paramètres qui régissent la fréquence de récupération des données. Vous pouvez configurer la période d'affichage des différents logs (en nombre de lignes) et des différents diagrammes (en minutes).

Vous accédez aux paramètres par défaut du Monitoring par le menu **Fichier\Paramètres par défaut du Monitoring**.

Mises à jour

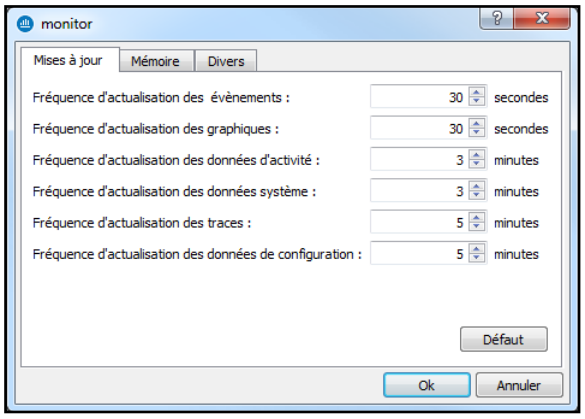


Figure 22 : Monitor - Mise à jour

Fréquence d'actualisation des événements	Spécification en secondes de l'actualisation de la liste des événements détectés. La fréquence de rafraîchissement est portée à 30 secondes par défaut et peut être au minimum à 1 seconde et au maximum à 3600 secondes.
Fréquence d'actualisation des graphiques	Spécification en secondes de l'actualisation des graphiques (Statistiques, Interfaces, QoS et SA VPN). La fréquence de rafraîchissement est portée à 30 secondes par défaut et peut être au minimum à 10 secondes.
Fréquence d'actualisation des données d'activité	Spécification en minutes de l'actualisation des données d'activités (Machines, utilisateurs authentifiés et Vulnerability Manager). La fréquence de rafraîchissement est portée à 3 minutes par défaut et peut être au minimum de 1 minute.
Fréquence d'actualisation des données système	Spécification en minutes de l'actualisation des données système (données de session, Haute Disponibilité, raid, carte cryptographique, Quarantaine, Services et Active Update). La fréquence de rafraîchissement est portée à 3 minutes par défaut et peut être au minimum de 1 minute.
Fréquence d'actualisation des traces	Spécification en minutes de l'actualisation des traces. (Occupation des traces, filtrage, VPN, Système, traces de trafic et de filtrage). La fréquence de rafraîchissement est portée à 5 minutes par défaut et peut être au minimum de 1 minute.
Fréquence d'actualisation des données de configuration	Spécification en minutes de l'actualisation des données de configuration. (Anti spam, anti-virus, proxies, SPD et propriétés système). La fréquence de rafraîchissement est portée à 5 minutes et peut être au minimum de 1 minute.

REMARQUE

Le bouton Défaut permet de redéfinir la configuration des paramètres dans leurs valeurs par défaut.

Mémoire

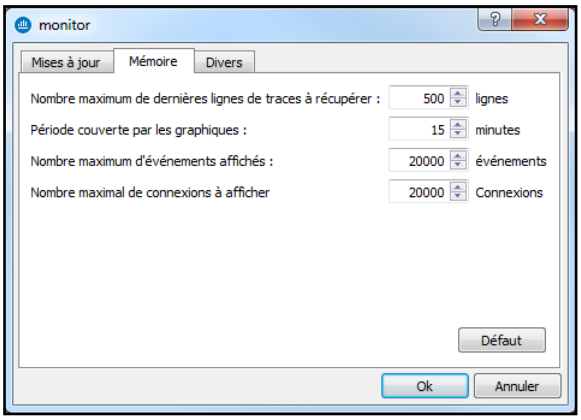


Figure 23 : Monitor - Mémoire

Nombre maximum de dernières lignes de trace à récupérer	Configuration du nombre de lignes de traces à afficher dans le menu **Trafic**.
Période couverte par les graphiques	Indication d'une durée pour les graphiques (Statistiques du menu **Interfaces**).
Nombre maximum d'événements affichés	Configuration du nombre de lignes d'événements à afficher dans le menu **Evénements**. Par défaut, la valeur est portée à 20 000 événements et peut être au minimum à 1 événement et au maximum à 2 000 000 événements. Le nombre de lignes d'alarmes indiqué influe sur la mémoire utilisée : La mémoire utilisée pour 150000 lignes d'événements indiquées pour un firewall est de 220 Mo environ. La mémoire utilisée pour 300000 lignes d'événements indiquées pour un firewall est de 430 Mo environ.
Nombre maximal de connexions à afficher	Configuration de la limite du nombre de connexions à afficher dans les modules **Machines**, **Interfaces**, **Politique de filtrage** et **Qualité de service**. Si leur valeur est nulle, la fonction est désactivée. Par défaut, la valeur est portée à 20 000 événements.

3. INFORMATIONS SUR LES FIREWALLS

3.1 VUE D'ENSEMBLE

3.1.1 Présentation

A partir de l'arborescence, Le menu **Vue d'ensemble** permet d'afficher un certain nombre d'informations au sujet de vos firewalls. Ces informations sont disponibles une fois la connexion établie avec le firewall.

Le menu **Vue d'ensemble** se compose de cinq zones :

- L'arborescence des menus.
- Une vue donnant des informations sur les vulnérabilités trouvées sur votre réseau (correspondant au menu Management de vulnérabilités).
- Une barre de recherche et d'icônes.
- Une vue qui liste vos firewalls.
- Une vue qui affiche les traces de connexion.

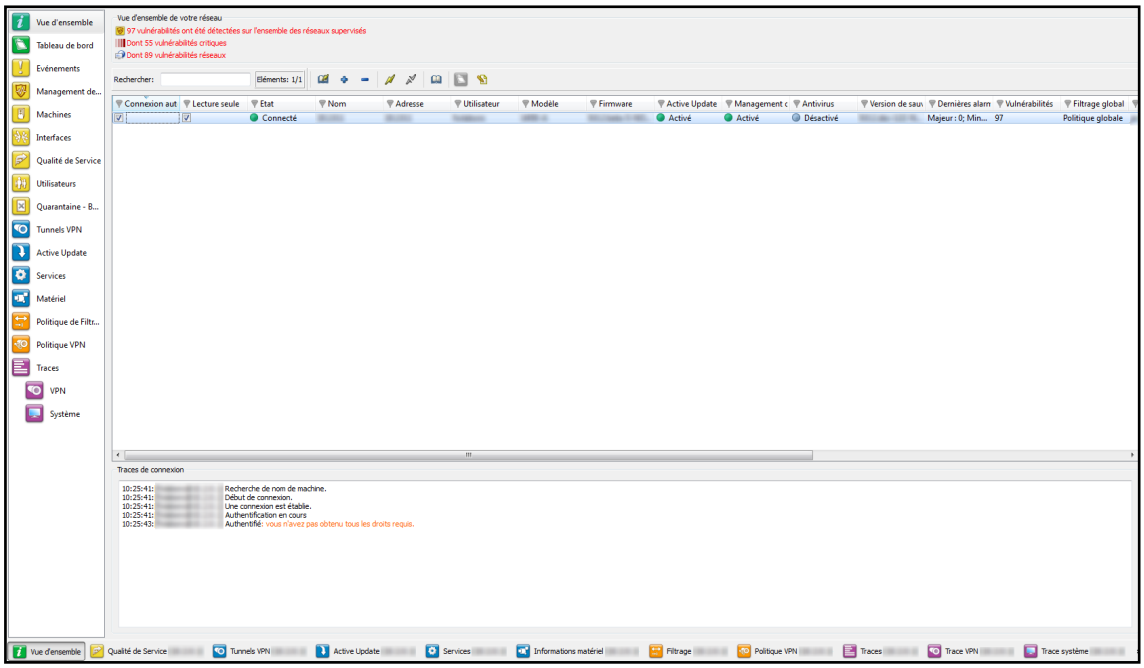


Figure 24 : Vue d'ensemble

3.1.2 Vue d'informations sur les vulnérabilités

Cette vue indique le nombre de vulnérabilités trouvées, le nombre de vulnérabilités critiques et le nombre de vulnérabilités accessibles à distance sur vos réseaux. Ces indications représentent des liens permettant d'accéder à ces vulnérabilités (menu **Management des vulnérabilités**).

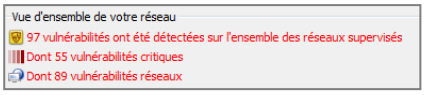


Figure 25 : Vue d'ensemble du réseau

3.1.3 Les colonnes d'informations des firewalls

Cette vue affiche les informations suivantes au sujet de votre/vos produit(s) :

Connexion auto.	En cochant cette option vous activez la reconnexion automatique du **Stormshield Network Real-Time Monitor** en cas de déconnexion.
Lecture seule	En cochant cette option, vous activez la lecture seule.
Etat	Indique l'état de connexion du produit. Les options sont les suivantes : **Connecté/Déconnecté**.
Nom	Nom ou adresse IP du produit si le nom n'a pas été indiqué.
Adresse	Adresse IP du firewall.
Utilisateur	Identifiant de l'utilisateur connecté au Firewall via **Stormshield Network Real-Time Monitor**.
Modèle	Modèle du produit : SN300, SN6000…
Firmware	Version logicielle du Firewall listé.
Active Update	Indication de l'état de mise à jour du module Active Update. Les options sont **OK** ou **x échec(s)**.
Management des vulnérabilités	Indication de l'état du service de Management de Vulnérabilités.
Antivirus	Indication de l'état de l'antivirus. Les options sont : **OK/Désactivé**.
Version de sauvegarde	N° de version du module de sauvegarde ou du Firmware de la partition passive.
Dernières alarmes	Indication du nombre d'alarmes majeures et mineures pour les dernières alarmes (durant le dernier quart d'heure). La valeur est au maximum à 100 même si le nombre des alarmes est supérieur à cette valeur.
Vulnérabilités	Indication du nombre de vulnérabilités.
Filtrage global	Indique si une règle de filtrage global est activée. Si c'est le cas, "Politique Global" est indiqué.
Filtrage	Indique le nom du slot de filtrage actif.
VPN	Indique du nom du slot VPN actif.
URL	Indique le nom du slot URL actif.
NAT	Indique le nom du slot de NAT actif.
Temps de fonctionnement	Temps de fonctionnement du firewall depuis le dernier démarrage (Up time).
Session	Indique le nombre de sessions ouvertes sur le firewall.
Commentaire	Commentaire ou description lié au firewall.

3.1.4 Traces de connexion

Cette fenêtre indique les traces de la connexion entre le Stormshield Network Real-Time Monitor et le firewall.

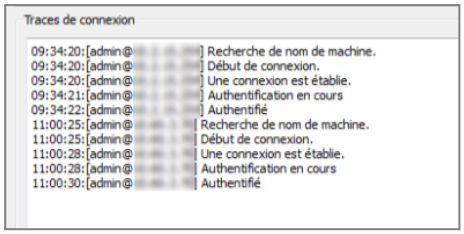


Figure 26 : Traces de connexion

ASTUCE
Vous pouvez effacer les traces en effectuant un clic droit dans la vue "Traces de connexion".

3.2 TABLEAU DE BORD

3.2.1 Présentation

Le menu **Tableau de bord** permet, sur un écran unique, d'afficher toutes les informations utiles à l'utilisateur concernant le monitoring temps réel.

Il synthétise les informations utiles de certains menus de l'arborescence du **Real-Time Monitor** et en fournit des supplémentaires. Les données affichées sur cet écran sont :

- Informations système
- Mémoire
- Température
- CPU
- Matériel
- Politiques réseaux actives
- Alarmes
- Vulnérabilités
- Tunnels VPN
- Active Update
- Traces
- Services
- Cache HTTP
- Interfaces.
- Top 5 des débits entrant des interfaces
- Top 5 des débits sortants des interfaces
- Top 5 des débits entrant des machines
- Top 5 des débits sortant des machines

Des cases à cocher permettent d'afficher ou non le détail de chacune de ces catégories d'information. L'état de chaque case (cochée / décochée) est mémorisé afin de proposer une disposition identique du tableau de bord au démarrage suivant de **SN Real-Time Monitor**.

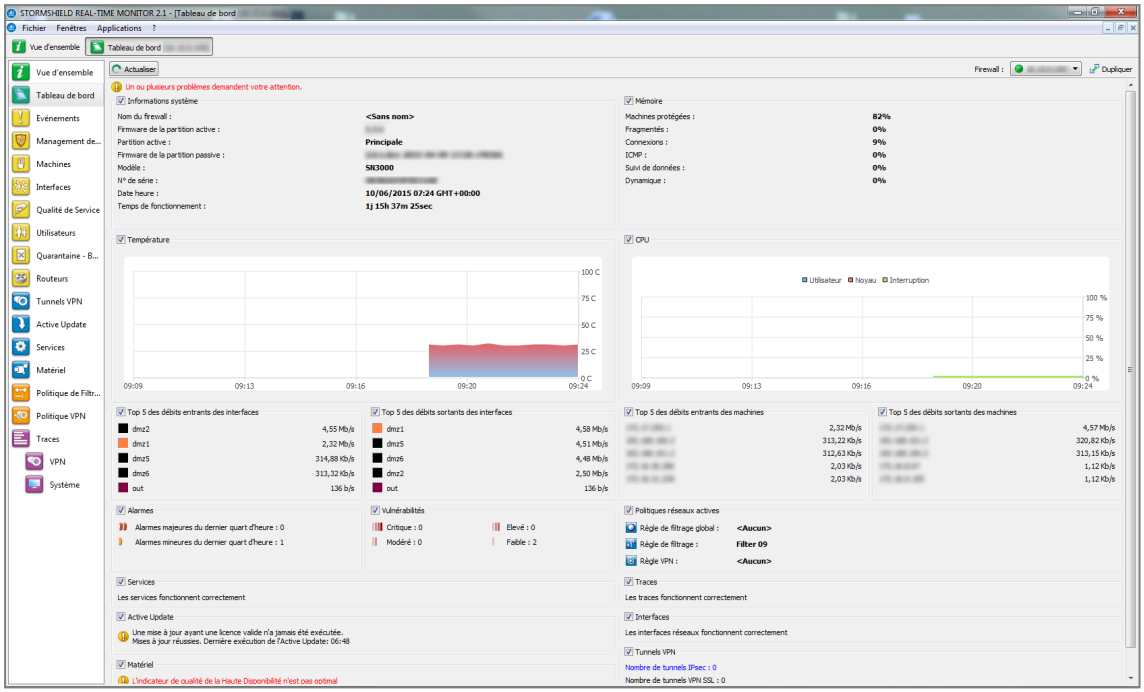


Figure 27 : Tableau de bord

3.2.2 Sélection du produit

En cliquant dans le menu **Tableau de bord**, il se peut qu'un écran de sélection de produit s'affiche si Stormshield Network Real-Time monitor est connecté à plusieurs firewalls.

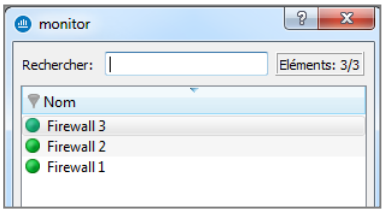


Figure 28 : Rechercher

1 Si la liste des firewalls est longue, recherchez le firewall pour lequel vous souhaitez accéder aux informations, à l'aide du champ "Rechercher".

2 Sélectionnez le firewall.

3 Cliquez sur OK. Le tableau de bord du firewall recherché s'affiche.

3.2.3 Informations système

Nom du firewall	Nom donné au produit au moment de son enregistrement dans le carnet d'adresses.
Firmware de la partition active	Version de firmware de la partition active.
Partition Active	Partition sur laquelle le firewall est démarré.
Firmware de la partition passive	Version de Firmware de la partition passive.
Modèle	N° du modèle du Firewall.

N° de série	N° de série du Firewall.
Date heure	Indication de la date et de l'heure courantes.
Temps de fonctionnement	Temps de fonctionnement du firewall depuis le dernier démarrage (Up time).

3.2.4 Mémoire

C'est le pourcentage d'utilisation d'une mémoire (buffer) réservée au stockage d'informations. Ce stockage d'informations est lié au *stateful* et correspond à l'enregistrement du contexte.

Machine protégées	Pile des machines protégées.
Fragmentés	Paquets découpés.
Connexions	L'ensemble des connexions TCP/IP.
ICMP	Requêtes ICMP (Ping, trace route...).
Suivi des données	Mémoire utilisée pour surveiller les connexions.
Dynamique	Pourcentage de la mémoire de l'ASQ en cours d'utilisation.

Les dimensions des buffers (mémoires) varient en fonction des types et des versions de produits.

Des algorithmes de nettoyage optimisent le fonctionnement des buffers (mémoires) des "Machines", "Fragmenté", "ICMP" et "Connexions". Les entrées dans les buffers (mémoires) "Fragmenté" et "ICMP" sont initialisées à intervalles fixes (chaque entrée a une durée de vie limitée : TTL).

Cela illustre une partie de la charge du boîtier firewall. Un pourcentage trop élevé correspond à une surcharge du firewall ou à une attaque.

3.2.5 CPU

DEFINITION

Plus connue sous le nom de processeur. Il s'agit d'une ressource interne au firewall responsable des calculs à effectuer.

Utilisateur :	Temps CPU alloué à la gestion des processus utilisateurs.
Noyau :	Temps CPU consommé par le noyau.
Interruption :	Temps CPU alloué aux interruptions.

3.2.6 Température

Ce graphique affiche la température en Degré Celsius (°C) de l'équipement. Celle-ci n'est pas disponible sur machine virtuelle. Pour les processeurs multi-cœurs, la valeur affichée est la moyenne de tous les CPU.

3.2.7 Matériel

DEFINITION « HAUTE DISPONIBILITE »

Il s'agit d'une architecture spécifique. Lorsque le firewall "principal" tombe en panne durant son utilisation, le second firewall prend le relais. Cette permutation est totalement transparente pour l'utilisateur.

Si la Haute Disponibilité est activée, une section supplémentaire vous donne les informations relatives à la Haute Disponibilité (Etat des firewalls, des licences, synchronisation).

Cliquez sur la phrase de description dans la zone "Matériel" pour afficher le menu **Matériel** et obtenir des informations au sujet de la Haute Disponibilité et de l'état des composants du firewall (périphériques S.M.A.R.T, volumes RAID éventuels, disques et modules d'alimentation).

Si le firewall de secours n'est pas disponible, des indications sur le firewall actif peuvent être vues.

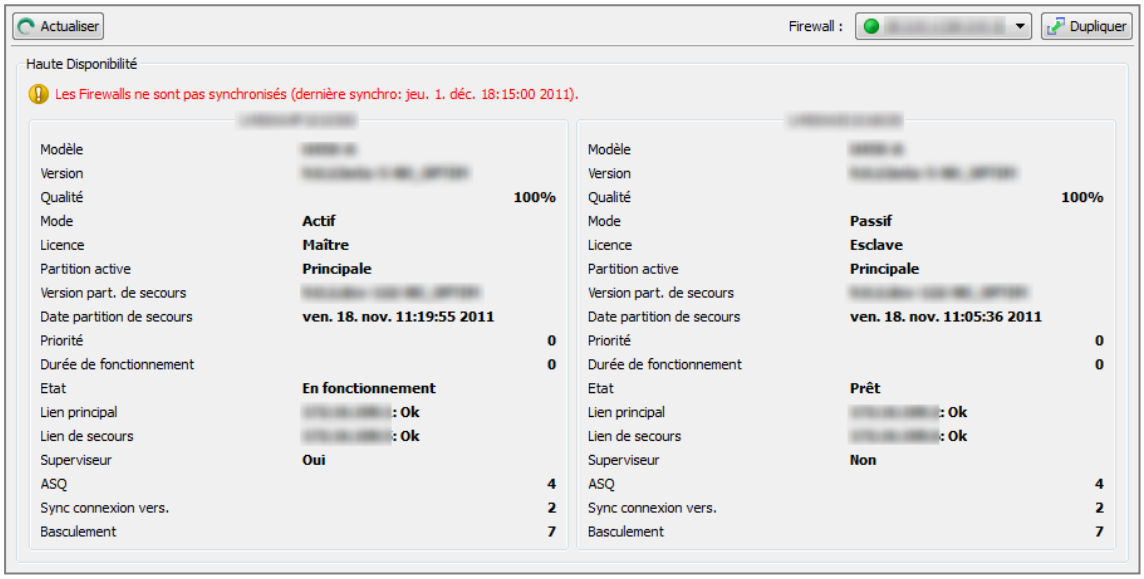


Figure 29 : Matériel

3.2.8 Politiques réseaux actives

Cette vue indique le nom des slots actifs. Si oui, le libellé de la règle activée est indiqué. Les règles mentionnées ici sont :

Règles de filtrage global	Nom de la politique de filtrage global activée.
Règle de filtrage	Nom de la politique de filtrage activée.
Règle VPN	Nom de la règle VPN activée.
Règle de translation	Nom de la politique de translation activée.
Règle de filtrage URL	Nom de la règle de filtrage URL activée.

REMARQUE
L'indication <Aucun> signifie qu'aucune politique n'est activée pour la règle qui contient cette mention.

3.2.9 Alarmes

Cette vue indique le nombre d'alarmes majeures et mineures durant le dernier quart d'heure de connexion du produit. La valeur maximale indiquée est portée à 100 même si le nombre des alarmes est supérieur à cette valeur.

Pour visualiser les alarmes, cliquez sur l'un ou l'autre lien de votre choix ; le menu **Evénements** s'affiche et énumère la liste des alarmes selon la criticité choisie.

3.2.10 Vulnérabilités

Cette vue indique le nombre de vulnérabilités selon un niveau spécifique. Les 4 niveaux de vulnérabilités sont : "Critique" ; "Elevé" ; "Modéré" ; "Faible".

Pour visualiser la liste éventuelle des vulnérabilités, cliquez sur l'un des niveaux ; le menu **Management des vulnérabilités** s'affiche (Cf. chapitre *Management de vulnérabilités*).

3.2.11 Tunnels VPN

Cette vue indique le nombre de tunnels VPN configurés. Pour visualiser la liste éventuelle des tunnels VPN configurés, cliquez sur le lien : le menu **Tunnels VPN** s'affiche.

3.2.12 Active Update

Cette vue indique l'état des mises à jour effectuées (échec ou réussite) ainsi que la date et l'heure de dernière exécution du module « Active Update ». Pour visualiser la liste éventuelle des mises à jour et de leur état, cliquez sur le lien : le menu **Active Update** s'affiche.

3.2.13 Traces

Cette vue indique s'il existe ou non des problèmes de traces. Pour visualiser le graphique qui représente en temps réel la taille actuelle du fichier de traces (Alarmes, Authentification, Connexions, Filtrage, Monitor, Plugins, POP3, Vulnerability Manager, Administration, SMTP, Système, VPN IP Sec, Web, VPN SSL) par rapport à la taille allouée sur le firewall pour chaque type de traces, cliquez sur le lien. Le menu **Traces** s'affiche.

3.2.14 Services

Cette zone indique s'il existe ou non des problèmes de services. Pour visualiser la liste des services ainsi que leur état (**Activé**/**Désactivé**), cliquez sur le lien. Le menu **Services** s'affiche.

3.2.15 Proxy Cache

Ces 3 diagrammes en secteurs (« camemberts ») représentent l'utilisation du cache HTTP, lorsque celui-ci est activé dans les règles de filtrage :

- Le premier graphe compare le nombre de requêtes mises en cache et le nombre de requêtes non mémorisées.
- Le second graphe compare la quantité de données mise en cache et la quantité de données non mémorisées.
- Le troisième diagramme présente la répartition des données mises en cache sur le disque dur, celles mises en cache dans la mémoire vive et celles non-mémorisées.

3.2.16 Interfaces

Cette zone indique s'il existe ou non des problèmes d'interfaces. Pour visualiser la bande passante, les connexions et le débit, cliquez sur le lien. Le menu **Interfaces** s'affiche.

3.2.17 Top 5 des débits entrants des interfaces

Cette zone affiche la liste des 5 premières interfaces pour le débit entrant. Cliquez sur l'une des interfaces pour afficher le graphique de l'onglet *Débit* du menu **Interfaces**.

3.2.18 Top 5 des débits sortants des interfaces

Cette zone affiche la liste des 5 premières interfaces pour le débit sortant. Cliquez sur l'une des interfaces pour afficher le graphique de l'onglet *Débit* du menu **Interfaces**.

3.2.19 Top 5 des débits entrants des machines

Cette zone affiche la liste des 5 premières machines pour le débit entrant. Cliquez sur l'une des interfaces pour afficher le graphique de l'onglet *Débit* du menu **Interfaces**.

3.2.20 Top 5 des débits sortants des machines

Cette zone affiche la liste des 5 premières machines pour le débit sortant. Cliquez sur l'une des interfaces pour afficher le graphique de l'onglet *Débit* du menu **Interfaces**.

3.2.21 Stormshield Management Center

Lorsque le firewall est administré depuis Stormshield Management Center, cette vue présente plusieurs indicateurs relatifs à la connexion au serveur SMC ainsi que sur la version de configuration actuellement déployée sur l'équipement :

Etat de la connexion	Indique si la connexion entre le firewall et le serveur Synapse est établie (Connecté / Déconnecté).
Adresse IP	Adresse IP du serveur Synapse
Connecté / Déconnecté depuis	Précise l'heure / la date depuis laquelle le firewall est connecté au serveur ou a été déconnecté du serveur Synapse.
Révision du déploiement	Indique le numéro du dernier déploiement de configuration effectué par le serveur Synapse sur le firewall.
Dernière mise à jour de configuration	Indique la date du dernier envoi de configuration par le serveur Synapse au firewall.

4. INFORMATIONS TEMPS RÉEL

4.1 ÉVÉNEMENTS

Les alarmes déclenchées par le firewall s'affichent dans cette fenêtre.

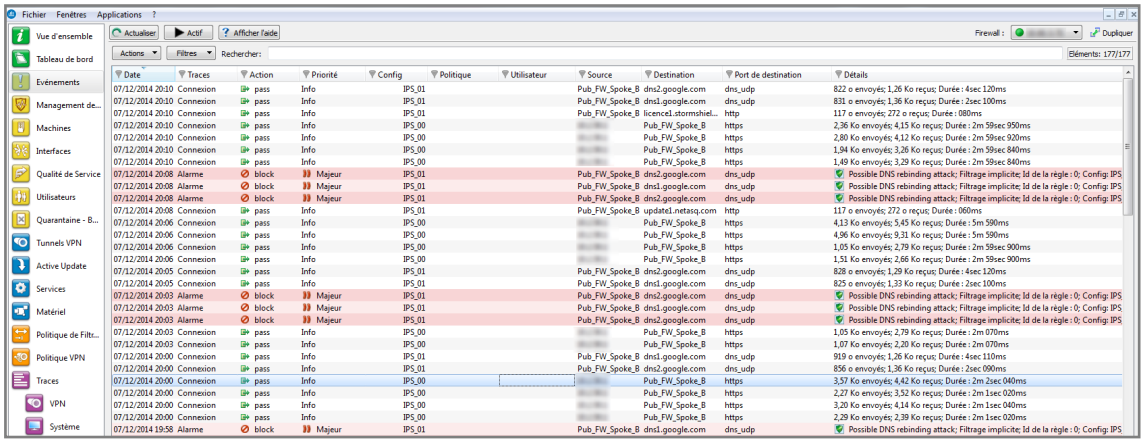


Figure 30 : Événements

Dans ce module, le bouton supplémentaire **Actif** / **Suspendu** permet de permuter l'état de l'actualisation des alarmes. Si ce bouton est dans un état suspendu, l'actualisation automatique est désactivée, ce qui facilite la lecture des traces.

En cliquant sur le menu **Evénements** de l'arborescence à gauche, les données affichées par défaut sont :

Date	Date et heure de génération de l'enregistrement de la ligne dans le fichier de log à l'heure locale du firewall.
Traces	Indication du type de traces. (les types de traces possibles sont : Alarme, Plugin, Connexion, Web, SMTP, FTP, POP3, Filtrage).
Action	Action, associé à la règle de filtrage et appliquée sur le paquet. (**Exemples** : Bloquer/Passer…)
Priorité	Détermine le niveau de l'alarme. Les valeurs possibles sont : 0 : emergency 1 : alert 2 : critical 3 : error 4 : warning 5 : notice 6 : information 7 : debug
Config	Nom du profil d'inspection applicative ayant remonté l'événement
Politique	Nom de la politique de filtrage SMTP, filtrage d'URL ou filtrage SSL ayant remonté l'alarme.
Utilisateur	Identifiant de l'utilisateur authentifié (ftp), adresse mail de l'émetteur (SMTP), identifiant de l'utilisateur si authentification active (WEB).
Source (src/srcname)	Adresse IP ou nom de l'objet correspondant à la machine source du paquet qui a déclenché l'alarme.

Port src. (num)	Numéro du port source impliqué, affiché en numérique.
Destination (dst/dstname)	Adresse IP ou nom de l'objet correspondant à la machine destinataire du paquet qui a déclenché l'alarme.
Port de destination (dst port/dstportname)	Numéro du port de destination du service ou nom de l'objet correspondant au port du service de la machine de destination s'il existe et demandé pour cette connexion.
Détails	Description de l'événement en rapport avec le log. Cette colonne regroupe à elle seule certaines des informations provenant des autres colonnes. **Exemple** S'il s'agit d'un log d'alarme, les informations d'alarme sensible, de numéro de règle de filtrage, d'identifiant de la règle (déjà renseignées dans les colonnes « Alarme sensible », « Règle » et « Identifiant ») sont regroupées dans cette colonne. Cette colonne fait apparaître l'icône précisant le type de détection selon les catégories **Applications**, **Malwares** et **Protections**.

Les autres données disponibles sont :

Firewall (fw)	Numéro de série du firewall ou nom (si connu) à l'origine de l'événement.
Date UTC (time+tz)	Date UTC (en remplacement de l'appellation GMT)
Date de début (startime)	Date « locale » du début d'un événement.
Date de début UTC (startime+tz)	Date UTC du début d'un événement (une connexion).
Fuseau horaire (tz)	Fuseau horaire du firewall.
Règle (ruleid)	Numéro de la règle de filtrage impliquée dans la remontée de l'alarme.
Protocole (proto)	Protocole du paquet qui a déclenché l'alarme.
Groupe de connexion (groupid)	Identifiant permettant le suivi des connexions filles.
Interface source (srcif/srcifname)	Nom de l'interface du firewall sur laquelle s'est déclenché l'événement. (Carte réseau de l'Interface Source.)
Adresse source (src)	Adresse IP de la machine source du paquet qui a déclenché l'événement.
Port source (srcport/srcportname)	Numéro de port de la source du service ou nom de l'objet correspondant au port du service de la machine source (uniquement si TCP/UDP).
Interface de destination (dstif/dstifname)	Carte réseau de l'interface de destination.
Adresse destination (dst)	Adresse IP de la machine destinataire du paquet qui a déclenché l'événement.
Authentification	Méthode d'authentification employée.
Alarme sensible (sensible)	Indication d'une alarme sensible ou non. Cette alarme est émise lorsque le système de prévention d'intrusion détecte un paquet sensible et pour lequel il a été configuré en mode détection d'intrusion. Si l'alarme est sensible, dans ce cas, une icône en forme de point d'exclamation suivie du texte « Oui » s'affiche, sinon, c'est « Non » qui est indiqué. Lorsque l'alarme est bloquée, l'icône apparaît en grisé (elle est désactivée). **NOTE** Seules les alarmes protocolaires peuvent être qualifiées de « sensible ». Pour les alarmes qui ne sont pas de cette classe, la colonne sera vide.

Copie (repeat)	Indication du nombre d'occurrences d'un événement dans un délai défini. Le délai est configuré dans Stormshield Network Global Administration, menu **Traces\Avancé**, option Ecriture des doublons de traces chaque.
Identifiant (Id/alarmid)	Indication du numéro de l'alarme.
Contexte (class)	Texte informatif sur la catégorie d'appartenance de l'alarme (Système, Protocole, Filtrage,...)
Type d'alarme (classification)	Code (nombre) indiquant l'appartenance à une catégorie d'alarmes. Cette colonne fait également apparaître le type de détection selon les catégories **Applications**, **Malwares** et **Protections**.
Appelant (caller)	VOIP : Indication de l'appelant
Appelé (callee)	VOIP : Indication de l'appelé.
Durée (duration)	Temps de la connexion en secondes.
Envoyé (sent)	Nombre de KB envoyés au cours de la connexion.
Reçu (rcvd)	Nombre de KB reçus au cours de la connexion.
Opération (op)	Commande identifiée du protocole. • FTP : PUT, MPUT, GET, DELETE, • HTTP : GET, PUT, POST, • EDONKEY : SENDPART • POP3 : RETR, LIST, • FTP : DELETE, LIST,
Résultat (result)	Résultat de l'opération dans le protocole (exemple : 404 qui indique une erreur).
Paramètre (arg)	Paramètre de l'opération.
Catégorie (cat_site)	Catégorie web d'appartenance du site web demandé.
Niveau de Spam (spamlevel)	Niveau de spam. : 0 (Message non spam) 1,2 et 3 (spam) x (erreur dans le traitement du message) et ? (la nature du message n'a pu être déterminée) si l'antispam est activé.
Virus (virus)	Existence d'un virus ou pas (si l'antivirus activé).
Protocole IP (ipproto)	Protocole Internet (tcp ou udp).
Média (media)	Type de flux détecté (audio, vidéo, application,...)
Message (Msg)	Description détaillée de l'alarme. On retrouve chaque commande passée par le client. Les informations sensibles telles que les mots de passe sont retirées.
Code ICMP (icmpcode)	Code ICMP dans les logs d'alarmes.
Type ICMP (icmptype)	Type ICMP dans les logs d'alarmes.
Paquet	Indication du paquet réseau IP pour lequel a été déclenchée une alarme. Un clic-droit sur ce paquet permet de le visionner à l'aide d'un analyseur de paquets. L'indication affichée dans cette colonne affiche la des paquets IPv4 (valeur commençant par 45). La taille des paquets capturés est de 1536 octets. **AVERTISSEMENT** Pour visionner le paquet, un logiciel doit être installé sur votre machine.
Analyse sandboxing	Indique le résultat de l'analyse sandboxing réalisée sur un fichier échangé lors de la connexion référencée. Ce résultat peut prendre les valeurs suivantes : Propre, Suspect, Malveillant, Inconnu, Transmis ou Echec.
Hash	Hash appliqué au fichier analysé et permettant de l'identifier dans les différents journaux de traces.
Niveau de criticité sandboxing	Cet indicateur n'est affiché que lorsqu'un fichier analysé par le sandboxing a été reconnu comme malveillant. Il se présente alors sous la forme d'un score compris entre le seuil de détection d'un fichier malicieux (fixé par défaut à 80) et 100.

NOTE
Les logs seront désormais affichés pour les modèles sans disque dur.

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Voir la machine source,
- Voir la machine de destination,
- Ajouter la machine source à la base Objets,
- Ajouter la machine de destination à la base Objets,
- Ping de la machine source,
- Traceroute vers la machine source,
- Ping de la machine destination,
- Traceroute vers la machine destination,
- Envoyer la source en quarantaine,
- Voir le paquet,
- Purger les alarmes.

4.2 SN VULNERABILITY MANAGER (SNVM)

4.2.1 Présentation

Stormshield Network Vulnerability Manager (aussi désigné par « Management de vulnérabilités ») est un module qui permet à l'administrateur réseau de collecter en temps réel des informations et de les analyser afin de découvrir d'éventuelles vulnérabilités susceptibles de compromettre son réseau. Il permet, entre autres, de remonter les alertes venant du moteur de prévention d'intrusion et de maintenir ainsi une politique de sécurité optimale.

Stormshield Network Vulnerability Manager collecte et archive les informations liées, notamment, au système d'exploitation, aux divers services activés ainsi qu'aux différentes applications installées. Cette collecte permet la création de notices descriptives des éléments du réseau.

Stormshield Network Vulnerability Manager a pour objectifs :

- De configurer la politique de sécurité de votre réseau d'entreprise.
- D'analyser l'état de risque.
- D'optimiser le niveau de sécurité.
- De reporter les évènements de sécurité.

Le procédé est le suivant :

1 Le moteur de prévention d'intrusion de Stormshield Network (ASQ) extrait en temps réel des données à l'aide de protocoles réseaux qu'il connaît.

2 Stormshield Network Vulnerability Manager combine et pondère ces données.

3 La vulnérabilité trouvée peut ensuite être traitée grâce à des bases de données indexées dynamiquement. Une fois ces informations collectées, elles sont exploitées dans le Monitor afin

de pouvoir corriger les failles sur le réseau, détecter des logiciels interdits par la politique de sécurité, ou obtenir en temps réel le véritable risque lié à une attaque.

4 La fiche d'informations est alors complétée.

5 Une ou plusieurs solutions peuvent être alors envisagées.

Exemple

Une entreprise possède un site Web public qu'elle met à jour 2 fois par mois en utilisant le protocole FTP. A une date et heure précises, une vulnérabilité qui affecte les serveurs FTP est remontée et est donc intégrée immédiatement dans le Monitor, ce qui permet sa détection par l'administrateur réseau de manière quasi-simultanée.

Cette vulnérabilité est représentée par une ligne qui indique le nombre de machines affectées et s'il y a une solution ou non.

En déployant cette ligne, le détail des machines concernées s'affiche ainsi que le service touché par la vulnérabilité. Une aide, constituée entre autres de liens, peut être proposée pour corriger la faille détectée.

Une fois que l'administrateur réseau a pris connaissance de la vulnérabilité, il peut à tout moment corriger la vulnérabilité, mettre en quarantaine la/les machine(s) affectée(s) et générer un rapport.

SNVM peut également effectuer une analyse hebdomadaire, mensuelle ou annuelle à l'aide de l'application **Stormshield Network Event Reporter** (Autoreport). (Voir le *manuel d'utilisation Stormshield Network Event Reporter*.)

En cliquant sur le menu **Management de vulnérabilités** de l'arborescence à gauche, l'écran d'analyse se décompose de la manière suivante :

- Un onglet *Vulnérabilités*.
- Un onglet *Applications*.
- Un onglet *Informations*.

4.2.2 Onglet « Vulnérabilités »

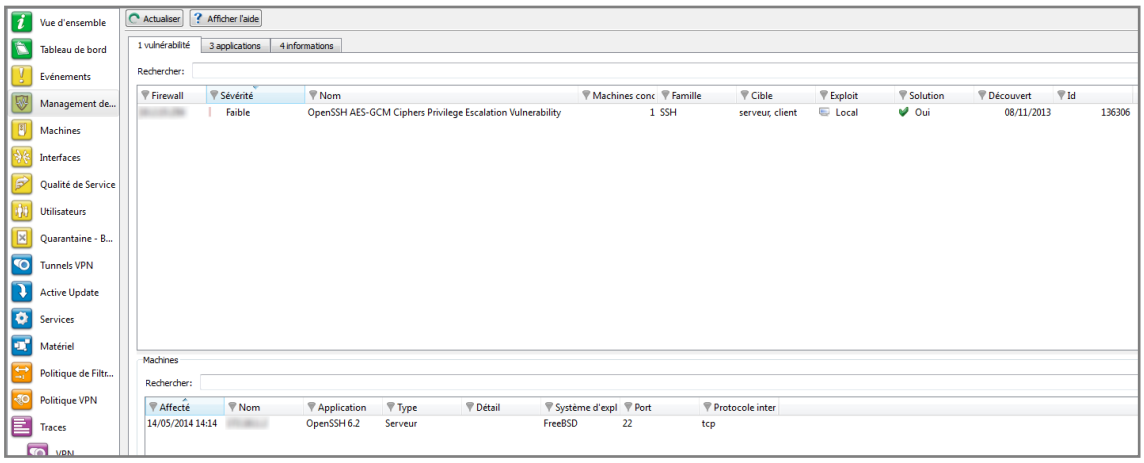


Figure 31 : Management de vulnérabilités

L'écran se compose de 3 vues :

- Une vue qui liste les vulnérabilités.
- Une vue qui liste des machines affectées par cette vulnérabilité.
- Une vue d'aide masquée que vous pouvez débloquer en cliquant sur le bouton « Afficher l'aide » (en haut à gauche de l'écran). Cela vous permet de solutionner la vulnérabilité sélectionnée si cette solution existe.

Vue « Vulnérabilité(s) »

Cette vue permet de visualiser toutes les vulnérabilités détectées par le firewall. Une ligne représente une vulnérabilité.

REMARQUE

Le nombre de vulnérabilités est affiché dans le libellé de l'onglet.

Les données de la vue « vulnérabilité » sont les suivantes :

Firewall	Numéro de série du firewall ou nom (si connu) à l'origine de la vulnérabilité.
Sévérité	Indication du niveau de sévérité de la/les machine(s) concernée(s) par la vulnérabilité. Il existe 4 niveaux de sévérité : Faible, Modéré, Elevé, Critique.
Nom	Indication du nom de la vulnérabilité.
Machines concernées	Nombre de machines affectées par la vulnérabilité.
Famille	Famille à laquelle est attachée la vulnérabilité.
Cible	Les 2 cibles sont : **client** et **serveur**.
Exploit	L'accès peut s'effectuer en local ou à distance (par le réseau). Il permet d'exploiter la vulnérabilité.
Solution	Indique si oui ou non il y a une solution proposée.
Découvert	Date de découverte de la vulnérabilité. **AVERTISSEMENT** Il s'agit de la date de découverte de la vulnérabilité et non pas de la date à laquelle cette vulnérabilité se trouve sur le réseau.
Id	Permet d'identifier la vulnérabilité de manière unique.

Vue « Machines »

Cette vue permet de visualiser toutes les vulnérabilités pour une machine donnée. Une ligne représente une machine.

Les données de la vue « Machines » sont les suivantes :

Affecté	Date d'affectation de la machine.
Nom	Nom de la machine affectée par l'attaque (s'il existe).
Adresse	Adresse IP de la machine affectée par l'attaque.
Application	Nom et version de l'application (si disponible).
Type	Type d'application (Client/Serveur/Système d'exploitation).
Détail	Nom du service susceptible d'être affecté par la vulnérabilité.
Système d'exploitation	Système d'exploitation de la machine vulnérable.
Port	N° de port sur lequel a été détectée la vulnérabilité.
Protocole Internet	Nom du protocole utilisé.

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Voir la machine,
- Ajouter la machine à la base Objets.

Zone d'aide

La zone d'aide permet de donner des détails supplémentaires concernant l'attaque. L'administrateur peut ainsi corriger la vulnérabilité.

Pour afficher ou masquer la zone d'aide associée à une ligne de vulnérabilité, cliquez sur le bouton **Afficher l'aide**.

Cette aide se caractérise par une fiche descriptive contenant des explications, des liens vers le site de l'éditeur ou vers des correctifs.

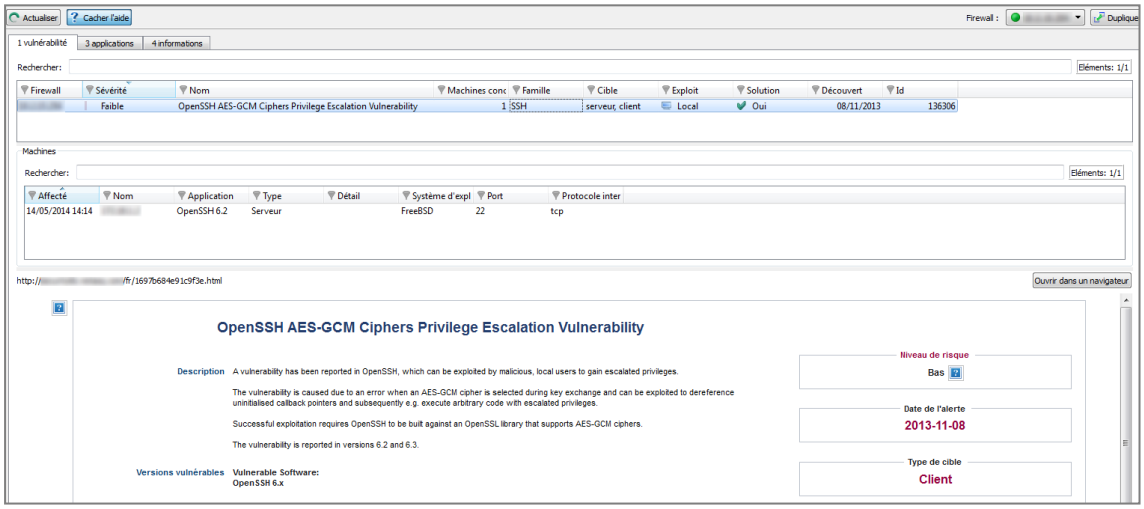


Figure 32 : Aide

4.2.3 Onglet « Applications »

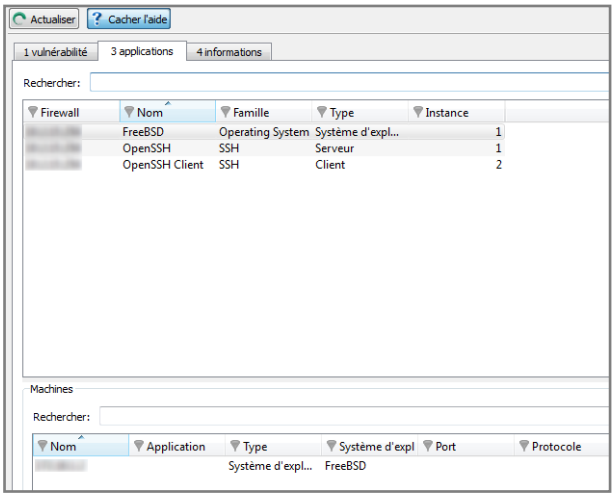


Figure 33 : Management de vulnérabilités – Applications

L'onglet *Applications* vous donne des informations au sujet des applications détectées au sein d'une entreprise.

Deux types d'applications peuvent être détectés :

- Les **produits** : sont des applications clientes installées sur une machine (exemple : Firefox 1.5).
- Les **services** : sont des applications serveurs attachées à un port (exemple : OpenSSH 3.5).

A partir des informations détectées par le moteur de prévention d'intrusion, Stormshield Network VULNERABILITY MANAGER remonte des informations sur les applications détectées. La conception de cette fonctionnalité autorise le regroupement des applications par famille. En couplant ces informations avec la base de vulnérabilités, Stormshield Network VULNERABILITY MANAGER propose également les failles probables de sécurité liées à ces applications.

Cet onglet offre des fonctionnalités de filtrage, d'affichage optionnel de colonnes, de redimensionnement lié a contenu et de copie de données dans le presse-papier. Il affiche les informations sur les applications détectées au travers des colonnes visibles dans l'écran ci-dessous :

L'écran se compose de 2 vues :

- Une vue qui liste les applications.
- Une vue détaillée qui liste les machines.

Vue « Application(s) »

Cette vue permet de visualiser toutes les applications détectées par le firewall. Une ligne représente une application.

REMARQUE

Le nombre d'applications est affiché dans le libellé de l'onglet.

L'onglet *Applications* affiche les données suivantes :

Firewall	Numéro de série du firewall ou nom (si connu).
Nom	Nom du logiciel. La version n'est pas spécifiée excepté pour les systèmes d'exploitation.
Famille	Famille logicielle de l'application (exemple : «client Web»).
Type	Type de logiciel (Client : le logiciel ne propose pas de service – Serveur : le logiciel propose un service – Système d'exploitation).
Instance	Nombre de logiciels détectés dans les réseaux supervisés. Pour un serveur, celui-ci peut proposer le même service sur plusieurs ports. Exemple : un serveur http Apache qui propose ses services sur le port 80 et le port 8080 (proxy web) apparaîtra deux fois.

Vue « Machines »

Cette vue permet de visualiser toutes les applications pour une machine donnée. Une ligne représente une machine.

Les données de la vue « Machines » sont les suivantes :

Nom	Nom de la machine.
Adresse IP	Adresse IP de la machine.
Application	Nom du logiciel complété de sa version si disponible.
Type	Type de logiciel (Client : le logiciel ne propose pas de service – Serveur : le logiciel propose un service – Système d'exploitation).
Système d'exploitation	Système d'exploitation de la machine.
Port	Port utilisé par le logiciel (s'il en utilise).
Protocole	Protocole Internet du logiciel (s'il en utilise).

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Voir la machine,
- Ajouter la machine à la base Objets.

4.2.4 Onglet « Informations »

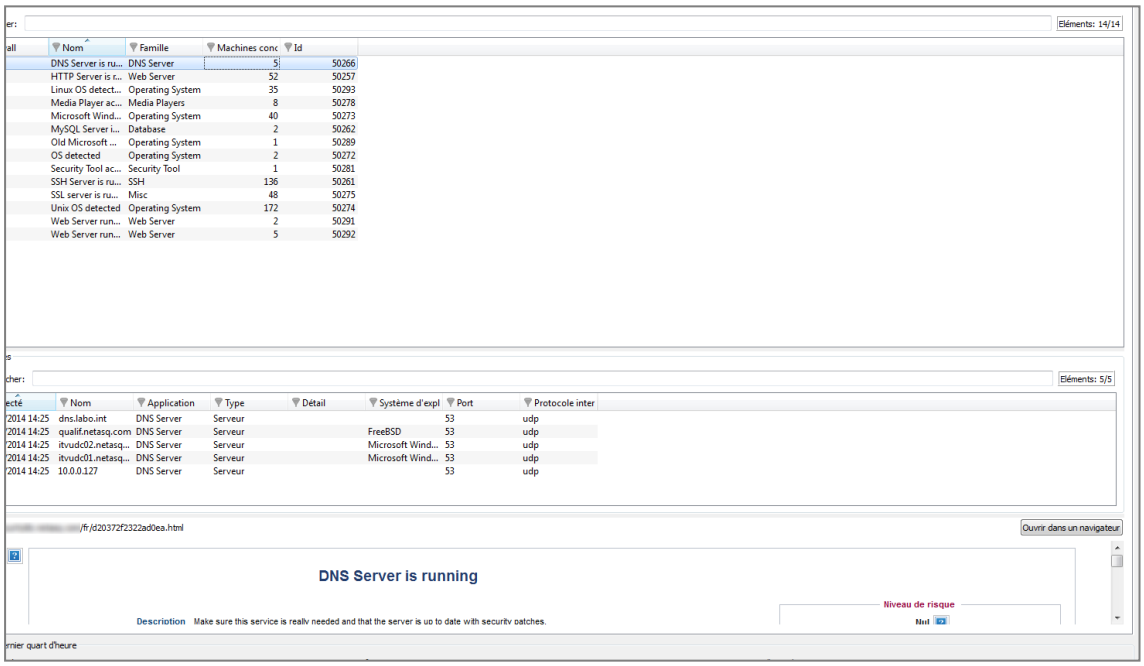


Figure 34 : Management de vulnérabilités-Informations

L'onglet *Information* vous donne des informations au sujet de l'activité de votre réseau. Vous pouvez ainsi visualiser les programmes susceptibles de générer des attaques.

L'écran se compose de 3 vues :

- Une vue qui liste les programmes.
- Une vue qui liste les machines.
- Une vue d'aide.

Vue « Information(s) »

Cette vue permet de visualiser toutes les informations détectées par le firewall. Une ligne représente une information.

REMARQUE
Le nombre d'informations est affiché dans le libellé de l'onglet.

Les données de la vue « Information » sont les suivantes :

Firewall	Numéro de série du firewall ou nom (si connu).
Nom	Nom de l'OS détecté ou d'un serveur (exemple : serveur SSH).
Famille	Famille de machines. **Exemple** SSH
Machines concernées	Nombre de machines concernées. Ces machines sont identifiées dans la vue Machines de cet onglet. **REMARQUE** Le nombre de machines indiquées dans la colonne "Machines concernées" n'est pas nécessairement identique au nombre des éléments indiqués dans la zone "Machines" de cet écran. En effet, un même service peut utiliser plusieurs ports. Par exemple, le service thttpd_server_2.25b peut écouter 2 ports différents : ce qui augmente sensiblement le nombre d'éléments.
Id	Identifiant.

Vue « Machines »

Cette vue permet de visualiser tous les événements pour une machine donnée. Une ligne représente une machine.

Les données de la vue « Machines » sont les suivantes :

Affecté	Date et heure de l'événement.
Nom	Nom de la machine.
Adresse	Adresse IP de la machine.
Application	Nom de l'application complété de sa version si disponible.
Type	Type de logiciel (Client : le logiciel ne propose pas de service – Serveur : le logiciel propose un service – Système d'exploitation).
Détail	Détail donné concernant le système d'exploitation.
Système d'exploitation	Système d'exploitation de la machine.
Port	Port utilisé par le logiciel (s'il en utilise).
Protocole Internet	Protocole Internet du logiciel (s'il en utilise).

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Voir la machine,
- Ajouter la machine à la base Objets.

Zone d'aide

La zone d'aide permet de donner des détails supplémentaires concernant l'attaque. L'administrateur peut ainsi corriger la vulnérabilité.

Pour afficher ou masquer la zone d'aide associée à une ligne d'informations, cliquez sur le bouton **Afficher l'aide**.

Cette aide se caractérise par une fiche descriptive contenant des explications, des liens vers le site de l'éditeur ou vers des correctifs.

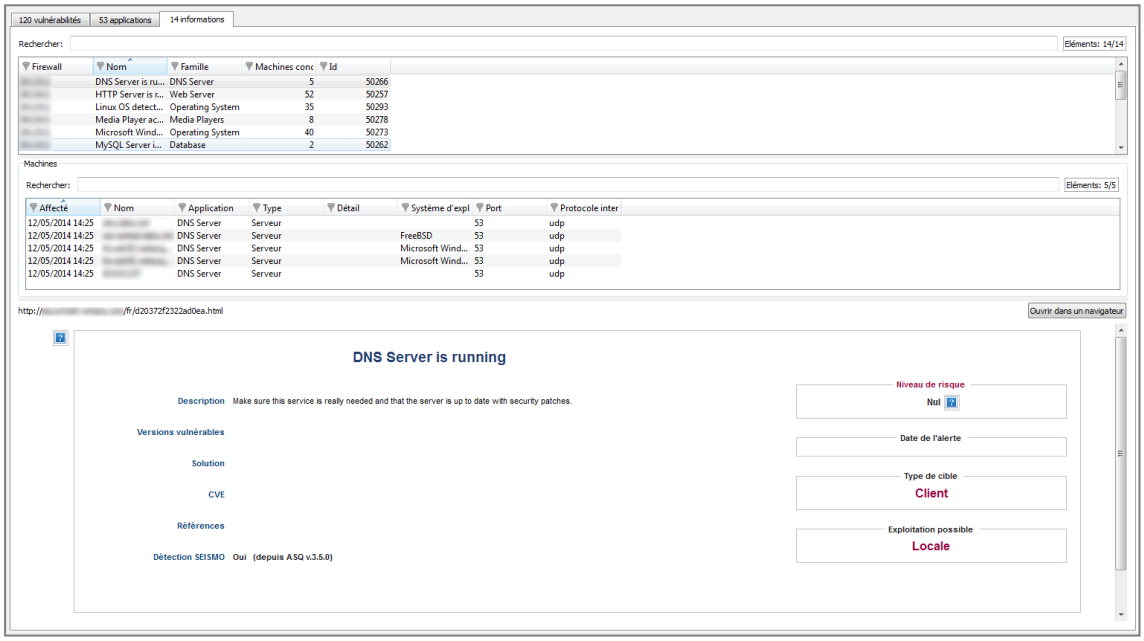


Figure 35 : Aide

REMARQUE
Pour configurer le Management des vulnérabilités, référez-vous à la documentation utilisateur Stormshield Network Global Administration.

4.3 MACHINES

A partir de l'arborescence, cliquez sur **Machines**.

Cet écran liste les machines connectées.

4.3.1 Onglet « Machines »

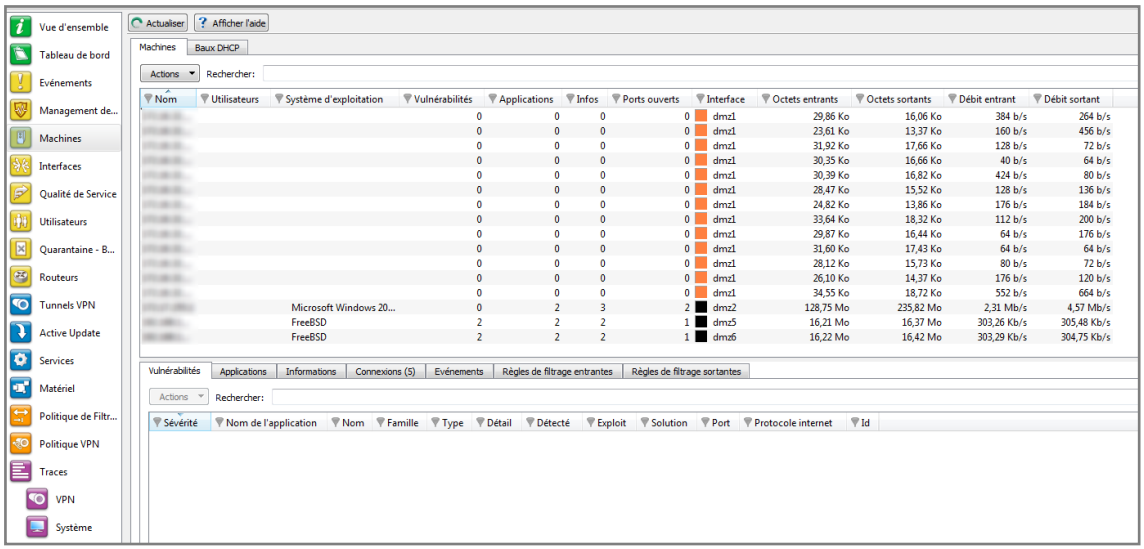


Figure 36 : Machines

L'écran se compose de 3 vues :

- Une vue qui liste les machines.
- Une vue qui liste les Vulnérabilités, Applications, Informations, Connexions et Evénements en rapport avec la machine sélectionnée.
- Une vue d'aide masquée que vous pouvez débloquer en cliquant sur le bouton « Afficher l'aide » (en haut à gauche de l'écran). Cela vous permet de solutionner la vulnérabilité sélectionnée si cette solution existe.

Vue « Machines »

Cette vue permet de visualiser toutes les machines détectées par le firewall. Une ligne représente une machine.

Les données de la vue « Machines » sont les suivantes :

Nom	Nom de la machine émettrice (si déclarée dans les objets) ou adresse IP de la machine (dans le cas contraire).
Adresse	Adresse IP de la machine.
Utilisateurs	Utilisateur connecté sur la machine (s'il existe).
Adresse MAC	Adresse MAC de la machine.
Système d'exploitation	Système d'exploitation utilisé par la machine.
Vulnérabilités	Nombre de vulnérabilités détectées.
Applications	Nombre d'applications présents sur la machine (s'il y en a).
Infos	Nombre d'informations détectées.
Ports ouverts	Nombre de ports ouverts.
Vulnerability Manager	Indication de la date et de l'heure du dernier événement VULNERABILITY MANAGER.
Interface	Interface à laquelle est rattaché l'utilisateur.
Octets entrants	Nombre d'octets ayant transité par le firewall à partir de la machine émettrice depuis le démarrage du firewall.

Octets sortants	Nombre d'octets ayant transité par le firewall à destination de la machine émettrice depuis le démarrage du firewall.
Débit entrant	Débit réel des flux à destination de la machine et transitant par le firewall.
Débit sortant	Débit réel des flux à destination de la machine et transitant par le firewall.

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Supprimer la machine de l'ASQ,
- Réinitialiser les informations Vulnerability Manager,
- Envoyer en quarantaine,
- Modifier l'OS de la machine,
- Ajouter la machine à la base Objets,
- Ping host,
- Traceroute vers la machine.

Vue « Vulnérabilités »

Cet onglet décrit, pour une machine sélectionnée, les vulnérabilités décelées. Il est possible ensuite de visualiser en détail une vulnérabilité.

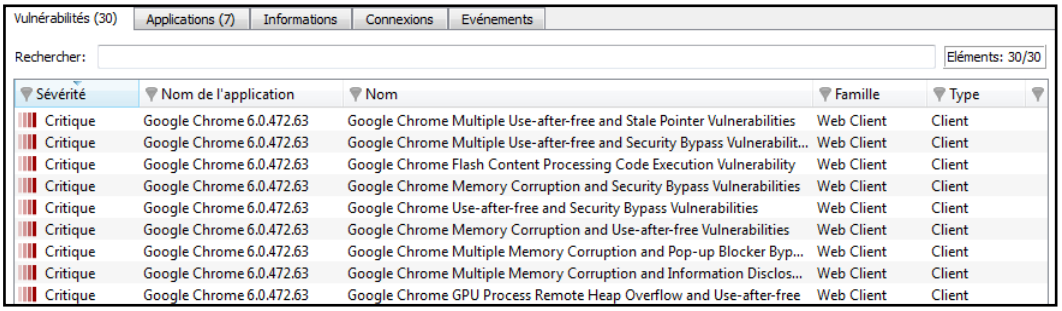


Figure 37 : Machines - Vulnérabilités

Les données de la vue « Vulnérabilités » sont les suivantes :

Sévérité	Indication du niveau de sévérité de la/les machine(s) concernée(s) par la vulnérabilité. Il existe 4 niveaux de sévérité : "**Faible**", "**Modéré**", "**Elevé**", "**Critique**".
Nom de l'application	Nom du logiciel et de sa version (si disponible).
Nom	Indication du nom de la vulnérabilité.
Famille	Nombre de machines affectées.
Type	Type de logiciel (Client : le logiciel ne propose pas de service – serveur : le logiciel propose un service).
Détail	Les 2 cibles sont : "**Client**" et "**Serveur**".
Détecté	Famille à laquelle est attachée la vulnérabilité.
Exploit	L'accès peut s'effectuer en local ou à distance (par le réseau). Il permet d'exploiter la vulnérabilité.
Solution	Indique si oui ou non il y a une solution proposée.

	Date de découverte de la vulnérabilité.
Port	**AVERTISSEMENT** Il s'agit de la date de découverte et non pas de la date à laquelle cette vulnérabilité se trouve sur le réseau.
Protocole Internet	Nom du protocole utilisé.
Id	Identifiant de la vulnérabilité.

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Lister les machines ayant la même vulnérabilité

Vue « Applications»

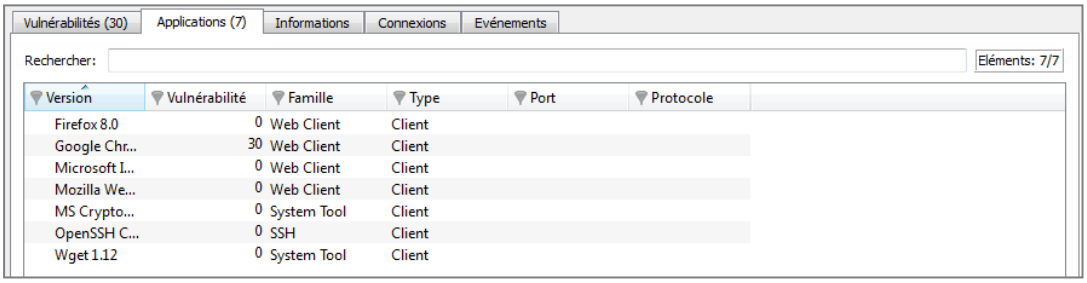


Figure 38 : Machines - Applications

Cet onglet décrit, pour une machine sélectionnée, les applications détectées. Il est possible ensuite de visualiser en détail une application.

Les données de la vue « **Applications** » sont les suivantes :

Version	Nom et version de l'application.
Vulnérabilité	Nombre de vulnérabilités détectées sur l'application.
Famille	Famille de l'application.
Type	Type d'application (Client : le logiciel ne propose pas de service – Serveur : le logiciel propose le service).
Port	Port utilisé par l'application (s'il en utilise).
Protocole	Protocole utilisé par l'application

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Lister toutes les machines qui utilisent cette application,
- Lister les vulnérabilités de cette application,
- Forcer l'application du serveur.

Vue « Informations »

Cet onglet décrit les informations liées à une machine donnée.

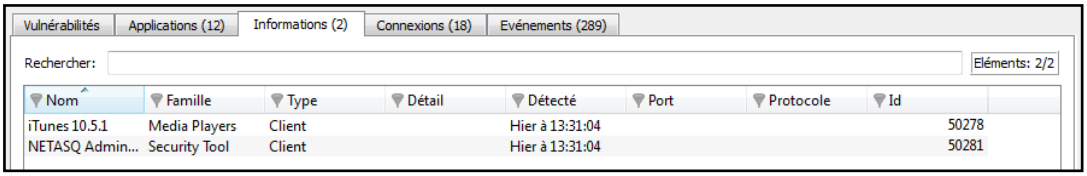


Figure 39 : Machines - Informations

REMARQUE

Le nombre d'informations est affiché dans le libellé de l'onglet.

Les données de la vue « **Informations** » sont les suivantes :

Nom	Nom de l'OS détecté.
Famille	Famille à laquelle est attachée la vulnérabilité susceptible d'apparaître. (Exemple : SSH).
Type	Type d'application (Client : le logiciel ne propose pas de service – Serveur : le logiciel propose un service).
Détail	Description des informations.
Détecté	Date et heure de détection.
Port	N° de port sur lequel a été détectée la vulnérabilité.
Protocole	Nom du protocole utilisé.
Id	Identifiant unique de la famille de vulnérabilité.

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Lister toutes les machines partageant la même information.

Vue « Connexions »

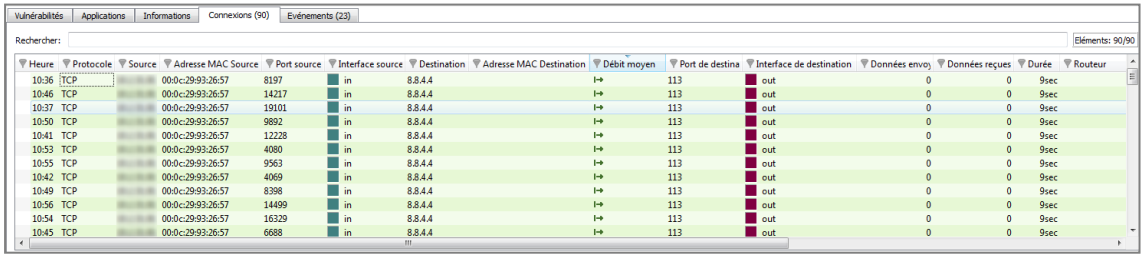


Figure 40 : Machines - Connexions

Cette vue permet de visualiser toutes les connexions détectées par le firewall. Une ligne représente une connexion. Les données disponibles pour la vue « **Connexions** » sont les suivantes :

Heure	Indication de la date et de l'heure de connexion de l'objet.
Protocole	Protocole de communication utilisé pour la connexion.
Source	Nom de l'objet qui s'est connecté sur la machine sélectionnée.
Adresse MAC source	Adresse MAC de l'objet à l'origine de la connexion

Port source	Indication du n° de port source utilisé pour la connexion.
Interface source	Nom de l'interface du firewall sur laquelle la connexion s'est établie.
Destination	Nom de l'objet pour lequel une connexion a été établie.
Adresse MAC destination	Adresse MAC de l'objet destinataire de la connexion
Débit moyen	Valeur moyenne calculée par la quantité de données échangées divisée par la durée de la session.
Port de destination	Indication du n° de port de destination utilisé pour la connexion.
Interface de destination	Nom de l'interface de destination utilisée par la connexion sur le firewall.
Données envoyées	Nombre de bits envoyés au cours de la connexion.
Données reçues	Nombre de bits reçus au cours de la connexion.
Durée	Temps de la connexion.
Routeur	Identifiant attribué par le firewall au routeur utilisé par la connexion
Nom du routeur	Nom du routeur enregistré dans la base objet utilisé par la connexion
Politique	Le nom de la politique autorisant la connexion
Règle	Le nom de l'identifiant de la règle autorisant la connexion
Opération	Commande identifiée du protocole.
Paramètre	Paramètre de l'opération.
Etat	Ce paramètre indique le statut de la connexion correspondant par exemple, à son initiation, son établissement ou sa fermeture.

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Ping de la machine source,
- Traceroute vers la machine source,
- Ping de la machine destination,
- Traceroute vers la machine destination,
- Envoyer la connexion en quarantaine.

Vue « Evénements »

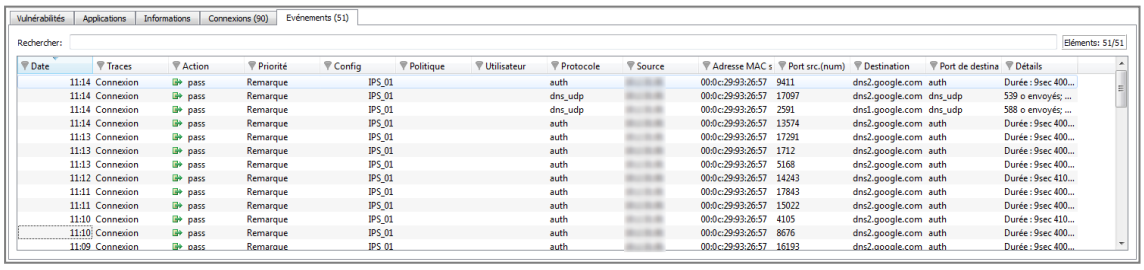


Figure 41 : Machines - Événements

Cette vue permet de visualiser toutes les événements détectés par le firewall. Une ligne représente une alarme. Les données de la vue « **Evénements** » sont les suivantes :

Date	Date et heure de génération de l'enregistrement de la ligne dans le fichier de log à l'heure locale du firewall.
Traces	Provenance de l'événement.
Action (action)	Action associée à la règle de filtrage et appliquée sur le paquet. (**Exemples** : Bloquer/Passer…)

Priorité	Détermine le niveau de l'alarme. Les valeurs possibles sont : 0 : emergency 1 : alert 2 : critical 3 : error 4 : warning 5 : notice 6 : information 7 : debug
Config	Nom du profil d'inspection applicative ayant remonté l'événement
Politique	Nom de la politique de filtrage SMTP, filtrage d'URL ou filtrage SSL ayant remonté de l'alarme.
Utilisateur	Identifiant de l'utilisateur demandant à être authentifié
Protocole	Protocole du paquet qui a déclenché l'alarme.
Source	Adresse IP ou nom de l'objet correspondant de la machine source du paquet qui a déclenché l'alarme.
Adresse MAC source	Adresse MAC de l'objet à l'origine de la connexion
Port source (num)	Numéro de port de la source (uniquement si TCP/UDP).
Destination	Adresse IP ou nom de l'objet correspondant de la machine destinataire du paquet qui a déclenché l'alarme.
Port de destination	Port demandé pour cette connexion (en toutes lettres, **exemple** : http).
Port de dst. (num)	Port de destination demandé pour cette connexion, en chiffres (**exemple** : 80).
Détails	Description de l'événement en rapport avec le log. Cette description regroupe l'information appartenant à d'autres colonnes en une seule. **Exemple** : *s'il s'agit d'un log d'alarme, les informations d'alarme sensible, de numéro de règle de filtrage, d'identifiant de la règle sont indiqués dans cette colonne ou alors sont des colonnes à part entière pour permettre le filtrage.* Veuillez consulter la note technique « *Description des journaux d'audit* »

Pour la description des données additionnelles disponibles par l'intitulé des colonnes, consultez le chapitre EVENEMENTS.

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Ping de la machine source,
- Traceroute vers la machine source,
- Ping vers la machine destination,
- Traceroute vers la machine destination.

Vue « Règles de filtrage entrantes »

Cette vue permet de lister les règles de filtrage entrantes pouvant être appliquées à la machine sélectionnée. Les règles de blocage sont affichées en rouge. Les règles ignorées sont grisées.

Vue « Règles de filtrage sortantes »

Cette vue permet de visualiser les règles de filtrage sortantes pouvant être appliquées à la machine sélectionnée. Les règles de blocage sont affichées en rouge. Les règles ignorées sont grisées.

4.3.2 Onglet « Baux DHCP »

Cet onglet affiche l'ensemble des machines ayant un bail en cours ou terminé récemment et précise l'état de ce bail. L'onglet *Baux DHCP* affiche les données suivantes :

Adresse IP	Adresse IP de la machine.
Nom	Nom de la machine ayant un bail en cours ou terminé (si déclarée dans les objets) ou adresse IP de la machine (dans le cas contraire).
Etat	L'état du bail peut être: • **Actif** : l'adresse est attribuée à une machine et cette attribution est toujours en cours. • **Libre** : le bail a expiré récemment, et l'adresse peut être réutilisée pour un autre bail.
Depuis le	Date et heure de début de l'attribution du bail.
Jusqu'au	Date et heure de fin de l'attribution du bail. Cette fin peut être passée ou future.
Adresse MAC	Identifiant physique réseau de la machine ayant un bail en cours ou terminé.

REMARQUE
Les baux attribués par réservations (adresse IP fixe réservée exclusivement à une adresse MAC) ne sont pas affichées dans cet écran.

REMARQUE
Lorsqu'une nouvelle machine se connecte sur un réseau, elle envoie une première requête (DHCPDISCOVER) à l'ensemble du réseau pour connaître les serveurs DHCP. A la réception, le serveur DHCP pré-réserve une adresse IP et l'envoie à la machine (DHCPOFFER). Or il est possible que cette machine utilise l'offre d'un autre serveur DHCP. Pendant ce temps de pré-réservation (2 minutes), l'adresse IP n'est plus disponible mais apparait dans la liste comme "libre". Si beaucoup de pré-réservations sont effectuées dans un cours intervalle de temps, il est possible que le serveur n'ait plus d'adresses disponibles alors que l'écran affiche des adresses comme étant "libre".

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Afficher la machine,
- Ping de la machine,
- Traceroute vers la machine.

4.4 INTERFACES

4.4.1 Présentation

DEFINITION
Une interface est une zone réelle ou virtuelle qui sépare deux éléments. L'interface désigne ainsi ce que chaque élément a besoin de connaître de l'autre pour pouvoir fonctionner correctement.

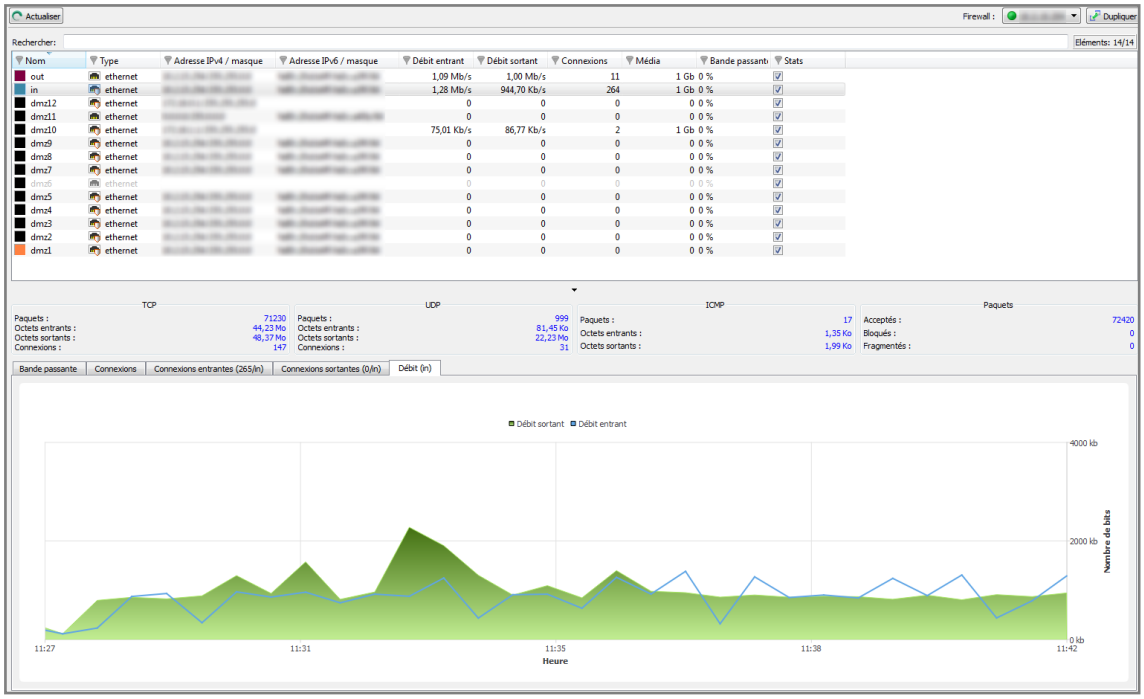


Figure 42 : Interfaces

Le menu **Interfaces** présente différentes statistiques concernant :

- La bande passante
- Les connexions
- Le débit

Les statistiques sont affichées sous forme de graphiques. Les deux axes verticaux et horizontaux sont gradués. La graduation horizontale est horaire. La graduation verticale est soit :

- Un pourcentage de bande passante.
- Un nombre de connexions.
- Un débit en octet, kilo octet ou méga octet.

Le type des interfaces

- Vlan.
- Ethernet.
- PPTP.
- Dialup.

REMARQUE
Les interfaces désactivées apparaissent en gris ou n'apparaissent pas.

L'écran se compose de 3 vues :

- Une vue tabulaire des interfaces (ou légende).
- Une zone de détails.
- Une zone de visualisation des graphiques.

4.4.2 Vue Légende (ou vue tabulaire des interfaces)

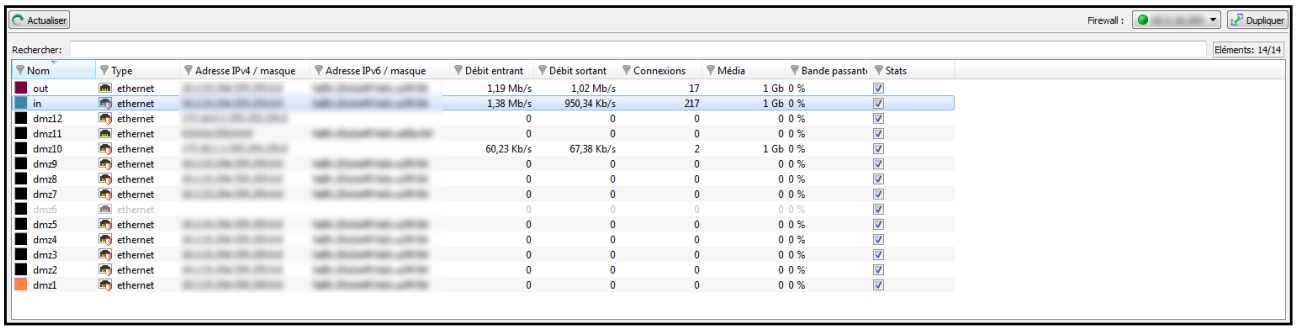


Figure 43 : Interfaces-Légende

Cette vue permet de visualiser toutes les interfaces détectées par le firewall. Une ligne représente une interface.

Les données de la vue « **Légende** » sont les suivantes :

Nom	Nom et couleur attribués à l'interface. Les couleurs permettent la reconnaissance de l'interface dans les différents graphiques.
Type	Type d'interface avec icône associé.
Adresse IPv4/ Masque	Adresse IPv4 et masque de sous-réseau de l'interface.
Adresse IPv6/ Masque	Adresse IPv6 et masque de sous-réseau de l'interface.
Débit entrant	Indication du débit réel entrant.
Débit sortant	Indication du débit réel sortant.
Connexions	Nombre de connexions en temps réel sur chaque interface du firewall sur une période définie.
Média	La valeur par défaut est 0. Le débit d'une interface réseau peut être configuré via **Stormshield Network Global Administration**.
Bande passante	Indication d'un pourcentage d'utilisation de la bande passante pour une interface.
Stats	En cochant cette option, vous affichez ou masquez le graphique correspondant à cette interface.

REMARQUE
Les interfaces déconnectées apparaissent grisées.

Vous remarquerez aussi les couleurs des interfaces visibles au haut de la fenêtre. Il s'agit de la couleur définie dans les paramètres réseau de **Stormshield Network Global Administration** pour chacune des interfaces (Voir le *Manuel utilisateur Stormshield Network Global Administration*).

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Filtrer cette colonne selon ce critère,
- Filtrer uniquement cette colonne selon ce critère,
- Afficher les machines associées à cette interface.

4.4.3 Vue « Détails »

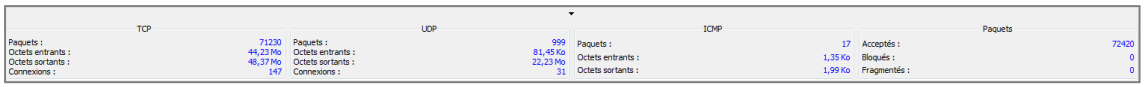


Figure 44 : Interfaces - Détails

Chaque tableau synthétise des informations statistiques de débit pour chacune des interfaces.

La zone de détails vous donne les informations suivantes :

- Le nom, l'adresse IP, le masque de sous réseau en formulation américaine (voir explications en annexe), le type de connexion (10 ou 100Mbit, half duplex ou full duplex).
- Le débit instantané (à gauche) et maximum (à droite).
- Le nombre de paquets et le volume en octets pour les protocoles TCP, UDP, ICMP.
- Le nombre de connexions TCP.
- Le nombre total de paquets acceptés, bloqués et fragmentés par le firewall.

4.4.4 Onglet « Bande passante »

Le diagramme bande passante affiche en temps réel le pourcentage d'utilisation de la bande passante disponible sur chaque interface.

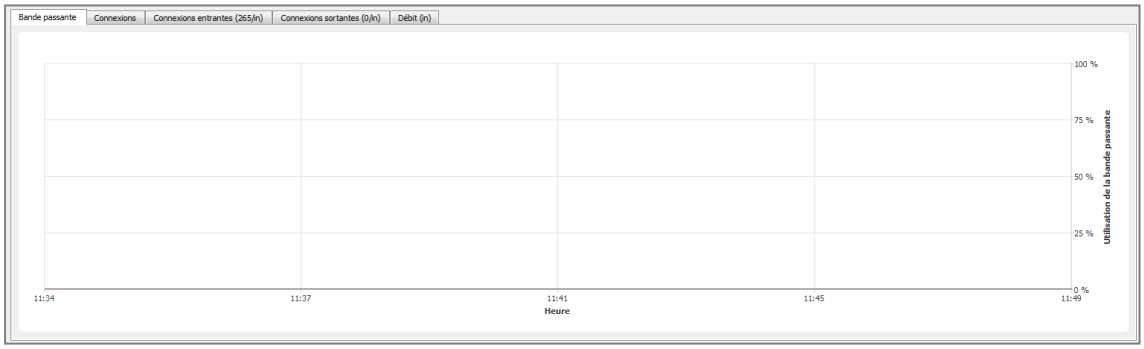


Figure 45 : Interfaces - Bande passante

Chaque interface est représentée par une couleur différente dont la légende figure au haut du diagramme. Le maximum de bande passante représente le débit théorique maximum supporté par l'interface.

Exemple

Pour une ligne à 100 Mbit/s utilisée en full duplex, ce maximum sera de 200 Mbit/s alors que pour une ligne à 10 Mbit/s en half duplex, ce maximum sera de 10 Mbit/s.

4.4.5 Onglet « Connexions »

Le diagramme de connexion affiche en temps réel le nombre de connexions sur chaque interface du firewall au cours de la période définie.

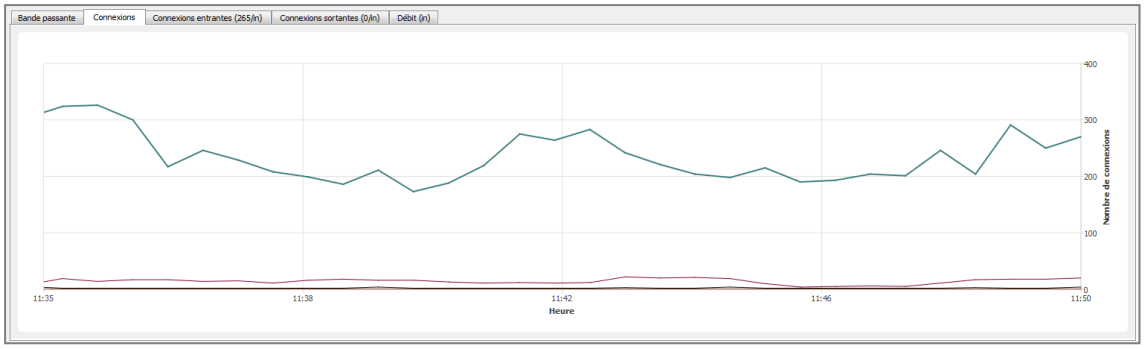


Figure 46 : Interfaces - Connexions

Chaque interface est représentée par une couleur différente dont la légende figure au haut du diagramme.

4.4.6 Onglet « Connexions entrantes »

L'écran affiche les connexions entrantes en cours relatives à l'interface sélectionnée. Pour connaître les données proposées, consultez le chapitre du module Machines, rubrique *Vue « Connexions »* de l'onglet *Machines*.

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Voir la machine source,
- Voir la machine de destination,
- Mettre la connexion en quarantaine.

4.4.7 Onglet « Connexions sortantes »

L'écran affiche les connexions sortantes en cours relatives à l'interface sélectionnée. Pour connaître les données proposées, consultez le chapitre du module Machines, rubrique *Vue « Connexions »* de l'onglet *Machines*.

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Voir la machine source,
- Voir la machine de destination,
- Mettre la connexion en quarantaine.

4.4.8 Onglet « Débit »

Le diagramme de débit représente le débit réel sur chaque interface du firewall. L'échelle des débits s'adapte automatiquement au débit maximal enregistré au cours de la période.

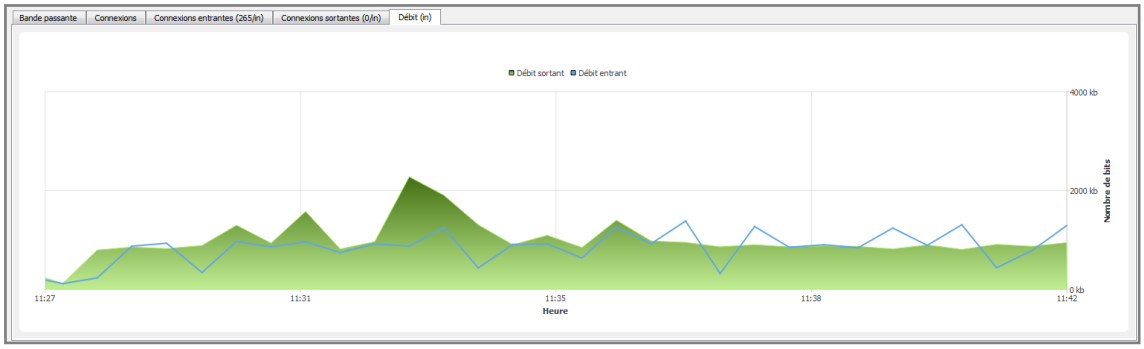


Figure 47 : Interfaces - Débit

Pour chaque interface le graphique de débit indique le débit sortant et le débit entrant.

Pour modifier l'interface sur laquelle sont visualisés les débits, cliquez sur cette interface dans la légende en haut du graphique. La ligne d'interface en cours de visualisation est surlignée en bleu.

4.5 QUALITÉ DE SERVICE (QoS)

REMARQUES

1. A un haut niveau d'abstraction, la "Qualité de service" fait référence à la capacité à fournir un service réseau en fonction de paramètres définis dans un contrat de niveau de service (SLA, "Service Level Agreement"). La "Qualité" du service est alors caractérisée par sa disponibilité, son taux de latence, ses fluctuations, son débit et son taux de paquets perdus.
2. Au niveau des ressources réseau, la "Qualité de service" fait référence à la capacité d'un équipement à fournir des services de priorisation de trafic, un contrôle de la bande passante ainsi que de son temps de latence.

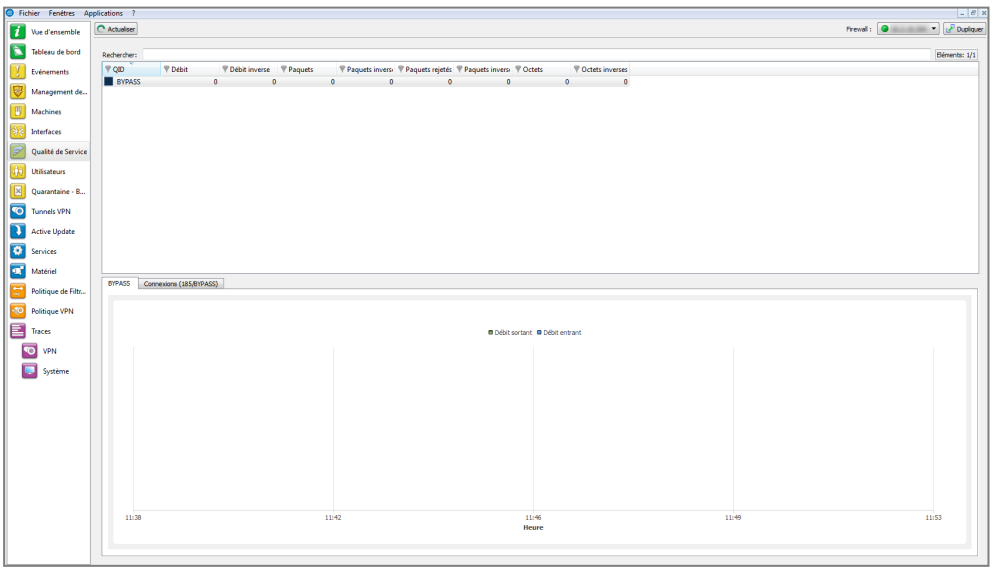


Figure 48 : Qualité de service

Cet écran se compose de 2 vues :

- Une vue tabulaire.
- Une vue graphique.

En cliquant sur le menu Qualité de Service, vous affichez les données suivantes :

QID	Nom de la politique définie pour l'acceptation ou le rejet de paquets.
Débit	Indication en temps réel du débit entrant géré par la QID.
Débit inverse	Indication en temps réel du débit sortant géré par la QID.
Paquets	Nombre de paquets entrants en temps réel sur une période définie.
Paquets inverses	Nombre de paquets sortants en temps réel sur une période définie.
Paquets rejetés	Nombre de paquets entrants rejetés sur le réseau.
Paquets inverses rejetés	Nombre de paquets sortants rejetés.
Octets	Valeur en Kbits ou Mbits.
Octets inverses	Valeur en Kbits ou Mbits.

4.5.1 Vue « Diagramme »

Cette vue affiche les débits entrant et sortant associés aux différentes Qid définies dans la politique QoS du firewall.

4.5.2 Vue « Connexions »

L'onglet Connexions détaille les connexions en cours passant dans la file sélectionnée. Pour connaître les données proposées, consultez le chapitre du module Machines, rubrique *Vue « Connexions »* de l'onglet *Machines*.

4.5.3 Vue « Règles de filtrage »

Cette vue permet de visualiser les règles de filtrage pouvant être appliquées à la classe de service sélectionnée. Les règles de blocage sont affichées en rouge. Les règles ignorées sont grisées.

4.6 UTILISATEURS

4.6.1 Présentation

Le menu **Utilisateurs** permet la visualisation des différents utilisateurs connectés sur le firewall, dans le cadre d'une session d'administration.

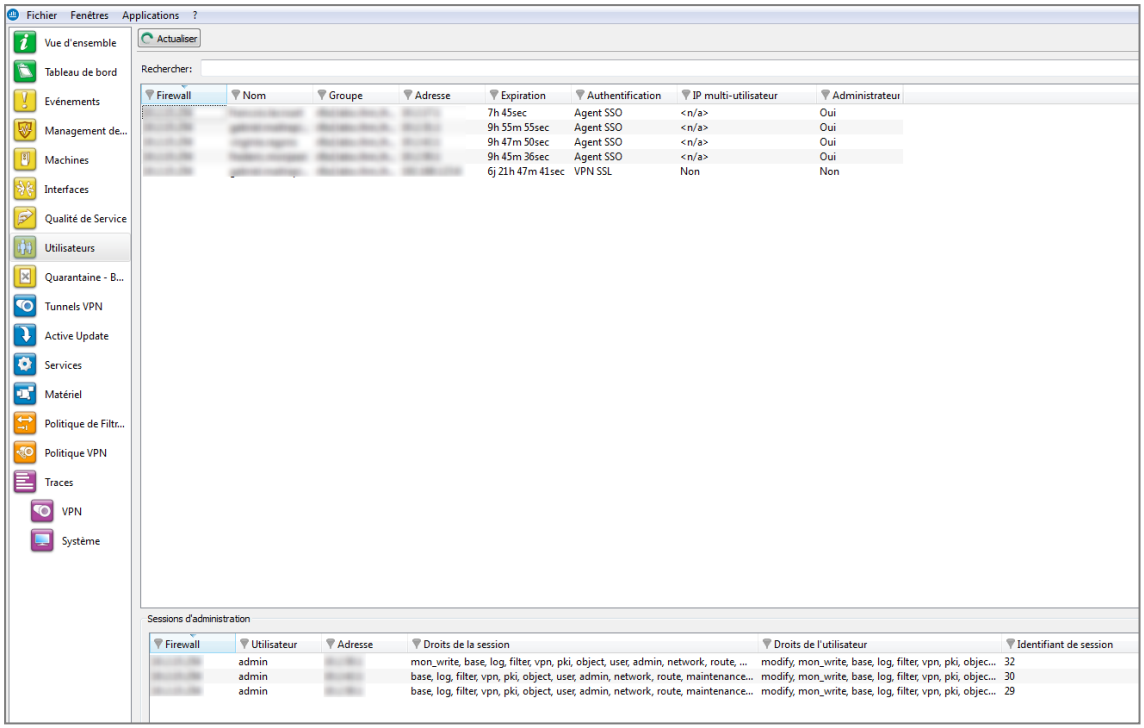


Figure 49 : Utilisateurs

Cet écran se compose de 2 vues :

- Une vue utilisateurs.
- Une vue « Sessions d'administration ».

Vue « Utilisateurs »

Les données de la vue « Utilisateurs » sont les suivantes :

Firewall	Numéro de série du firewall ou nom (si connu).
Nom	Nom de l'utilisateur authentifié.
Groupe	Nom du groupe auquel appartient l'utilisateur.
Adresse	Adresse IP de l'utilisateur.
Expiration	Temps restant pour l'authentification. (Un utilisateur est authentifié pour une certaine durée).
Authentification	Méthode d'authentification employée.
IP multi-utilisateur	Indication de l'emploi ou non de l'authentification multi-utilisateur (une adresse IP partagée par plusieurs utilisateurs). **REMARQUE** La méthode Agent SSO ne permettant qu'une seule authentification par adresse IP, la valeur n'est donc pas disponible (valeur *<n/a>* affichée).
Administrateur	Indication du type de droits 'Administrateur' accordé ou non à l'utilisateur connecté.

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Supprimer l'utilisateur de l'ASQ.

Vue « Sessions d'administration »

Cet écran permet de connaître les droits de session et les droits de l'utilisateur connecté au firewall.

Les données de la vue « Sessions d'administration » sont les suivantes :

Firewall	Numéro de série du firewall ou nom (si connu).
Utilisateur	Identifiant de l'utilisateur authentifié.
Adresse	Adresse IP de la machine de l'utilisateur connecté.
Droits de la session	Indication des droits pour la session. Un seul administrateur est autorisé à effectuer des modifications par session (droits *modify* et *mon_write*).
Droits de l'utilisateur	Indication des droits accordés à l'utilisateur connecté (ces droits concernent l'ajout, la modification, la suppression ou la lecture dans les différentes applications).
Identifiant de la session	N° d'identifiant de la session.

4.7 QUARANTAINE - ASQ BYPASS

DEFINITIONS

1. **Quarantaine dynamique** : la mise en quarantaine est manuelle et pour une durée déterminée.
2. **Quarantaine statique** : la mise en quarantaine est automatique et pour une durée permanente. La configuration de la quarantaine statique est effectuée à l'aide de l'application **Stormshield Network Global Administration**.

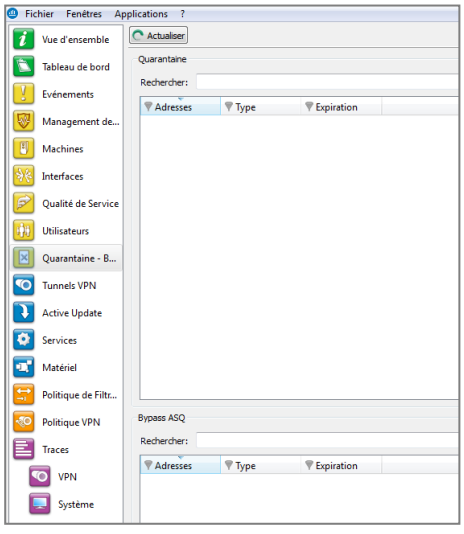


Figure 50 : Quarantaine

Cet écran se compose de 2 vues :

- Une vue « Quarantaine ».
- Une vue « Bypass ASQ ».

4.7.1 Vue « Quarantaine-Bypass ASQ »

Les machines qui ont été placées en quarantaine dynamique. Les machines en quarantaine statique ne sont pas représentées dans cette liste.

Les données de la vue « Quarantaine-Bypass ASQ » sont les suivantes :

Adresses	Adresse IP de la/les machine(s) concernée(s) par la quarantaine.
Type	2 options sont possibles : **Machine vers machine** et **Machine vers tous**.
Expiration	Heure d'expiration de la quarantaine.

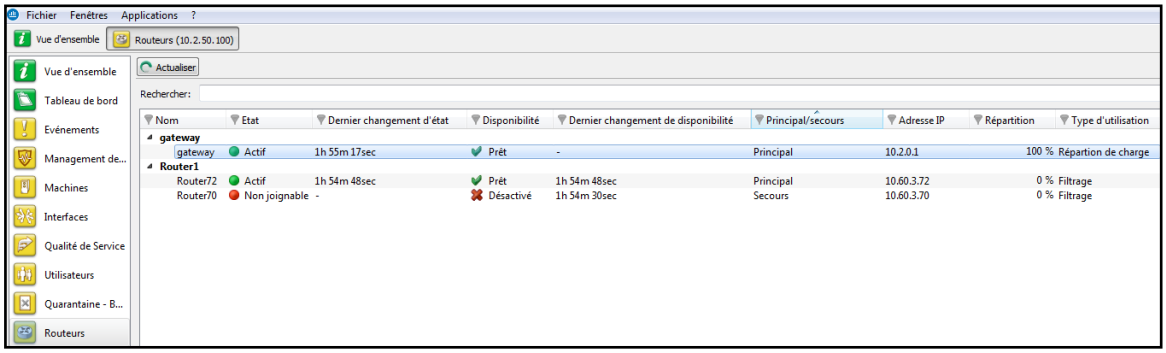
4.7.2 Vue « Bypass-ASQ »

Les données de la vue « Liste blanche » sont les suivantes :

Adresses	Adresse IP de la/les machine(s) concernée(s) par la liste blanche.
Type	2 options sont possibles : **Machine vers machine** et **Machine vers tous**.
Expiration	Heure d'expiration de la liste blanche.

4.8 ROUTEURS

Le module **Routeurs** reprend la liste des routeurs utilisés dans la configuration du firewall : passerelle par défaut et routeurs configurés dans des règles de filtrage (PBR : Policy Based Routing).



En cliquant sur le menu **Routeurs** de l'arborescence à gauche, les données affichées par défaut sont :

Nom	Nom du routeur et des passerelles qui le composent.
Etat	Indique l'état de chaque passerelle. Trois valeurs sont possibles : • **Actif** : cas d'une passerelle utilisée, • **En veille** : cas d'une passerelle de secours, • **Non joignable** : la passerelle ne répond pas aux tests de disponibilité (Ping).
Dernier changement d'état	Date du dernier changement d'état de la passerelle.
Disponibilité	Indique si la passerelle est disponible à l'utilisation. Deux valeurs sont possibles : *Prêt* ou *Désactivé*.
Disponible depuis	Délai écoulé depuis le dernier changement de disponibilité de la passerelle.

Principal / secours	Indique si la passerelle est utilisée (principale) ou est une passerelle de secours.
Adresse IP	Adresse IP de la passerelle.
Répartition	Indique le pourcentage d'utilisation de la passerelle au sein de l'objet routeur.
Type d'utilisation	Précise dans quel type de configuration la passerelle est utilisée : règle de filtrage ou répartition de charge, etc.

5. ACTIVITÉ DU RÉSEAU

5.1 TUNNELS VPN

Le module Tunnels VPN présente les tunnels VPN IPsec et VPN SSL dans deux onglets distincts.

5.1.1 Onglet Tunnels VPN IPSec

En cliquant sur l'onglet *Tunnels VPN IPSEC* du menu **Tunnels VPN**, l'écran ci-dessous s'affiche :

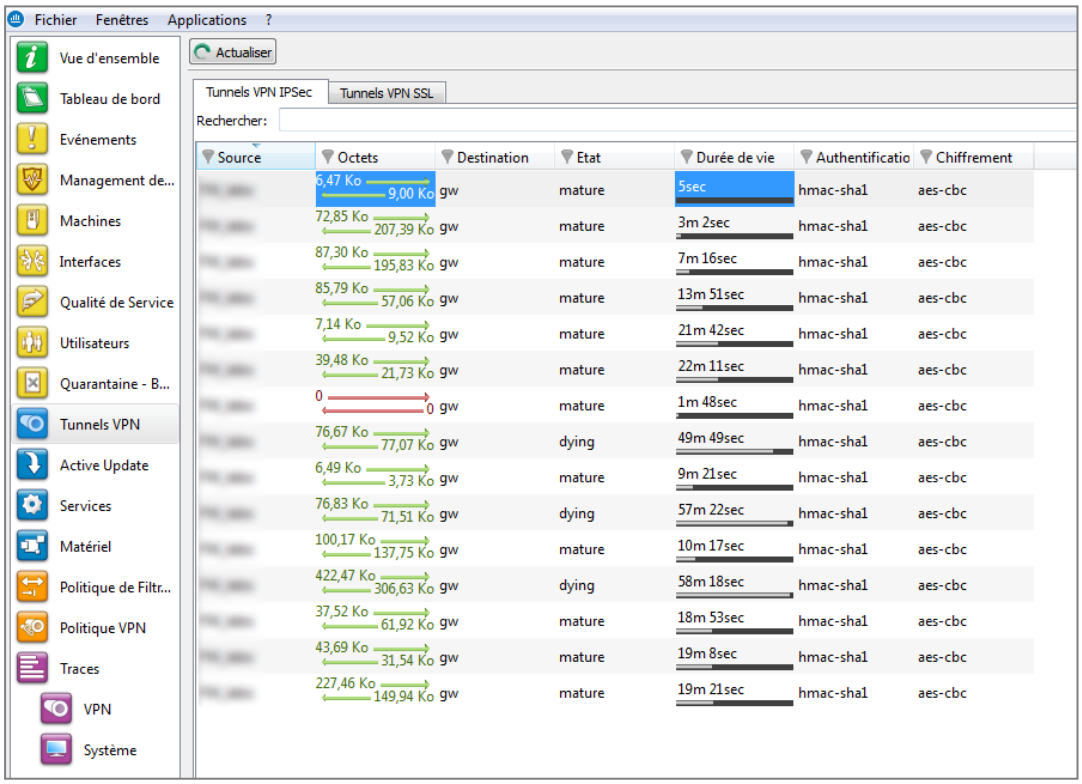


Figure 51 : Tunnels VPN IPSec

Il présente les informations statistiques sur le fonctionnement du tunnel.

Les données affichées sur cet écran sont les suivantes :

Source	IP ou nom de l'initiateur du tunnel.
Adresse source	Adresse IP de l'initiateur du tunnel

Octets	Indication des débits entrants et sortants.
Destination	Adresse IP de destination.
Etat	Indication de l'état du tunnel. (Exemple : Mature).
Durée de vie	La durée de vie de la SA (Security Association) par une représentation graphique de la position dans cette durée de vie ainsi que la valeur chiffrée (heures, minutes, secondes).
Authentification	Nom de l'algorithme d'authentification.
Chiffrement	Nom de l'algorithme de chiffrement.

Le tunnel se décompose en deux sous-tunnels, un dans un sens, un dans l'autre sens de circulation des datagrammes.

REMARQUE

Les algorithmes et les limites maximum ont été configurés dans le **Stormshield Network Global Administration**. (Référez-vous au *Manuel d'utilisation et de configuration de Stormshield Global Administration* pour plus de détails).

ASTUCE

Vous trouverez d'autres informations sur les paramètres visibles dans cette fenêtre en vous référant à la RFC.

Des informations complémentaires peuvent être trouvées dans la RFC 2401 IPSEC :

http://www.ietf.org/rfc/rfc2401.txt ou sur d'autres sites tel que : http://www.guill.net/reseaux/Ipsec.html

Cet état est représenté par un code couleur. La ligne contenant les informations du VPN prendra une des couleurs suivantes en fonction de l'état du tunnel.

	Etat non déterminé.
	Larval : la SA est en cours de négociation ou n'a pas été complètement négociée.
	Mature : la SA est établie et disponible, le tunnel VPN est correctement monté.
	Dying : la SA va bientôt expirer, une nouvelle SA est en cours de négociation.
	Dead : la SA est expirée et inutilisable, le tunnel n'a pas été remonté et n'est donc plus actif.
	Orphan : un problème a été rencontré, généralement cet état signifie que le tunnel n'est monté que dans un seul sens.

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Voir les traces des SPI sortants,
- Voir les traces des SPI entrants,
- Voir la politique sortante,
- Voir la politique entrante,
- Réinitialiser ce tunnel,
- Réinitialiser tous les tunnels.

5.1.2 Onglet Tunnels VPN SSL

En cliquant sur l'onglet *Tunnels VPN SSL* du menu **Tunnels VPN**, l'écran ci-dessous s'affiche:

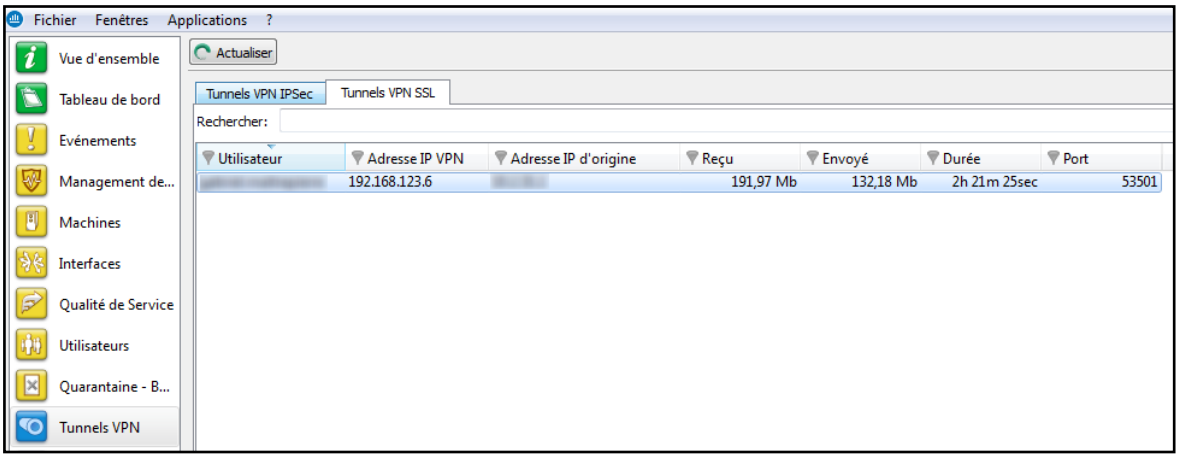


Figure 52: Tunnels VPN SSL

Il présente les informations statistiques sur le fonctionnement des tunnels VPN SSL établis.

Les données affichées sur cet écran sont les suivantes :

Utilisateur	Nom de l'utilisateur ayant initié le tunnel.
Adresse IP VPN	Adresse IP attribuée par le serveur OpenVPN au client, pour les communications au travers du tunnel VPN SSL.
Adresse IP d'origine	Adresse IP du poste client hors tunnel VPN SSL (adresse de réseau local).
Reçu	Quantité de données reçues par le client au travers du tunnel VPN SSL (unité : bits).
Envoyé	Quantité de données envoyées par le client au travers du tunnel VPN SSL (unité : bits).
Durée	Durée écoulée depuis l'établissement du tunnel VPN SSL (exprimée en jours, heures, minutes et secondes).
Port	Port source utilisé par le client pour établir le tunnel VPN SSL

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Voir la machine,
- Supprimer ce tunnel.

5.2 ACTIVE UPDATE

DEFINITION : ACTIVE UPDATE

Permet la mise à jour de la base des antivirus, les signatures contextuelles ASQ, la liste des serveurs anti spam, les autorités de certification racines de confiance et les URL utilisées pour le filtrage URL dynamique.

Cet écran affiche l'état de l'Active Update sur le firewall pour chaque type de mise à jour disponible (Anti spam, Antivirus, Signatures Contextuelles, Certificats racines et URL dynamiques).

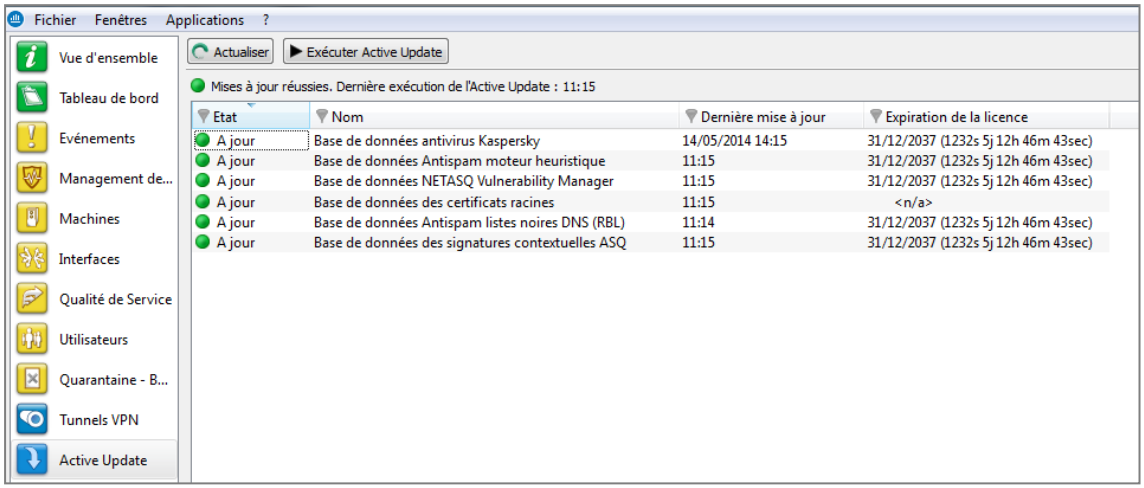


Figure 53 : Active Update

Active Update sert à maintenir automatiquement à jour les bases d'URL, en les téléchargeant sur les serveurs updateX.stormshield.eu.

L'écran du Monitor précise le résultat de la dernière mise à jour effectuée (échouée ou réussie) et la date de la dernière mise à jour.

En cliquant sur le menu Active Update, vous affichez les données suivantes :

Etat	Indication de l'état de la mise à jour de l'Active Update. 2 options sont possibles : **La dernière mise à jour a échoué** / **A jour**.
Nom	Indication des catégories de données mises à jour.
Dernière mise à jour	Indication des Date et heure de la dernière mise à jour effectuée.
Expiration de la licence	Indication de la date d'expiration de l'option de licence pour cette catégorie.

5.3 SERVICES

Cet écran énumère les services (actifs et non actifs) présents sur le firewall et depuis combien de temps ils ont été activés/désactivés.

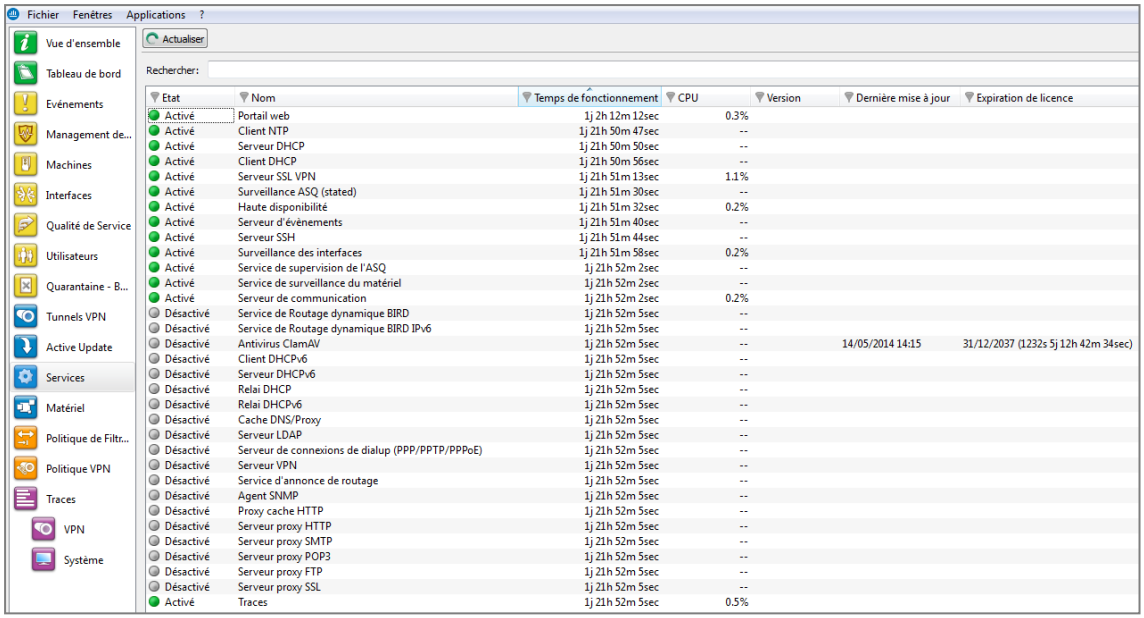


Figure 54 : Services

Cet écran contient également des informations concernant l'antivirus (activité, version, dernière mise à jour, l'expiration de la licence).

En cliquant sur le menu **Services**, vous affichez les données suivantes :

Etat	Indication de l'activation ou la désactivation des services
Nom	Indication du nom des services.
Temps de fonctionnement	Indication du nombre de jours et heure d'activation.
CPU	Part des ressources processeur consommées par le service (pourcentage)
Version	N° de version du service.
Dernière mise à jour	Date de dernière mise à jour du service.
Expiration de licence	Indication de la date d'expiration de la licence.

5.4 MATÉRIEL

5.4.1 Haute Disponibilité

Cet écran affiche des informations concernant l'initialisation de la Haute Disponibilité.

DEFINITION HD (HAUTE DISPONIBILITE)

La Haute Disponibilité est une option permettant à deux firewalls (distingués par une licence MasterHA ou BackupHA) d'échanger des informations sur leur état, au travers d'un lien dédié afin d'assurer une continuité du service en cas de défaillance de l'un d'entre eux. Des firewalls en HD possèdent la même configuration ; seul leur numéro de série, leur licence (Master ou Backup) et surtout leur état (actif ou passif) diffèrent.

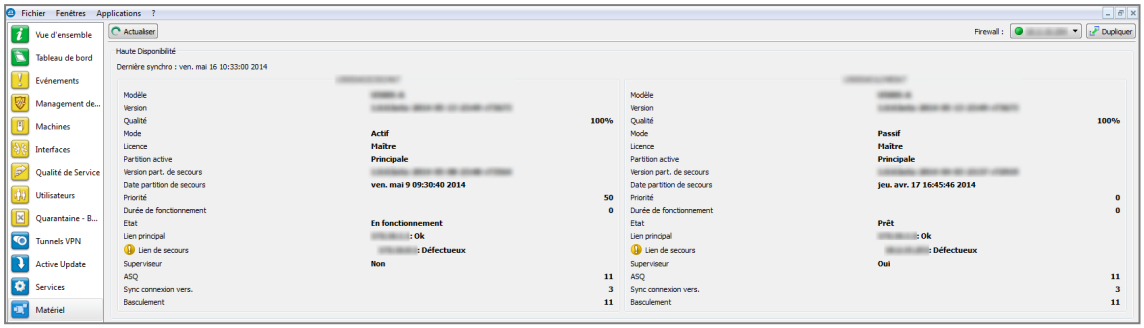


Figure 55 : Matériel

NOTE

La version 1 des Firewalls Stormshield Network vous permet de bénéficier d'un support de Haute Disponibilité de nouvelle génération, avec affichage de la date de la dernière synchronisation des boîtiers.

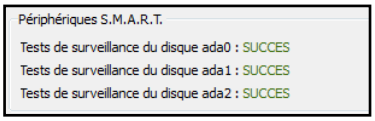
Vous pourrez également noter une évolution du support du RAID.

5.4.2 Alimentations

Si votre modèle de firewall supporte des modules d'alimentation redondants (modèles haut de gamme SN3000 et SN6000), l'état de ces alimentations est affiché.

5.4.3 Périphériques S.M.A.R.T.

Le résultat d'exécution des tests de surveillance est affiché pour chacun des périphériques S.M.A.R.T. détectés.



5.4.4 RAID

Les informations affichées, relatives à l'état des volumes RAID et des disques les composant, sont les suivantes :

Type de disque	Indication du type de volume RAID ou du type de disque composant un volume RAID. **Exemple** : Mirrored array (Raid1) pour un volume RAID.
Adresse du disque	Emplacement physique du disque participant à un volume RAID. **Exemple** : Tiroir supérieur.
Etat du disque	Etat du volume RAID ou d'un disque le composant. **Exemple** : Degraded, Optimal.

5.4.5 Disques de stockage des traces

Les informations affichées relatives au support de stockage sont les suivantes :

Type	Indication du type de support de stockage.
Identifiant	Identifiant du support de stockage attribué par l e firewall.
Etat	Indication de la reconnaissance ou non du support de stockage.
Espace disque	Dans le cas de support formaté, indication de la taille de la partition en Gigaoctet.
Formaté	Indication du formatage ou non du support de stockage.

En cas de problème avec l'un des disques, un message est affiché dans le tableau de bord.

6. POLITIQUE

6.1 POLITIQUE DE FILTRAGE

Le menu **Politique de Filtrage**, accessible depuis l'arborescence du Monitor récapitule la politique de filtrage active en regroupant les règles implicites, les règles de filtrage globales et les règles de filtrage locales.

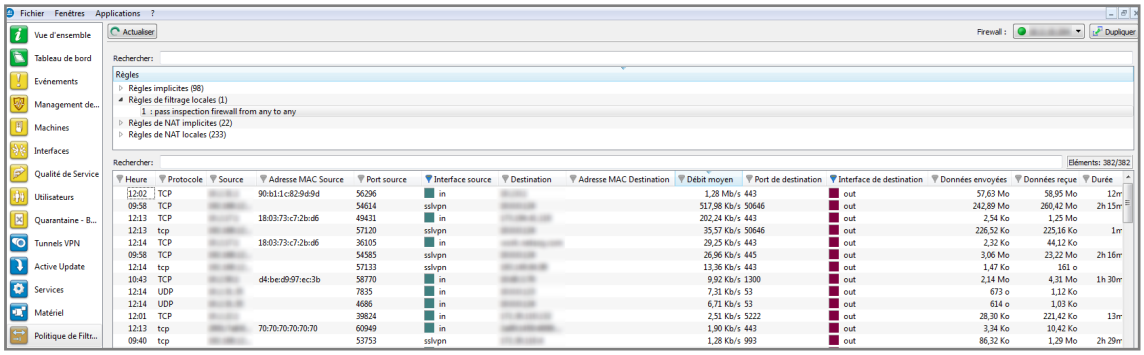


Figure 56 : Politique de Filtrage

Chaque ligne présentée s'affiche de la manière suivante :

- <Identifiant du type de règle> peut être "0" s'il s'agit de règles implicites, "1" s'il s'agit du filtrage global et 2 s'il s'agit du filtrage local.
- <Identifiant de la règle dans le slot> : dans le cas des règles implicites, cet identifiant est toujours "0".
- <Règle de filtrage> : règle de filtrage selon la grammaire Stormshield Network.
- <Règle de NAT> : règle de NAT selon la grammaire Stormshield Network.

6.1.1 Vue « Connexions »

La vue « Connexions » détaille pour chaque règle, l'ensemble des connexions autorisées par les politiques de filtrage implicites, locales et globales.

6.2 POLITIQUE VPN

DEFINITION VPN (VIRTUAL PRIVATE NETWORK)

Interconnexion de réseaux de manière transparente et sécurisée pour les applications et protocoles participants ; généralement utilisé pour relier des réseaux privés au travers d'Internet.

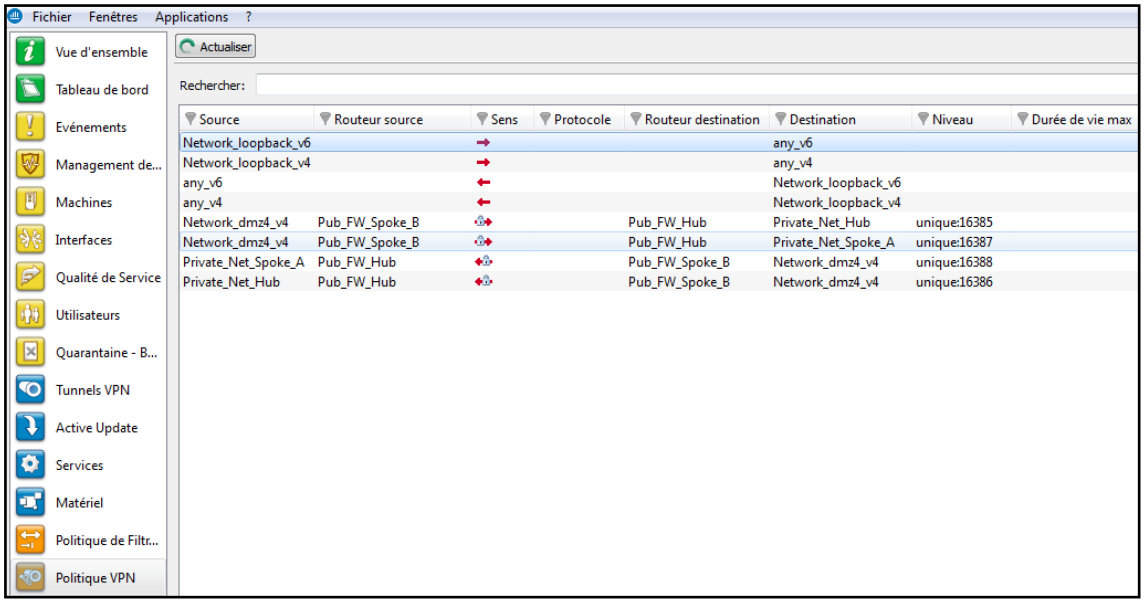


Figure 57 : Politique VPN

La section VPN permet la visualisation de la configuration des différentes politiques de tunnels VPN définies dans le slot VPN actif. Il n'est pas nécessaire que ces politiques VPN soient réellement utilisées pour qu'elles soient affichées. Il est juste nécessaire que le slot VPN soit activé.

Les données affichées sur cet écran sont les suivantes :

Source	Extrémité du trafic. Indication du réseau source.
Routeur source	Extrémité émettrice de la passerelle qui forme le tunnel VPN.
Sens	Indication du sens du trafic représenté par les icônes suivantes : 
Protocole	Indication du/des protocole(s) autorisé(s) à traverser le tunnel.
Routeur destination	Extrémité réceptrice de la passerelle qui forme le tunnel VPN.
Destination	Extrémité du trafic. Indication du réseau de destination.

	Niveau de sécurité associé au tunnel.
Niveau	**REMARQUE** Ce niveau est défini lors de la création du tunnel VPN en fonction de l'algorithme de chiffrement et d'authentification).
Durée de vie max	Durée de vie maximale de la politique VPN configurée.

Le bouton **Actions** permet de réaliser un certain nombre d'actions sur la ligne d'événement sélectionnée (pour plus d'informations, consultez le chapitre Menu contextuel sur les lignes):

- Voir les tunnels correspondants.

7. TRACES

7.1 ÉTAT D'UTILISATION

Un graphique représente en temps réel la taille actuelle du fichier de traces ("Alarmes", "Authentification", "Connexions", "Filtrage", « ftp », « Monitor", "Plugins", "POP3", "S", "Administration", "SMTP", "Système", "VPN IPSec", "Web", "VPN SSL") par rapport à la taille allouée sur le firewall pour chaque type de traces.

DEFINITION TRACES (OU LOGS).

Enregistrement chronologique de l'activité d'un ordinateur, qui constitue le journal des évènements qui se sont produit dans les programmes et les systèmes selon une période donnée.

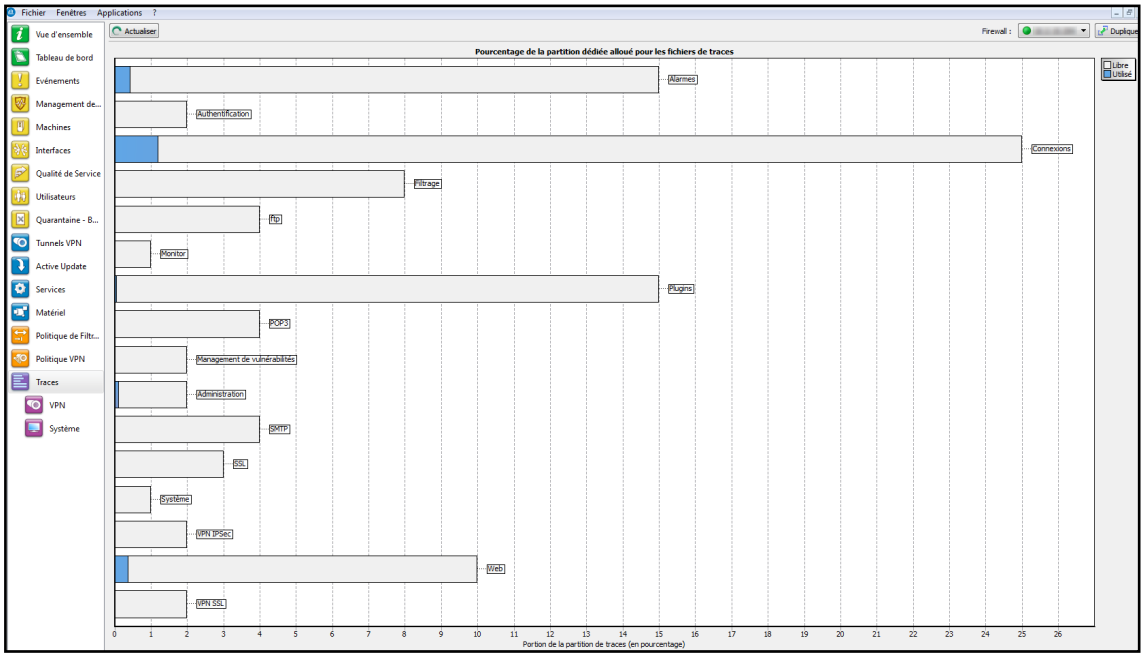


Figure 58: Traces

7.2 TYPES DE TRACES

7.2.1 VPN

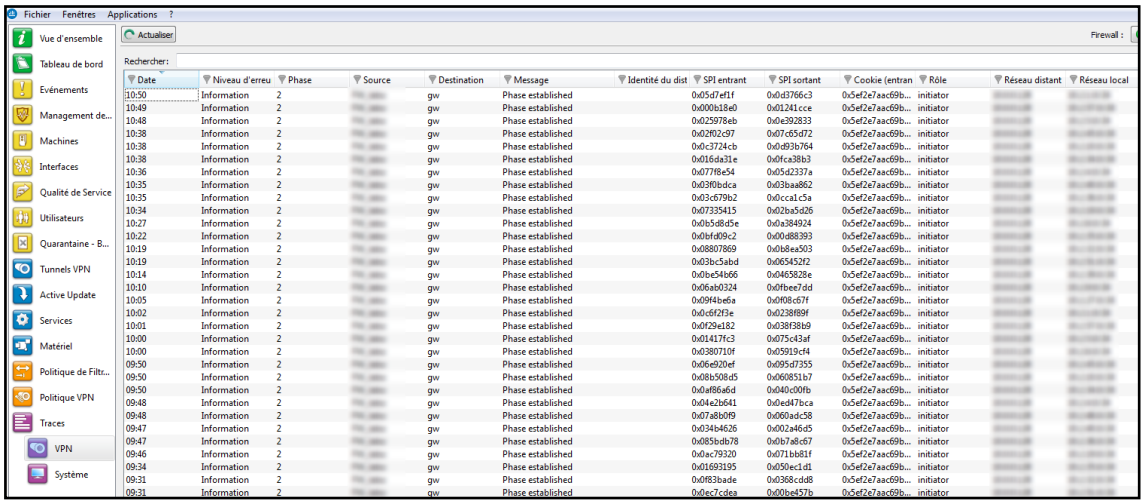


Figure 59 : VPN

En cliquant dans le menu VPN, vous affichez les données suivantes :

Date	Date et heure de génération de la ligne de traces (logs).
Niveau d'erreur	Message d'erreur.
Phase	Phase de négociation de la SA.
Source	Adresse source de la connexion (initiateur du tunnel).
Destination	Adresse IP ou nom de la destination.
Message	Message concernant la tentative de mise en place d'un tunnel.
Identité du distant	Identité du correspondant indiquée dans la configuration des clés pré-partagées dans le cas où le type d'identité spécifié n'est pas "Adresse IP".
SPI entrant	N° de SPI de la SA entrante négociée (en hexadécimal).
SPI sortant	N° de SPI de la SA sortante négociée.
Cookie (entrant/sortant)	Marqueur temporaire d'identité de l'initiateur et du destinataire de la négociation.
Rôle	Indique à quelle extrémité on se trouve.
Réseau distant	Adresse IP du réseau distant à l'extrémité du trafic.
Réseau local	Adresse IP du réseau local à l'extrémité du trafic.

NOTE

Les logs VPN sont également affichés pour les modèles sans disque dur.

7.2.2 Système

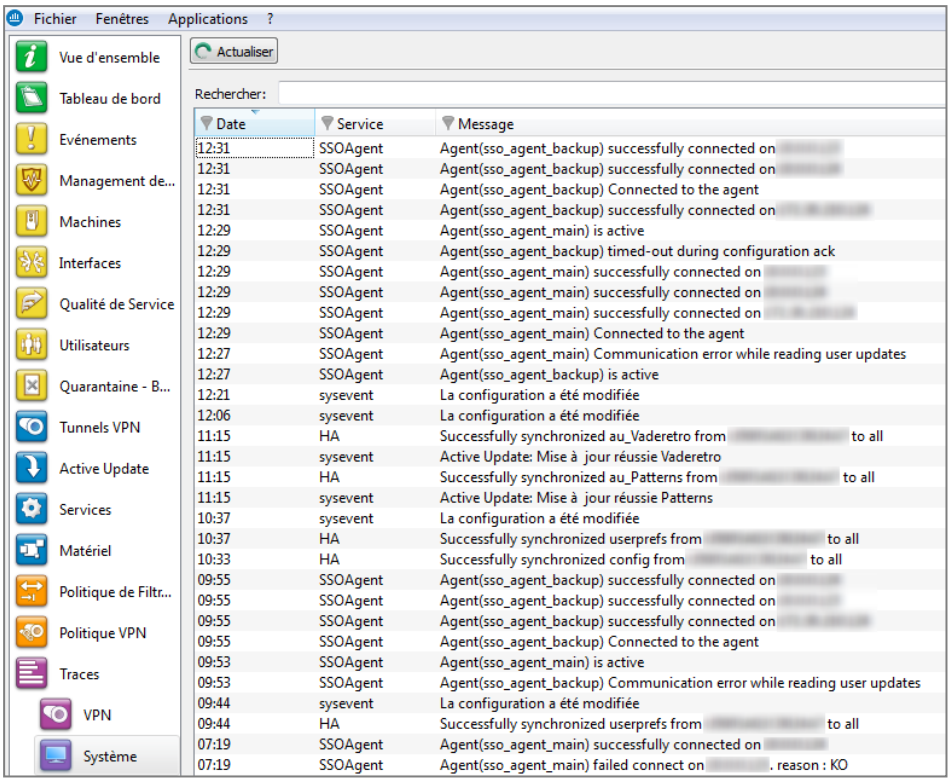


Figure 60 : Système

En cliquant dans le menu Système, vous affichez les données suivantes :

Date	Date et heure de génération de l'enregistrement.
Service	Indication du nom du service.
Message	Indication de l'action effectuée.

NOTE

Les logs SYSTEM sont également affichés pour les modèles sans disque dur.

8. ANNEXES

8.1 Annexe A : Foire aux questions

1) Que signifie le message : “Impossible de localiser la machine en x.x.x.x” ?

2) Comment vérifier la (les) adresse(s) IP réellement affectée(s) au firewall ?

3) Que signifie le message : "Vous avez perdu le privilège MODIFY" ?

4) Que signifie le message : "L'opération a dépassé le temps imparti" ?

5) Comment suis-je au courant d'une tentative d'intrusion ?

6) Est-il possible de laisser passer d'autres protocoles qu'IP ?

1) Que signifie le message “Impossible de localiser la machine en x.x.x.x” ?

Ce message signifie que la machine sur laquelle vous êtes connecté ne peut pas joindre le firewall avec l'adresse IP que vous avez précisée dans la fenêtre de connexion. Le problème peut être dû à plusieurs choses.

Vérifiez:

- Que l'adresse IP que vous avez spécifiée dans la fenêtre de connexion est bien celle du firewall (celle de l'interface interne en mode avancé).
- Que votre machine possède bien une adresse IP différente du firewall mais dans le même sous-réseau.
- Que les branchements sont corrects (utilisez un câble croisé uniquement si vous branchez le firewall directement à une machine ou un routeur). Saisissez "`arp -a`" dans une fenêtre DOS sous Windows pour voir si le PC connaît l'adresse physique (Ethernet) du firewall Stormshield Network. Si ce n'est pas le cas, vérifier vos câbles, les connexions physiques à votre hub.
- Que vous n'avez pas changé de mode de fonctionnement du firewall (transparent ou avancé).
- Que l'adresse IP est bien prise en compte au niveau du firewall (cf. Comment vérifier l'adresse IP affectée au firewall).
- Que le serveur d'accès à l'interface graphique n'a pas été désactivé sur le firewall.

2) Comment vérifier l'(les) adresse(s) IP réellement affectée(s) au firewall ?

Afin de vérifier la(les) adresse(s) IP affectée(s) au firewall ainsi que le mode de fonctionnement, il suffit de se connecter en mode console au firewall. Pour cela, vous pouvez soit faire un SSH sur le firewall (si le SSH est activé et autorisé), soit vous connecter directement sur le boîtier par le port série ou en branchant un écran et un clavier sur le boîtier.

Une fois connecté en mode console (avec le login admin), saisissez la commande "`if info`". Le résultat vous donne la configuration des cartes réseau et le mode de fonctionnement actuel.

3) Que signifie le message "Vous avez perdu le privilège MODIFY" ?

Il ne peut y avoir qu'un seul utilisateur ayant les droits de modification connecté au firewall. Ce message signifie qu'une session est ouverte par un utilisateur ayant le droit de modification.

Pour forcer la fermeture de cette session, il suffit de se connecter en ajoutant un point d'exclamation devant le nom d'utilisateur (!admin).

AVERTISSEMENT

Si une session avec le droit MODIFY est ouverte sur une autre machine, elle sera fermée.

4) Que signifie le message "L'opération a dépassé le temps imparti" ?

Par mesure de sécurité, toute connexion, aboutie ou non, entre le firewall et l'interface graphique est stoppée au bout d'un certain temps. Cela évite notamment d'attendre indéfiniment la connexion dans le cas où le firewall n'est pas joignable sur le réseau.

5) Comment suis-je au courant d'une tentative d'intrusion ?

Chaque tentative d'intrusion peut être configurée pour déclencher une alarme majeure ou mineure suivant son importance. Vous êtes informés de ces alarmes par quatre moyens différents :

- Premièrement, les leds sur la face avant du boîtier s'allument (rouge) ou clignotent (jaune) pour vous signaler l'alarme.
- Ensuite, les alarmes sont tracées dans un fichier spécifique consultable à partir de l'interface graphique (**Stormshield Network Real-Time Monitor** ou **Stormshield Network Event Reporter**).
- Vous pouvez recevoir un rapport d'alarmes à une fréquence régulière (cf. *réception des alarmes*) via l'application **Stormshield Network Global Administration**. Celui-ci peut-être configuré pour que la levée d'une alarme entraîne l'envoi d'un mail. Lorsque plusieurs alarmes sont levées dans un laps de temps très courts, elles sont regroupées au sein d'un mail commun.
- Enfin, **Stormshield Network Real-Time Monitor** affiche à l'écran, en temps réel, les alarmes reçues.

6) Est-il possible de laisser passer d'autres protocoles qu'IP ?

Le firewall ne peut analyser (cohérence avec l'alarme "protocole IP non-analysé") que les protocoles s'appuyant sur IP (modèle OSI=architecture en couches). Tout protocole qui n'est pas analysé par le firewall est considéré comme suspect et se retrouve bloqué.

Cependant, avec le mode de fonctionnement transparent, il est possible de laisser passer d'autres protocoles bien qu'ils ne soient pas analysés. Ces protocoles sont "IPX" de Novell, "IPv6", "PP Poe", "Appletalk" et "NetBIOS".

8.2 Annexe B : Droits de la session et droits des utilisateurs

Intitulé	Description	Droit attribués
Traces (L)	Consultation des traces	base, log_read
Filtrage (L)	Consultation de la politique de filtrage	base, filter_read
VPN (L)	Consultation de la configuration VPN	base, vpn_read

Traces (E)	Droit de modification de la configuration des traces	modify, base, log
Filtrage (E)	Droit de modification de la politique de filtrage	modify, base, filter
VPN (E)	Droit de modification de la configuration VPN	modify, base, vpn
Monitoring	Droit de modification de la configuration à partir de Stormshield Network Real-Time Monitor	modify, base, mon_write
Filtrage de contenu	Droits pour les politiques de filtrage URL, Mail, SSL et la gestion des antivirus	modify, base, contentfilter
PKI	Droit de modification de la PKI	modify, base, pki
Objets	Droit de modification de la base objet	modify, base, object
Utilisateurs	Droit de modification des utilisateurs	modify, base, user
Réseau	Droit de modification de la configuration réseau (interfaces, bridges, modems, VLANs et configuration du DNS dynamique)	modify, base, network
Routage	Droits de modification du routage (route par défaut, routes statiques and réseaux de confiance)	modify, base, route
Maintenance	Droits d'effectuer des opérations de maintenance (sauvegardes, restaurations, mises à jour, arrêt et redémarrage du firewall, mise à jour de l'antivirus, modification de la fréquence de mise à jour de l'antivirus, configuration de la haute disponibilité et actions relatives au RAID dans Stormshield Network Real-Time Monitor).	modify, base, maintenance
Prévention d'intrusion	Droits de modifier la configuration de la prévention d'intrusion (IPS)	modify, base, asq
Management de vulnérabilités	Droit de modifier la configuration de management de vulnérabilités (Stormshield Network Vulnerability Manager)	modify, base, pvm
Objets (global)	Droits d'accès aux objets globaux	modify, base, globalobject
Filtrage (global)	Droits d'accès à la politique de filtrage globale	modify, base, globalfilter

Le droit *base* est systématiquement attribué à tous les utilisateurs. Ce droit permet la lecture de toute la configuration hormis le filtrage, le VPN, les traces et le filtrage de contenu. Le droit *modify* est affecté à tout utilisateur ayant un droit d'écriture. L'utilisateur connecté en tant que admin obtient le droit *admin*. Seul ce droit permet d'ajouter ou de retirer des droits d'administration aux autres utilisateurs.

8.3 Annexe C : Etats de la SA

-	Etat non déterminé.
Larval	La SA est en cours de négociation ou n'a pas été complètement négociée.
Mature	La SA est établie et disponible, le tunnel VPN est correctement monté.
Dying	La SA va bientôt expirer, une nouvelle SA est en cours de négociation.
Dead	La SA est expirée et inutilisable, le tunnel n'a pas été remonté et n'est donc plus actif.
Orphan	Un problème a été rencontré, généralement cet état signifie que le tunnel n'est monté que dans un seul sens.

STORMSHIELD

documentation@stormshield.eu