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 4 août 2016

N° DAT-NT-32/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 18

Note technique

Recommandations et méthodologie pour le nettoyage 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 et méthodologie pour le nettoyage 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
BRT, LRP	BSS	SDE	4 août 2016

Évolutions du document :

Version	Date	Nature des modifications
1.0	4 août 2016	Version initiale

Pour toute question :

Contact	Adresse	@mél
Division Assistance Technique de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	conseil.technique@ssi.gouv.fr

Table des matières

1 Préambule

Ce document s'incrit dans la suite logique d'une précédente publication ANSSI intitulée *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*[1]. Il a pour objectif de proposer un cadre permettant « d'assainir » la politique de filtrage réseau d'un pare-feu d'interconnexion dont la maîtrise ou la compréhension n'est plus garantie.

Les pare-feux ont connu des évolutions récentes importantes et sont par exemple maintenant dotés de fonctionnalités permettant l'analyse des flux au niveau applicatif. Cependant, les politiques de filtrage au niveau réseau jouent encore un rôle très important dans la sécurisation des systèmes d'information et doivent à ce titre être parfaitement maîtrisées avant de mettre en place des contrôles avancés des flux.

La perte de contrôle d'une politique de filtrage d'un pare-feu d'interconnexion peut avoir différentes causes, parmi lesquelles :

- la complexité de la politique de filtrage, qui peut dans certains cas contenir plusieurs centaines (voire des milliers) de règles ;
- l'absence de conventions précises régissant la rédaction des politiques de pare-feu (règles techniques ou organisationnelles) ;
- le renouvellement trop fréquent des personnes en charge de l'exploitation des pare-feux ;
- le manque de maîtrise de la cartographie des systèmes d'information.

La conséquence évidente de la perte de contrôle d'une politique de filtrage d'un pare-feu est l'autorisation de flux illégitimes. La présence de ce type de flux expose davantage le système d'information à de nombreuses attaques (intrusion, vol de données, etc.). Mais cela peut également faciliter l'exploration du réseau par un utilisateur mal intentionné ou par un attaquant qui aurait déjà compromis une partie du système d'information. Enfin, maintenir une politique de filtrage la plus simple possible permet de réduire les coûts de maintenance du système d'information.

Ce document s'articule en deux parties. Dans un premier temps sont présentées les informations utiles qui permettent de détecter des anomalies dans une politique de filtrage et donc l'usage réel de cette dernière. La seconde partie présente une méthode de nettoyage de politique de filtrage qui s'appuie sur ces informations. Le schéma 1, en annexe de ce document, synthétise la logique générale de la méthode proposée.

Ce document a vocation à proposer une méthode de nettoyage d'une politique de filtrage. Cette méthode n'est pas la seule qui existe et elle n'est pas forcément adaptée à tous les contextes.
Il revient au lecteur de vérifier que cette méthode est adaptée à son contexte d'emploi.

2 Prérequis

Le nettoyage d'une politique de filtrage d'un pare-feu a deux objectifs principaux :

1. rendre cohérents et compréhensibles la politique de filtrage et les objets qui la composent ;
2. restreindre au maximum la politique de filtrage pour qu'elle n'autorise que les flux légitimes.

Deux sources de données sont utilisées pour conduire ce processus :

1. Se reporter à http://www.ssi.gouv.fr/politique-filtrage-parefeu.

– **la politique de filtrage :** l'analyse de la politique de filtrage et des objets qui la composent permet de détecter certaines incohérences « structurelles » (les règles en double par exemple) ;
– **les fichiers de journaux issus de cette politique de filtrage :** l'analyse du contenu de ces fichiers permet d'obtenir des indicateurs relatifs à l'usage réel de la politique de sécurité (une règle qui n'est pas utilisée par exemple).

Pour que la démarche proposée dans ce document soit applicable, plusieurs prérequis concernant ces sources de données doivent être remplis.

2.1 Politique de filtrage

Voici les prérequis qui doivent être respectés par la politique de filtrage :
– la politique doit être parcourue séquentiellement (de « haut en bas ») ;
– lorsqu'un flux correspond à une règle de filtrage, la décision associée à cette règle est appliquée [2]. La suite de la politique ne doit pas être évaluée pour ce flux ;
– chaque règle doit disposer d'un identifiant unique indépendant de sa position dans la politique de filtrage. Cet identifiant n'est pas nécessairement visible par l'administrateur depuis l'interface d'administration de la solution. Cet identifiant doit apparaître dans la configuration détaillée de la politique de filtrage, il permet de garantir la cohérence dans le temps entre une règle et les évènements qu'elle génère ;
– les règles qui autorisent les flux métiers doivent être placées avant les règles d'interdiction regroupées à la fin de la politique. Il existe au moins une règle d'interdiction finale qui bloque l'ensemble des flux qui ne sont pas explicitement acceptés avant. L'organisation de la politique de filtrage doit être si possible conforme à celle détaillée dans la note technique ANSSI intitulée *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu.*

2.2 Fichiers de journaux

Voici les prérequis qui doivent être remplis par les fichiers de journaux :
– lorsqu'un évènement associé à une règle de filtrage est journalisé, il doit contenir l'identifiant unique correspondant à cette règle. Cela permet d'assurer la cohérence dans le temps entre la règle et les évènements qu'elle engendre, et ce quelle que soit la position de la règle dans la politique ;
– l'horloge du pare-feu doit être à l'heure et si possible synchronisée sur un serveur de temps interne.

2.3 Méthode d'extraction des informations

Les deux sources de données mentionnées précédemment doivent être traitées afin d'obtenir des informations permettant de conduire des actions correctrices sur la politique de filtrage. Ces traitements peuvent être complexes à mener car :
– la politique de filtrage peut être importante en taille (plusieurs centaines/milliers de règles) et difficilement lisible dans sa globalité, que ce soit à partir de l'interface d'administration de la solution de pare-feu ou à partir de sa forme exportée (fichier texte, html, xml, etc.) ;
– les journaux d'évènements produits par une politique de filtrage d'un pare-feu peuvent rapidement représenter un volume de données très important, en particulier si la période d'analyse choisie est longue.

2. Logique dite de *first-match.*

Si l'analyse manuelle de ces deux sources de données est théoriquement possible, cette méthode est difficilement envisageable lorsque la politique de filtrage est composée de plusieurs dizaines de règles et lorsqu'elle génère plusieurs dizaines de mégaoctets (voir plusieurs gigaoctets) de fichiers de journaux par jour.

Pour extraire des informations utiles de ces deux sources de données, il est préférable de s'appuyer sur des outils automatisés, par exemple :

- la solution de pare-feu elle-même peut parfois indiquer les anomalies présentes dans une politique de filtrage et/ou fournir des indicateurs concernant l'usage réel de la politique de filtrage ou des objets qui la composent ;
- une solution tierce d'analyse de configurations et de journaux de pare-feux [3] ;
- une solution d'analyse de mégadonnées (ou *Big Data*) ;
- des scripts développés spécifiquement pour traiter les données de la solution de pare-feu employée.

Le choix de l'outillage peut dépendre de la technologie de pare-feu et de l'éventuel écosystème qui l'accompagne. Il est possible d'appliquer des traitements automatisés à la politique de filtrage ou aux journaux d'évènements uniquement s'il est possible de les extraire de la solution de pare-feu (export de fichiers, interrogation à l'aide d'une API, etc.).

R1 - Utiliser des outils d'analyse automatisée

Pour mettre en œuvre la méthode présentée dans ce document, il est recommandé de disposer d'outils permettant l'analyse automatisée des politiques de filtrage pare-feu et des fichiers de journaux produits.

Dans la suite de ce document, il est fait l'hypothèse que la solution d'analyse est « idéale » et qu'elle permet d'extraire l'ensemble des informations présentées dans la section 3 et employées dans la méthode décrite à la section 4. Le lecteur doit donc adapter la méthode proposée en fonction des outils et des informations qui sont réellement à sa disposition.

3 Définition des informations utiles et des traitements associés

Cette section a pour objectif de présenter les informations utiles qui seront ensuite utilisées dans la méthodologie de nettoyage détaillée à la section 4 de ce document.

3.1 Anomalies de la politique de filtrage

L'analyse de la politique de filtrage permet de détecter certaines anomalies au niveau des objets et des règles qui la composent. Ces incohérences peuvent être décelées sans avoir à corréler le contenu de la politique avec une autre source de données (les journaux par exemple).

3.1.1 Anomalies concernant les objets

Les règles qui constituent une politique de filtrage sont généralement définies à l'aide d'objets (adresse IP, service, etc.) présents dans une base de données propre à la solution de pare-feu employée.

3. Désignée parfois en anglais sous le terme de *Network Aware Firewall Policy Assessment*.

Cette base d'objets peut dans certains cas être utilisée pour définir plusieurs politiques de filtrage (administration centralisée de plusieurs pare-feux à partir d'un même serveur de configuration). Chacun des objets constituant cette base possède des caractéristiques minimales qui lui sont propres, par exemple :

- un objet représentant un réseau (ou une machine) est généralement défini par les caractéristiques suivantes : une adresse IP, un masque réseau et un nom d'objet ;
- un objet représentant un service est généralement défini par les caractéristiques suivantes : un numéro de protocole IP, un type de protocole (TCP/UDP), des numéros de port source et destination et un nom d'objet ;
- un objet représentant un groupe d'objets est généralement défini par les caractéristiques suivantes : la liste des objets (ou groupes d'objets) qui le compose et un nom d'objet.

3.1.1.1 Objets doublons

La détection des objets doublons a pour objectif d'identifier les objets qui portent des noms différents mais dont les autres caractéristiques sont rigoureusement identiques. Il est en effet fréquent que des objets définis en double coexistent dans une même base d'objets et qu'ils soient par conséquent utilisés dans plusieurs règles de filtrage. En effet, les solutions de pare-feu n'obligent généralement pas les objets à être uniques (un avertissement peut être affiché à la création d'un nouvel objet).

La multiplicité d'objets aux caractéristiques identiques engendre de nombreux problèmes dans la mise en œuvre des politiques de pare-feu (perte de sens, difficultés de mise à jour, accroissement de la base d'objets). La présence de ce type d'objets complique également la production d' indicateurs, en particulier ceux relatifs à l'usage réel des objets constituant la base.

Exemple d'objets doublons :

nom d'objet	adresse IP	masque réseau
`srv_bdd`	`192.168.10.1`	`255.255.255.255`
`srv_mysql`	`192.168.10.1`	`255.255.255.255`

R2 - Identifier les objets doublons

Il est recommandé d'identifier les objets identiques en double.

En fonction de la solution de pare-feu employée, un objet peut être défini par de nombreuses caractéristiques. Un objet associé à un service peut par exemple inclure des paramètres définissant le comportement que doit adopter le pare-feu au niveau de sa table de connexion (timeout associé au service par exemple). La comparaison entre deux objets doit donc être extrêmement précise et prendre en compte les spécificités de la solution employée avant de considérer les deux objets comme étant parfaitement identiques.

3.1.1.2 Objets inutilisés

Les mises à jour successives d'une politique de filtrage d'un pare-feu tout au long de son cycle d'exploitation conduisent à la modification ou à la suppression de règles de filtrage. Ces interventions

peuvent induire des dérives au niveau de la base d'objets, elles peuvent conduire à l'apparition d'objets « orphelins », c'est-à-dire des objets définis par les administrateurs mais qui ne sont utilisés dans aucune politique de filtrage (sont exclus les objets présents à l'initialisation de la solution). La présence de ce type d'objets accroit inutilement la taille de la base et peut être source d'erreur ou d'incompréhension.

R3 - Identifier les objets inutilisés

Il est recommandé d'identifier les objets inutilisés.

3.1.2 Anomalies concernant les règles de filtrage

3.1.2.1 Règles redondantes

Une règle est considérée comme redondante si elle autorise un trafic réseau déjà permis par une autre règle placée en amont dans la politique de filtrage. La présence de telles règles est caractéristique d'une politique de filtrage dont la gestion a dérivé avec le temps et qui ne représente plus rigoureusement les flux métiers qu'elle doit autoriser. Ce type de règle est une source importante d'erreurs d'exploitation qui peuvent conduire à l'affaiblissement du niveau de sécurité par l'autorisation de flux illégitimes. Plusieurs cas de règles redondantes sont possibles :

Cas n°1 : la règle redondante est rigoureusement identique à celle placée en amont. Dans ce cas il est possible de supprimer l'une des deux règles facilement, le choix de la règle à supprimer dépend de l'organisation adoptée au niveau de la politique de filtrage (se reporter à la note technique intitulée *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*).

Prenons l'exemple suivant :

Id.	source	destination	service	action
Section 1				
R1	srv_web	srv_bdd	tcp_mysql	autoriser
Section 2				
R2	...	...	...	...
Section 3				
R3	srv_web	srv_bdd	tcp_mysql	autoriser

Les règles R1 et R3 sont identiques si les propriétés des objets qui les composent sont identiques, il est donc possible de supprimer l'une des deux sans affecter la politique de filtrage.

Cas n°2 : la règle redondante « contient » rigoureusement la règle située en amont, cela signifie qu'il est facile de modifier la politique de filtrage pour faire disparaître la redondance.

L'exemple suivant illustre ce cas :

Id.	source	destination	service	action
Section 1				
R1	srv_web_compta	srv_bdd_prod	tcp_mysql	autoriser
Section 2				
R2	...	...	...	...
Section 3				
R3	srv_web_compta srv_web_rh	srv_bdd_prod	tcp_mysql	autoriser

La politique peut être modifiée de différentes façons pour faire disparaitre la redondance :
– soit la règle `R1` est supprimée ;
– soit l'objet `srv_web_compta` est supprimé de la règle `R3`.
Le choix est principalement conditionné par la logique retenue pour organiser la politique de filtrage.

Cas n°3 : la règle redondante « contient » la règle située en amont, mais il est difficile de la modifier pour qu'elle ne soit plus redondante (règle d'autorisation ouverte trop largement). Dans ce cas la règle redondante doit être « affinée » (processus « d'affinage » itératif décrit dans la section 5) pour que la redondance puisse disparaître.

Un tel cas est illustré dans l'exemple suivant :

Id.	source	destination	service	action
Section 1				
R1	srv_web_compta	srv1_bdd_prod	tcp_mysql	autoriser
Section 2				
R2	...	...	...	...
Section 3				
R3	srv_web_compta	net_bdd_prod	tcp_mysql	autoriser

Si l'adresse IP de l'objet `srv1_bdd_prod` appartient au réseau `net_bdd_prod`, la règle `R3` est en partie redondante vis-à-vis de la règle `R1`. Plusieurs solutions sont envisageables pour supprimer la redondance :
– la règle `R3` représente réellement le besoin métier, elle n'est pas jugée trop permissive (autorisation du flux à destination d'un réseau entier) : la règle `R1` peut être désactivée avant d'être définitivement supprimée. Cette solution simple n'a aucun impact sur le comportement de la politique de filtrage (au delta près de la durée de parcours de la politique), le trafic précédemment autorisé par la règle R1 va maintenant être autorisé par la règle `R3` ;
– la règle `R3` ne représente pas correctement le besoin métier, elle est jugée trop permissive et la règle `R1` correspond bien à une partie du besoin métier : la règle `R1` ne doit pas être supprimée car cela représenterait une perte de sens et d'information. Pour supprimer la redondance, la règle `R3` doit passer par un processus « d'affinage » itératif (décrit dans la section 5) permettant à terme sa suppression.

R4 - Identifier et catégoriser les règles redondantes

Il est recommandé d'identifier et de catégoriser les règles redondantes dans la politique de filtrage.

3.1.2.2 Règles désactivées

Une politique de filtrage peut comporter des règles désactivées, la présence de ce type de règle est généralement due à l'arrêt de certains éléments du système d'information. La suppression de ces règles contribue à rendre plus lisible la politique de filtrage. Cependant, des règles désactivées peuvent être provisionnées pour de nouveaux projets, elles ne seront activées que lors de la mise en production de ces derniers.

R5 - Marquer les règles désactivées à conserver

Il est recommandé de disposer d'un marquage spécifique (commentaire daté, section, etc.) permettant d'identifier correctement les règles volontairement désactivées afin d'éviter leur suppression durant le processus de nettoyage de la politique de filtrage.

3.2 Indicateurs issus de l'analyse des journaux de trafic

L'analyse des journaux de trafic permet d'obtenir des indicateurs relatifs à l'usage réel de la politique de filtrage en place sur un pare-feu. La pertinence de cette source de données est dépendante de plusieurs critères :

- des règles de filtrage (d'autorisation) pour lesquelles la journalisation est activée : si une règle ne journalise pas son activité, il est impossible de déterminer des indicateurs relatifs à son usage réel à l'aide des journaux produits par le pare-feu. Il est donc nécessaire de s'assurer que la journalisation est activée pour les règles de filtrage que l'on souhaite nettoyer ;
- de la durée de l'analyse : si les journaux issus de la politique de filtrage sont étudiés sur un intervalle de temps trop court, les indicateurs obtenus risquent de ne pas être représentatifs de l'activité réelle. Si l'étude se déroule par exemple sur quinze jours, les journaux générés par une règle autorisant une sauvegarde mensuelle n'apparaîtront peut-être pas. A contrario, l'analyse des journaux de trafic sur une très longue période sera trop couteuse (volumes de données trop importants) pour obtenir des indicateurs dans des délais acceptables. L'étude de journaux trop anciens risque également de prendre en compte les évènements correspondant à des règles associées à des éléments qui ont été retirés du système d'information.

R6 - Activer la journalisation sur toutes les règles à nettoyer

> Afin de mener une analyse pertinente, il est recommandé d'activer la journalisation sur toutes les règles de filtrage à nettoyer. Dans le cas contraire, l'application de cette méthode risque de mener à la suppression ou à la modification intempestive de certaines règles.

R7 - Analyser les journaux sur une période représentative

> Pour mener une analyse pertinente, il est nécessaire de travailler sur une période représentative de l'activité normale du système d'information. Il devra être vérifié que celle-ci est suffisamment longue et ne comporte pas d'évènements exceptionnels susceptibles de perturber les statistiques.

3.2.1 Règles inutilisées

Si une règle journalisée ne produit pas de journaux durant l'intervalle de temps retenu pour l'analyse (jugé suffisant pour contenir l'ensemble des flux « actuels »), cela signifie qu'elle n'est pas utilisée. Ce phénomène peut avoir plusieurs origines :

- il s'agit d'une règle redondante. Une autre règle présente en amont dans la politique autorise déjà le trafic décrit par cette règle (se reporter au paragraphe 3.1.2.1), elle n'est donc jamais parcourue lorsque le trafic qu'elle autorise passe par le pare-feu ;
- il s'agit d'une règle correspondant à un projet qui a été retiré de la production. Cela signifie que la règle n'a pas été correctement décommissionnée de la politique de filtrage lors de l'arrêt de ce projet ;
- il s'agit d'une règle qui n'est utilisée que dans une situation très particulière, non couverte par l'intervalle de temps retenu (une règle relative à un PCA [4] par exemple). Dans ce cas il est nécessaire de l'identifier à l'aide d'un marqueur (un commentaire par exemple) pour s'assurer qu'elle ne sera pas supprimée durant le processus de nettoyage.

4. Plan de Continuité d'Activité.

R8 - Identifier les règles inutilisées

Il est recommandé d'identifier les règles inutilisées en analysant les journaux d'évènements produits par la politique de filtrage.

3.2.2 Objets inutilisés dans les règles

Une règle de filtrage peut contenir plusieurs objets (ou groupes d'objets), aussi bien en source, en destination ou en service. Lorsqu'un flux est autorisé par cette règle (journalisée), l'évènement généré ne contient qu'une adresse IP en source, une adresse IP en destination et un seul service. En comptant le nombre d'occurrences d'un objet dans les journaux générés par une règle de filtrage durant l'intervalle de temps de l'étude, il est possible de déterminer l'usage réel de cet objet pour cette règle. Si aucun des évènements générés par la règle ne contient un des objets qui la compose, cela signifie que sa présence dans la règle n'est pas utile, il peut donc être retiré de la règle.

L'exemple suivant illustre ce propos :

Id.	source	destination	service	action
R3	srv_web_compta srv_web_rh	srv_bdd_prod	tcp_mysql	autoriser

Si les journaux de trafic générés par la règle `R3` ne contiennent en source que l'adresse IP de l'objet `srv_web_compta`, l'objet `srv_web_rh` peut alors être retiré de la règle (si l'intervalle de temps retenu est jugé suffisant).

R9 - Identifier les objets inutilisées dans les règles de filtrage

Il est recommandé d'identifier les objets inutilisés dans les règles de filtrage en analysant les journaux d'évènements produits par ces dernières.

4 Méthodologie de nettoyage

La méthode proposée s'incrit dans un cycle permanent de maintien en condition de sécurité d'une politique de filtrage d'un pare-feu, elle sera d'autant plus pertinente si elle est rejouée à intervalles réguliers.

La méthode seule n'est pas suffisante. Elle apporte uniquement un cadre et doit être conduite par des personnes qui disposent d'une connaissance précise du contexte d'usage du pare-feu étudié.

R10 - Nettoyer les règles de pare-feu régulièrement

Il est recommandé de jouer régulièrement (fréquence biannuelle par exemple) la méthodologie de nettoyage sur l'ensemble des pare-feux d'interconnexion.

Le nettoyage d'une politique de filtrage d'un pare-feu peut avoir un fort impact au niveau des flux métiers (suppression malencontreuse d'une règle ou d'un objet), l'administrateur doit donc prendre

les précautions nécessaires tout au long des manipulations. Il doit en en particulier communiquer avec les équipes métier et valider au préalable les procédures de sauvegarde et de restauration.

Lorsqu'une architecture réseau comporte plusieurs pare-feux, une logique doit être établie dans l'ordre de traitement des différentes politiques de filtrage afin d'optimiser les moyens mis en œuvre. Lorsque les politiques de filtrage de différents pare-feux intègrent des règles identiques, le travail de nettoyage doit être réalisé de concert afin de conserver la cohérence entre les différentes politiques.

4.1 Préparation

Avant de débuter le nettoyage d'une politique de filtrage, il est nécessaire de vérifier les points suivants :

- un modèle d'organisation est défini pour la politique de filtrage et une convention de nommage est choisie pour définir les objets qui la composent (se référer à la note technique ANSSI *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*[5]) ;
- une convention de marquage est définie pour repérer les règles de filtrage qui ne doivent pas être supprimées ou qui ont déjà fait l'objet d'un traitement (ajout d'un marqueur daté dans le champ « commentaire » de la règle par exemple) ;
- les mécanismes de sauvegarde et de restauration de la politique de filtrage sont fonctionnels et correctement maitrisés.

4.2 Étape 1 : mise en conformité

La première étape consiste à mettre en conformité la politique de filtrage en effectuant quelques modifications n'ayant aucun impact sur le contrôle de flux.

R11 - Mettre la politique de filtrage en conformité

Il est recommandé d'effectuer dans l'ordre indiqué les actions suivantes,

1. **Traitement des règles désactivées :** ces règles doivent être soit marquées comme étant volontairement désactivées (ajout de règles en vue de la mise en production d'un projet par exemple), soit être supprimées (ancien projet dont les règles sont encore présentes par exemple) ;
2. **Suppression des objets inutilisés :** les objets qui ne sont utilisés dans aucune politique de filtrage doivent être supprimés afin d'alléger la base d'objets et éviter les fausses manipulations ;
3. **Fusion des objets en double :** les objets qui présentent les mêmes caractéristiques doivent être fusionnés, renommés en respectant les conventions en vigueur et remplacés dans les règles concernées ;
4. **Application de la convention de nommage :** les objets restants doivent être vérifiés et renommés si nécessaire en respectant la convention en vigueur[6].

5. Se reporter à http://www.ssi.gouv.fr/politique-filtrage-parefeu.
6. Il est possible d'utiliser celle proposée dans la note technique ANSSI relative à la définition d'une politique de filtrage pare-feu.

4.3 Étape 2 : suppression des règles inutilisées

Les règles qui apparaissent comme n'étant pas utilisées sur la période d'analyse peuvent normalement être supprimées de la politique si elles ne sont pas identifiées comme étant des règles très spécifiques (se reporter au paragraphe 3.2.1). Cette opération comporte des risques (coupure de flux) et doit donc être conduite avec prudence.

Les règles ainsi désactivées doivent être marquées et la date de désactivation doit être indiquée. Une fois désactivées, elles pourront être supprimées définitivement après un intervalle de temps à définir par l'administrateur en fonction de son contexte (de quelques jours à quelques semaines par exemple).

R12 - Analyser les règles inutilisées avec les personnes concernées

> Afin d'éviter tout risque d'interruption de service, il est recommandé de contacter la ou les personnes en charge du périmètre métier couvert par les règles concernées afin de comprendre pourquoi ces règles n'ont pas été utilisées durant la période observée.

R13 - Désactiver puis supprimer les règles inutilisées

> Une fois l'aval des équipes métier concernées obtenu, il est recommandé de désactiver les règles inutilisées. Dans un premier temps, les règles doivent être conservées pour permettre un retour arrière en cas d'erreur d'analyse.
> Après un temps de validation suffisamment long, les règles inutilisées peuvent être supprimées définitivement.

R14 - Désactiver les règles par petit lot

> Afin d'éviter les effets de bord et pour faciliter la résolution d'incident en cas de problème, il est recommandé de désactiver les règles par petit lot (n règles par semaine par exemple).

Après chaque suppression de règles, des objets inutilisés peuvent apparaître, il est nécessaire de les supprimer pour alléger progressivement la base. Une sauvegarde de la politique de filtrage et des objets qui la composent doit être réalisée après le traitement de chaque lot.

4.4 Étape 3 : suppression des règles redondantes

L'objectif de l'étape 3 est de catégoriser les règles redondantes selon la méthode proposée dans le paragraphe 3.1.2.1 en vue de leur simplification ou de leur suppression.

R15 - Supprimer les règles redondantes

Il est recommandé de catégoriser les règles redondantes selon la méthode détaillée dans le paragraphe 3.1.2.1. Lorsque les redondances sont similaires à l'un des deux premiers cas exposés, la politique de filtrage peut être simplifiée rapidement et sans impact sur les flux qu'elle autorise ; les modifications (suppression de règles ou d'objets dans les règles) doivent être réalisées selon une logique cohérente qui respecte l'organisation qui a été retenue pour la politique de filtrage.
Si les redondances observées sont similaires au 3e cas présenté dans le paragraphe 3.1.2.1, la règle redondante peut être « affinée » en suivant le processus décrit dans la section 5 de ce document.

R16 - Sauvegarder la politique de filtrage

La politique de filtrage doit être sauvegardée avant et après la suppression des règles redondantes.

4.5 Étape 4 : simplification des règles

La simplification d'une règle consiste à supprimer certains de ses objets qui apparaissent inutilisés sur la période de temps étudiée : hôte, réseau, service, groupe, etc. (se reporter au paragraphe 3.2.2). La suppression de ces objets contribue à simplifier la règle en la limitant au strict nécessaire, ce qui contribue à la sécurisation du système d'information.

R17 - Simplifier les règles

Afin d'améliorer la lisibilité de la politique de filtrage et pour améliorer la sécurité du système d'information, il est recommandé de simplifier les règles de filtrage.
Afin de limiter les effets de bord, cette simplification doit être faite par lots.

R18 - Supprimer les objets orphelins

La simplification peut engendrer des objets orphelins (se reporter au paragraphe 3.1.1.2) qui devraient être supprimés à chaque itération.

R19 - Sauvegarder régulièrement la politique de filtrage

Une sauvegarde de la politique de filtrage et des objets qui la composent doit être réalisée avant et après chaque simplification de règles.

5 Processus d'affinage des règles de filtrage

Le processus d'affinage présenté dans ce paragraphe est utilisé pour pouvoir supprimer une règle redondante correspondant au 3e cas présenté dans le paragraphe 3.1.2.1. Cette démarche doit être menée uniquement s'il est difficile d'obtenir des informations précises de la part du métier concernant les flux qui traversent le pare-feu.

La solution proposée consiste à étudier les journaux produits par la règle redondante dans le but d'extraire des informations (adresse IP, port) qui sont ensuite utilisées pour enrichir les règles placées en amont. Ce processus itératif est répété jusqu'à ce que la règle redondante ne produise plus d'évènements. Les règles enrichies placées en amont autorisent ainsi le trafic avant que la règle redondante soit parcourue. Celle-ci peut ensuite être désactivée puis supprimée.

Id.	source	destination	service	action	journ.
Section 1					
R1	srv_web_compta	srv1_bdd_prod	tcp_mysql	autoriser	activée
Section 2					
R2	...	...	...	...	...
Section 3					
R3	srv_web_compta	net_bdd_prod	tcp_mysql	autoriser	activée

Supposons que l'adresse IP de l'objet `srv1_bdd_prod` soit `192.168.10.1` et que celle de `net_bdd_prod` soit `192.168.10.0/24`. Supposons également que l'observation des journaux générés par la règle `R3` durant la période choisie montre des journaux dont les adresses IP de destinations sont `192.168.10.1`, `192.168.10.2` et `192.168.10.3`.

La politique de filtrage peut donc être modifiée (par exemple) de la façon suivante :

Id.	source	destination	service	action	journ.	comm.
Section 1						
R1	srv_web_compta	srv1_bdd_prod srv2_bdd_prod srv3_bdd_prod	tcp_mysql	autoriser	activé	20160210 ticket #39380 ajout srv2 et srv3
Section 2						
R2	...	...	...	...	...	...
Section 3						
R3	srv_web_compta	net_bdd_prod	tcp_mysql	autoriser	activée	20160210 ticket #39380 remplacée par R1 à désactiver au au 20160410

La politique a été modifiée de façon à enrichir la règle située en amont en utilisant uniquement les adresses de destination observées dans les journaux. Les deux objets `srv2_bdd_prod` et `srv3_bdd_prod` représentant les adresses `192.168.10.2` et `192.168.10.3` sont soit nouvellement créés soit déjà présents dans la base d'objets car utilisés dans d'autres règles de la politique.

La date de modification de la règle doit être renseignée dans son champ commentaire, par exemple. Elle va être utilisée comme point de départ pour la nouvelle analyse des journaux.

Une fois la modification effectuée, les journaux générés par les deux règles (la règle redondante et la règle modifiée) doivent être observés sur une période suffisamment représentative pour le type de flux qu'elles autorisent. Si la règle `R3` ne produit plus de journaux, cela signifie que l'ensemble des flux qu'elle autorisait sont désormais couverts par la règle amont modifiée. La règle `R3` n'est plus utile, elle peut être désactivée avant d'être définitivement supprimée de la politique. Si la règle `R3` continue à générer des journaux, de nouvelles itérations doivent être réalisées et la règle située en amont doit être enrichie jusqu'à ce que la règle redondante ne produise plus de journaux.

L'exemple utilisé pour illustrer la méthode d'affinage est volontairement très simple, des cas beaucoup plus complexes peuvent se présenter :

- il peut être nécessaire d'affiner à la fois les IP sources, les IP destinations et les services utilisés dans une règle redondante. Dans ce cas, il est important d'affiner méthodiquement et de prioriser les éléments à affiner en fonction des informations disponibles dans les journaux ;
- il peut exister plusieurs règles amonts, elles doivent être enrichies en respectant la logique de contruction afin d'éviter de complexifier la politique de filtrage. De nouvelles règles amonts peuvent être créées si nécessaire.

Plusieurs précautions doivent être prises pour conduire le processus d'affinage avec succès.

R20 - Analyser de manière critique les journaux

> Il est recommandé d'interpréter les informations obtenues à partir des journaux afin de déterminer si les flux observés semblent légitimes. Les règles amonts doivent être enrichies uniquement à l'aide de données cohérentes avec le système d'information et les flux concernés. Seules des personnes qui disposent d'une connaissance précise du système d'information (mais pas nécessairement de vision métier suffisante) peuvent être en mesure de prendre ce type de décision.

R21 - Réutiliser les objets existants

> Il est recommandé de réutiliser les objets existants au maximum lors de l'enrichissement des règles amont afin d'éviter de générer des doublons. Si des objets sont créés il doivent respecter les pratiques en vigueur.

R22 - Fixer un niveau de précision maximal

> Il est recommandé de fixer le niveau de « précision » maximal que les règles placées en amont peuvent atteindre. Il ne sera par exemple pas toujours possible et pertinent d'aboutir à des règles amonts n'autorisant que des flux entre des adresses IP représentant des machines uniquement. Il est fréquent que des besoins métiers nécessitent l'ouverture de flux ayant comme source ou destination des réseaux.

R23 - Limiter les processus d'affinage en parallèle

> Afin de maîtriser la charge de travail induite, il est recommandé de limiter le nombre de processus d'affinage lancés simultanément.

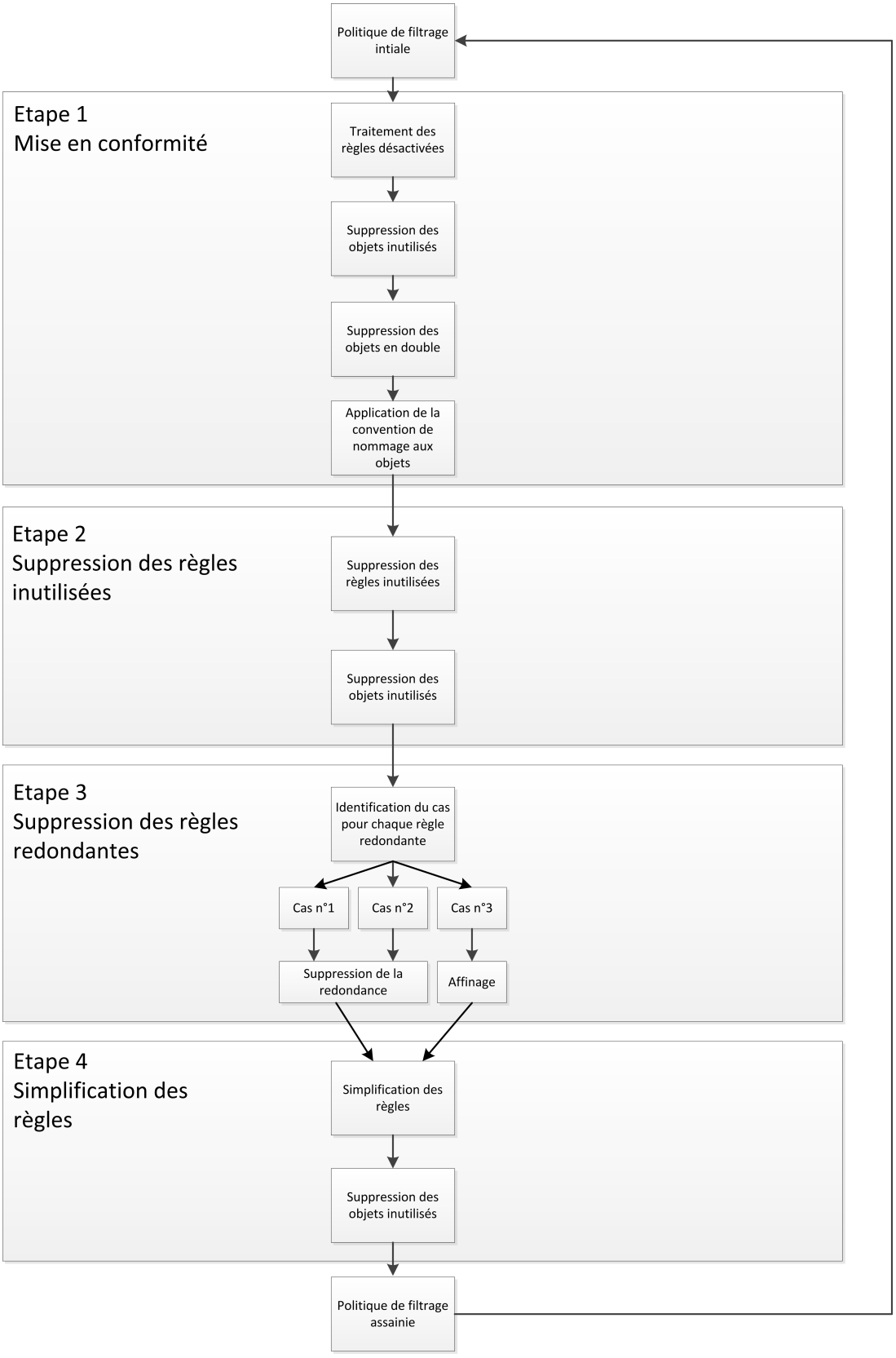

FIGURE 1 – Processus itératif de nettoyage d'une politique de filtrage d'un pare-feu

Liste des recommandations