

**PROCEDURE
D'INSTALLATION
: FILTRAGE
STORMSHIELD**



**PROJET
CUB**

- **Objectif :** Assurer la sécurité du réseau via le filtrage du trafic, le chiffrement des communications (VPN), la gestion sécurisée, la surveillance des événements et la sauvegarde des configurations, afin de garantir la confidentialité, l'intégrité et la disponibilité des systèmes.

- **Prérequis**

- **Système d'exploitation**

- OS Stormshield

- **Ressources matérielles (minimum recommandé)**

- **CPU** : 1 cœurs
 - **RAM** : 1 Go
 - **Disque** : 32 Go (SSD recommandé)
 - **Connexion réseau** : 1 Gbit/s

Menu filtrage

MENUS « FILTRAGE »

- Affichage des règles globales

Application settings

- ☐ Always display advanced properties
- ☐ Display button to save commands
- ☐ Display users at startup of module
- ☒ Display network objects at startup of module
- ☒ Display global policies (Network objects, Certificates, Filter NAT and IPsec VPN)
- ☒ Apply a default comment to rules (filtering, NAT and IPsec)

Number of rules per page (filtering, NAT and IPsec): Automatic

Local policy
Global policy

SECURITY POLICY / FILTER - NAT

Global policy (1) Global Filter 01

FILTERING NAT

Searching...

+ New rule X Delete

Cut Copy Paste Search in logs Search in monitoring

	Status	Name	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	global_block_icmp	block	Internet interface: out	Firewall_Lout	Any	icmp	IPS

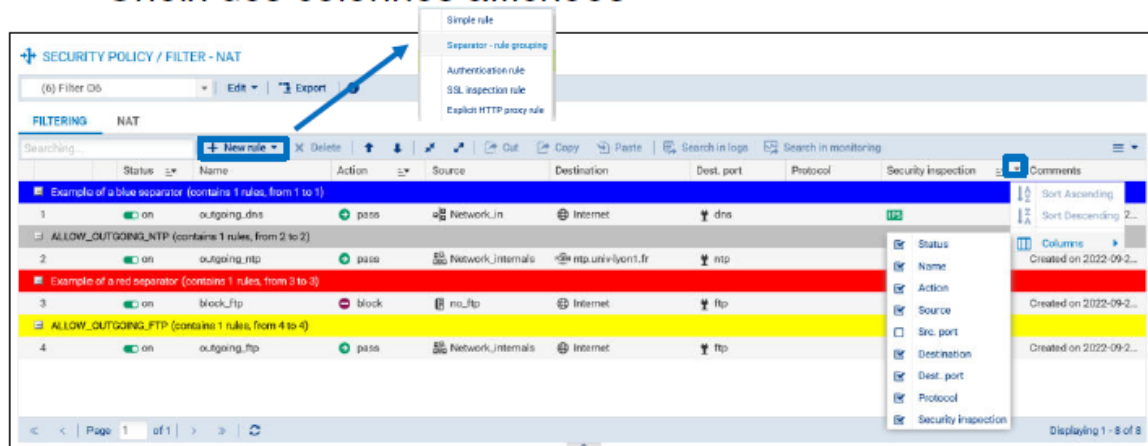
STORMSHIELD

10

Pour afficher les règles globales, il faut cocher l'option **Afficher les politiques globales (Filtrage, NAT, VPN IPsec et Objets)** dans le menu **Préférences** accessible directement depuis l'icône de l'en-tête encadré en rouge. Cette option fait apparaître dans l'en-tête du menu **CONFIGURATION ⇒ POLITIQUE DE SÉCURITÉ ⇒ Filtrage et NAT** une liste déroulante qui permet de sélectionner les politiques globales ou locales. Par défaut, aucune règle de filtrage et NAT n'est présente dans les slots globaux.

MENUS « FILTRAGE »

- Création d'une règle
- Ajout, édition et colorisation de séparateurs
- Choix des colonnes affichées



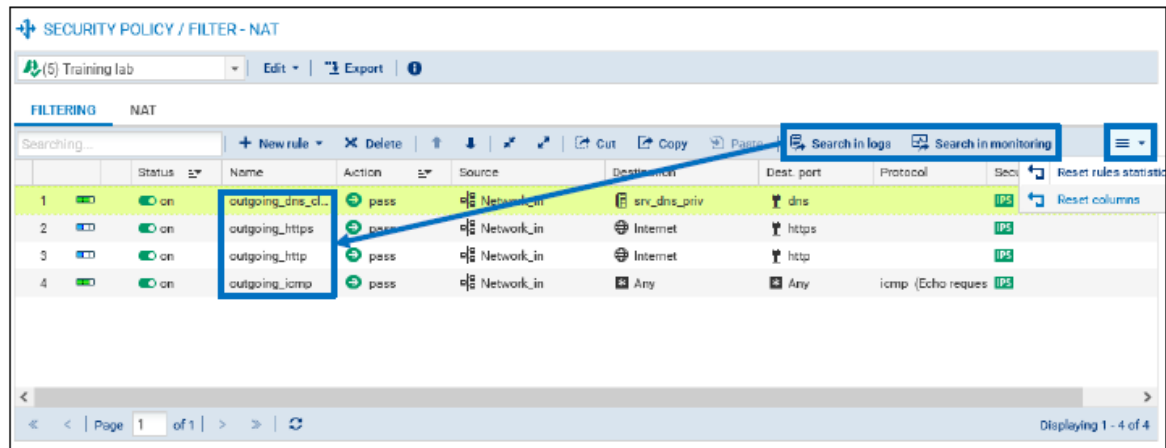
L'onglet FILTRAGE est composé d'un en-tête pour la gestion des règles de filtrage :

- **Nouvelle règle :**
 - **Règle simple** : Ajouter une règle de filtrage standard.
 - **Séparateur – regroupement de règles** : Ajouter un séparateur qui regroupe toutes les règles se trouvant au-dessous (ou jusqu'au prochain séparateur). Cela permet de faciliter l'affichage d'une politique contenant un nombre de règles important.
 - **Règle d'authentification** : Démarrer un assistant facilitant l'ajout d'une règle dont le rôle est de rediriger les connexions des utilisateurs non-authentifiés vers le portail captif
 - **Règle d'inspection SSL** : Démarrer un assistant qui facilite l'ajout de règles pour l'activation du proxy SSL.
 - **Règle de proxy HTTP explicite** : Démarrer un assistant qui facilite l'ajout de règles pour l'activation du proxy HTTP explicite.
 - **Supprimer** : Supprimer une règle.

- **Monter / Descendre** : Monter ou descendre la/les règle(s) sélectionnée(s) d'une position dans la liste.

MENUS « FILTRAGE »

- Nommage des règles
- Options d'en-tête



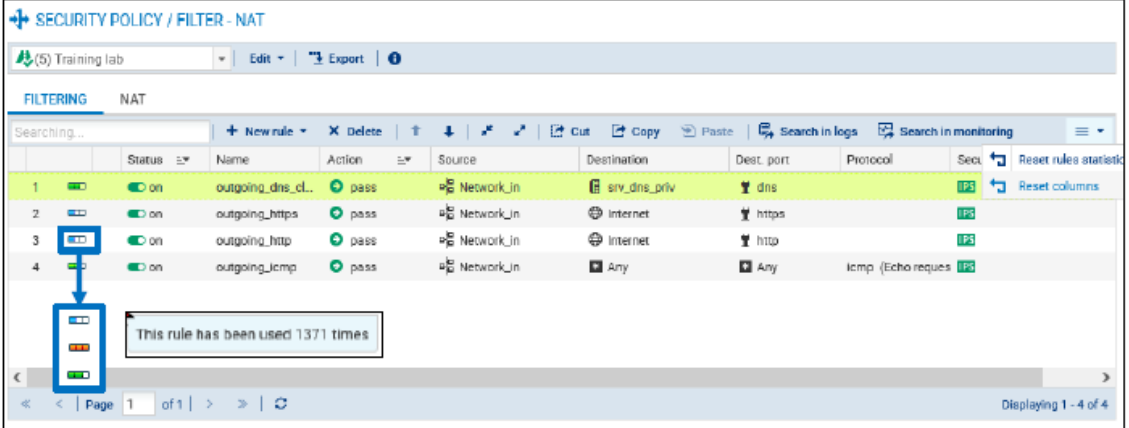
12

- **Tout dérouler / Tout fermer** : Dérouler/Fermer tous les séparateurs pour afficher/cacher les règles de filtrage.
- **Couper** : Couper la/les règle(s) sélectionnée(s).
- **Copier** : Copier la/les règle(s) sélectionnée(s).
- **Coller** : Coller la/les règle(s) auparavant copiée(s)/coupée(s) de la même ou d'une autre politique.
- **Chercher dans les logs** : Chercher les traces générées par l'application de cette règle dans les journaux d'audit (la recherche s'effectue sur le nom de la règle).
- **Chercher dans la supervision** : Chercher le nom de cette règle dans la supervision des connexions.
- **Réinitialiser les statistiques des règles** : Réinitialiser les compteurs d'utilisation de toutes les règles de filtrage et NAT de la politique active. La date de la dernière réinitialisation s'affiche en positionnant la souris sur l'icône.

- **Reinit Colonnes** : Réinitialiser l'affichage des colonnes qui composent la fenêtre des règles comme le prévoit l'affichage par défaut.

MENUS « FILTRAGE »

- Indicateur d'utilisation des règles de filtrage
- Composition d'une règle de filtrage



The screenshot shows the 'SECURITY POLICY / FILTER - NAT' window. Under the 'FILTERING' tab, there is a table with columns: Status, Name, Action, Source, Destination, Dest. port, Protocol, and Sect. Four rules are listed, all with a status of 'on'. A blue box highlights the usage indicator (a small bar chart) in the first column of the table. A tooltip appears over this indicator, stating 'This rule has been used 1371 times'.

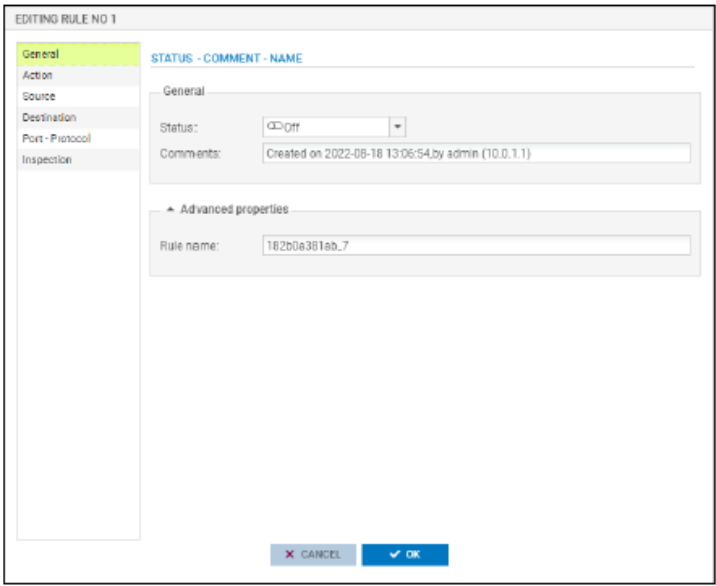
La fenêtre des règles est composée de plusieurs colonnes listées ci-dessous :

- Numéro de la règle et un indicateur (encadré en bleu) sur le nombre de fois où les éléments du paquet reçu correspondent aux critères de la règle de filtrage. Le compteur numérique s'affiche en passant la souris par dessus. Il peut afficher 4 couleurs qui sont le résultat d'un rapport mathématique entre le nombre de hits de la règle et le nombre de hits maximum atteint par une règle dans le même slot:
 - Blanc (vide) : la règle n'a jamais été appliquée,
 - Bleue : la valeur affichée est comprise entre 0 et 2% du hit maximal,
 - Vert : la valeur affichée est comprise entre 2% et 20% du hit maximal,

- Orange : la valeur affichée est supérieure ou égale à 20% du hit maximal et est supérieure à 10 000 hits.
- **État** : Permet d'activer/désactiver une règle de filtrage.
- **Action** : Indique l'action appliquée sur la connexion : passer, bloquer, tracer, renvoyer vers un portail captif, etc.
- **Source** : Spécifie la source du trafic : adresse IP ou réseau source, interface d'entrée, utilisateur, etc.
- **Destination** : Spécifie la destination du trafic : adresse IP ou réseau destination, interface de sortie.
- **Port de dest** : Indique le port destination du trafic.

MENUS « FILTRAGE »

- OmniBox pour éditer tous les champs de la règle à la fois



STORMSHIELD

14

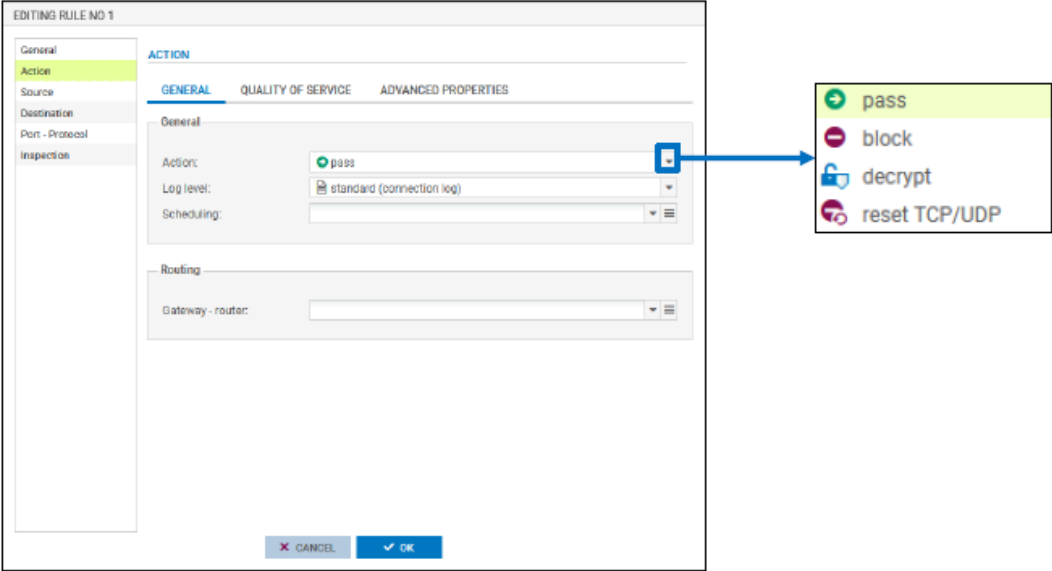
Les paramètres d'une règle peuvent être renseignés directement dans la fenêtre des règles ou sur une nouvelle fenêtre (omnibox) qui s'affiche en double cliquant sur n'importe quel paramètre de cette règle.

Les valeurs des paramètres étant des objets, ils peuvent être copiés d'une règle à une autre par un simple glisser/déposer. Ce procédé permet également de déplacer les règles de filtrage en cliquant à gauche sur le numéro de la règle. Enfin, les nouvelles règles ajoutées doivent

être sauvegardées et activées explicitement avec le bouton **Sauvegarder et activer**.

MENUS « FILTRAGE »

- Menu Action : définition de l'action



STORMSHIELD

15

Le menu **ACTION** est constitué de plusieurs onglets, nous nous intéresserons principalement à l'onglet **GÉNÉRAL** qui permet de spécifier les paramètres suivants :

- **Action** : Définit l'action à appliquer au paquet correspondant à la règle de filtrage :
 - **passer** : Autorise le paquet,
 - **bloquer** : Bloque le paquet,
 - **déchiffrer** : Renvoie le paquet vers le proxy SSL,
 - **réinit. TCP/UDP** : Dans le cas d'un trafic TCP, le firewall renvoie un paquet « TCP RST » à l'émetteur. Dans le cas d'un trafic UDP, le firewall renvoie une notification ICMP port inaccessible (port unreachable) à l'émetteur.

MENUS « FILTRAGE »

- Menu Action : définition du niveau de trace

EDITING RULE NO 1

General
Action
Source
Destination
Port - Protocol
Inspection

ACTION

GENERAL QUALITY OF SERVICE ADVANCED PROPERTIES

General

Action:

Log level:

Scheduling:

Routing

Gateway - router:

standard (connection log)
advanced (connection log and filtering log)
minor alarm
major alarm

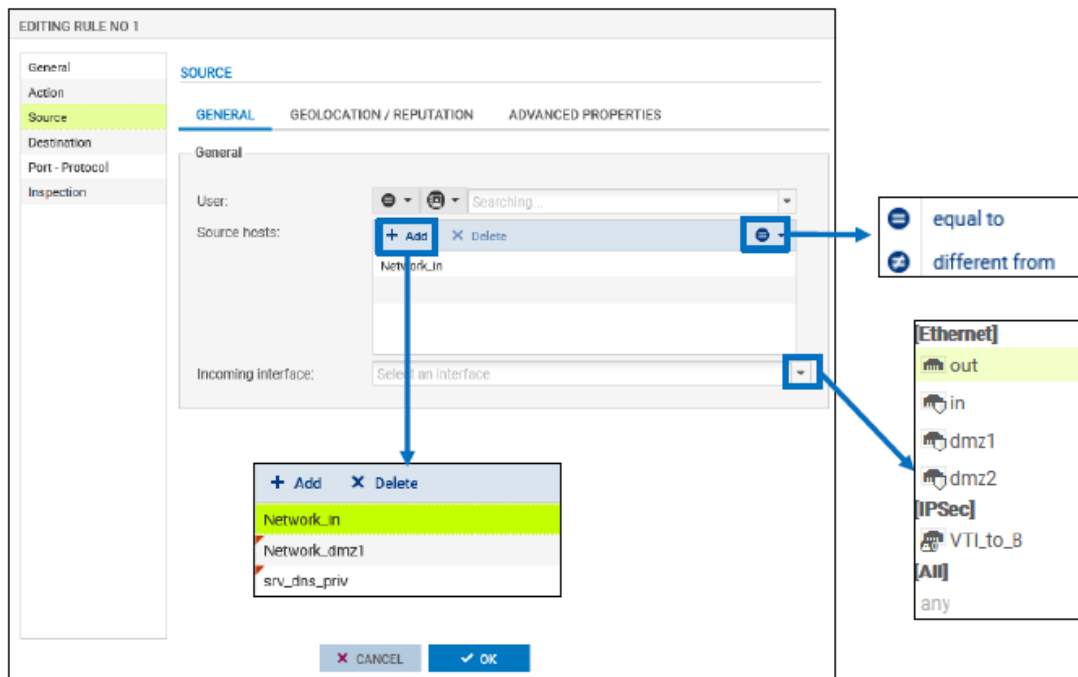
16

Niveau de trace : Permet de tracer les flux traités par la règle. Il peut avoir plusieurs valeurs :

- **Standard (journal de connexions)** : C'est la valeur par défaut, seules les connexions établies ayant leur couche de transport en TCP/UDP sont journalisées.
- **Avancé (journal de filtrage)** : Les flux sont tracés dans le journal « Filtrage ».
- **Alarme mineure** : La connexion est tracée dans le journal « Alarmes » avec une alarme mineure.
- **Alarme majeure** : La connexion est tracée dans le journal « Alarmes » avec une alarme majeure.

MENUS « FILTRAGE »

- Menu Source : onglet général



18

Le menu **Source** ⇒ **GÉNÉRAL** regroupe les paramètres qui identifient la source du trafic concerné par la règle de filtrage :

- Utilisateur** : Permet de renseigner l'utilisateur ou le groupe d'utilisateurs qui est à l'origine du trafic.
- Machines sources** : Indique l'adresse IP, le Fully Qualified Domain Name (FQDN) ou l'adresse réseau du trafic.
- Interface d'entrée** : Permet de préciser l'interface d'entrée du trafic.

MENUS « FILTRAGE »

- Menu Source : onglet géolocalisation et réputation

EDITING RULE NO 1

General
Action
Source
Destination
Port - Protocol
Inspection

SOURCE

GENERAL GEOLOCATION / REPUTATION ADVANCED PROPERTIES

Geolocation

Select a region:

Public IP addresses reputation

Select a reputation category:

Host reputation

☐ Enable filtering based on reputation score

Reputation score: [min] [max]

CANCEL OK

Continents

- Africa
- Antarctica
- Asia
- Europe
- North America
- Oceania
- South America

Country

- Afghanistan
- Albania
- Algeria
- American Samoa
- Andorra

Categories

- Exchange Online
- Office 365 common
- SharePoint Online
- Skype for Business
- anonymizer
- botnet
- malware
- phishing
- scanner
- spam
- tor exit node

Groups

- hard

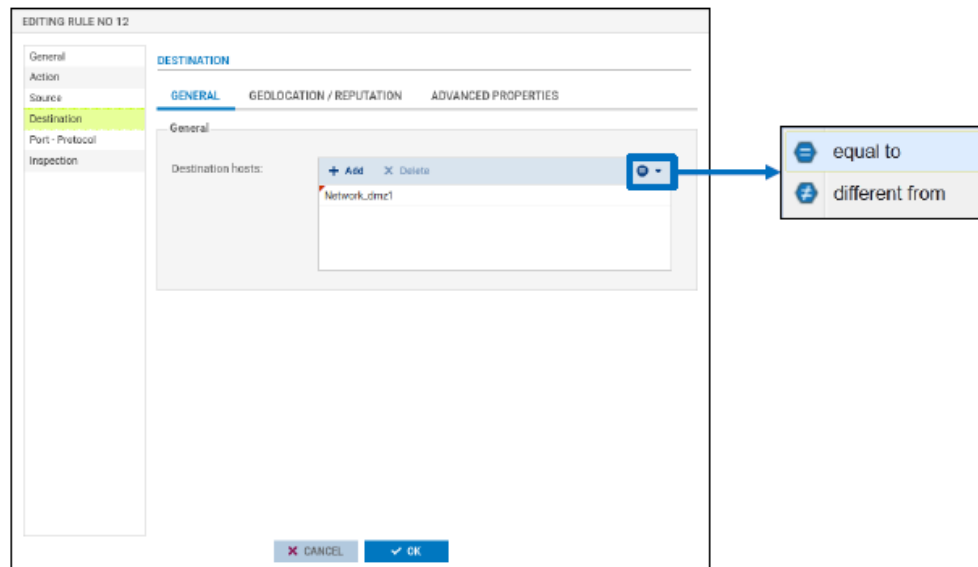
19

Le menu **Source** ⇒ **GÉOLOCALISATION / RÉPUTATION** regroupe les paramètres suivants :

- Géolocalisation** : Permet de renseigner un continent ou un pays à l'origine du trafic.
- Réputation des adresses IP publiques** : Une IP publique peut avoir une réputation à la limite de deux catégories.
- Réputation des machines** : Il est possible d'activer le filtrage selon le score de réputation des machines du réseau interne.

MENUS « FILTRAGE »

- Menu Destination : onglet général



20

Le menu **Destination** regroupe les paramètres qui identifient la destination du trafic. Dans l'onglet **GÉNÉRAL**, le paramètre **Machines destination** indique l'adresse IP, l'adresse réseau ou le FQDN destination du trafic. Nous pouvons également choisir si le paramètre doit être égal ou différent de la valeur et renseigner une liste d'objets.

MENUS « FILTRAGE »

- Menu Destination : configuration avancée

The screenshot shows the 'EDITING RULE NO 1' window. On the left is a sidebar with tabs: General, Action, Source, Destination (highlighted), Port - Protocol, and Inspection. The main area has three sub-tabs: GENERAL, GEOLOCATION / REPUTATION, and ADVANCED PROPERTIES (highlighted). Under 'Advanced properties', there is a section 'Outgoing interface' with a dropdown menu labeled 'Select an interface'. A blue arrow points from this dropdown to a list of interface options. Below this is a 'NAT on the destination' section with a 'Destination' dropdown and a checkbox for 'ARP publication on external destination (public)'. At the bottom are 'CANCEL' and 'OK' buttons.

Outgoing interface options:

- [Ethernet] out
- in
- dmz1
- dmz2
- [Bridge] bridge
- [IPSec] VTI_to_B
- [All] any

21

Dans l'onglet **CONFIGURATION AVANCÉE**, nous pouvons restreindre l'application de la règle uniquement au trafic sortant par l'interface indiquée dans **interface de sortie**.

MENUS « FILTRAGE »

- Menu Port – Protocole : définition d'un port

EDITING RULE NO 1

General
Action
Source
Destination
Port - Protocol
Inspection

PORT AND PROTOCOL

Port

Destination port: + Add X Delete

https

Protocol

Protocol type: Automatic protocol detection (default)

Application protocol: Based on default port or content

IP protocol: All

X CANCEL ✓ OK

Legend:

- equal to
- different from
- lower than
- higher than

Le menu **PORT / PROTOCOLE** permet de renseigner le **Port destination** avec la possibilité de choisir s'il doit être égal, différent, inférieur ou supérieur à la valeur sélectionnée. Il est également possible de renseigner une liste de ports de destination.

MENUS « FILTRAGE »

- Menu Port – Protocole : définition d'un protocole

EDITING RULE NO 1

General
Action
Source
Destination
Port - Protocol
Inspection

PORT AND PROTOCOL

Port

Destination port: + Add X Delete

Any

Protocol

Protocol type: IP protocol

Application protocol: No applicative analysis

IP protocol: icmp

ICMP message: Echo request (Ping)

☐ Stateful tracking

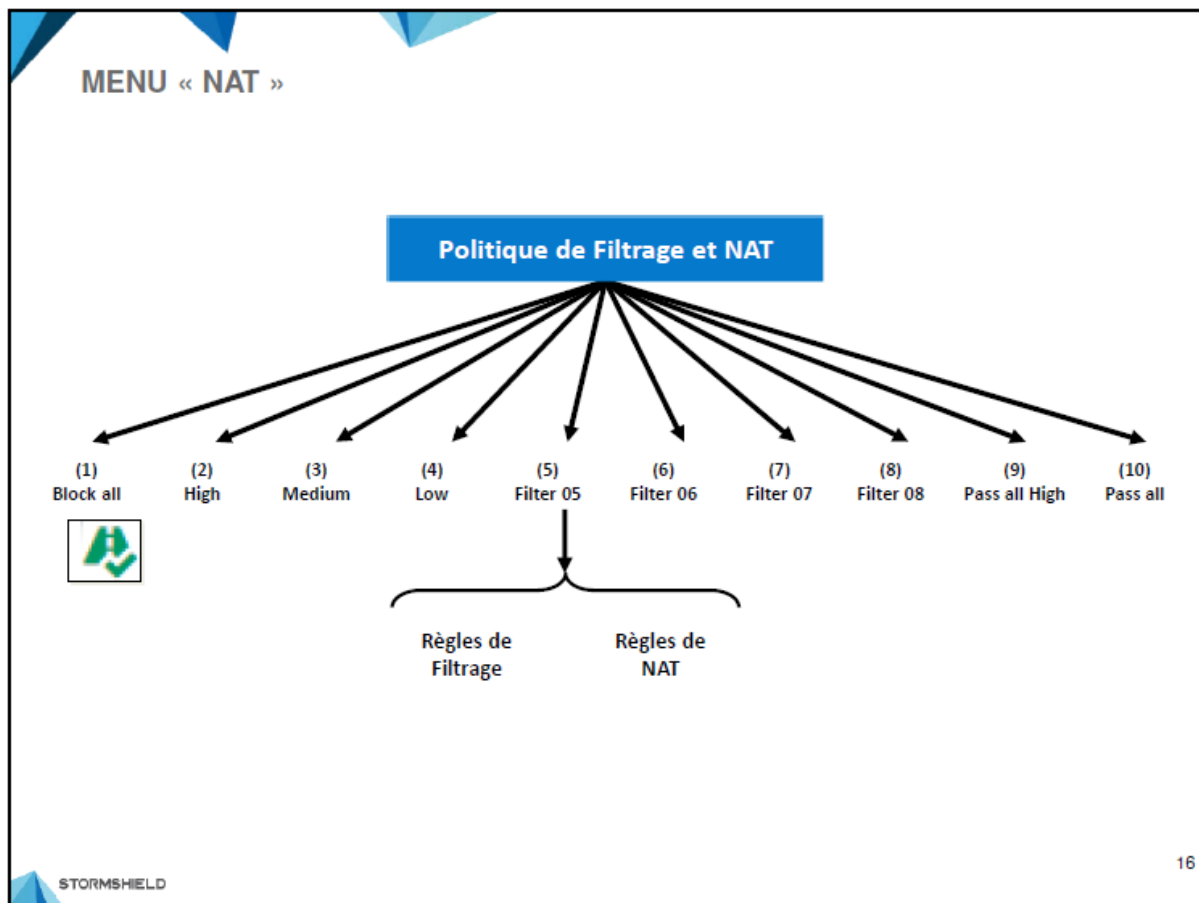
X CANCEL ✓ OK

- icmpv6
- vpn-ah
- vpn-esp
- gre
- sctp
- udp
- tcp
- icmp
- icmp
- ggp
- ipencap
- egp
- ldp
- hmp
- rdp
- ipv6encap
- rsrp
- swipe
- mobile
- ipv6-nmxt
- eigrp
- ospf
- ipip

23

Le menu **PORT / PROTOCOLE** permet également de spécifier le protocole IP concerné par la règle de filtrage. Pour cela, il faut sélectionner le paramètre **Type de protocole** et choisir la valeur **Protocole IP**, puis préciser le protocole dans le champ **Protocole IP**. Si le protocole ICMP est sélectionné, le paramètre **Message ICMP** s'affiche automatiquement pour permettre d'affiner le filtrage en choisissant le type de notification ICMP concerné par la règle de filtrage.

Menu NAT



Dans les firewalls Stormshield Network, les règles de filtrage et NAT (translation d'adresses) sont regroupées sous une même politique. Il est possible de définir 10 politiques différentes mais une seule politique est active à la fois, identifiée par l'icône.

MENU « NAT »

- Édition de la politique de sécurité

SECURITY POLICY / FILTER - NAT

(4) Filter 04

Filtering NAT

Last modification: 12:15:13 PM
Comments: The profile has no comments

(1) Block all
(2) High
(3) Medium
(4) Filter 04
(5) LAB_5_Filter_NAT
(6) LAB_6_Content_Filtering
(7) LAB_7_Authentication
(8) LAB_8_IPSec_Filter
(9) LAB_9_VPN_SSL
(10) Pass all

Rename
Reinitialize
Copy to

(1) Block all
(2) High
(3) Medium
(4) Low
(5) Training lab(active policy)
(6) Filter 06
(7) Filter 07
(8) Filter 08
(9) Pass all High
(10) Pass all

STORMSHIELD

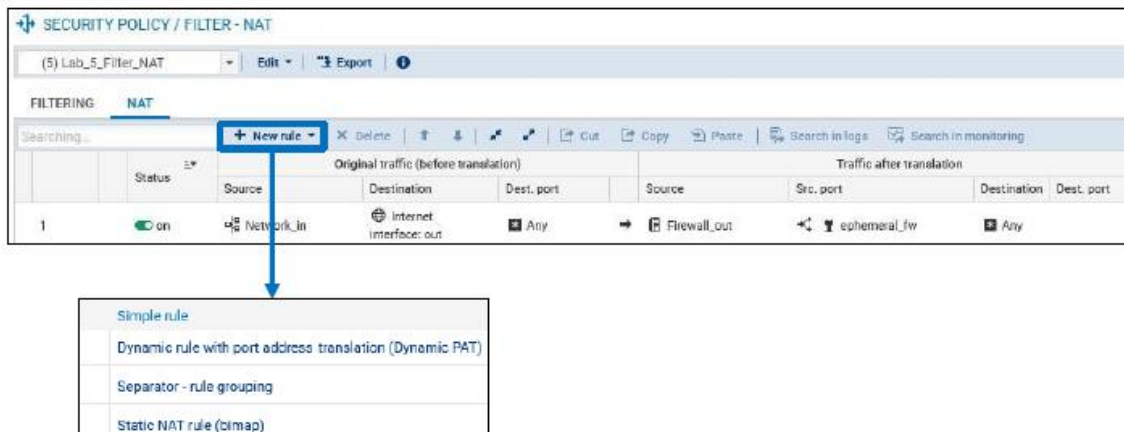
17

La configuration des règles de filtrage et NAT s'effectue dans le menu **CONFIGURATION ⇒ POLITIQUE DE SÉCURITÉ ⇒ Filtrage** et NAT. L'entête du menu permet :

- La sélection de la politique de filtrage et NAT grâce à une liste déroulante.
- Éditer** :
 - Renommer** : Modifier le nom de la politique.
 - Réinitialiser** : Remettre les règles de filtrage et NAT par défaut.
 - Copier vers** : Copier une politique vers une autre.
 - Exporter** : Permet d'exporter les règles de filtrage/NAT de la politique sélectionnée dans un fichier CSV,
 - Filtrage** : Pour la configuration des règles de filtrage.
 - NAT** : Pour la configuration des règles de translation d'adresses.

MENU « NAT »

- Création d'une règle et entête



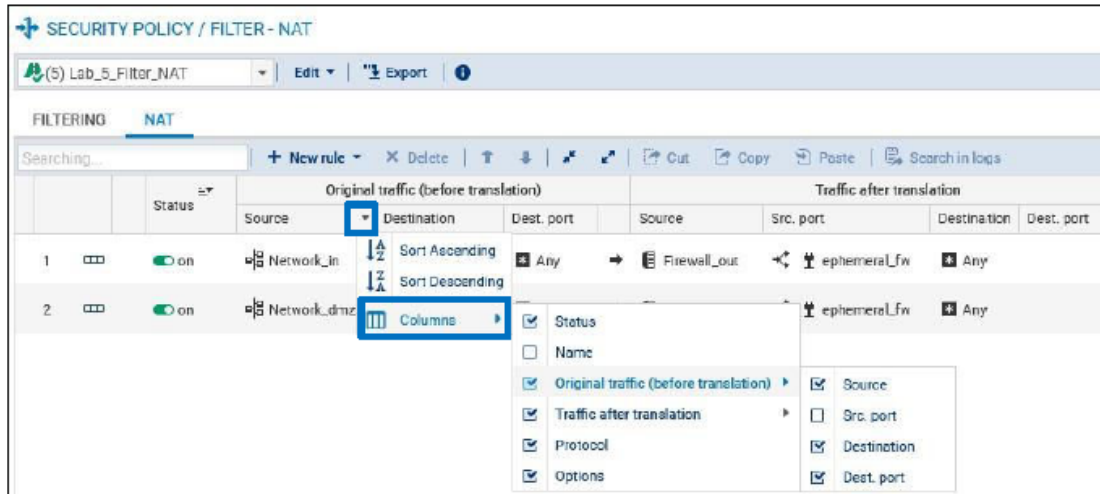
L'onglet **NAT** est composé d'un entête pour la gestion des règles de translation :

- **Nouvelle règle :**
 - **Règle standard :** Ajouter une règle de translation standard.
 - **Règle de partage d'adresse source (masquering) :** Ajouter une règle pour la translation dynamique en précisant la plage de port **ephemeral_fw**.
 - **Séparateur – regroupement de règles :** Ajouter un séparateur qui regroupe toutes les règles se trouvant au-dessous, ce qui permet de fermer le séparateur pour masquer l'affichage de toutes les règles lui appartenant.
 - **Règle de NAT statique (bimap) :** Lancer un assistant qui facilite l'ajout de règles de translation statique bimap.
 - **Supprimer :** Supprimer la/les règle(s) sélectionnée(s).
 - **Monter / Descendre :** Monter ou descendre la/les règle(s) sélectionnée(s) d'une position dans la liste.
 - **Tout dérouler / Tout fermer :** Dérouler/fermer tous les séparateurs pour afficher/cacher les règles de NAT.

- **Couper** : Couper la/les règle(s) sélectionnée(s).
- **Copier** : Copier la/les règle(s) sélectionnée(s).
- **Coller** : Coller la/les règle(s) auparavant copiée(s)/coupée(s) de la même ou d'une autre politique.
- **Chercher dans les logs** : Chercher le nom de cette règle dans les journaux d'audit.
- **Chercher dans la supervision** : Chercher le nom de cette règle dans la supervision des connexions.
- **Réinitialiser les statistiques des règles** : Réinitialiser les compteurs de toutes les règles filtrage et NAT de la politique. En positionnant la souris sur l'icône, la date de la dernière réinitialisation s'affiche.
- **Réinitialiser Colonnes** : Réinitialiser l'affichage des colonnes qui compose la fenêtre des règles.
- **Trafic avant translation** : Permet de renseigner les valeurs des paramètres du trafic original.
 - **Source** : L'adresse IP ou le réseau source.
 - **Destination** : L'adresse IP ou le réseau destination.
 - **Port dest** : Port destination.
- **Trafic après translation** : Permet de renseigner les nouvelles valeurs des paramètres après translation. Dans le cas où cette partie n'est pas renseignée, le trafic gardera les valeurs originales.
 - **Source** : L'adresse IP ou le réseau source.
 - **Port src** : Port source.
 - **Destination** : L'adresse IP ou le réseau destination.
 - **Port dest** : Port destination.
- **Options** : Le passage d'un flux par une règle de translation n'est pas journalisé en mode standard. En mode « Tracer », le trafic est journalisé dans le journal « Filtrage ».
- **Commentaire** : Permet d'ajouter un commentaire. La date, l'heure, l'administrateur et l'adresse IP du PC d'administration sont ajoutés par défaut lors de la création de la règle.

MENU « NAT »

- Affichage des colonnes



L'affichage des colonnes de la fenêtre peut être personnalisé en cliquant sur l'icône indiquée par la flèche bleue ci-dessus, ensuite sur colonnes. Il suffit de sélectionner une colonne pour qu'elle s'affiche. Les règles de NAT peuvent être déplacées dans la fenêtre par un glisser/déposer en cliquant à gauche sur le numéro de la règle.

MENU « NAT »

- Paramètres d'une règle

SECURITY POLICY / FILTER - NAT

(S) Lab_5_Filter_NAT | Edit | Export

FILTERING NAT

Searching...

+ New rule | Delete | Cut | Copy | Paste | Search in logs

	Status	Original traffic (before translation)			Traffic after translation			
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
1	on	Network_In	Internet Interface: out	Any	Firewall_out	ephemeral_fw	Any	

Page 1 of 1

EDITING RULE NO 1

General

Original source

Original destination

Translated source

Translated destination

Protocol

Options

STATUS - COMMENT - NAME

General

Status: On

Comments: Created on 2021-11-09 14:37:25, by admin (192.168.56.20)

Advanced properties

CANCEL OK

22

Les paramètres d'une règle peuvent être renseignés directement dans la fenêtre des règles ou sur une nouvelle fenêtre qui s'affiche en double cliquant sur n'importe quel paramètre de cette règle. Cette fenêtre permet aussi l'accès aux paramètres de configuration avancée. Les valeurs des paramètres étant des objets, ils peuvent être copiés d'une règle à une autre par un simple glisser/déposer.