Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 30 mars 2013

N° DAT-NT-006/ANSSI/SDE/NP

Nombre de pages du document : 1+15

Note technique

Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu

Public visé:

Développeur	
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	✓

Informations

Avertissement

Ce document rédigé par l'ANSSI présente les « **Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu** ». Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (www.etalab.gouv.fr). Il est par conséquent diffusable sans restriction.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Personnes ayant contribué à la rédaction de ce document:

Contributeurs	Rédigé par	Approuvé par	Date
BSS, BAI, BAS, LAM	BSS	SDE	30 mars 2013

Évolutions du document :

Version	Date	Nature des modifications
1.0	30 mars 2013	Version initiale

Pour toute remarque:

Contact	Adresse	@mél	Téléphone
Bureau Communication de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	communication@ssi.gouv.fr	01 71 75 84 04

Table des matières

1 Préambule

L'objectif de ce document est de fournir les éléments organisationnels permettant de structurer la base de règles constituant la politique de filtrage réseau appliquée sur un pare-feu d'interconnexion. Cette note est indépendante de la fonction du pare-feu (accès internet, cloisement de *datacenter*, isolation d'un partenaire) ; elle fait l'abstraction des solutions techniques qui peuvent être employées [1] (logiciel, équipement dédié) et ne tient pas compte de son mode d'administration (ligne de commande, interface web, client lourd). Certaines des préconisations mentionnées dans ce document ne seront donc applicables que si la technologie utilisée le permet ; il appartient au lecteur d'apprécier et de déterminer si les différentes recommandations sont adaptées à son cas d'usage. Ceci dépend notamment de la famille [2] à laquelle appartient le pare-feu.

Cette note technique s'adresse à l'ensemble des personnes qui ont la charge de définir, de mettre en œuvre ou d'administrer des architectures d'interconnexion sécurisées et qui souhaitent inscrire dans leur démarche la volonté d'assurer la pérénnité des politiques de filtrage réseau appliquées sur les pare-feux.

Dans la suite de ce document les termes « pare-feu » et « passerelle » seront utilisés indifférement, ils désignent tous les deux un équipement d'interconnexion capable de réaliser un filtrage réseau en tenant compte de l'état des connexions préalablement établies (stateful).

Les bonnes pratiques relatives au positionnement d'un pare-feu dans une architecture ne sont pas présentées dans ce guide, celles-ci sont détaillées dans un document complémentaire publié par l'ANSSI intitulé « Définition d'une architecture de passerelle d'interconnexion sécurisée ». Ce guide est disponible dans la section « Bonnes pratiques → Recommandations et guides → Sécurité des réseaux » sur www.ssi.gouv.fr.

1. Pour rappel, la liste des pare-feux qualifiés par l'ANSSI est disponible dans la section « Certification/ Qualification » sur www.ssi.gouv.fr.

2. En effet, il existe deux catégories de pare-feux, la première concerne ceux dont les règles de filtrage sont définies par paire d'interfaces réseaux (une entrante, une sortante), la seconde ceux dont les règles sont définies globalement. Dans ce deuxième cas, ce n'est pas l'administrateur qui détermine les interfaces d'entrée/sortie auxquelles s'appliquent chacune des règles mais le pare-feu lui même.

2 Pourquoi cette note ?

La rédaction de cette note technique a été motivée par les raisons suivantes :

- Les architectures d'interconnexion se complexifient de plus en plus pour pouvoir faire face aux nouvelles menaces, différentes briques techniques y sont régulièrement ajoutées (exemple : IDS, Firewall Web Applicatif). Le pare-feu reste cependant l'un des éléments majeurs d'une défense en profondeur [3] efficace, il est le premier rempart pour stopper les attaques ou ralentir leur progression.

- L'ajout permanent de nouvelles fonctionnalités aux pare-feux (ou à leurs outils de management) complexifie leur administration et peut rendre la lisibilité des politiques de filtrage réseau plus difficile.

- L'historique parfois lourd des passerelles dégrade naturellement l'état des politiques de pare-feux (méconnaissance de l'utilité des certaines règles, non suppression de règles liées à des équipements retirés de la production).

- La rotation des équipes en charge de l'administration des passerelles peut conduire à une dérive des configurations (réutilisation d'adresses, règles surchargées).

3. Le concept de défense en profondeur est détaillé dans un mémento disponible dans la section « Bonnes pratiques → Outils méthodologiques » sur www.ssi.gouv.fr

3 Organisation d'une politique de filtrage réseau

3.1 Présentation du modèle

La politique de filtrage d'une passerelle peut être construite en suivant un modèle d'organisation de règles applicable dans la majorité des cas d'usage.

L'organisation proposée dans ce document a pour objectifs :

- de renforcer la protection du pare-feu et des réseaux de confiance qu'il isole ;
- de faciliter la lisibilité de la politique de filtrage ;
- de minimiser les sources d'erreurs et les dérives.

Cette organisation est construite selon un modèle de sécurité positif (tout ce qui n'est pas explicitement autorisé est interdit), il est possible de la décomposer en **6 sections rigoureusement ordonnées de la façon suivante** :

Ordre	Contenu
Section n°1	Règles d'autorisation des flux à destination du pare-feu
Section n°2	Règles d'autorisation des flux émis par le pare-feu
Section n°3	Règle de protection du pare-feu
Section n°4	Règles d'autorisation des flux métiers
Section n°5	Règles "antiparasites"
Section n°6	Règle d'interdiction finale

3.2 Conditions d'application du modèle

Les conditions d'application du modèle présenté sont les suivantes :

- les règles de filtrage sont évaluées séquentiellement par le pare-feu (de haut en bas) ;
- une règle de filtrage unique est appliquée à un flux (la première qui autorise ou interdit ce flux) ;
- il est possible de définir précisement les flux ayant pour origine ou destination le pare-feu [4]. Si cela n'est pas possible les sections n°1 et n°2 ne seront pas présentes dans la politique de filtrage.

4. Certaines solutions ne permettent pas de gérer finement les flux émis ou reçus par le pare-feu. Dans ces cas précis, des règles sont automatiquement ajoutées à la politique de filtrage, elles sont directement liées à l'activation de certains paramètres d'administration de la solution, et il n'est pas toujours possible de les désactiver (se référer au paragraphe 5.1).

3.3 Détail du modèle

3.3.1 Section n°1 : règles d'autorisation des flux à destination du pare-feu

Cette première section contient un nombre minimal de règles car un pare-feu n'offre qu'un nombre restreint de services, sa surface d'attaque doit être la plus réduite possible. Un pare-feu doit idéalement être administré et supervisé via une interface réseau physique dédiée connectée à un réseau d'administration.

Deux types de règles constituent cette section :

- les règles autorisant les services d'administration de la passerelle ;
- les règles autorisant les services de supervision de la passerelle.

Voici une illustration simple :

Source	Destination	Service	Action	Journalisation
Serveurs d'administration	Interface d'administration de la passerelle	ssh, https	Autoriser	Oui
Serveurs de supervision	Interface d'administration de la passerelle	get-snmp	Autoriser	Oui

R1	Les règles de sécurité qui autorisent l'accès aux services proposés par un pare-feu doivent être regroupées dans la politique de filtrage. Ces règles sont peu nombreuses et doivent être définies précisément, en particulier au niveau de leurs adresses sources et de leurs services.

3.3.2 Section n°2 : règles d'autorisation des flux émis par le pare-feu

Cette seconde section contient également un nombre limité de règles, elle ne décrit que les flux ayant pour origine la passerelle elle-même.

Trois types de règles constituent cette section :

- les règles autorisant les services d'envoi de journaux de la passerelle ;
- les règles autorisant les services d'alerte de la passerelle ;
- les règles autorisant les services qui permettent le maintien en condition opérationelle de la passerelle (par exemple les flux de sauvegarde).

Voici une illustration simple :

Source	Destination	Service	Action	Journalisation
Interface d'administration de la passerelle	Serveur de journaux	syslog	Autoriser	Oui
Interface d'administration de la passerelle	Serveur de supervision	trap-snmp	Autoriser	Oui
Interface d'administration de la passerelle	Serveur de sauvegarde	ssh	Autoriser	Oui

R2	Les règles de sécurité qui autorisent les flux ayant pour origine le pare-feu doivent être regroupées dans la politique de filtrage. Ces règles sont peu nombreuses et doivent être définies précisément, en particulier au niveau de leurs adresses de destinations et de leurs services.

3.3.3 Section n°3 : règle de protection du pare-feu

Cette section ne comporte qu'une seule règle dite de protection de la passerelle ; elle est toujours la même et peut être décrite de la façon suivante :

Source	Destination	Service	Action	Journalisation
Toutes	Toutes les interfaces de la passerelle	Tous	Interdire	Oui

L'action « Interdire » correspond à une suppression du trafic **sans réponse du pare-feu** (action drop en anglais), cela permet d'éviter un signalement trop explicite de la passerelle aux éventuels attaquants.

Cette protection permet de « verrouiller » l'accès à la passerelle, si dans la suite de la politique est ajoutée une règle qui va à l'encontre (autorisation de flux à destination du pare-feu), celle-ci ne sera pas prise en compte. Elle pourra même être signalée comme incohérente si la solution technique est en mesure d'effectuer cette vérification. La journalisation est obligatoirement activée pour cette règle afin de conserver la trace de l'ensemble des flux non légitimes à destination de la passerelle.

R3	La mise en place d'une règle de protection du pare-feu est impérative pour prévenir l'ouverture de flux non légitimes à destination de la passerelle ; la journalisation de cette règle permet de conserver la trace de ces flux illégitimes.

3.3.4 Section n°4 : règles d'autorisation des flux métiers

Cette section contient les règles d'autorisation qui décrivent les flux métiers, celles-ci sont ordonnées selon une logique établie ; plusieurs orientations sont possibles, en voici deux exemples :

- Organisation des règles en fonction des entités métier : les règles sont regroupées en fonction des entités métiers auxquelles elles ouvrent des services (comptabilité, ressources humaines).
- Organisation des règles en fonction des services offerts : les règles sont regroupées en fonction des services autorisés (navigation internet, accès aux *proxy*, accès aux bases de données).

Le choix de l'organisation des règles est dépendant de plusieurs éléments du contexte comme le nombre de règles de la politique ou encore le rôle de la passerelle (accès internet, cloisement de *datacenter*, accès partenaire).

R4	Les règles qui autorisent les flux métiers doivent être regroupées et organisées selon une logique établie et adaptée au contexte. Ces règles constituent l'essentiel de la politique de filtrage, elles doivent être définies précisement au niveau de leurs adresses sources, de leurs adresses de destination et de leur services.

3.3.5 Section n°5 : règles "antiparasites"

Cette section est facultative, elle s'inscrit dans le cadre d'une politique globale de journalisation. Elle contient la liste des règles décrivant **les flux non autorisés dont la trace n'est volontairement pas conservée** (certains flux de broadcast par exemple) afin de maintenir les journaux de la passerelle exploitables. Cela suppose qu'une trace de ces flux est conservée par une autre brique de l'architecture (cela doit être documenté dans la politique globale de journalisation).

La règle suivante illustre cette section :

Source	Destination	Service	Action	Journalisation
Réseau de test	255.255.255.255	udp-137,udp-138 (netbios)	Interdire	Non

R5	Les règles "antiparasites" peuvent être utilisées pour alléger les journaux de la passerelle, mais doivent être établies en accord avec la politique globale de journalisation de l'architecture.

3.3.6 Section n°6 : règle d'interdiction finale

Cette section ne comporte qu'une seule règle d'interdiction ; celle-ci est dite finale car celle se trouve toujours en dernière position dans la politique. Cette règle a pour objectifs d'une part d'interdire le trafic qui n'a pas été explicitement autorisé par les règles précédentes, d'autre part de conserver une trace des flux non légitimes. La règle de protection est toujours la même et peut être décrite de la façon suivante :

Source	Destination	Service	Action	Journalisation
Toutes	Toutes	Tous	Interdire	Oui

Certaines solutions techniques appliquent automatiquement une règle d'interdiction à la fin de la politique de filtrage, mais celle-ci n'est généralement pas journalisée ou n'apparaît pas explicitement à la fin de la politique ; c'est la raison pour laquelle une règle finale **explicite** est ajoutée dans tous les cas.

R6	L'ajout d'une règle explicite d'interdiction finale journalisée garantit l'application du modèle de sécurité positif (tout ce qui n'a pas été autorisé précédemment est interdit) et permet de conserver la trace des flux non légitimes.

4 Mise en forme d'une politique de filtrage réseau

La lisibilité et la maintenabilité d'une politique de filtrage dépend avant tout de sa forme ; c'est la raison pour laquelle il est primordial de définir et de documenter les conventions à respecter lors de son élaboration et de sa mise à jour.

Une politique de filtrage se traduit par une liste de règles, elles même composées d'objets de différentes natures :

- des machines (Une adresse IP) ;
- des réseaux (Une adresse de réseau combinée à un masque) ;
- des plages réseau (Une suite d'adresses IP consécutives) ;
- des services (tcp, udp, autres) ;
- des groupes d'objets.

R7	La gestion rigoureuse d'une politique de sécurité commence par la définition précise de la représentation des objets et des règles qui la composent.

4.1 Mise en forme des objets

4.1.1 Convention de nommage

La définition d'une convention de nommage rigoureuse pour chacun des types d'objets utilisés dans la politique de sécurité facilite les opérations suivantes :

- la recherche (dans une liste de taille conséquente) ;
- la manipulation (tri, mise à jour, suppression) ;
- l'audit.

Plusieurs orientations sont possibles pour définir une convention de nommage, voici deux exemples :

- Convention de nommage fonctionnelle : les objets sont nommés en fonction de leur rôle, par exemple : srv_dns-interne, tcp_appli1.
- Convention de nommage technique : les objets sont nommés en fonction d'une caractéristique technique qui leur est propre (adresse IP, nom d'hote, port), par exemple : srv_appollo, tcp_21000.

Le choix de l'orientation d'une convention dépend d'éléments liés au contexte, en particulier de la connaissance précise du métier. Il est possible de combiner différentes conventions, mais il faut garder à l'esprit de ne pas trop alourdir la lecture. La solution technique utilisée pourra également être un facteur limitant à prendre en considération (existence d'une taille maximale des noms d'objets ou

encore présence de termes réservés). La casse fait également partie des paramètres à définir dans la convention.

R8	Une convention de nommage doit être définie pour l'ensemble des types d'objets qui composent les règles de la politique de filtrage.

4.1.2 Convention de mise en forme

Certaines solutions offrent la possibilité de colorer une partie des objets (machine, réseau, plage réseau), c'est un moyen supplémentaire utilisé pour augmenter la lisibilité de la politique de sécurité. Des incohérences grossières peuvent ainsi être détectées visuellement plus rapidement.
La logique consiste à utiliser une couleur pour l'ensemble des objets appartenant à une même zone, le code couleur est établi en fonction d'un critère ; par exemple :

- Le niveau de confiance de la zone : un jeu de dégradé est choisi afin d'associer une couleur à chacun des niveaux de confiance existant dans l'architecture. Le tableau 1 est un exemple illustrant ce type de code couleur :

Couleur	Type de zone
	Réseau externe
	DMZ publique
	DMZ privée
	Réseau interne

TABLE 1 – Coloration selon le niveau de confiance

- Le rôle de la zone : une couleur est associée selon un critère fonctionnel des différents types de zone existant dans l'architecture. Le tableau 2 est un exemple illustrant ce type de code couleur :

Couleur	Type de zone
	DMZ hébergeant les serveurs d'authentification
	DMZ hébergeant les serveurs de base de données
	DMZ hébergeant les *proxys*
	DMZ hébergeant les *reverse proxys*

TABLE 2 – Coloration selon un critère fonctionnel

R9	La définition d'une convention de coloration des objets qui composent les règles de sécurité est une aide supplémentaire à la compréhension de la politique.

4.2 Mise en forme des règles de sécurité

4.2.1 Convention de nommage

4.2.1.1 Nommage des règles

Certaines solutions permettent d'attribuer un nom aux règles de sécurité, ce champ est utilisé pour aider à la compréhension de la politique, des flêches peuvent être employées pour indiquer le sens de communication que chacune des règles doit transcrire.

Exemple : Relais DNS -> DNS publiques

4.2.1.2 Commentaires des règles

Certaines solutions autorisent l'ajout de commentaires aux règles de sécurité, ce champ est utilisé pour décrire plus précisement la signification de chacune des règles composant la politique de filtrage. Voici une liste non exhaustive d'éléments qui peuvent apparaître dans un commentaire :

- le descriptif fonctionnel de la règle ;
- la date d'implémentation ou de mise à jour de la règle dans un format court ;
- la référence de la demande dans l'outil de gestion de tickets (s'il existe) qui a conduit à la création ou à la modification de la règle ;
- l'identifiant de l'intervenant qui a implémenté ou mis à jour la règle dans un format court.

Les éléments choisis doivent être réfléchis et adaptés au contexte, la solution technique utilisée pourra également être un facteur limitant à prendre en considération lors du choix des éléments à inclure dans les commentaires (taille maximale du champ commentaire par exemple).

R10	Si des champs textuels éditables spécifiques à chacune des règles de sécurité sont disponibles, il est important de les utiliser pour expliciter le contenu de la politique de filtrage. Les élements constitutifs de ces champs doivent respecter une structure préalablement définie et adaptée au contexte.

4.3 Séparateurs de règles

Certaines solutions sont capables de scinder la politique de filtrage à l'aide de séparateurs de règles, cette fonctionnalité est utilisée pour augmenter la lisibilité de la politique et faciliter son exploitation. Ces séparateurs sont employés pour faire apparaître les sections présentées précédemment et mettre en évidence les regroupements opérés pour les flux métiers (contenu de la section n°4). Si les séparateurs disposent d'un champ texte éditable, une convention de nommage doit également être définie pour celui-ci.

Voici une illustration simple reprenant les 6 sections et quelques exemples de flux métiers :

Section	Intitulé du séparateur
1	Flux à destination de la passerelle
2	Flux émis par la passerelle
3	Règle de protection de la passerelle
4	Flux métiers
	–|Flux d'accès aux bases de données
	––|Flux concernant la ferme 1 de bases de données
	––|Flux concernant la ferme 2 de bases de données
	–|Flux d'accès aux *proxys*
	––|Flux concernant le *proxy* x
	––|Flux concernant le *proxy* y
5	Règles "antiparasites"
6	Règle d'interdiction finale

5 Bonnes pratiques d'ordre général

5.1 Désactivation des flux implicites

Certaines solutions permettent l'ouverture de flux implicites dans le but de faciliter l'administration de la passerelle ou de simplifier l'ouverture de services considérés parfois à tort comme non risqués. Malheureusement cela conduit souvent à l'ouverture de règles trop permissives ou méconnues des administrateurs.

Voici le type de flux implicites que l'on peut rencontrer :

- flux nécessaires à l'administration de la passerelle (https, ssh) ;
- flux nécessaires au fonctionnement de la passerelle (snmp, ntp, syslog) ;
- flux permettant l'établissement des VPN (IKE, IPsec) ;
- flux DNS ;
- flux ICMP.

R11	Une gestion rigoureuse de la politique de filtrage conduit à désactiver les flux implicites s'ils existent et si la désactivation est possible ; les flux légitimes quels qu'ils soient doivent être définis manuellement et précisément par les administrateurs.

L'objectif de cette démarche est double :

- porter à la connaissance des administrateurs l'ensemble des règles de sécurité appliquées par le pare-feu ;
- réduire la surface d'attaque de la passerelle et des réseaux qu'elle protège on n'autorisant que les flux stritement nécessaires au besoin.

5.2 Vérification de la séquence de démarrage

Un pare-feu peut être vulnérable lors de sa séquence de démarrage. En effet, durant le laps de temps qui sépare l'allumage électrique de l'équipement et l'application effective de la politique de filtrage réseau, le pare-feu peut se retrouver dans un état ne lui permettant pas d'assurer la sécurité des réseaux qu'il protège ainsi que sa propre protection. Dans le pire des cas, le pare-feu ne filtrera pas les paquets et les routera en effectuant aucun contrôle. Il convient donc de vérifier à quelle étape de la séquence de démarrage le routage s'active sur l'équipement.

R12	Afin d'éviter toute exposition inutile des réseaux et du pare-feu, il est recommandé de se documenter sur le fonctionnement précis de la solution employée, de réaliser des tests et de prendre en considération leurs résultats lors des opérations nécessitant un redémarrage de l'équipement (maintenance par exemple).

6 Documentation, validation et maintenance

6.1 Documentation

Les choix réalisés en application des bonnes pratiques décrites dans ce guide doivent être formalisés dans un document transmis à l'ensemble des intervenants opérant sur les pare-feux concernés. L'effort de rédaction est nécessaire pour assurer le respect des consignes au delà des personnes qui les ont établies.

R13	Les consignes permettant la gestion des politiques de filtrage réseau doivent être documentées et diffusées aux personnes en charge de la mise en oeuvre et la gestion des pare-feux.

6.2 Validation

Les politiques de filtrage mises en place doivent être validées en pratique pour s'assurer que la solution technique adoptée se comporte correctement (utilisation d'outil d'analyse réseau par exemple). Le respect du modèle présenté dans ce document contribue au maintien des politiques de filtrage, mais il ne permet pas de se prémunir contre certaines erreurs humaines ou certains fonctionnements spécifiques ; charge à l'administrateur de rester vigilant quant à la compréhension des opérations qu'il exécute.

R14	Une politique de filtrage réseau doit être testée une fois implémentée.

6.3 Maintenance

Pour conserver son efficacité et sa fonction de sécurisation, une politique de filtrage doit être passée en revue régulièrement.

Ces vérifications ont pour objectifs :

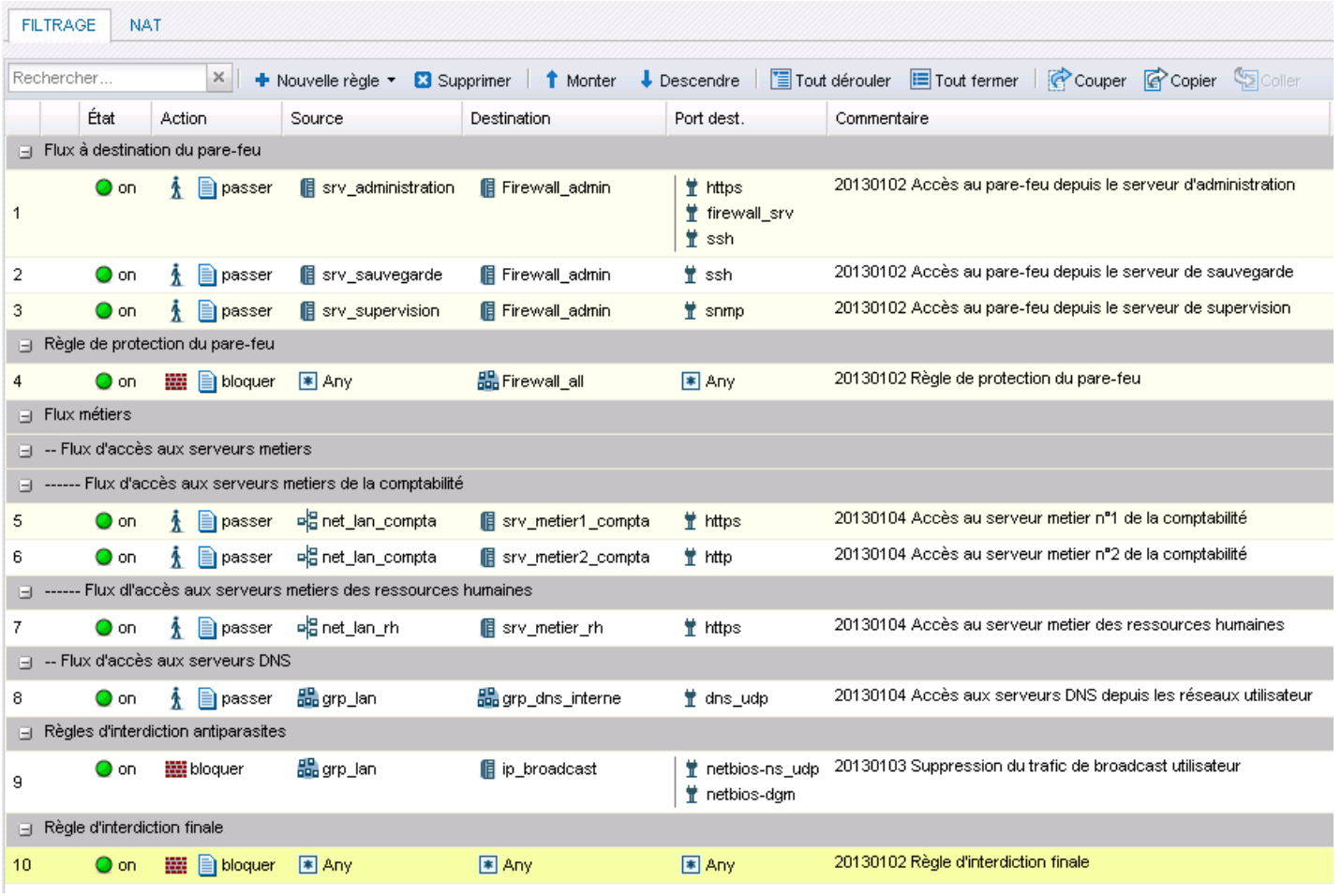
- de supprimer les règles temporaires obsolètes créées depuis la dernière revue ;
- de corriger les éventuels écarts par rapport aux conventions en vigueur ;
- de vérifier la cohérence des règles ajoutées depuis la dernière revue : origine, utilité, précision, etc.

La présence de mécanismes techniques ou organisationnels visant à conserver sous contrôle la politique de filtrage ne dispense pas de la réalisation de ces revues régulières.

R15	Une politique de filtrage réseau doit être passée en revue à une fréquence bi-annuelle ou annuelle à minima.

7 Illustration

Une partie des recommandations présentées dans ce document sont illustrées à l'aide d'un jeu de règles simple défini sur un pare-feu NetAsq (solution qualifiée par l'ANSSI).



FILTRAGE | NAT

Rechercher... | Nouvelle règle | Supprimer | Monter | Descendre | Tout dérouler | Tout fermer | Couper | Copier | Coller

	État	Action	Source	Destination	Port dest.	Commentaire
Flux à destination du pare-feu						
1	on	passer	srv_administration	Firewall_admin	https firewall_srv ssh	20130102 Accès au pare-feu depuis le serveur d'administration
2	on	passer	srv_sauvegarde	Firewall_admin	ssh	20130102 Accès au pare-feu depuis le serveur de sauvegarde
3	on	passer	srv_supervision	Firewall_admin	snmp	20130102 Accès au pare-feu depuis le serveur de supervision
Règle de protection du pare-feu						
4	on	bloquer	Any	Firewall_all	Any	20130102 Règle de protection du pare-feu
Flux métiers						
-- Flux d'accès aux serveurs metiers						
------ Flux d'accès aux serveurs metiers de la comptabilité						
5	on	passer	net_lan_compta	srv_metier1_compta	https	20130104 Accès au serveur metier n°1 de la comptabilité
6	on	passer	net_lan_compta	srv_metier2_compta	http	20130104 Accès au serveur metier n°2 de la comptabilité
------ Flux dl'accès aux serveurs metiers des ressources humaines						
7	on	passer	net_lan_rh	srv_metier_rh	https	20130104 Accès au serveur metier des ressources humaines
-- Flux d'accès aux serveurs DNS						
8	on	passer	grp_lan	grp_dns_interne	dns_udp	20130104 Accès aux serveurs DNS depuis les réseaux utilisateur
Règles d'interdiction antiparasites						
9	on	bloquer	grp_lan	ip_broadcast	netbios-ns_udp netbios-dgm	20130103 Suppression du trafic de broadcast utilisateur
Règle d'interdiction finale						
10	on	bloquer	Any	Any	Any	20130102 Règle d'interdiction finale

FIGURE 1 – Politique de filtrage réseau sur NetAsq

Les flux émis par le pare-feu (section n°2) n'apparaissent pas dans l'exemple ci-dessous car ils sont définis implicitement (par exemple ntp et syslog) par la solution technique employée.