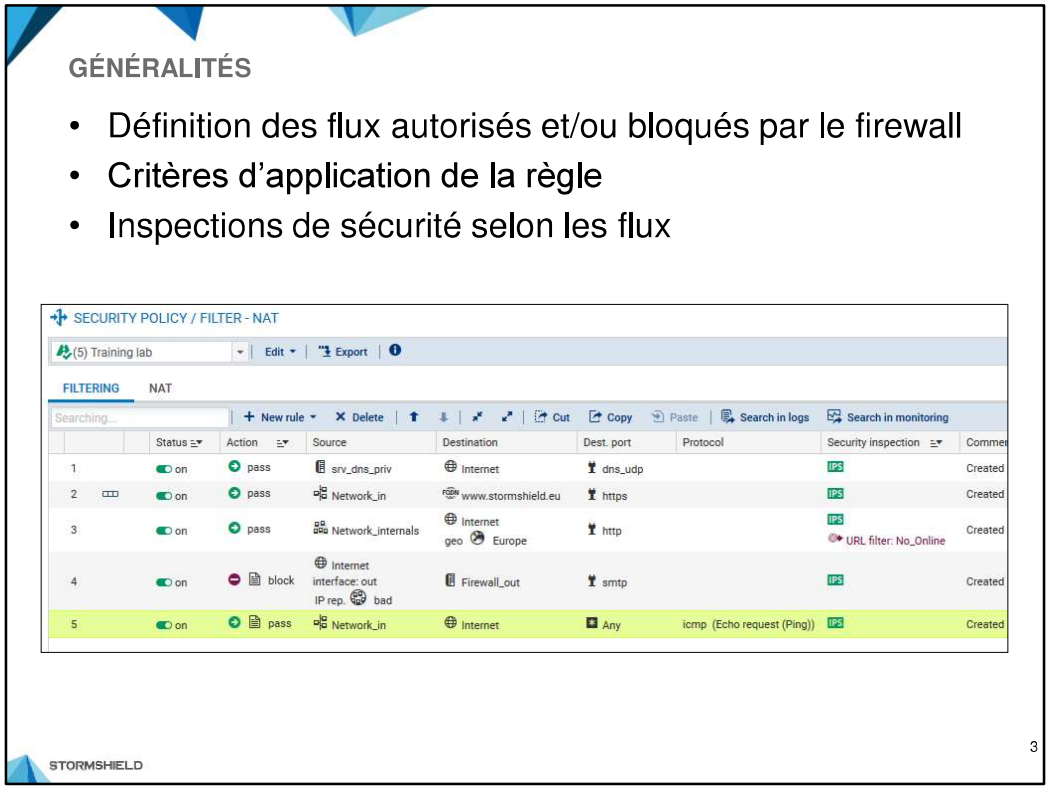
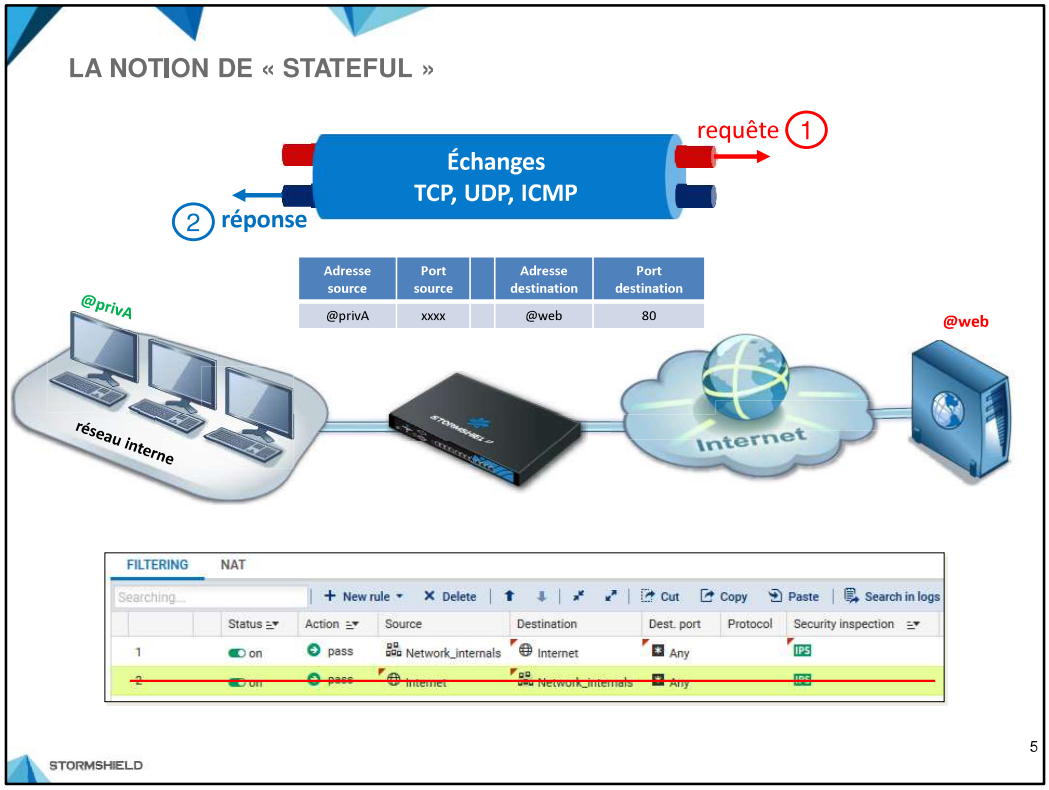


Grâce à la politique de filtrage, l'administrateur est capable de définir les règles qui permettront d'autoriser ou de bloquer les flux au travers de l'UTM Stormshield Network. Selon les flux, certaines inspections de sécurité (analyse antivirale, analyse antispam, filtrage URL, …) peuvent être activées (nous détaillerons ces analyses dans le module « Protection applicative »). Les règles de filtrage définies doivent respecter la politique de sécurité de l'entreprise.

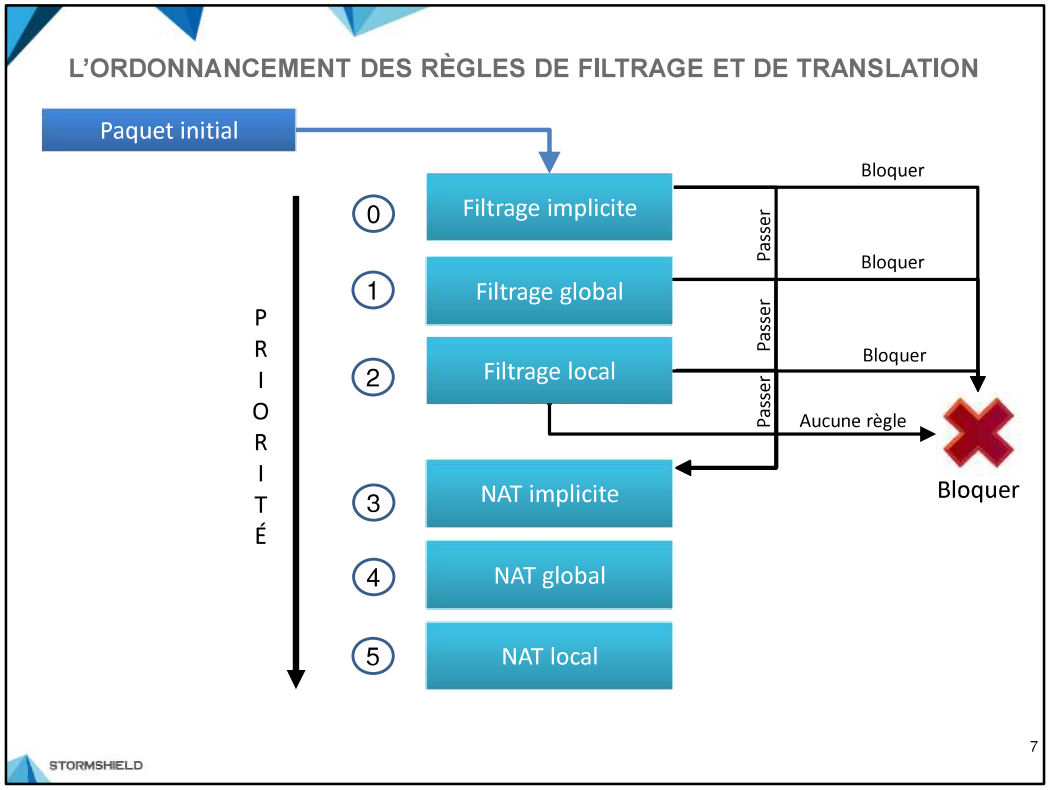
Pour définir un flux, une règle de filtrage se base sur de nombreux critères ; ce qui offre un haut niveau de granularité. Parmi ces critères, il est notamment possible de préciser:

- L'adresse IP source et/ou destination,
- La réputation et la géolocalisation de l'adresse IP source et/ou destination,
- L'interface d'entrée et/ou sortie,
- L'adresse réseau source et/ou destination,
- Le FQDN source et/ou destination,
- La valeur du champ DSCP,
- Le service TCP/UDP (n° de port de destination),
- Le protocole IP (dans le cas d'ICMP, le type de message ICMP peut être précisé),
- L'utilisateur ou le groupe d'utilisateurs devant être authentifié.

Le nombre de règles de filtrage actives dans une politique est limité. Cette limite dépend exclusivement du modèle de firewall.
Le premier paquet appartenant à chaque nouveau flux reçu par l'UTM est confronté aux règles de filtrage de la première à la dernière ligne. Il est donc recommandé d'ordonner au mieux les règles de la plus restrictive à la plus généraliste.
Par défaut, tout trafic qui n'est pas autorisé explicitement par une règle de filtrage est bloqué.



Les firewalls Stormshield Network utilisent la technologie SPI (Stateful Packet Inspection) qui leur permet de garder en mémoire l'état des connexions TCP et des pseudo-connexions UDP et ICMP afin d'en assurer le suivi et de détecter d'éventuelles anomalies ou attaques. La conséquence directe de ce suivi « Stateful » est l'autorisation d'un flux par une règle de filtrage uniquement dans le sens de l'initiation de la connexion ; les réponses faisant partie de la même connexion sont implicitement autorisées. Ainsi, nous n'avons nul besoin d'une règle de filtrage supplémentaire pour autoriser les paquets réponse d'une connexion établie au travers du firewall.



Dans les firewalls Stormshield Network, les règles de filtrage et de NAT sont organisées en différents niveaux appelés « slot » représentés selon leur priorité dans la figure ci-dessus :

- **Le filtrage implicite** : Regroupe les règles de filtrage préconfigurées ou ajoutées dynamiquement par le firewall pour autoriser ou bloquer certains flux après l'activation d'un service. Par exemple, une règle implicite autorise les connexions à destination des interfaces internes de l'UTM sur le port HTTPS (443/TCP) afin d'assurer un accès continu à l'interface d'administration Web. Autre exemple, dès l'activation du service SSH, un ensemble de règles implicites sera ajouté pour autoriser ces connexions depuis toutes les machines des réseaux internes.
- **Le filtrage global** : Regroupe les règles de filtrage injectées au firewall depuis l'outil d'administration « Stormshield Management Server » (SMC) ou après affichage des politiques globales.
- **Le filtrage local** : Représente les règles de filtrage ajoutées par l'administrateur depuis l'interface d'administration.

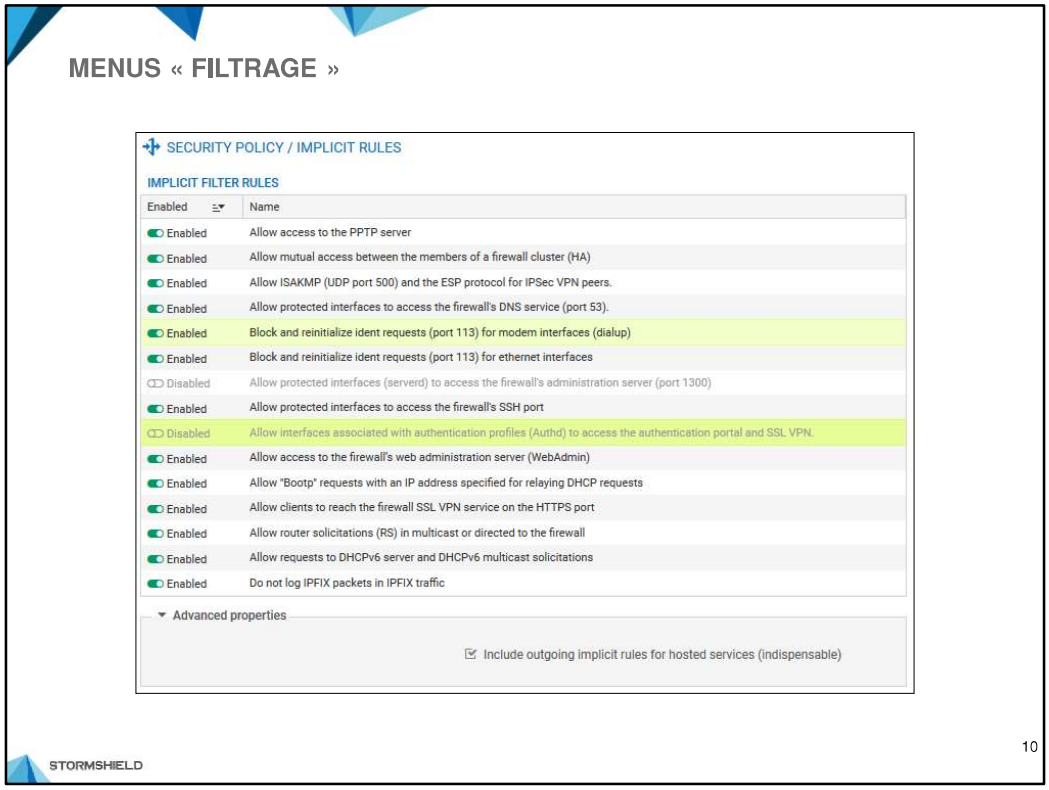
Ce que vous allez faire

- **Le NAT implicite** : Regroupe les règles de NAT ajoutées dynamiquement par le firewall. Ces règles sont utilisées principalement lors de l'activation de la haute disponibilité.
- **Le NAT global** : à l'instar du filtrage global, il regroupe les règle de NAT injectées au firewall depuis l'outil d'administration « Stormshield Management Server » (SMC) ou après affichage des politiques globales.
- **Le NAT local** : Regroupe les règles de NAT ajoutées par l'administrateur depuis l'interface d'administration.

Ce que vous allez faire

Tenir compte compte de l'ordre d'application de vos règles si vous constatez que l'une d'elles ne semble pas fonctionner !

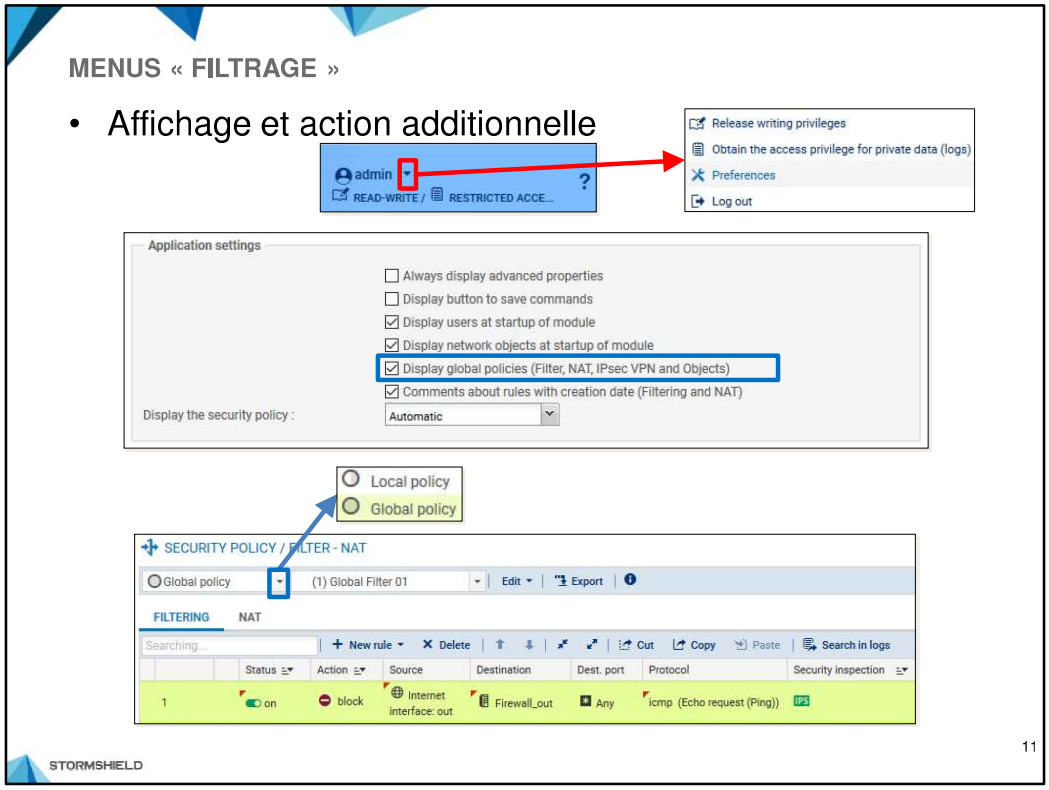
Le premier paquet reçu est confronté aux règles de filtrage des différents slots suivant l'ordre présenté dans la figure ci-dessus. Dès que les éléments du paquet correspondent à une règle dans un slot, l'action de la règle (bloquer ou autoriser) est appliquée et le paquet n'est plus confronté aux règles suivantes. Si aucune règle de filtrage ne correspond, le paquet est bloqué par défaut.
Dans le cas où le paquet est autorisé, il est confronté aux règles de NAT des différents slots toujours suivant l'ordre présenté ci-dessus.



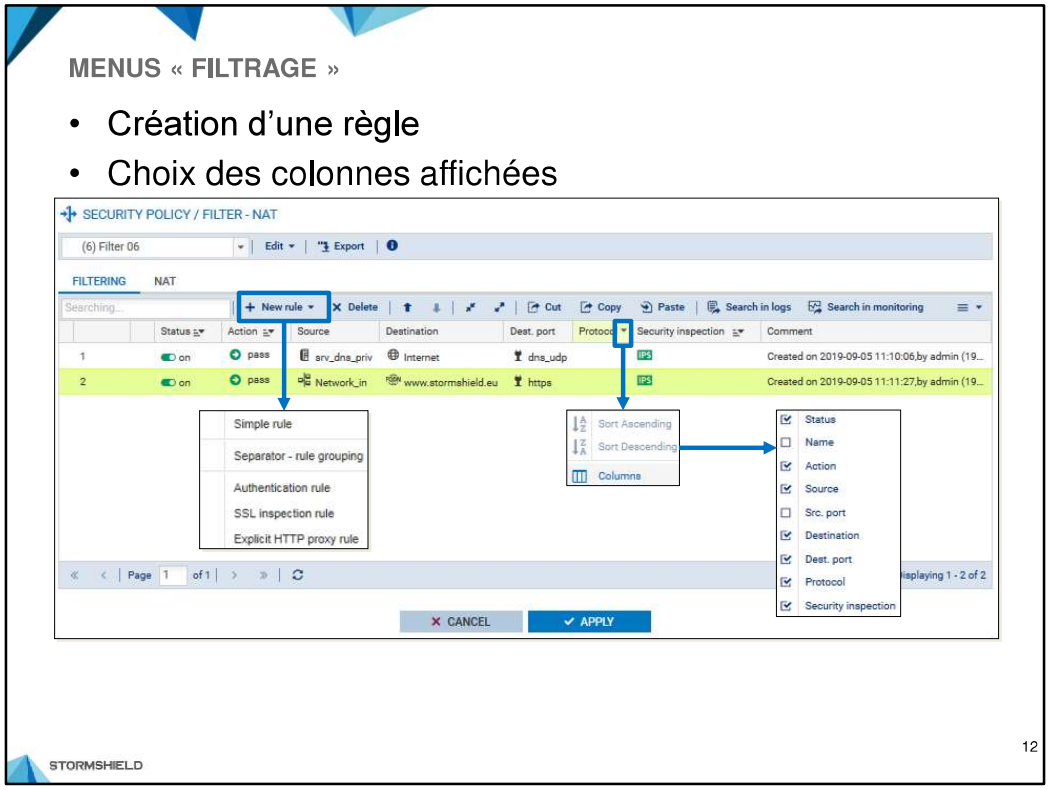
Les règles implicites sont accessibles depuis le menu **CONFIGURATION ⇒ POLITIQUE DE SÉCURITÉ ⇒ Règles implicites**. Chaque règle peut être activée/désactivée.

NOTE : La modification de l'état de ces règles a un impact direct sur le fonctionnement des services du firewall. Pour que le service concerné fonctionne toujours, il faut s'assurer au préalable que le flux est autorisé par les règles de priorité moindre telles que globales ou locales.

pour information



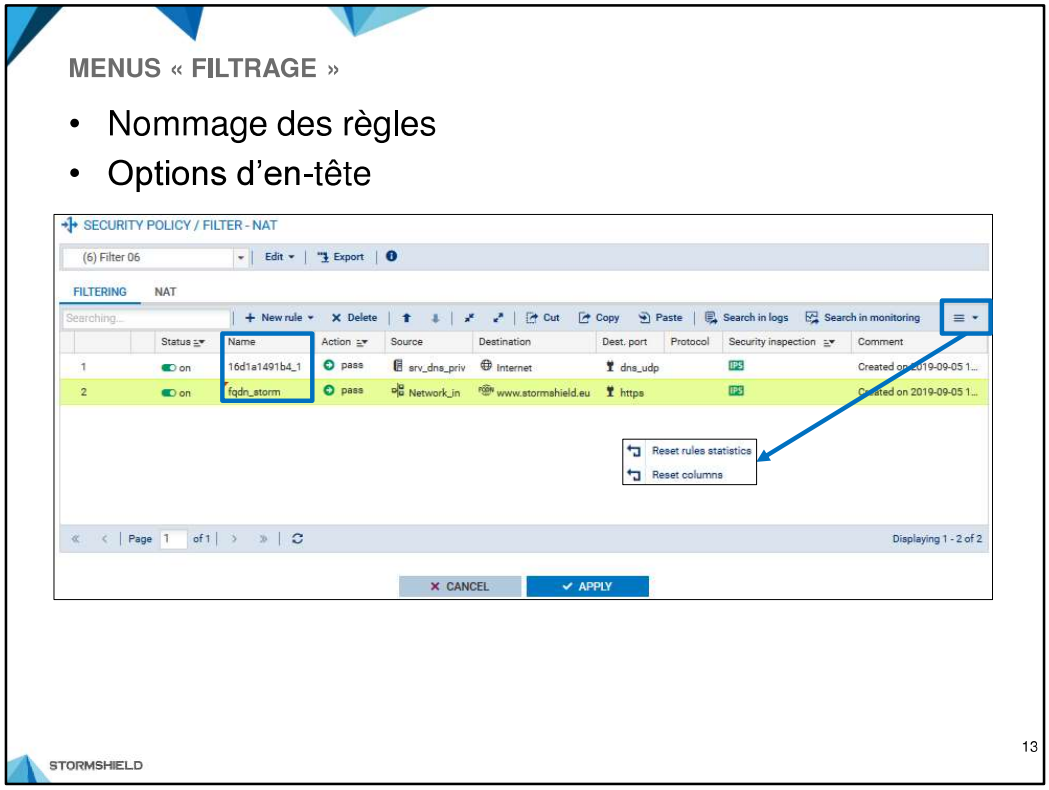
Pour afficher les règles globales, il faut cocher l'option **Afficher les politiques globales (Filtrage, NAT, VPN IPsec et Objets)** dans le menu **Préférences** accessible directement depuis l'icône de l'en-tête encadré en rouge. Cette option fait apparaître dans l'en-tête du menu **CONFIGURATION ⇒ 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.



Les règles de filtrage font partie d'une politique présentée précédemment dans le module « Translation d'adresses ».
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. Par défaut, une nouvelle règle est désactivée et tous ses critères sont paramétrés à Any.
  - **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. Le séparateur peut être personnalisé par une couleur et un commentaire.
  - **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 (voir module « Utilisateurs et Authentification » pour plus de détails à ce sujet).
  - **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.

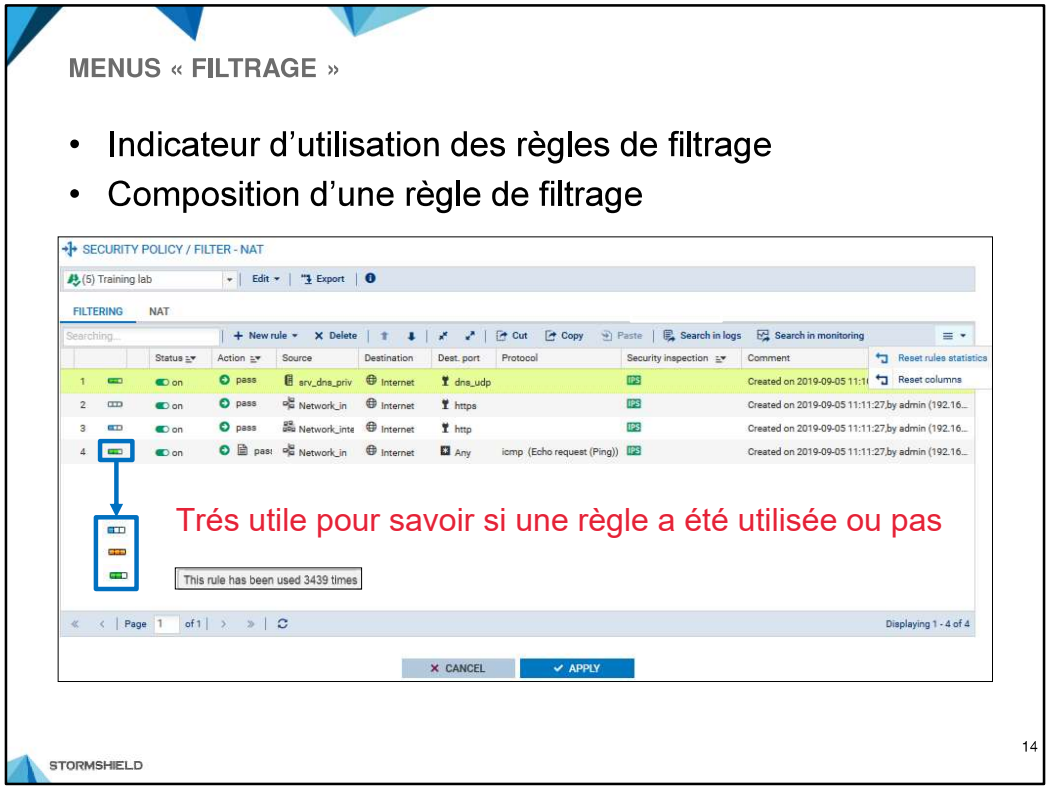
pratique pour séparer des groupes de règles



- **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.

NOTE : La recherche dans les logs ou la supervision s'effectuant sur le nom d'une règle, remarquez ci-dessus qu'une règle a forcément un nom par défaut, modifiable par l'administrateur.

il est conseillé de nommer ses règles



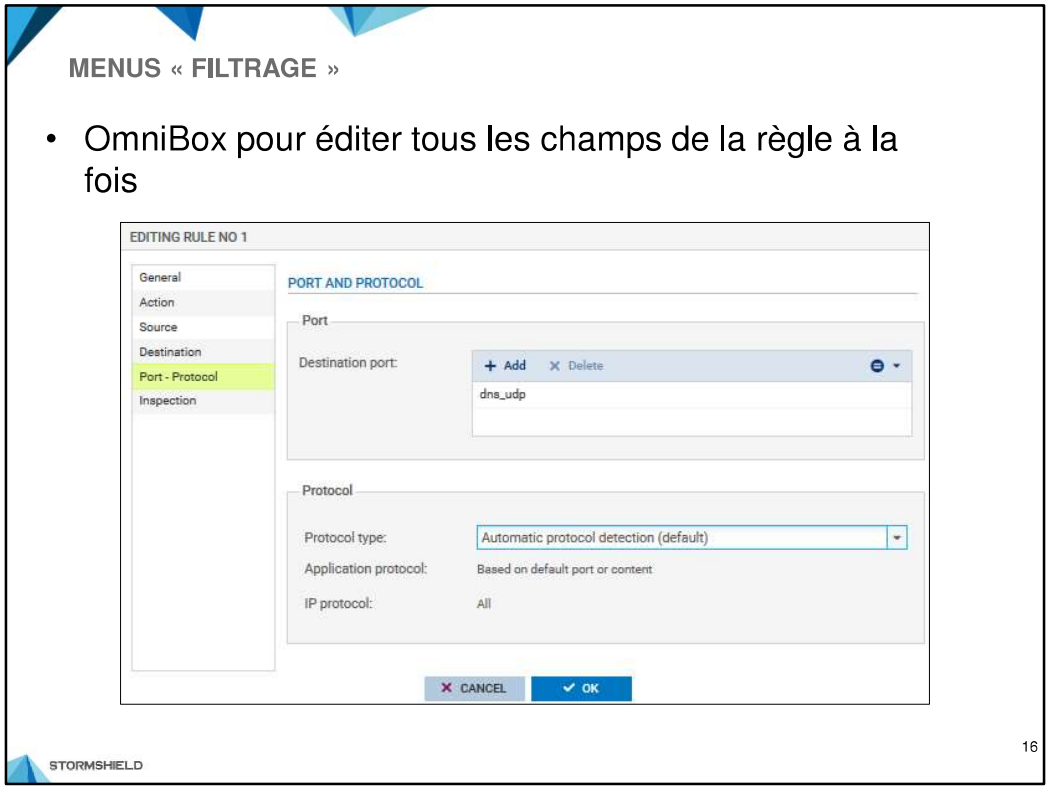
La fenêtre des règles est composée de plusieurs colonnes listées ci-dessous :

- 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.

- **Protocole** : Permet de renseigner le protocole utilisé par le trafic.
- **Inspection de sécurité** : Permet de sélectionner le niveau d'inspection (IPS/IDS/Firewall) et d'activer l'inspection applicative. (Cette partie sera traitée plus en détail dans le module « Protection Applicative »)

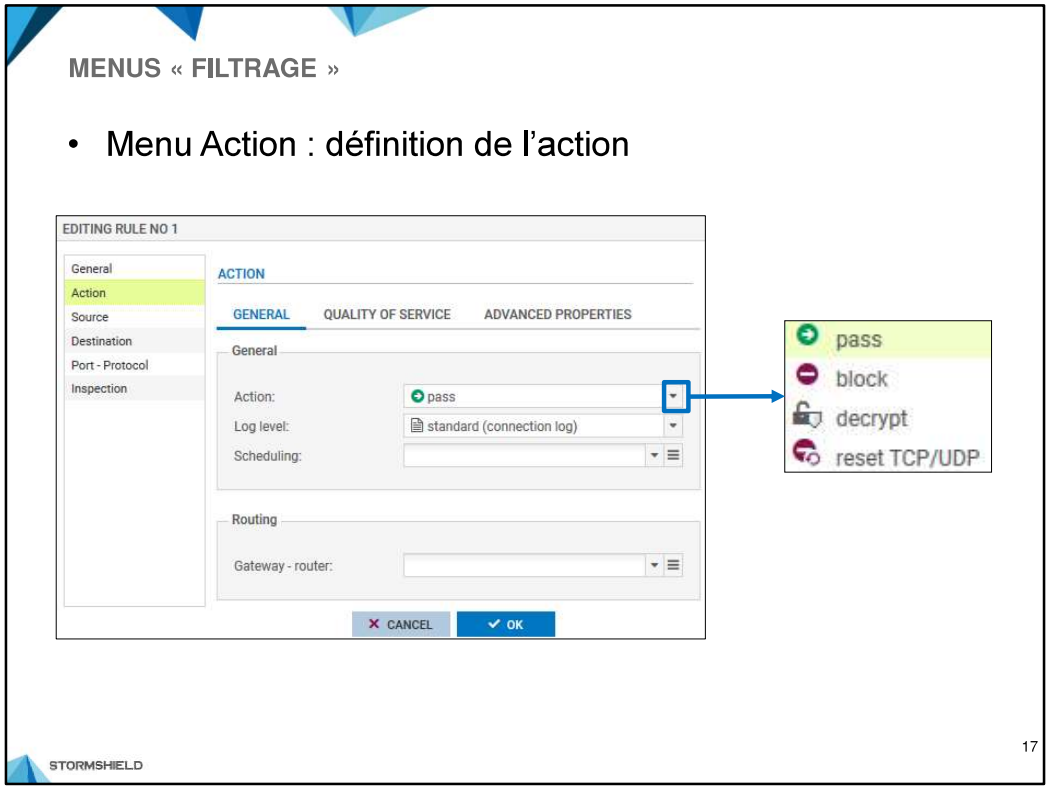
NOTE : L'intérêt principal de l'indicateur est de réordonner les règles de filtrage les plus utilisées en les plaçant en tête de liste tout en respectant la politique de sécurité. Cela permet d'optimiser le temps de lecture de la politique avant de trouver l'action à appliquer.

Donc utile aussi pour optimiser le filtrage



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**.

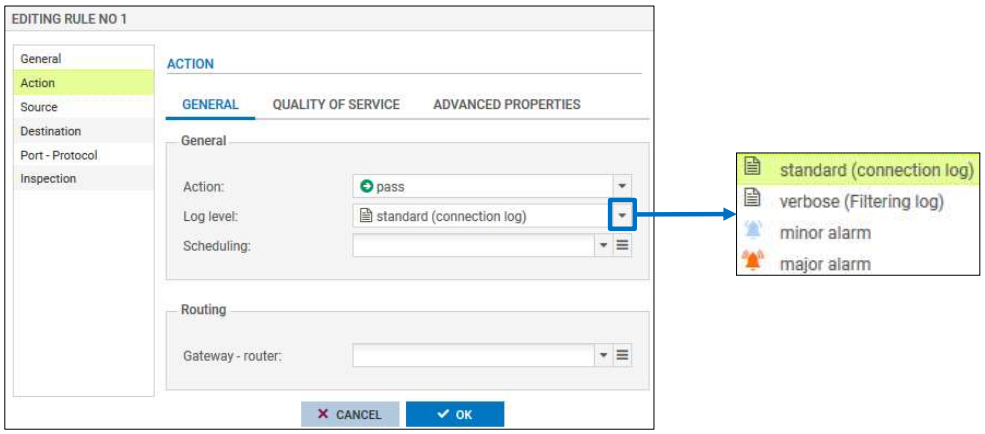


Le menu **ACTION** est constitué de plusieurs onglets, nous nous intéresserons principalement à l'onglet **GÉNÉRAL** qui permet de spécifier les paramètres suivants :

- **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



Très utile pour tester le bon fonctionnement d'une règle

18

STORMSHIELD

- **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 :
    - Dans le journal « Connexions réseau » ou dans le journal « Connexions applicatives » si une analyse applicative est menée par un plugin (en mode IPS, IDS),
    - Les connexions avec action « Bloquer » ne sont pas journalisées.
  - **verbeux (journal de filtrage)** : Les flux sont tracés dans le journal « Filtrage ». Cette option n'est utile que pour :
    - Journaliser des flux directement au-dessus d'IP (ICMP, GRE, ESP,…),
    - Journaliser le blocage d'un flux par l'action « Bloquer ».
  - **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.

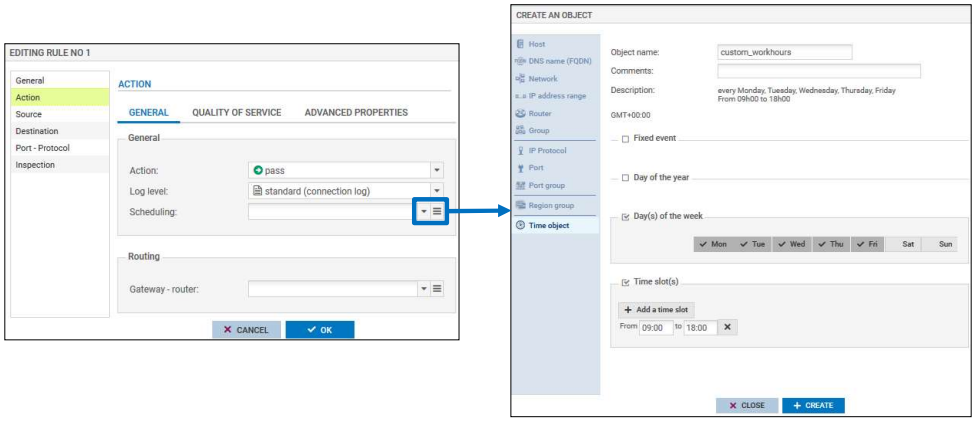
Vous allez mettre en oeuvre des alarmes

NOTE : L'utilisation du mode verbeux sur une connexion en TCP/UDP est non seulement inutile, mais crée des doublons avec une écriture dans un des journaux de connexions et une écriture dans le journal de filtrage pour le même flux.

MENUS « FILTRAGE »

- Menu Action : Programmation horaire et routage par politique

Pour information

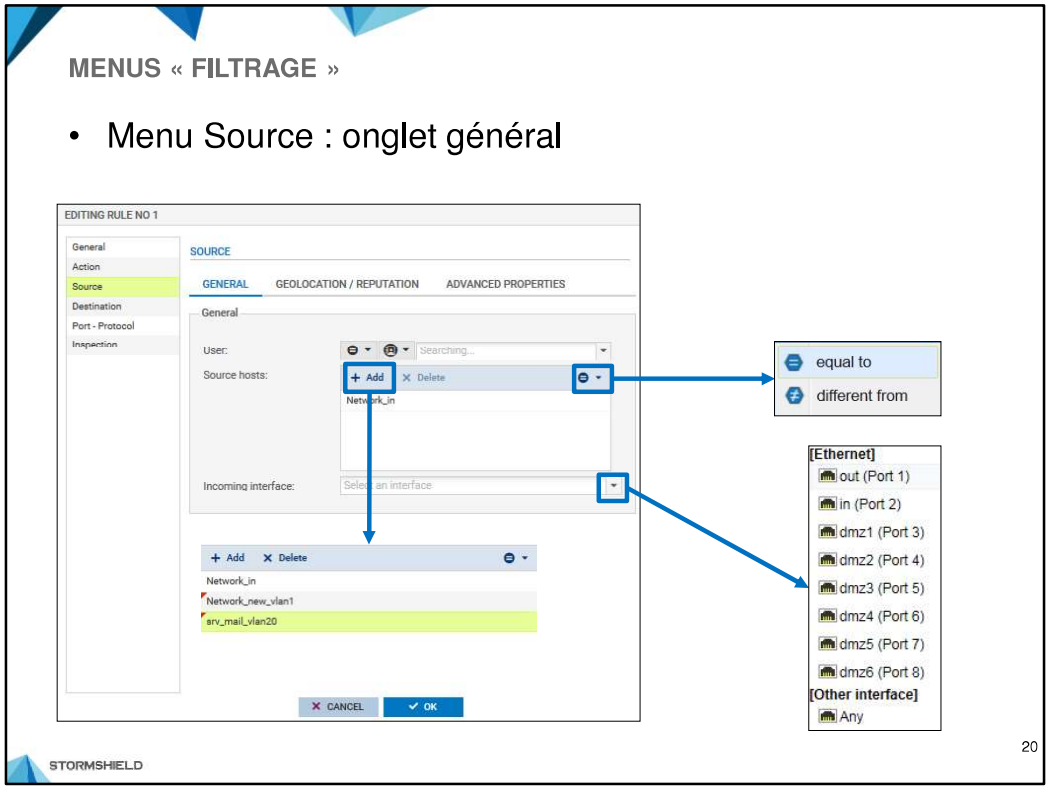


19

STORMSHIELD

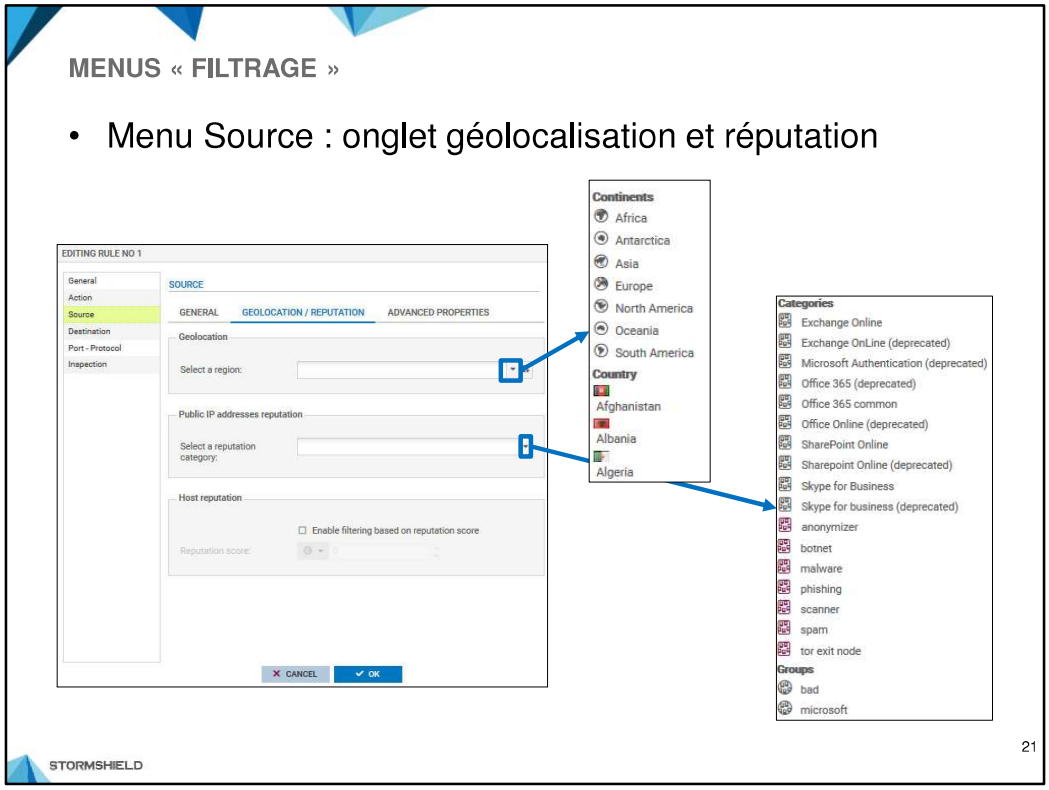
- **Programmation horaire** : Sélection d'un objet temps qui permet de définir des plages horaires hebdomadaires, des évènements annuels ou ponctuels. Les objets temps peuvent être créés dans le menu **CONFIGURATION ⇒ OBJETS ⇒ Objets temps** ou en cliquant sur le bouton encadré en bleu. Si ce paramètre est renseigné, la règle de filtrage sera active uniquement durant la plage horaire définie par l'objet temps.
- **Passerelle – routeur** : Ce paramètre permet de mettre en œuvre le routage par politique (présenté dans le module « Configuration réseau »). Dès lors qu'une passerelle est renseignée, tout le trafic traité par cette règle de filtrage sera transmis à cette passerelle et non à la passerelle par défaut si aucune autre directive de routage plus prioritaire n'est configurée.

STORMSHIELD



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. Ce paramètre est fonctionnel dans le cadre d'un système d'authentification basé sur un annuaire utilisateurs (voir module « Utilisateurs et Authentification »).
- **Machines sources** : Indique l'adresse IP, le Fully Qualified Domain Name (FQDN) ou l'adresse réseau du trafic. Les icônes « = » ou « ≠ » signifient que le paramètre peut être égal ou différent de la valeur spécifiée. De plus, il est possible de renseigner une liste d'objets en cliquant sur le bouton **Ajouter**, le coin rouge en haut à gauche des objets ajoutés signifie que cet ajout n'a pas encore été sauvegardé.
- **Interface d'entrée** : Permet de préciser l'interface d'entrée du trafic. Ce paramètre est utile dans le cas des bridges où les interfaces partagent le même plan d'adressage.

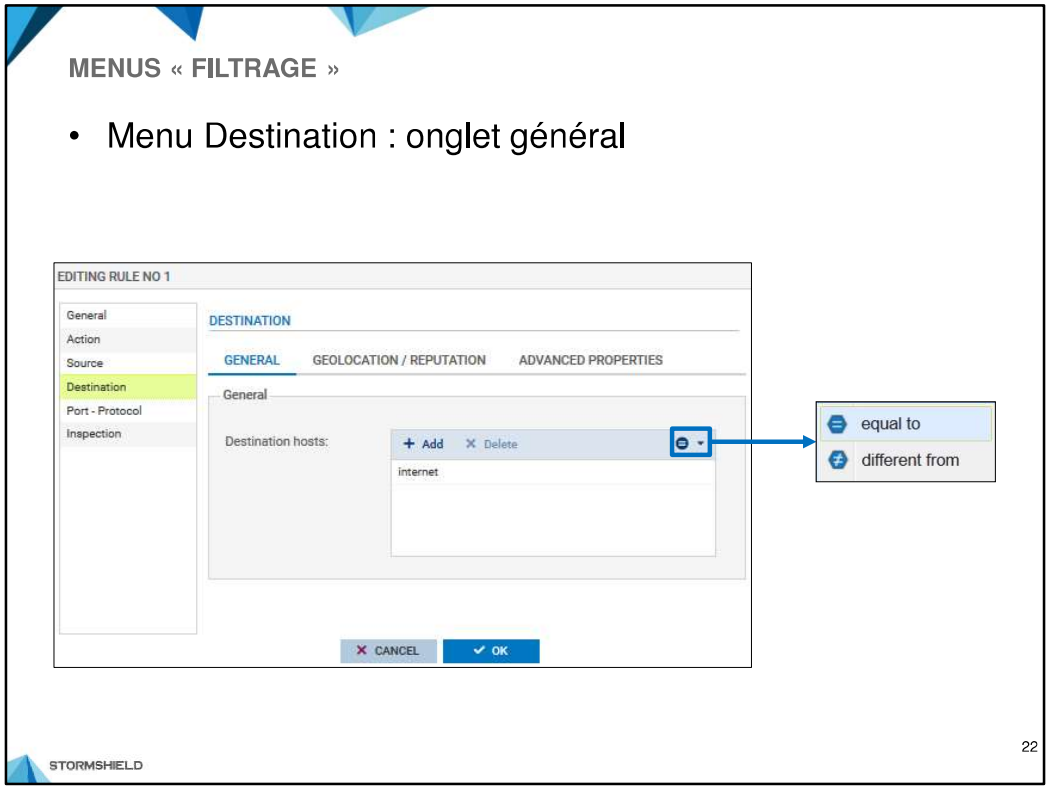


Le menu **Source ⇒ GÉOLOCALISATION / RÉPUTATION** regroupe les paramètres suivants :

- **Géolocalisation** : permet de renseigner un continent ou un pays à l'origine du trafic. La liste ne contient pas d'adresses IP, le Firewall détermine le pays auquel appartient une IP, plutôt que de charger toutes les IP (les blocs d'adressage sont très fragmentés sur Internet).
- **Réputation des adresses IP publiques** : une IP publique peut avoir une réputation à la limite de deux catégories. Le groupe « Bad » regroupe les catégories : anonymizer, botnet, malware, phishing, scanner, spam et tor.
- **Réputation des machines** : Il est possible d'activer le filtrage selon le score de réputation des machines du réseau interne. Il faut au préalable activer la gestion de réputation des machines et définir les machines concernées par le calcul d'un score de réputation, ce point est détaillé dans les annexes.

Dans le menu **Source**, les paramètres **Géolocalisation** et **Réputation des adresses IP publiques** sont utilisés généralement pour qualifier le flux entrant (provenant d'Internet), alors que le paramètre **Réputation des machines** est utilisé pour qualifier le flux sortant.

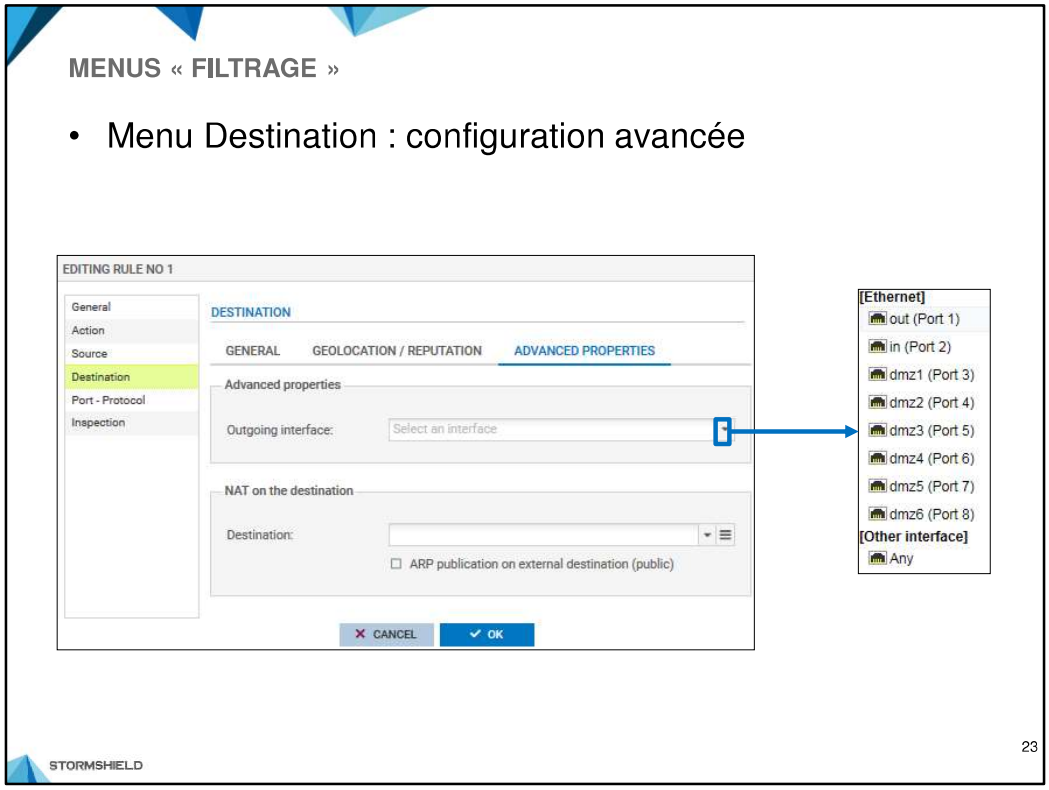
NOTE : Le score de réputation des machines internes, configurable dans ce menu, permet de préciser le score au-dessus duquel ou en-dessous duquel la règle de filtrage s'appliquera aux machines supervisées.



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.

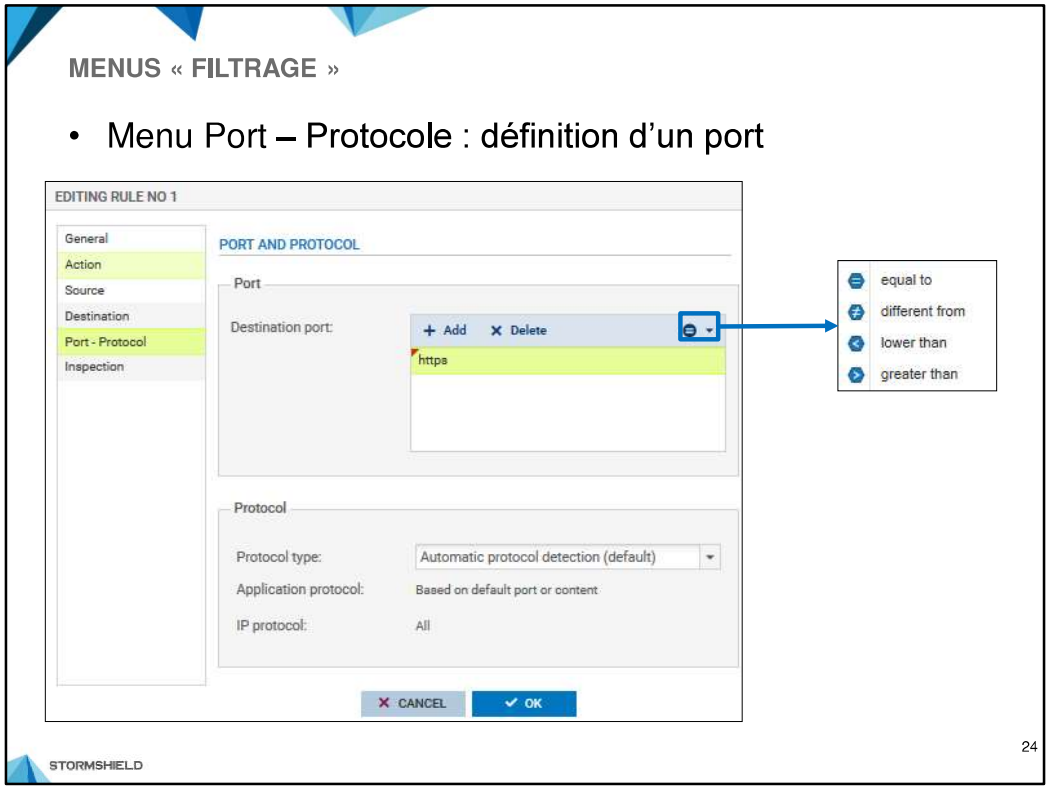
La géolocalisation et la réputation des adresses IP publiques ainsi que la réputation des machines peuvent être utilisées également dans les paramètres de destination depuis l'onglet **GÉOLOCALISATION / RÉPUTATION**.

NOTE : Lorsque l'objet de destination est un objet FQDN, il doit être le seul objet de la liste.

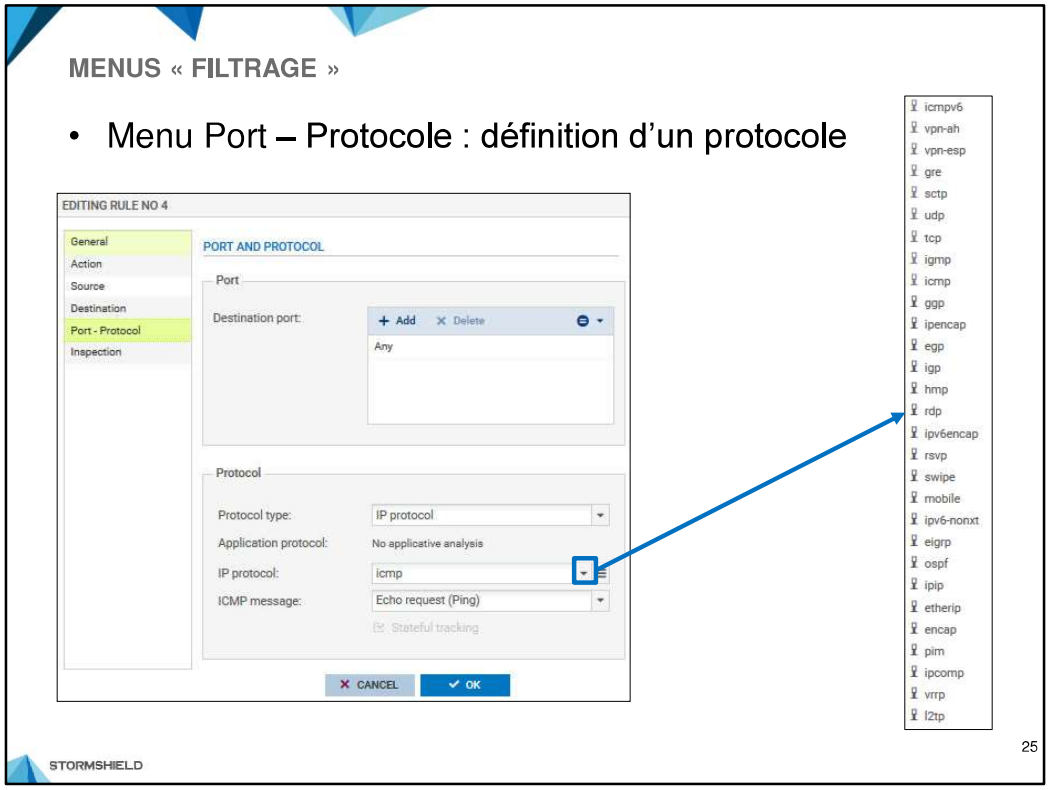


Dans l'onglet **CONFIGURATION AVANCÉE**, nous pouvons restreindre l'application de la règle uniquement au trafic sortant par l'interface indiquée dans **interface de sortie** .

NOTE : Pour les règles autorisant un flux sortant, il n'est pas conseillé de renseigner l'interface de sortie car la route à emprunter pour joindre la destination du flux n'est pas encore connue.

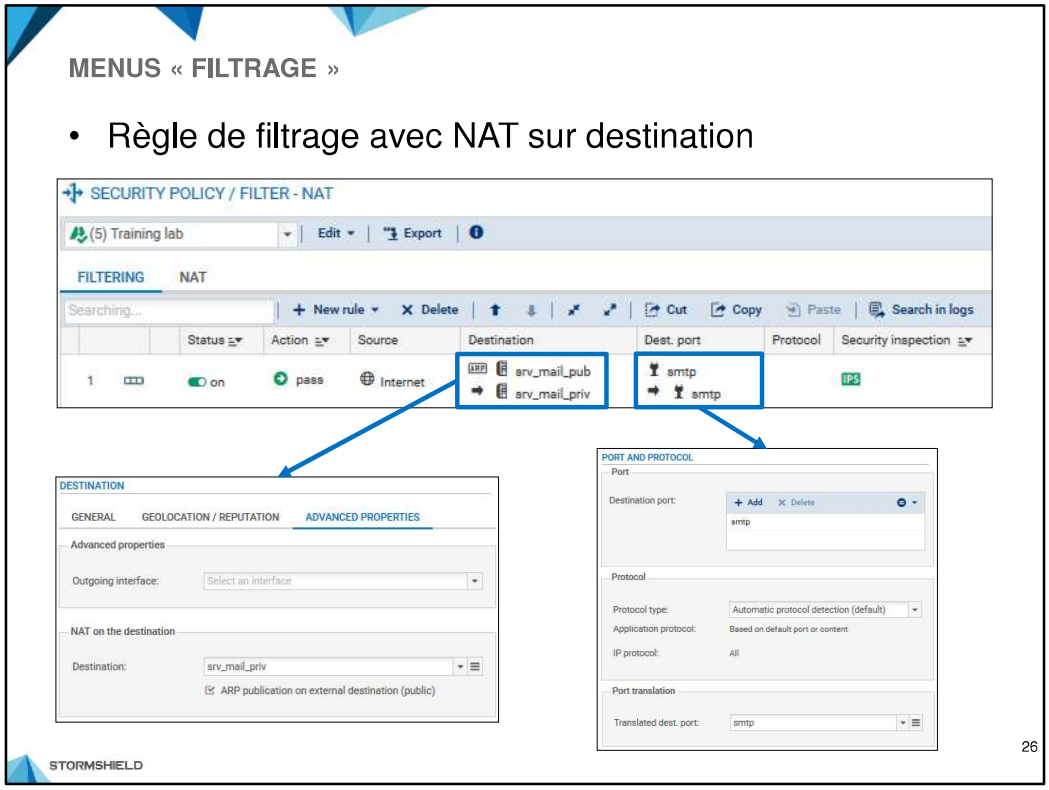


Le menu **PORT / PROTOCOLE** permet de renseigner le **Port destination** avec la possibilité de choisir s'il doit être égal, différent, inférieur ou supérieur à la valeur sélectionnée. Il est également possible de renseigner une liste de ports de destination.



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.

NOTE : Le suivi des états « stateful » qui permet de mémoriser et de suivre les connexions traversant le firewall est activé et figé (non modifiable) uniquement pour les protocoles TCP, UDP et ICMP. Pour les autres protocoles (GRE, ESP, etc.), il faut cocher cette option pour activer le suivi.

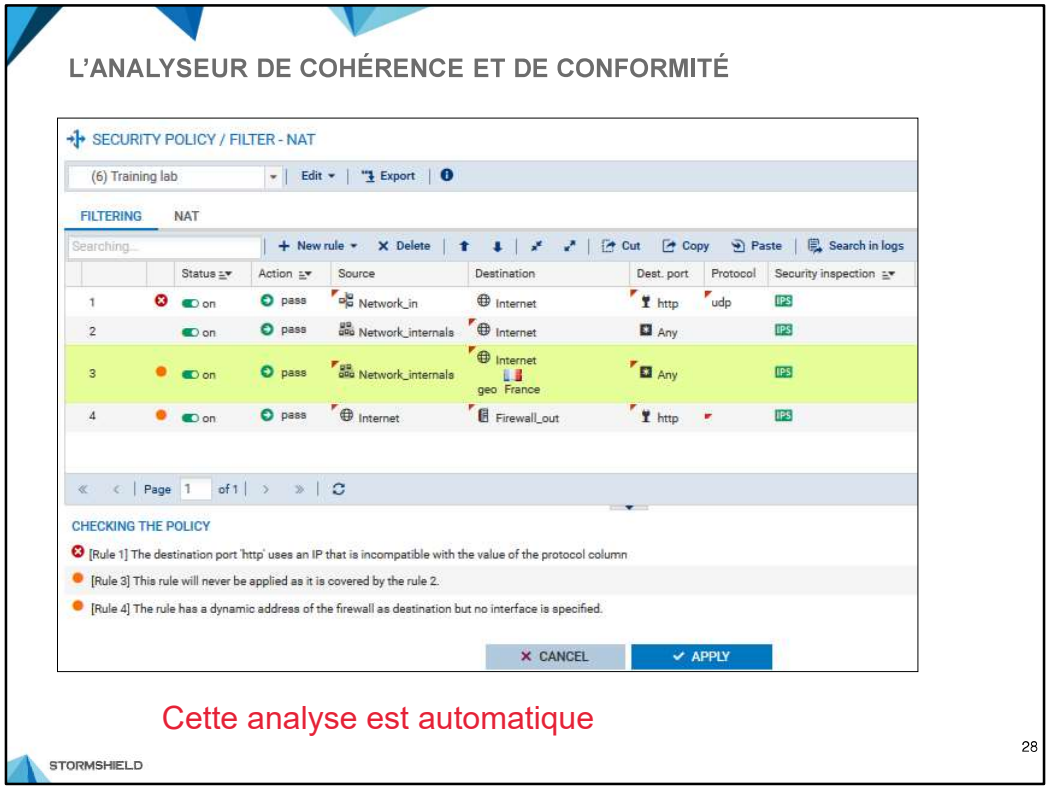


Dans une règle de filtrage, une directive de NAT sur la destination (DNAT) peut être appliquée, sauf si elle contient un objet FQDN, ou des éléments de géolocalisation et /ou de réputation.

Exemple : La figure ci-dessus illustre une translation sur la destination d'un trafic SMTP entrant. La règle de filtrage autorise ce trafic en provenance d'un réseau externe et à destination de l'adresse IP publique du serveur STMP sur le port SMTP/25. L'adresse et le port destination sont translatés respectivement par l'adresse IP privée du serveur SMTP et le port SMTP/25 directement dans la règle de filtrage où la publication ARP est également activée. Grâce à cette configuration, il n'est pas nécessaire d'ajouter une règle de translation pour rediriger ce trafic.

Il existe plusieurs avantages à créer une directive de NAT sur destination au sein d'une règle de filtrage:

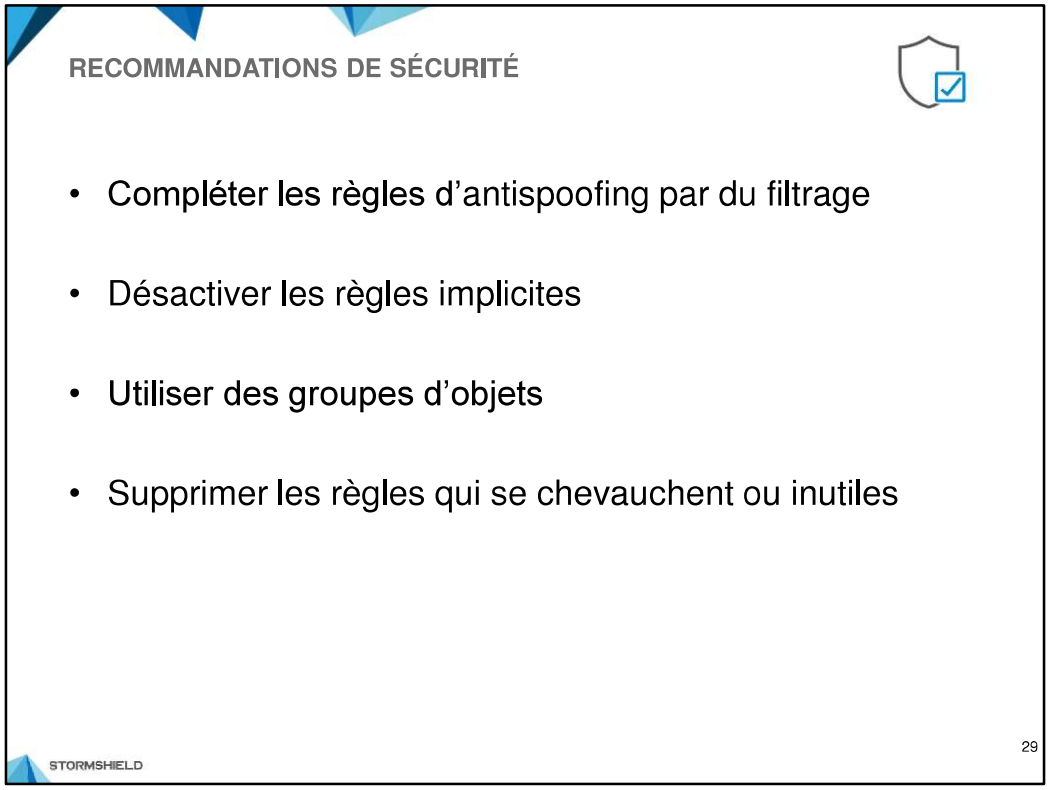
- Indication rapide du flux autorisé avec redirection vers la machine interne,
- Gestion et supervision des règles entrantes dans un seul menu,
- Optimisation du temps de traitement des règles puisque les règles présentes dans l'onglet NAT ne sont pas parcourues,
- Activation de protections applicatives (filtrage SMTP, antispam, etc.) à des connexions entrantes translatées.



Les firewalls Stormshield Network embarquent un moteur de vérification qui permet de détecter d'éventuelles situations de recouvrement ou d'incohérence créées dans la politique de filtrage. Ce type de situation est signalé par un message d'avertissement en bas du menu.
Tris exemples sont illustrés dans la figure ci-dessus :

- Dans la règle n°1, le port destination HTTP est incompatible avec le protocole UDP parce que le protocole applicatif HTTP utilise le protocole de transport TCP,
- La règle n°3 ne sera jamais utilisée parce qu'elle est recouverte par la règle n°2,
- La règle n°4 souligne que le flux arrive sur un objet dont l'IP peut changer (IP dynamique associée à la patte out), et qu'il faut préciser l'interface d'entrée (dans le champ source).

NOTE : Les messages signalés avec une croix rouge bloquent la sauvegarde et l'activation de la politique.



L'antispoofing a ses limites et ne bloque pas les réseaux privés arrivant par internet par exemple. Il est donc nécessaire de compléter la protection avec des règles de blocage déduites de la topologie du réseau. Par exemple bloquer les IP RFC5735 sur les réseaux publics.

ATTENTION à ne pas perdre l'accès au pare-feu

Les règles implicites étant évaluées avant les autres, elle peuvent rendre inopérantes des règles créées par l'administrateur. Attention à bien préparer les règles d'autorisation d'accès à l'interface web pour ne pas perdre la main sur le pare-feu. Le SSH vers le SNS étant accessible par défaut sur toutes les interfaces internes, c'est l'occasion de le limiter.

Les groupes d'objets simplifient la modification des règles. Il est recommandé d'utiliser des groupes plutôt que de créer des listes de machines dans les règles. Cela améliore aussi la lisibilité.

Tout comme pour les NAT, il est recommandé de ne jamais laisser des règles se recouvrir. De même, il faut traquer et supprimer régulièrement toutes les règles inutilisées.