

Groupe de travail Réseau  
**Request for Comments : 3871**  
 Catégorie : Information

G. Jones, Ed., The MITRE Corporation  
 septembre 2004  
 Traduction Claude Brière de L'Isle

## Exigences de sécurité de fonctionnement pour l'infrastructure de réseau IP des grands fournisseurs d'accès Internet (FAI)

### Statut de ce mémoire

Le présent mémoire apporte des informations pour la communauté de l'Internet. Il ne spécifie aucune norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

### Notice de copyright

Copyright (C) The Internet Society (2004). Tous droits réservés

### Résumé

Le présent document définit une liste des exigences de sécurité de fonctionnement pour l'infrastructure des grands réseaux (routeurs et commutateurs de fournisseurs d'accès Internet (FAI)). On définit un cadre pour spécifier des "profils", qui sont des collections d'exigences applicables à certains contextes de topologie de réseau (tous, seulement le cœur, seulement la bordure...). L'objectif est de fournir aux opérateurs de réseau un moyen concis et clair de communiquer leurs exigences de sécurité aux fabricants.

## Table des Matières

1. Introduction.....	2
1.1 Objectifs.....	2
1.2 Motifs.....	2
1.3 Domaine d'application.....	2
1.4 Définition d'un réseau sûr.....	2
1.5 Public visé.....	2
1.6. Format.....	3
1.7 Utilisation prévue.....	3
1.8 Définitions.....	3
2. Exigences fonctionnelles.....	5
2.1 Exigences de gestion d'appareil.....	5
2.2 Exigences de gestion dans la bande.....	5
2.3 Exigences de gestion hors bande.....	7
2.4 Exigences d'interface de configuration et de gestion.....	9
2.5 Exigences pour la pile IP.....	12
2.6 Exigences de limitation de débit.....	15
2.7 Capacités de base de filtrage.....	16
2.8 Critère de filtrage de paquet.....	17
2.9 Exigence d'un compteur de filtrage de paquet.....	18
2.10 Autres exigences de filtrage de paquets.....	20
2.11 Exigence d'enregistrement des événements.....	20
2.12 Exigences d'authentification, autorisation, et comptabilité (AAA).....	23
2.13 Les appareils de couche 2 doivent satisfaire les exigences des couches supérieurs.....	27
2.14 Les dispositifs de sécurité ne devraient pas causer de problème de fonctionnement.....	28
2.15 Les dispositifs de sécurité devraient avoir un impact minimal sur les performances.....	28
3. Exigences de documentation.....	28
3.1 Identifier les services autorisés à écouter.....	29
3.2 Documenter les valeurs par défaut du service.....	29
3.3 Documenter le processus d'activation du service.....	29
3.4 Documenter l'interface de ligne de commande.....	29
3.5 Documentation du profil de communication 'Console' par défaut.....	30
4. Exigences d'assurance.....	30
4.1 Identifier l'origine de la pile IP.....	30
4.2 Identifier l'origine du système d'exploitation.....	30
5. Considérations sur la sécurité.....	30
6. Références.....	31
Appendice A Profils d'exigences.....	32

A.1 Profil minimum d'exigences.....	32
A.2 Profil de bordure réseau de couche 3.....	34
Appendice B. Remerciements.....	34
Adresse de l'auteur.....	35
Déclaration complète de droits de reproduction.....	35
Propriété intellectuelle.....	35

## 1. Introduction

### 1.1 Objectifs

Le présent document définit une liste d'exigences de sécurité de fonctionnement pour les infrastructures des grands réseaux IP (routeurs et commutateurs). L'objectif est de fournir aux opérateurs de réseau une façon claire et concise de communiquer leurs exigences de sécurité aux fabricants d'équipements.

### 1.2 Motifs

Les opérateurs de réseau ont besoin d'outils pour s'assurer qu'ils sont capables de gérer leurs réseaux de façon sûre et de s'assurer qu'ils conservent la capacité de fournir leur service à leurs abonnés. Certaines des menaces sont précisées au paragraphe 3.2 de la [RFC2196]. Le présent document énumère les caractéristiques qui sont exigées pour la mise en œuvre de beaucoup des politiques et procédures suggérées par la [RFC2196] dans le contexte de l'infrastructure des grands réseaux fondés sur IP. Voir aussi la [RFC3013].

### 1.3 Domaine d'application

Le domaine d'application de ces exigences est destiné à couvrir les infrastructure gérées des grands réseaux IP de fournisseurs d'accès (FAI, fournisseur d'accès Internet) (par exemple, les routeurs et les commutateurs). Certains groupes (ou "profils", voir ci-dessous) ne s'appliquent que dans des situations spécifiques (par exemple, seulement en bordure).

Les situations suivantes sont explicitement exclues :

- o hôtes génériques qui ne font pas de transit de trafic, incluant les hôtes d'infrastructure comme les serveurs de nom/heure/journaux/AAA, etc.,
- o appareils non gérés,
- o appareils gérés par les abonnés (par exemple, pare-feu, systèmes de détection d'intrusion, appareils de VPN dédiés, etc.),
- o appareils SOHO (*Small Office, Home Office*) (par exemple, pare-feu personnels, points d'accès WiFi, modems câbles, etc.),
- o confidentialité des données d'abonné,
- o intégrité des données d'abonné,
- o sécurité physique .

Cela signifie qu'alors que les exigences du profil minimum (et des autres) peuvent s'appliquer, des exigences supplémentaires n'ont pas été ajoutées pour tenir compte de leurs besoins uniques.

Bien que les exemples donnés aient été écrits en pensant à IPv4, la plupart des exigences sont assez générales pour s'appliquer à IPv6.

### 1.4 Définition d'un réseau sûr

Pour les besoins du présent document, un réseau sûr est celui dans lequel :

- o le réseau continue de passer le trafic des abonnés légitimes (disponibilité) ;
- o le trafic va où il est supposé aller, et seulement où il est supposé aller (disponibilité, confidentialité) ;
- o les éléments de réseau restent gérables (disponibilité) ;
- o seuls les usagers autorisés peuvent gérer des éléments de réseau (autorisation) ;
- o il y a un enregistrement de tous les événements relatifs à la sécurité (comptabilité) ;
- o l'opérateur du réseau a les outils nécessaires pour détecter et faire face au trafic illégitime.

### 1.5 Public visé

Deux types d'audiences sont visés : les opérateurs de réseau qui choisissent, achètent et font fonctionner les équipements de réseau IP, et les fabricants qui les créent.

## 1.6. Format

Les exigences individuelles figurent dans les trois sections qui suivent.

- o La Section 2 donne la liste des exigences fonctionnelles.
- o La Section 3 donne la liste des exigences de documentation.
- o La Section 4 donne la liste des exigences d'assurance.

Dans ces domaines, les exigences sont groupées en domaines fonctionnels majeurs (par exemple, amorçage, authentification, filtrage, etc.)

Chaque exigence a les sous paragraphes suivants :

- o Exigences (lesquelles)
- o Justification (pourquoi)
- o Exemples (comment)
- o Avertissements (si applicable)

Les exigences décrivent une politique à prendre en charge par l'appareil. La justification dit pourquoi et dans quel contexte l'exigence est importante. la partie exemples est destinée à donner des exemples de mises en œuvre qui peuvent satisfaire cette exigence. Les exemples citent les technologies et les standard courants au moment de la rédaction. Voir la [RFC3631]. On s'attend à ce que le choix des mises en œuvre qui satisfont aux exigences change avec le temps. Les avertissements font la liste des problèmes de fonctionnement, des variantes par rapport aux standard, des mises en garde, etc.

Les exigences de sécurité vont varier selon les différents types d'appareils et les différentes organisations, selon la politique et d'autres facteurs. Une caractéristique désirée dans un environnement peut être une exigence dans un autre. Les classifications doivent être faites selon les besoins locaux.

Pour aider à la classification, l'Appendice A définit plusieurs "profils" d'exigences pour différents types d'appareils. Les profils sont des listes concises d'exigences qui s'appliquent à certaines classes d'appareils. Les profils dans ce document devraient être revus pour déterminer si ils sont appropriés à l'environnement local.

## 1.7 Utilisation prévue

Il est prévu que les exigences du présent document soient utilisées aux fins suivantes :

- o comme liste de vérifications lors de l'évaluation des produits de réseautage,
- o pour créer des profils de différents sous ensembles des exigences qui décrivent les besoins des différents appareils, organisations, et environnements de fonctionnement,
- o pour aider les opérateurs à communiquer de façon claire leurs exigences de sécurité,
- o comme lignes directrices générales pour la création de plans d'essais détaillés.

## 1.8 Définitions

Mots clés de la RFC2119

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans la [RFC2119].

L'utilisation des mots clés de la RFC 2119 est une tentative de l'éditeur pour allouer les niveaux d'exigence corrects ("DOIT", "DEVRAIT", "PEUT"...). On doit noter que des environnements de fonctionnement, de politique et d'environnement juridique différents vont générer des niveaux d'exigence différents. Les opérateurs et fabricants devraient considérer avec attention les exigences individuelles citées ici dans leur propre contexte. Une seule taille ne convient pas à tous.

Bogon : Un "bogon" (pluriel : "bogons") est un paquet qui a une adresse de source IP dans un bloc d'adresses qui n'est pas encore alloué par l'IANA ou le registraire régional Internet ARIN, RIPE, APNIC...) ainsi que toutes les adresses réservées pour utilisation privée ou spéciale par les RFC. Voir les [RFC3330] et [RFC1918].

CLI : Plusieurs exigences se réfèrent à une interface de ligne de commande (CLI, *Command Line Interface*). Bien que ceci se réfère à présent à une interface classique de commande en mode texte, ce n'est pas destiné à empêcher d'autres mécanismes qui peuvent satisfaire toutes les exigences qui font référence à une "CLI".

Console : Plusieurs exigences se réfèrent à une "console". Le modèle en est l'accès de série classique RS232 qui a pendant les trente dernières années ou plus, fourni une interface de gestion simple, stable, fiable, bien comprise et utilisée presque partout

pour les appareils du réseau. Là encore, ces exigences sont destinées principalement à codifier les avantages fournis par cette vénérable interface, et non d'empêcher d'autres mécanismes qui satisfont aux mêmes exigences.

**Filtre** : Dans le présent document, un "filtre" est défini comme un groupe d'une ou plusieurs règles où chaque règle spécifie un ou plusieurs critères de correspondance, comme spécifié au paragraphe 2.8.

**Gestion dans la bande** : La "gestion dans la bande" est définie comme toute gestion faite sur le même canal et les mêmes interfaces qu'utilisés pour les données de l'utilisateur/abonné. Des exemples incluraient SSH pour la gestion via l'abonné ou Internet sur des interfaces réseau.

**Heure à haute résolution** : "heure à haute résolution" est défini dans le présent document comme "une heure qui a une résolution inférieure à la seconde" (par exemple, des millisecondes).

**IP** : Sauf indication contraire, "IP" se réfère à IPv4.

**Gestion** : Le présent document utilise une définition large du terme "gestion". Dans le présent document, "gestion" se réfère à toute interaction autorisée avec l'appareil destiné à changer son état ou sa configuration de fonctionnement. Les fonctions de plan de données/transmission (par exemple, le transit du trafic des abonnés) ne sont pas considérées comme de la gestion. Les fonctions de plan de contrôle comme les protocoles d'acheminement, de signalisation et de gestion de liaison et les fonctions de plan de gestion comme l'accès à distance, la configuration et l'authentification sont considérées comme de la gestion.

**Martien** : Selon la [RFC1208] "Martien : terme humoristique appliqué aux paquets qui se retrouvent de façon inattendue sur le mauvais réseau à cause d'entrées d'acheminement erronées. Aussi utilisé comme nom pour un paquet qui a une adresse Internet tout à fait erronée (non enregistrée ou mal formée)". Pour les besoins du présent document, les martiens sont définis comme des "paquets ayant une adresse de source qui, par l'application des tableaux de transmission actuels, n'aurait pas son trafic de retour acheminé à l'expéditeur". Les "paquets leurre" sont une source courante de martiens.

Noter que dans certains cas, le trafic peut être asymétrique, et une simple vérification dans le tableau d'acheminement peut produire des faux positifs. Voir la [RFC3704]

**Gestion hors bande** : La "gestion hors bande" est définie comme une gestion faite sur des canaux et des interfaces qui sont séparés de ceux utilisés pour les données des usagers/abonnés. Des exemples incluraient une interface de console de série ou une interface réseau connectée à un réseau de gestion dédié qui n'est pas utilisé pour porter du trafic d'abonnés.

**Révision ouverte (*Open Review*)** : "révision ouverte" se réfère aux processus conçus pour générer une discussion et une révision publiques des solutions techniques proposées comme des protocoles de communications de données et des algorithmes de chiffrement dans le but d'améliorer et de construire la confiance dans les solutions finales. Pour les besoins du présent document "révision ouverte" est défini dans la [RFC2026]. Tous les documents en voie de normalisation sont pris en compte à travers un processus de révision ouverte. On notera que des organisations peuvent avoir des exigences locales qui définissent ce qu'elles considèrent comme "révision ouverte" acceptable. Par exemple, il peut être exigé d'adhérer à certaines normes nationales ou internationales. De telles modifications de la définition du terme "révision ouverte", bien qu'importantes, sont considérées comme des questions locales qui devraient être discutées entre l'organisation et le fabricant. On notera aussi que la section 7 de la [RFC2026] permet que les documents sur la voie de la normalisation incorporent d'autres "normes et spécifications externes".

**Service** : Un certain nombre d'exigences se réfèrent aux "services". Pour les besoins du présent document un "service" est défini comme "tout processus ou protocole fonctionnant dans les plans de contrôle ou de gestion auxquels des paquets qui ne sont pas de transit peuvent être livrés". Des exemples pourraient inclure un serveur SSH, un processus BGP ou un serveur NTP. Cela pourrait aussi inclure des protocoles de couche transport, réseau et de liaison car, par exemple, un paquet TCP adressé à un accès sur lequel aucun service n'écoute sera "livré" à la pile IP, et va éventuellement résulter en le renvoi d'un message ICMP.

**Canal sûr** : Un "canal sûr" est un mécanisme qui assure l'intégrité et la confidentialité de bout en bout des communications. Des exemples incluent TLS [RFC2246] et IPsec [RFC2401]. Connecter un terminal à un accès de console en utilisant un câble blindé physiquement sûr, fournirait la confidentialité mais peut-être pas l'intégrité.

**Réseau à un seul rattachement** : Un "réseau à un seul rattachement" est défini comme celui pour lequel il y a seulement une connexion vers l'amont et où l'acheminement est symétrique. Voir dans la [RFC3704] la discussion des questions et mécanismes relatifs aux réseaux multi rattachements.

**Paquet truqué** : Un "paquet truqué" se définit comme un paquet qui a une adresse de source qui ne correspond à aucune adresse allouée au système qui a envoyé le paquet. Les paquets truqués sont souvent des "bogons" ou des "martiens".

## 2. Exigences fonctionnelles

Les exigences de cette section sont destinées à faire la liste des exigences fonctionnelles vérifiables qui sont nécessaires pour faire fonctionner les services en toute sécurité.

### 2.1 Exigences de gestion d'appareil

#### 2.1.1 Prise en charge de canaux sûrs pour la gestion

Exigence : L'appareil DOIT fournir des mécanismes pour assurer l'intégrité et la confidentialité de bout en bout pour tout le trafic réseau et les protocoles utilisés pour prendre en charge les fonctions de gestion. Ceci DOIT inclure au moins les protocoles utilisés pour la configuration, la surveillance, la sauvegarde et la restauration de la configuration, les journaux d'événements, la synchronisation temporelle, l'authentification, et l'acheminement.

Justification : La protection de l'intégrité est exigée pour assurer que des usagers non autorisés ne peuvent pas gérer l'appareil ou altérer les données des journaux ou les résultats des commandes de gestion. La confidentialité est exigée afin que des usagers non autorisés ne puissent pas voir des informations sensibles, comme des clés, mots de passe, ou l'identité des usagers.

Exemples : Voir dans la [RFC3631] une liste actuelle des mécanismes qui peuvent être utilisés pour la prise en charge d'une gestion sûre.

Les paragraphes qui suivent font la liste des exigences pour la prise en charge de la gestion dans la bande (paragraphe 2.2) et de la gestion hors bande (paragraphe 2.3) ainsi que les compromis qui doivent être évalués en considérant ce qui est approprié à une certaine situation.

Avertissement : aucun.

### 2.2 Exigences de gestion dans la bande

Ce paragraphe fait la liste des exigences de sécurité qui prennent en charge la gestion sûre dans la bande. La gestion dans la bande présente l'avantage d'un coût inférieur (pas d'interfaces ou de lignes supplémentaires) mais a des inconvénients de sécurité significatifs :

- o La saturation des lignes ou interfaces d'abonnés peut rendre l'appareil ingérable sauf si des ressources de gestion hors bande ont été réservées.
- o Comme des interfaces/canaux publics sont utilisés, il est possible que des attaquants s'adressent et atteignent directement l'appareil et tentent des fonctions de gestion.
- o Le trafic de gestion dans la bande sur des interfaces publiques peut être intercepté ; cependant, cela va normalement exiger une compromission significative dans le système d'acheminement.
- o Les interfaces publiques utilisées pour la gestion dans la bande peuvent devenir indisponibles à cause de fautes (par exemple, des débordements de mémoire tampon sont exploités) tandis que les interfaces hors bande (comme un appareil de console de série) restent disponibles.

Il y a de nombreuses situations où la gestion dans la bande a du sens, est utilisée, et/ou est la seule option. Les exigences suivantes sont destinées à fournir des moyens de sécuriser le trafic de gestion dans la bande.

#### 2.2.1 Utilisation d'algorithmes de chiffrement soumis à révision ouverte

Exigence : Si le chiffrement est utilisé pour fournir des fonctions de gestion sûres, il DOIT alors y avoir l'option d'utiliser des algorithmes qui sont sujets à "révision ouverte" comme défini au paragraphe 1.8 pour fournir ces fonctions. Celles-ci DEVRAIENT être utilisées par défaut. L'appareil PEUT facultativement prendre en charge des algorithmes qui ne sont pas ouverts à la révision.

Justification : Les algorithmes de chiffrement qui n'ont pas été soumis à une large révision extensive par le public et les pairs ont une plus forte probabilité d'avoir des faiblesses ou des fautes cachées qu'un standard ouvert et des algorithmes revus en public. Les opérateurs de réseaux peuvent avoir le besoin ou le désir d'utiliser des algorithmes de chiffrement non ouverts. Il devrait leur être permis d'évaluer les avantages et inconvénients et de faire un choix informé entre chiffrement ouvert et non ouvert. Voir plus sur ce sujet dans [Schneier].

Exemples : Les algorithmes qui suivent satisfont l'exigence au moment de la rédaction du présent document : AES [FIPS.197], et 3DES [ANSI.X9-52] pour les applications qui exigent le chiffrement symétrique ; RSA [RFC3447] et Diffie-Hellman [PKCS.3], [RFC2631] pour les applications qui exigent un échange de clés ; HMAC [RFC2401] avec SHA-1 [RFC3174] pour

les applications qui exigent la vérification du message.

Avertissements : Cette liste n'est pas exhaustive. D'autres algorithmes forts et bien relus peuvent satisfaire l'exigence. La nature dynamique du domaine signifie que ce qui est assez bon aujourd'hui peut ne plus l'être à l'avenir. La révision ouverte est nécessaire, mais pas suffisante. La force de l'algorithme et la longueur de clé doivent aussi être considérées. Par exemple, DES à 56 bits satisfait à l'exigence de révision ouverte mais est aujourd'hui considéré comme trop faible et est donc non recommandé.

### 2.2.2 Utiliser un chiffrement fort

Exigence : Si le chiffrement est utilisé pour satisfaire aux exigences de gestion de canal sûr, les longueurs de clés et les algorithmes DEVRAIENT alors être "forts".

Justification : Les clés faibles et les algorithmes faibles menacent la confidentialité et l'intégrité des communications.

Exemples : Les algorithmes suivants satisfont à l'exigence au moment de cette rédaction : AES [FIPS.197], et 3DES [ANSI.X9-52] pour les applications qui exigent le chiffrement symétrique ; RSA [RFC3447] et Diffie-Hellman [PKCS.3], [RFC2631] pour les applications qui exigent un échange de clés ; HMAC [RFC2401] avec SHA-1 [RFC3174] pour les applications qui exigent la vérification du message.

Noter que pour les \*nouveaux protocoles\* [RFC3631] dit ce qui suit : "Les hachages chiffrés simples fondés sur MD5 [RFC1321], tels que ceux utilisés dans le mécanisme de sécurité de session BGP [RFC2385], sont particulièrement à éviter dans les nouveaux protocoles, étant donnés les signes de faiblesse de MD5". Bien que l'utilisation de tels hachages dans les produits et protocoles déployés soit préférable à un manque complet de vérification d'intégrité et d'authentification, le présent document se joint à la recommandation forte que les nouveaux produits et protocoles recherchent d'autres solutions de remplacement.

Avertissements : Cette liste n'est pas exhaustive. D'autres algorithmes forts, bien revus, peuvent satisfaire l'exigence. La nature dynamique du champ signifie que ce qui est assez bon aujourd'hui peut ne pas l'être à l'avenir. La force est relative. Les clés longues et les algorithmes forts sont destinés à augmenter le facteur de travail requis pour compromettre la sécurité des données protégées. Avec le temps, et l'augmentation des puissances de traitement, la sécurité fournie par un certain algorithme et une certaine longueur de clé se dégrade. La définition de "fort" doit être constamment réévaluée. Il peut y avoir des problèmes juridiques qui gouvernent l'utilisation de la cryptographie et de la force du chiffrement utilisé. Le présent document ne tente explicitement pas de faire de déclaration d'autorité sur les longueurs de clé qui constituent un chiffrement "fort". Voir les [RFC3562] et [RFC3766] pour déterminer les longueurs de clé appropriées. Voir aussi [Schneier] chapitre 7 pour une discussion des longueurs de clé.

### 2.2.3 Utiliser des protocoles soumis à révision ouverte pour la gestion

Exigence : Si le chiffrement est utilisé pour assurer la sécurité des canaux de gestion, son utilisation DOIT être prise en charge dans les protocoles qui sont soumis à "révision ouverte" comme défini au paragraphe 1.8. Ceci DEVRAIT être utilisé par défaut. L'appareil PEUT facultativement prendre en charge l'utilisation du chiffrement dans des protocoles qui ne sont pas ouverts à la révision.

Justification : Les protocoles qui n'ont pas été soumis à une large révision ouverte au public et aux pairs sont plus sujets à des faiblesses ou fautes non découvertes que les normes ouvertes et les protocoles soumis à relecture publique. Les opérateurs de réseau peuvent avoir le besoin ou le désir d'utiliser des protocoles non ouverts. Il devraient en peser les avantages et les inconvénients pour faire un choix raisonné entre protocoles ouverts et non ouverts.

Exemples : Voir TLS [RFC2246] et IPsec [RFC2401].

Avertissement : Noter que la révision ouverte est nécessaire mais peut n'être pas suffisante. Il est parfaitement possible qu'un protocole ayant fait l'objet d'une révision publique fasse un mauvais usage (ou pas d'usage du tout) de la cryptographie.

### 2.2.4 Permettre le choix des paramètres de chiffrement

Exigence : L'appareil DEVRAIT permettre à l'opérateur de choisir les paramètres cryptographiques. Ceux-ci DEVRAIENT inclure les longueurs de clé et les algorithmes.

Justification : La cryptographie utilisant certains algorithmes et longueurs de clés peut être considérée comme "forte" à un certain moment, mais "faible" à un autre. L'augmentation constante de la puissance de calcul réduit continuellement le temps nécessaire pour casser la cryptographie d'une certaine force. Des faiblesses peuvent être découvertes dans les algorithmes. La

capacité de choisir un algorithme différent est un outil utile pour maintenir la sécurité en face de telles découvertes.

Exemples : DES à 56 bits a été considéré comme sûr. En 1998, il a été cassé par une machine personnalisée en moins de trois jours. La capacité à choisir des algorithmes et des longueurs de clés donnerait à l'opérateur des options (des algorithmes différents, des clés plus longues) en face de tels développements.

Avertissement : aucun.

### 2.2.5 Les fonctions de gestion devraient avoir une priorité accrue

Exigence : Les fonctions de gestion DEVRAIENT être traitées à une priorité supérieure à celle du trafic qui n'est pas de gestion. Ceci DEVRAIT inclure l'entrée, la sortie, la transmission interne, et le traitement. Ceci DEVRAIT inclure au moins les protocoles utilisés pour la configuration, la surveillance, la sauvegarde de configuration, l'enregistrement des événements, la synchronisation horaire, l'authentification, et l'acheminement.

Justification : Certaines attaques (et le fonctionnement normal) peuvent causer une saturation des ressources comme l'encombrement des liaisons, l'épuisement de la mémoire ou la surcharge de la CPU. Dans ces cas, il est important que les fonctions de gestion aient la priorité pour assurer que les opérateurs ont les outils nécessaires pour récupérer de l'attaque.

Exemples : Imaginons un fournisseur de service avec 1 000 000 d'abonnés DSL, dont la plupart n'ont pas de pare-feu de protection. Imaginons qu'une large portion de ces machines d'abonné aient été infectées par un nouveau ver permettant de les utiliser de façon coordonnée au titre d'une grande attaque de déni de service qui implique l'inondation. Il est entièrement possible que sans cette priorité une telle attaque causerait l'encombrement des liaisons d'où résulterait la perte des adjacences d'acheminement. Une attaque de DoS contre les hôtes est juste devenue une attaque de DoS contre le réseau.

Avertissements : La priorisation n'est pas une panacée. Les paquets de mise à jour d'acheminement peuvent ne pas passer sur une liaison saturée. Cette exigence dit simplement que l'appareil devrait donner la priorité aux fonctions de gestion au sein de la portée de contrôle (par exemple, entrée, sortie, transit interne, traitement). Dans la mesure où ceci est fait sur un réseau entier, l'effet global sera d'assurer que le réseau reste gérable.

## 2.3 Exigences de gestion hors bande

Voir au paragraphe 2.2 la discussion des avantages et inconvénients de la gestion dans la bande contre la gestion hors bande.

Ces exigences supposent deux topologies hors bande différentes possibles :

- o connexions de console de ligne de série (ou équivalent) utilisant une CLI,
- o interfaces réseau connectées à un réseau séparé dédié à la gestion.

Les hypothèses suivantes sont faites sur la gestion hors bande :

- o le réseau de gestion hors bande est sûr,
- o les communications au delà de l'interface de gestion (par exemple, accès de console, interface de réseau de gestion) sont sûres,
- o il n'est pas nécessaire de chiffrer la communication sur les interfaces de gestion hors bande, (par exemple, sur une connexion série entre un serveur terminal et l'accès de console d'un appareil),
- o des mesures de sécurité sont en place pour empêcher les accès physiques non autorisés.

Même si ces hypothèses sont vérifiées, il serait sage, au titre de la défense en profondeur d'une application, d'appliquer les exigences dans la bande (par exemple, le chiffrement) aux interfaces hors bande.

### 2.3.1 Prise en charge d'une interface de 'console'

Exigence : L'appareil DOIT prendre en charge la configuration et la gestion complète via une interface de 'console' qui fonctionne indépendamment des plans de transmission et de contrôle IP.

Justification : Il est des fois où il est nécessaire au fonctionnement d'être capable d'accéder immédiatement et facilement à un appareil pour la gestion ou la configuration, même lorsque le réseau est indisponible, que les interfaces d'acheminement et de réseau sont incorrectement configurées, que la pile IP et/ou le système d'exploitation peuvent ne pas fonctionner (ou peuvent être vulnérables à une exploitation récemment découverte qui rend leur utilisation impossible/inopportune) ou que des chemins à forte bande passante vers l'appareil sont indisponibles. Dans de telles situations, une interface de console peut fournir le moyen de gérer et configurer l'appareil.

Exemples : Une interface RS232 (EIA232) qui fournit la capacité de charger de nouvelles versions du logiciel système et

d'effectuer la configuration via un interface de ligne de commande. Les interfaces RS232 sont omniprésentes et bien comprises.

Un simple appareil incorporé qui fournit l'accès à la gestion et la configuration via une interface Ethernet ou USB.

Au moment de la rédaction, RS232 est toujours fortement recommandé car il fournit les avantages suivants :

- \* Simplicité. RS232 est bien plus simple que les autres solutions. C'est simplement une spécification de matériel. À l'opposé, une solution fondée sur Ethernet peut exiger une interface Ethernet, un système d'exploitation, une pile IP et un serveur HTTP pour fonctionner et être correctement configurée.
- \* Prouvé. RS232 a plus de 30 années d'utilisation.
- \* Bien compris. Les opérateurs ont beaucoup d'expérience avec RS232.
- \* Disponibilité. Cela fonctionne même en présence de défaillances du réseau.
- \* Omniprésence. Il est très largement déployé dans les parties moyennes et d'extrémité des infrastructures réseau.
- \* Faible coût. Le coût d'ajout d'un accès RS232 à un appareil est faible.
- \* Compatible CLI. Une interface RS232 et une CLI sont suffisants dans la plupart des cas pour gérer un appareil. Aucun autre logiciel n'est exigé.
- \* Intégré. Les opérateurs ont de nombreuses solutions (serveur terminal, etc.) actuellement déployées pour prendre en charge la gestion via RS232.

Bien que d'autres interfaces puissent être fournies, les propriétés citées ci-dessus méritent considération. Les interfaces qui n'ont pas ces propriétés peuvent présenter des défis en termes de facilité d'utilisation, d'intégration ou d'adoption. Des problèmes dans un de ces domaines pourraient avoir des impacts négatifs sur la sécurité, en particulier dans des situations où la console doit être utilisée pour répondre rapidement aux incidents.

Avertissements : Il est de pratique courante de connecter les accès RS232 aux serveurs terminaux qui permettent un accès en réseau pratique. Cela augmente l'exposition potentielle de la sécurité des mécanismes qui ne sont disponibles que via des accès RS232. Par exemple, un mécanisme de récupération de mot de passe qui n'est disponible que via RS232 peut permettre à un pirate distant de reconfigurer complètement un routeur. Bien que les procédures de fonctionnement sortent du domaine d'application du présent document, il est important de noter ici qu'une forte attention devrait être portée aux politiques, procédures, mécanismes d'accès et à la sécurité physique qui gouvernent l'accès aux accès de console.

### **2.3.2 Le profil de communication de 'console' doit prendre en charge la réinitialisation**

Exigence : Il DOIT y avoir une méthode définie et publiée pour ramener les paramètres de communication de console à leurs réglages par défaut. Cette méthode ne doit pas exiger que les réglages actuels soient connus.

Justification : Avoir à deviner les réglages de communications serait une perte de temps. Dans une situation de crise, l'opérateur peut avoir besoin de prendre rapidement le contrôle de la console d'un appareil.

Exemples : Une méthode peut être d'envoyer une coupure sur une ligne de série.

Avertissement : aucun.

### **2.3.3 La 'console' exige les fonctionnalités minimales des appareils rattachés**

Exigence : L'utilisation de l'interface 'console' NE DOIT PAS exiger des appareils propriétaires, des extensions de protocole ou un logiciel client spécifique.

Justification : L'objectif d'avoir une interface console est d'avoir une interface de gestion qu'on puisse faire fonctionner rapidement à tout moment. Exiger un comportement complexe ou non standard de la part des appareils rattachés réduit la probabilité que la console fonctionne sans problèmes.

Exemples : Si la console est fournie via une interface RS232, elle devrait alors fonctionner avec un appareil rattaché qui ne met en œuvre qu'un terminal "sourde". La prise en charge de caractéristiques/types de terminal "avancés" devrait être facultative.

Avertissement : aucun.

### **2.3.4 Prise en charge d'une authentification de repli par la 'console'**

Exigence : La 'console' DEVRAIT prendre en charge un mécanisme d'authentification qui n'exige pas le fonctionnement de IP ou ne dépende pas de services externes. Ce mécanisme d'authentification PEUT être désactivé jusqu'à ce que soit détectée une défaillance des autres mécanismes préférés.

Justification : Il ne paraît pas bon d'avoir une interface de console sur un appareil si on ne peut pas entrer dans l'appareil avec elle quand le réseau ne fonctionne pas.

Exemples : Certains appareils qui utilisent TACACS ou RADIUS pour l'authentification vont revenir à un compte local si le serveur TACACS ou RADIUS ne répond pas à une demande d'authentification.

Avertissements : Cette exigence représente un compromis entre être capable de gérer l'appareil (fonctionnalité) et sécurité. Il y a de nombreuses façons de mettre cela en œuvre qui réduiraient la sécurité pour l'appareil, (par exemple, une porte dérobée pour l'accès non autorisé). La politique locale devrait être consultée pour déterminer si "ouvert par défaut" ou "fermé par défaut" est la posture correcte. Les implications de "fermé par défaut" (par exemple, ne pas être capable de gérer un appareil) devraient être considérées dans tous leurs aspects.

Si le mécanisme de repli est désactivé, il est important que la défaillance du mécanisme d'authentification fondé sur IP soit détectée de façon fiable et que le mécanisme de repli soit automatiquement activé. Autrement l'opérateur peut se retrouver sans moyen d'authentifier.

### 2.3.5 Prise en charge d'interfaces IP de plan de gestion séparées

Exigence : L'appareil PEUT fournir une ou des interfaces réseau désignées qui sont utilisées pour le trafic du plan de gestion.

Justification : Une interface séparée du plan de gestion permet que le trafic de gestion soit séparé des autres trafics (données/plan de transmission, plan de contrôle). Cela réduit le risque que des individus non autorisés soient capables d'observer le trafic de gestion et/ou de compromettre l'appareil.

Cette exigence s'applique dans des situations où existe un réseau de gestion hors bande séparé.

Exemple : un accès Ethernet dédié à la gestion et isolé du trafic des consommateurs satisfait à cette exigence.

Avertissements : L'utilisation de ce type d'interface dépend du bon fonctionnement des deux systèmes d'exploitation et de la pile IP, ainsi que d'une bonne configuration connue au moins sur les portions de l'appareil dédiées à la gestion.

### 2.3.6 Pas de transmission entre le plan de gestion et les autres interfaces

Exigence : Si l'appareil met en œuvre des interfaces réseau séparées pour le plan de gestion selon le paragraphe 2.3.5, alors l'appareil NE DOIT PAS transmettre de trafic entre les interfaces du plan de gestion et les interfaces qui ne le sont pas.

Justification : Cela empêche le flux, intentionnel ou non, du trafic de gestion de/vers des endroits d'où il ne devrait pas avoir son origine/terminaison (par exemple, tout ce qui est au delà des interfaces qui sont en face du consommateur).

Exemple : mettre en œuvre des tableaux de transmission séparés pour les interfaces de plan de gestion et les interfaces qui n'en sont pas qui ne propagent pas de chemins les uns vers les autres satisfait cette exigence.

Avertissement : aucun.

## 2.4 Exigences d'interface de configuration et de gestion

Ce paragraphe fait la liste des exigences qui prennent en charge des méthodes sûres de configuration et gestion des appareils. Dans la plupart des cas, cela implique habituellement une sorte d'interface de ligne de commande (CLI, *command line interface*) et des fichiers de configuration. Il est possible de satisfaire ces exigences avec d'autres mécanismes, par exemple SNMP ou une interface HTML inscriptible qui fournisse un plein accès aux fonctions de gestion et de configuration. À l'avenir, il pourrait y en avoir d'autres (par exemple, une configuration fondée sur XML).

### 2.4.1 Une 'CLI' fournit l'accès à toutes les fonctions de configuration et de gestion

Exigence : L'interface de ligne de commande (CLI) ou son équivalent DOIT permettre un accès complet à toutes les fonctions de configuration et de gestion. La CLI DOIT être prise en charge sur la console (voir au paragraphe 2.3.1) et DEVRAIT être supportée sur toutes les autres interfaces utilisées pour la gestion.

Justification : La CLI (ou son équivalent) est nécessaire pour donner la capacité de faire une gestion et une surveillance fiables,

rapides, directes, et locales d'un appareil. Elle est particulièrement utile dans les situations où il n'est pas possible de gérer et surveiller l'appareil dans la bande via des moyens "normaux" (par exemple, SSH ou SNMP [RFC3410], [RFC3411]) qui dépendent du réseautage fonctionnel. De telles situations surviennent souvent durant des incidents de sécurité comme des attaques de déni de service fondées sur la bande passante.

Exemples : les exemples de configuration incluent le réglage des adresses d'interface, la définition et l'application des filtres, la configuration de l'amorçage et l'authentification, etc. Des exemples de fonctions de gestion incluent l'affichage d'informations d'état dynamiques comme la charge de CPU, l'utilisation des mémoires, les statistiques du traitement des paquets, etc.

Avertissement : aucun.

#### **2.4.2 Une 'CLI' prend en charge les scripts de configuration**

Exigence : La CLI (ou son équivalent) DOIT prendre en charge l'inscription externe des fonctions de configuration. Cette CLI DEVRAIT prendre en charge le même ensemble de commandes et de syntaxe qu'au paragraphe 2.4.1.

Justification : Durant le traitement des incidents de sécurité, il est souvent nécessaire de faire rapidement des changements de configuration sur un grand nombre d'appareils. Le faire manuellement est lent et entraîne des erreurs. Les solutions de gestion fournies par les fabricants ne prévoient pas toujours, ou ne traitent pas le type ou niveau de solutions requis. La capacité de réaliser un script donne une solution à ces problèmes.

Exemples : les exemples d'utilisation de scripts incluent de retracer une attaque à travers un grand réseau, de mettre à jour les paramètres d'authentification, de mettre à jour les paramètres d'amorçage, de mettre à jour les filtres, d'aller chercher/analyser la configuration, etc. Certains langages couramment utilisés pour les scripts incluent expect, Perl et TCL.

Avertissements : certaines propriétés de langage de commande qui améliorent la capacité à faire des scripts sont la simplicité, la régularité et la cohérence. Certaines mises en œuvre qui rendraient les scripts difficiles ou impossibles incluent les interfaces de style "menu de texte" (par exemple, "curses" sur UNIX) ou des interfaces graphiques d'utilisateur (GUI, *Graphical User Interface*) codées dans le matériel (par exemple, une application GUI native Windows ou Macintosh) qui communiquent en utilisant un protocole propriétaire ou non documenté non fondé sur une CLI.

#### **2.4.3 Une 'CLI' prend en charge la gestion sur des liaisons 'lentes'**

Exigence : L'appareil DOIT prendre en charge une interface de ligne de commande (CLI) ou un mécanisme équivalent qui fonctionne sur les connexions à faible bande passante.

Justification : Il y a des situations où une forte bande passante n'est pas disponible pour la gestion, par exemple lorsque les connexions dans la bande sont surchargées durant une attaque ou lorsque des connexions à faible bande passante hors bande, comme des modems doivent être utilisées. C'est souvent dans ces conditions qu'il est le plus crucial d'être capable d'effectuer les fonctions de gestion et de configuration.

Exemples : Le réseau est par terre. L'ingénieur réseau a désactivé l'acheminement par mégarde sur le seul routeur passerelle dans un centre de données distant non désigné. Le seul accès à l'appareil est sur un modem connecté à un accès de console. Les clients du centre de données commencent à appeler la ligne d'assistance. L'interface de gestion GUI redessine l'écran plusieurs fois... lentement... à 9 600 bit/s.

Un mécanisme qui prend en charge le fonctionnement sur les liaisons lentes est la capacité à appliquer des filtres à la sortie des commandes de CLI qui ont un potentiel de sortie fort. Cela peut être mis en œuvre avec quelque chose de similaire à la facilité pipe de UNIX et à la commande "grep". Par exemple, `cat largefile.txt | grep interesting-string`. Un autre est la capacité de "page" à travers une grande sortie de commande, par exemple, la commande UNIX "more" :. Par exemple, `cat largefile.txt | more`

Avertissements : une conséquence de cette exigence peut être qu'exiger une interface GUI pour la gestion n'est acceptable que si il peut être montré qu'elle fonctionne de façon acceptable sur des liaisons lentes.

#### **2.4.4 Une 'CLI' prend en charge une temporisation de fin de session sur inactivité**

Exigence : L'interface de ligne de commande (CLI) ou un mécanisme équivalent DOIT prendre en charge une valeur de temporisation d'inactivité configurable.

Justification : Les administrateurs du réseau vont déjeuner. Ils restent eux-mêmes connectés avec leurs privilèges administratifs. Ils oublient d'utiliser des économiseurs d'écran avec une protection par mot de passe. Ils font cela dans des

conférences et d'autres lieux publics. Ce comportement offre une opportunité pour des accès non autorisés. Les temporisations d'inactivité réduisent la fenêtre d'exposition.

Exemples : La CLI peut fournir une commande de configuration qui permet d'établir une temporisation d'inactivité. Si l'opérateur ne rentre pas de commande pendant cette durée, la session de connexion sera automatiquement terminée.

Avertissement : aucun.

#### 2.4.5 Prise en charge de l'installation de logiciel

Exigence : L'appareil DOIT fournir un moyen d'installer de nouvelles versions de logiciel. Il DOIT être possible d'installer un nouveau logiciel alors que l'appareil est déconnecté de tous les réseaux IP publics. Ceci NE DOIT PAS s'appuyer sur une installation et/ou configuration précédente. Alors qu'un nouveau logiciel PEUT être chargé à partir d'un support inscriptible (disque, mémoire flash, etc.) la capacité de charger un nouveau logiciel DOIT dépendre seulement d'un support non inscriptible (ROM, etc.). Les procédures d'installation DEVRAIENT prendre en charge des mécanismes qui assurent la fiabilité et l'intégrité des transferts de données.

Justification :

- \* Des vulnérabilités sont souvent découvertes dans le logiciel de base (systèmes d'exploitation, etc.) livré par les fabricants. L'atténuation du risque présenté par ces vulnérabilités ne peut souvent être réalisée que par des mises à jour au logiciel fournies par le fabricant (par exemple, réparation de bogues, nouvelles versions du code, etc.). Sans un mécanisme pour charger le nouveau code fourni par le fabricant, il peut n'être pas possible d'atténuer les risques présentés par ces vulnérabilités.
- \* Il est aussi concevable qu'un comportement malveillant de la part de pirates ou des comportements non intentionnels de la part des opérateurs puisse causer la corruption ou l'écrasement de logiciel sur les appareils. Dans ces situations, il est nécessaire d'avoir un moyen pour (re)charger le logiciel sur l'appareil pour restaurer le fonctionnement correct.
- \* Il est important d'être capable de charger un nouveau logiciel alors qu'on est déconnecté de tous les réseaux publics IP parce que l'appareil peut être vulnérable à de vieilles attaques avant l'achèvement de la mise à jour.
- \* On doit supposer que les pirates, les opérateurs, etc. peuvent écraser ou corrompre tous les supports incriptibles (disques, mémoires flash, etc.). Dans de telles situations, il est nécessaire d'être capable de récupérer en commençant avec seulement des supports non inscriptibles (par exemple, un CD-ROM, un vrai surveillant fondé sur une ROM).
- \* Les images systèmes peuvent être corrompues dans le transit (du fabricant au consommateur, ou durant le processus de chargement) ou dans la mémorisation (défaut binaire, support défectueux, etc.). L'échec d'un chargement fiable d'une nouvelle image, par exemple après qu'un pirate a supprimé ou corrompu l'image installée, pourrait résulter en de larges pertes de disponibilité.

Exemples : L'appareil pourrait prendre en charge l'amorçage dans un simple moniteur fondé sur une mémoire en lecture seule qui prene en charge un ensemble de commandes suffisant pour charger un nouveau code de système d'exploitation et de données de configuration à partir d'autres appareils. Le système d'exploitation et la configuration pourraient être chargés à partir de :

RS232 : L'appareil pourrait prendre en charge le chargement du nouveau code via un accès de console RS232.

CD-ROM : L'appareil pourrait prendre en charge l'installation du nouveau code à partir d'un pilote sur CD-ROM rattaché en local.

Réseau : L'appareil pourrait prendre en charge l'installation du nouveau code via une interface réseau, en supposant que (a) il est déconnecté de tous les réseaux publics et (b) l'appareil peut amorcer un système d'exploitation et une pile IP à partir d'un support en lecture seule avec des capacités suffisantes pour charger le nouveau code à partir du réseau.

FLASH : L'appareil pourrait prendre en charge l'amorçage à partir de cartes de mémoire flash.

Les mécanismes simples actuellement utilisés pour protéger l'intégrité des images systèmes et des transferts de données incluent les sommes de contrôle d'image et de simples protocoles de transfert de fichier en série tels que XMODEM et Kermit.

Avertissement : aucun.

#### 2.4.6 Prise en charge de la sauvegarde de configuration à distance

Exigence : L'appareil DOIT fournir un moyen pour mémoriser la configuration du système sur un serveur distant. La configuration mémorisée DOIT avoir des informations suffisantes pour restaurer l'appareil dans son état opérationnel au moment où la configuration est sauvegardée. Les versions mémorisées de la configuration PEUVENT être compressées en utilisant un algorithme soumis à révision ouverte, pour autant que le fait soit clairement identifié et que la compression puisse être désactivée. Les informations sensibles comme les mots de passe qui pourraient être utilisés pour compromettre la sécurité de l'appareil PEUVENT être exclues de la configuration sauvegardée.

Justification : L'archivage des configurations est essentiel pour permettre l'audit et la récupération.

Exemples : les mises en œuvre possibles incluent SCP, SFTP ou FTP sur un canal sûr. Voir au paragraphe 2.1.1 pour les exigences relatives à la sécurisation des canaux de communication pour les protocoles et données de gestion.

Avertissement : la sécurité du serveur distant est supposée, avec des mesures appropriées qui sortent du domaine d'application du présent document.

#### **2.4.7 Prise en charge de la restauration de la configuration à distance**

Exigence : L'appareil DOIT fournir un moyen pour restaurer une configuration qui a été sauvegardée comme décrit au paragraphe 2.4.6. Le système DOIT être restauré à son état opérationnel au moment où la configuration a été sauvegardée.

Justification : La restauration d'une configuration archivée permet une restauration rapide du service à la suite d'une panne (relative à la sécurité aussi bien que pour d'autres causes).

Exemples : Les configurations peuvent être restaurées en utilisant SCP, SFTP ou FTP sur un canal sûr. Voir au paragraphe 2.1.1 les exigences relatives aux canaux de communication sûrs pour les protocoles et données de gestion.

Avertissements : La sécurité du serveur distant est supposée, avec des mesures appropriées qui sortent du domaine d'application de ce document.

Noter que si des mots de passe ou d'autres informations sensibles sont exclus de la copie de la configuration sauvegardée, comme permis par le paragraphe 2.4.6, la restauration peut n'être pas complète. L'opérateur peut devoir établir de nouveaux mots de passe ou fournir d'autres informations qui n'ont pas été sauvegardées.

#### **2.4.8 Prise en charge de fichiers de configuration de texte**

Exigence : L'appareil DOIT prendre en charge l'affichage, la sauvegarde et la restauration de la configuration du système dans un format textuel simple bien défini. La configuration DOIT aussi être visible comme texte sur l'appareil lui-même. Il NE DOIT PAS être nécessaire d'utiliser un programme propriétaire pour voir la configuration.

Justification : Une configuration textuelle simple, bien définie facilite la compréhension par l'homme de l'état de fonctionnement de l'appareil, permet des audits hors ligne, et facilite l'automatisation. Exiger l'utilisation d'un programme propriétaire pour accéder à la configuration entrave ces objectifs.

Exemples : un fichier de configuration ASCII à 7 bits qui montre les réglages actuels des diverses options de configuration satisferait l'exigence, comme le ferait une configuration Unicode ou toute autre représentation "textuelle". Un format structuré binaire destiné seulement à la consommation des programmes ne serait pas acceptable.

Avertissements : Les copies hors ligne de configurations devraient être bien protégées car elles contiennent souvent des informations sensibles comme des chaînes de communauté SNMP, des mots de passe, des blocs réseau, des informations d'abonnés, etc.

"Bien défini" et "textuel" sont des termes ouverts à l'interprétation. Il est clair qu'un fichier de configuration ASCII avec une commande régulière, documentée avec une syntaxe, satisferait la définition. Ils sont actuellement largement utilisés. De futures options, comme une configuration fondée sur XML peut satisfaire l'exigence. Le déterminer exige une évaluation par rapport aux justifications énumérées ci-dessus.

## **2.5 Exigences pour la pile IP**

### **2.5.1 Capacité à identifier tous les services en écoute**

Exigence : Le fabricant DOIT :

- \* fournir un moyen d'afficher tous les services qui écoutent le trafic réseau dirigé sur l'appareil à partir de toute source externe,
- \* afficher les adresses auxquelles chaque service est lié,
- \* afficher les adresses allouées à chaque interface,
- \* afficher tous les accès sur lesquels le service écoute,
- \* inclure à la fois les services de norme ouverte et propriétaires du fabricant.

Justification : Ces informations sont nécessaires pour permettre une évaluation précise des risques pour la sécurité associés au fonctionnement de l'appareil (par exemple, "ce protocole permet-il une gestion complète de l'appareil sans aussi exiger d'authentification, d'autorisation, ou d'identification ?"). Ces informations aident aussi à déterminer quelles étapes devraient être suivies pour atténuer le risque (par exemple, "devrais je fermer ce service ?")

Exemples : si l'appareil écoute le trafic SNMP provenant de toute source dirigée sur les adresses IP de toutes ses interfaces locales, cette exigence pourrait alors être satisfaite par la fourniture d'une commande qui affiche ce fait.

Avertissement : aucun.

### 2.5.2 Capacité de désactiver tout service

Exigence : L'appareil DOIT fournir un moyen pour fermer tous "services" (voir au paragraphe 1.8).

Justification : La capacité de désactiver des services pour lesquels il n'y a pas de besoin de fonctionnement permet aux administrateurs de réduire les risques globaux subis par l'appareil.

Exemples : des processus qui écoutent sur les accès TCP et UDP seraient les principaux exemples de services qu'il doit être possible de désactiver.

Avertissement : aucun.

### 2.5.3 Capacité de contrôler les liens de service pour les services qui écoutent

Exigence : L'appareil DOIT fournir un moyen pour que l'utilisateur spécifie les liens utilisés pour tous les services écoutants. Il DOIT prendre en charge le lien avec toute adresse ou bloc réseau associé à toute interface locale pour l'appareil. Cela doit inclure les adresses liées à des interfaces physiques ou non physiques (par exemple, rebouclage).

Justification : Il est de pratique courante chez les opérateurs de configurer des pseudo interfaces de "rebouclage" à utiliser comme source et destination du trafic de gestion. Elles sont préférées aux interfaces physiques parce que elles fournissent une adresse stable, acheminable. Les services liés aux adresses d'interfaces physiques peuvent devenir injoignables si le matériel associé tombe en panne, est supprimé, etc.

Cette exigence rend possible de restreindre l'accès aux services de gestion en utilisant l'acheminement. Les services de gestion peuvent être liés seulement aux adresses des interfaces de rebouclage. Les interfaces de rebouclage peuvent être atteintes par des blocs réseau qui ne sont acheminés qu'entre les appareils gérés et les réseaux/hôtes de gestion autorisés. Ceci a pour effet de rendre impossible à quiconque de se connecter (ou de tenter un déni de service) aux services de gestion de partout sauf des réseaux/hôtes de gestion autorisés.

Cela réduit beaucoup le besoin de filtres complexes. Cela réduit le nombre d'accès d'écoute, et donc le nombre de chemins potentiels d'attaque. Cela assure que seul le trafic qui arrive d'adresses légitimes et/ou sur des interfaces désignées peut accéder aux services sur l'appareil.

Exemples : si l'appareil écoute les connexions SSH entrantes, cette exigence signifie qu'il devrait être possible de spécifier que l'appareil va seulement écouter les connexions destinées à des adresses spécifiques (par exemple, l'adresse de l'interface de rebouclage) ou reçues sur certaines interfaces (par exemple, une interface Ethernet désignée comme interface "de gestion"). Il devrait être possible dans cet exemple de configurer l'appareil de telle sorte que SSH N'ÉCOUTE PAS chaque adresse configurée sur l'appareil. Des effets similaires peuvent être réalisés avec l'utilisation de filtres globaux, parfois appelés des ACL "de réception" ou "de rebouclage", qui filtrent le trafic destiné à l'appareil lui-même sur toutes les interfaces.

Avertissement : aucun.

### 2.5.4 Capacité de contrôler les adresses de source des services

Exigence : L'appareil DOIT fournir un moyen pour permettre à l'utilisateur de spécifier les adresses de source utilisées pour toutes les connexions sortantes ou transmissions originaires de l'appareil. Il DEVRAIT être possible de spécifier les adresses de source indépendamment pour chaque type de connexion ou transmission sortante. Les adresses de source DOIVENT être limitées aux adresses qui sont allouées aux interfaces (y compris de rebouclage) locales de l'appareil.

Justification : Cela permet aux appareils distants qui reçoivent des connexions ou transmissions d'utiliser le filtrage de source comme moyen d'authentification. Par exemple, si des pièges SNMP ont été configurés à utiliser une adresse de rebouclage connue comme source, la station de travail SNMP qui reçoit le piège (ou un pare-feu en façade) pourrait être configurée à recevoir des paquets SNMP de cette seule adresse.

Exemples : L'opérateur peut allouer un bloc distinct d'adresses à partir desquelles tous les rebouclages sont numérotés. NTP et syslog peuvent être configurés à utiliser ces adresses de rebouclage comme source, alors que SNMP et BGP peuvent être configurés à utiliser des adresses d'interface physique spécifiques. Cela va faciliter le filtrage sur la base de l'adresse de source comme moyen pour rejeter les tentatives non autorisées de se connecter aux homologues/serveurs.

Avertissements : On devrait bien s'assurer que les adresses choisies sont acheminables entre les appareils d'envoi et de réception (par exemple, régler SSH à utiliser l'adresse de rebouclage de 10.1.1.1 qui n'est pas acheminée entre un routeur et toutes les destinations souhaitées pourrait causer des problèmes).

Noter que certains protocoles, comme SCTP [RFC3309], peuvent utiliser plus d'une adresse IP comme point d'extrémité d'une seule connexion. Noter aussi que la [RFC3631] classe l'authentification fondée sur l'adresse comme un "mécanisme d'insécurité". L'authentification fondée sur l'adresse devrait être remplacée ou renforcée par d'autres mécanismes chaque fois que possible.

### 2.5.5 Prise en charge de l'anti fraude automatique pour les réseaux à un seul rattachement

Exigence : L'appareil DOIT fournir un moyen pour désigner des interfaces particulières comme desservant des "réseaux à un seul rattachement" (voir au paragraphe 1.8) et DOIT fournir l'option d'élimination automatique des "paquets contrefaits" (paragraphe 1.8) reçus sur de telles interfaces où l'application du tableau de transmission actuel n'acheminerait pas le trafic retour par la même interface. Cette option DOIT fonctionner en présence d'acheminement dynamique et d'adresses allouées de façon dynamique.

Justification : Voir la Section 3 de la [RFC1918], les paragraphes 5.3.7 et 5.3.8 de la [RFC1812], et la [RFC2827].

Exemples : Cette exigence pourrait être satisfaite de plusieurs façons : par la fourniture d'une seule commande qui génère automatiquement et applique des filtres à une interface qui met en œuvre l'anti-falsification; par la fourniture d'une commande qui cause la vérification du chemin de retour pour les paquets reçus par rapport aux tableaux de transmission actuels et les élimine si ils ne seraient pas transmis en retour à travers la même interface que celle de leur réception. Voir la [RFC3704].

Avertissements : Cette exigence ne tient que pour les réseaux à un seul rattachement. Noter que la simple vérification dans un tableau de transmission n'est pas suffisante dans les scénarios plus complexes de réseaux multi-rattachements, c'est-à-dire où le trafic peut être asymétrique. Dans ces cas, une vérification plus approfondie telle que celle d'une transmission sur le chemin inverse praticable (*Feasible Path RPF*) pourrait être très utile.

### 2.5.6 Prise en charge de l'élimination automatique des bogues et des martiens

Exigence : L'appareil DOIT fournir un moyen pour éliminer automatiquement toutes les "bogues" et les "martiens" (paragraphe 1.8). Cette option DOIT fonctionner en présence d'acheminement dynamique et d'adresses allouées de façon dynamique.

Justification : Ces sortes de paquets n'ont que peu (pas ?) d'utilisation légitime et sont principalement utilisés pour permettre à des individus et organisations d'éviter l'identification (et donc la prise en compte) et apparaissent le plus souvent dans des attaques de déni de service, des messages abusifs, des actions de piratage, etc. De plus, assurer le transit de ces paquets consomme sans nécessité des ressources et peut conduire à des problèmes de capacité et performances pour les consommateurs. Voir la section 3 de la [RFC1918], les paragraphes 5.3.7 et 5.3.8 de la [RFC1812], et la [RFC2827].

Exemples : Cette exigence pourrait être satisfaite par la fourniture d'une commande qui cause la vérification du chemin de retour pour les paquets reçus par rapport aux tableaux de transmission actuels et leur élimination si il n'existe pas de chemin de retour viable. Cela suppose que des mesures soient prises pour assurer qu'aucune entrée boguée n'est présente dans les tableaux d'acheminement (par exemple le filtrage des mises à jour d'acheminement selon le paragraphe 2.7.5 pour rejeter les annonces d'adresses non allouées). Voir la [RFC3704].

Avertissements : Cette exigence ne tient que pour les réseaux à un seul rattachement. Noter qu'une simple vérification de tableau d'acheminement n'est pas suffisante dans les scénarios plus complexes des réseaux multi rattachements, c'est-à-dire, où le trafic peut être asymétrique. Dans ces cas, une vérification plus approfondie telle que celle d'une transmission sur le chemin inverse praticable (*Feasible Path RPF*) pourrait être très utile.

### 2.5.7 Prise en charge de compteurs de paquets éliminés

Exigence : L'appareil DOIT fournir un compte précis par interface des paquets falsifiés éliminés conformément aux paragraphes 2.5.5 et 2.5.6.

Justification : les compteurs peuvent aider à identifier la source du trafic falsifié.

Exemples : Un routeur bordure peut avoir plusieurs consommateurs à un seul rattachement. Lorsque est détectée une attaque qui utilise des paquets falsifiés, une rapide vérification des compteurs peut permettre d'identifier quels consommateurs tentent d'envoyer du trafic falsifié.

Avertissement : aucun.

## 2.6 Exigences de limitation de débit

### 2.6.1 Prise en charge de la limitation de débit

Exigence : L'appareil DOIT fournir la capacité de limiter le débit auquel il va passer le trafic sur la base du protocole, de l'adresse IP de source et de destination ou du bloc de CIDR, de l'accès de source et destination, et de l'interface. Les protocoles DOIVENT inclure au moins IP, ICMP, UDP, et TCP et DEVRAIENT inclure tous les protocoles.

Justification : Cette exigence donne un moyen pour réduire ou éliminer l'impact de certains types d'attaques. Aussi, la limitation présente l'avantage que dans certains cas, elle peut être activée a priori, offrant par là une capacité à atténuer les effets d'attaques futures avant toute réaction explicite de l'opérateur aux attaques.

Exemples : Supposons qu'une société d'hébergement sur la Toile fournisse de l'espace dans son centre de données à une société qui devient impopulaire auprès de certains des utilisateurs du réseau, qui décident alors d'inonder le serveur de la Toile avec du trafic ICMP entrant. Il serait utile dans une telle situation d'être capable de filtrer en débit le trafic ICMP aux routeurs bordures du centre de données. D'un autre côté, supposons qu'un nouveau ver se répande qui infecte les serveurs de bases de données vulnérables de telle façon qu'ils commencent alors à déverser du trafic sur l'accès TCP 1433 destiné à des adresses de destination aléatoires aussi vite que le système et l'interface réseau du serveur infecté sont capables de le faire. Supposons de plus qu'un centre de données ait de nombreux serveurs vulnérables qui soient infectés et envoient simultanément de grandes quantités de trafic avec pour résultat que toutes les liaisons sortantes soient saturées. La mise en œuvre de cette exigence permettrait à l'opérateur du réseau de limiter en débit le trafic entrant et/ou sortant de TCP 1433 (éventuellement à un taux de 0 paquets/octets par seconde) pour répondre à l'attaque et conserver les niveaux de service pour les autres consommateurs/trafic légitime.

Avertissement : aucun.

### 2.6.2 Prise en charge de l'application directionnelle de la limitation de débit par interface

Exigence : L'appareil DOIT fournir la prise en charge de la limitation de débit en entrée et/ou en sortie séparément sur chaque interface.

Justification : Ce niveau de granularité du contrôle permet de cibler de façon appropriée les commandes qui minimisent l'impact sur les tiers.

Exemples : Si une inondation ICMP est dirigée par un seul consommateur sur un routeur bordure, il peut être approprié de limiter le débit d'ICMP sortant sur cette seule interface de consommateur.

Avertissement : aucun.

### 2.6.3 Prise en charge de la limitation de débit sur la base de l'état

Exigence : L'appareil DOIT être capable de limiter en débit sur la base de tous les bits de fanion de contrôle TCP. L'appareil DEVRAIT accepter la limitation de débit des autres protocoles à états pleins lorsque le traitement normal du protocole donne à l'appareil l'accès à l'état du protocole.

Justification : Cela permet une réponse appropriée à certaines classes d'attaques.

Exemples : Par exemple, pour les sessions TCP, il devrait être possible de limiter le débit sur la base des états de SYN, SYN-ACK, RST, ou d'autres bits.

Avertissement : aucun.

## 2.7 Capacités de base de filtrage

### 2.7.1 Capacité de filtrer le trafic

Exigence : L'appareil DOIT fournir un moyen pour filtrer les paquets IP sur toute interface mettant en œuvre IP.

Justification : Le filtrage de paquets est important parce qu'il fournit un moyen de base pour mettre en œuvre des politiques qui spécifient quel trafic est permis et quel trafic ne l'est pas. Il fournit aussi un outil de base pour répondre au trafic malveillant.

Exemples : Les listes de contrôle d'accès qui permettent le filtrage sur la base du protocole et/ou de l'adresse de source/destination et ou de l'accès de source/destination en sont un exemple.

Avertissement : aucun.

### 2.7.2 Capacité de filtrer le trafic VERS l'appareil

Exigence : Il DOIT être possible d'appliquer le mécanisme de filtrage au trafic adressé directement à l'appareil via n'importe laquelle de ses interfaces – y compris les interfaces de rebouclage.

Justification : Cela permet à l'opérateur d'appliquer des filtres qui protègent l'appareil lui-même contre les attaques et accès non autorisés.

Exemples : cela peut inclure des filtres qui permettent BGP seulement des homologues et SNMP et SSH provenant d'un segment de gestion autorisé et dirigé sur l'appareil lui-même, et en éliminant tout autre trafic adressé à l'appareil.

Avertissement : aucun.

### 2.7.3 Capacité de filtrer le trafic À TRAVERS l'appareil

Exigence : Il DOIT être possible d'appliquer le mécanisme de filtrage au trafic qui est acheminé (commuté) à travers l'appareil.

Justification : cela permet de mettre en œuvre des politiques de base sur des appareils qui portent du trafic de transit (routeurs, commutateurs, etc.).

Exemples : une façon simple et courante de satisfaire cette exigence est de fournir la capacité de filtrer le trafic entrant dans chaque interface et/ou sortant de chaque interface. Le filtrage d'entrée décrit dans la [RFC2827] donne un exemple de l'utilisation de cette capacité.

Avertissement : aucun.

### 2.7.4 Capacité de filtrer sans dégradation significative des performances

Exigence : L'appareil DOIT fournir un moyen pour filtrer les paquets sans dégradation significative des performances. Ceci s'applique spécifiquement au filtrage de paquets sans état fonctionnant sur les en-têtes de couche 3 (IP) et de couche 4 (TCP ou UDP) ainsi qu'aux informations normales de transmission de paquet comme les interfaces entrantes et sortantes.

L'appareil DOIT être capable d'appliquer des filtres de paquet sans état à TOUTES les interfaces (jusqu'au nombre maximum possible) simultanément et avec plusieurs filtres par interface (par exemple, entrante et sortante).

Justification : Cela permet la mise en œuvre du filtrage chaque fois et partout où c'est nécessaire. Dans la mesure où le filtrage cause une dégradation, il peut n'être pas possible d'appliquer des filtres qui mettent en œuvre les politiques appropriées.

Exemples : Une autre façon de formuler l'exigence est de dire que les performances du filtrage ne devraient pas être le facteur limitant du débit de l'appareil. Si un appareil est capable de transmettre 30 Mbit/s sans filtrage, il devrait alors être capable de transmettre la même quantité avec le filtrage.

Avertissements : La définition de "significatif" est subjective. D'un côté cela peut signifier que "l'application de filtres peut causer la panne de l'appareil". À l'autre extrémité ce serait une perte de débit de moins de un pour cent avec des dizaines de milliers de filtres appliqués. Le niveau de dégradation des performances qui est acceptable devra être déterminé par l'opérateur.

Des données d'essais répétables montrant l'impact des performances de filtre seraient très utiles pour évaluer la conformité à cette exigence. Les essais devraient inclure des informations comme la taille de paquet, le débit de paquet, le nombre

d'interfaces essayées (source/destination), les types d'interfaces, la taille du tableau d'acheminement, les protocoles d'acheminement utilisés, la fréquence des mises à jour d'acheminement, etc. Voir [bmgw-acc].

Cette exigence ne vise pas le filtrage à états pleins, le filtrage sur les en-têtes au dessus de la couche 4 ou d'autres types de filtrage plus avancés qui peuvent être importants dans certains environnements de fonctionnement.

### 2.7.5 Prise en charge du filtrage de chemin

Exigence : L'appareil DOIT fournir un moyen pour filtrer les mises à jour d'acheminement pour tous les protocoles utilisés pour échanger des informations d'acheminement externes.

Justification : voir la [RFC3013] et le paragraphe 3.2 de la [RFC2196].

Exemples : Les opérateurs peuvent souhaiter ignorer les annonces de chemin pour des adresses allouées à des internets privés. Voir eBGP.

Avertissement : aucun.

### 2.7.6 Capacité à spécifier des actions de filtrage

Exigence : L'appareil DOIT fournir un mécanisme pour permettre la spécification de l'action à prendre lorsque une règle de filtre correspond. Les actions DOIVENT inclure "permet" (admet le trafic), "rejet" (élimine avec la notification appropriée à l'expéditeur) et "élimine" (abandon sans notification à l'expéditeur). Voir aussi aux paragraphes 2.7.7 et 2.9.

Justification : cette capacité est essentielle pour l'utilisation de filtres pour mettre en application une politique.

Exemples : Supposons qu'on ait un petit réseau en zone neutre (DMZ) connecté à l'Internet. On veut permettre la gestion avec SSH venant des bureaux de l'entreprise. Dans ce cas, on peut "permettre" tout le trafic à l'accès 22 dans la DMZ à partir du réseau d'entreprise, "rejetant" tous les autres. Le trafic de l'accès 22 provenant du réseau d'entreprise peut passer. Le trafic à l'accès 22 provenant de toutes les autres adresses résulte en un message ICMP à l'expéditeur. Pour ceux qui sont un peu plus paranoïaques, on peut choisir "d'éliminer" au lieu de "rejeter" le trafic provenant d'adresses non autorisées, avec pour résultat que \*rien\* n'est renvoyé à la source.

Avertissement : Bien que l'élimination en silence de trafic sans envoi de notification puisse être l'action correcte en termes de sécurité, on devrait considérer les implications opérationnelles. Voir dans la [RFC3360] les considérations sur les problèmes potentiels causés par l'envoi de Reset TCP inappropriés.

### 2.7.7 Capacité à enregistrer les actions de filtrage

Exigence : Il DOIT être possible d'enregistrer toutes les actions de filtrage. La capacité d'enregistrement DOIT être capable de capturer au moins les données suivantes :

- \* l'état permet/rejet/éliminer,
- \* l'adresse IP de source et destination,
- \* les accès de source et destination (si applicable au protocole),
- \* quel élément de réseau a reçu le paquet (interface, adresse MAC ou autres informations de couche 2 qui identifient la source du bond précédent du paquet).

L'enregistrement des actions de filtre est soumis aux exigences du paragraphe 2.11.

Justification : L'enregistrement est essentiel pour l'audit, la réponse aux incidents, et pour le fonctionnement.

Exemples : un réseau privé peut ne pas fournir de service qui devrait être accessible de "l'extérieur". Dans ce cas, toutes les tentatives de connexion entrante devraient être enregistrées comme de possibles tentatives d'intrusion.

Avertissement : aucun.

## 2.8 Critère de filtrage de paquet

### 2.8.1 Capacité de filtrage sur les protocoles

Exigence : L'appareil DOIT fournir un moyen pour filtrer le trafic sur la base de la valeur du champ Protocole dans l'en-tête IP.

Justification : être capable de filtrer sur le protocole est nécessaire pour permettre la mise en œuvre d'une politique, d'un fonctionnement sûr, et pour prendre en charge la réponse aux incidents.

Exemples : certaines attaques de déni de service se fondent sur la capacité à inonder la victime avec du trafic ICMP. Une façon rapide (avec certains effets collatéraux négatifs) d'atténuer les effets de telles attaques est d'éliminer tout le trafic ICMP dirigé sur la victime.

Avertissement : aucun.

### 2.8.2 Capacité de filtrage sur les adresses

Exigence : La fonction DOIT être capable de contrôler le flux de trafic sur la base de l'adresse IP de source et/ou destination ou blocs d'adresses comme les blocs d'acheminement inter domaine sans classe (CIDR, *Classless Inter-Domain Routing*).

Justification : la capacité de filtrer sur les adresses et blocs d'adresses est un outil fondamental pour établir des frontières entre des réseaux différents.

Exemple : un exemple d'utilisation du filtrage fondé sur l'adresse est la mise en œuvre du filtrage d'entrée selon la [RFC2827].

Avertissement : aucun.

### 2.8.3 Capacité de filtrage sur les champs d'en-tête de protocole

Exigence : Le mécanisme de filtrage DOIT prendre en charge le filtrage fondé sur la ou les valeurs de toute portion des en-têtes de protocole pour IP, ICMP, UDP et TCP. Il DEVRAIT prendre en charge le filtrage de tous les autres protocoles pris en charge aux couches 3 et 4. Il PEUT supporter le filtrage fondé sur les en-têtes de protocoles de niveau supérieur. Il DEVRAIT être possible de spécifier les champs par noms (par exemple, "protocole = ICMP") plutôt que par des valeurs de décalage binaire/longueur/numérique (par exemple, 72:8 = 1).

Justification : être capable de filtrer sur des portions de l'en-tête est nécessaire pour permettre la mise en œuvre d'une politique, d'un fonctionnement sûr, et prendre en charge la réponse aux incidents.

Exemples : Cette exigence implique qu'il soit possible de filtrer sur la base des numéros d'accès TCP ou UDP, des fanions TCP tels que les bits SYN, ACK et RST, et les champs de type et code ICMP. Un exemple courant est de rejeter les tentatives de connexion TCP "entrantes" (bit TCP, SYN établi + bit ACK à zéro ou bit SYN établi + bits ACK, FIN et RST à zéro). Un autre exemple courant est la capacité de contrôler quels services sont permis en entrée et sortie d'un réseau. Il peut être souhaitable de ne permettre que les connexions entrantes sur l'accès 80 (HTTP) et 443 (HTTPS) avec un réseau qui héberge des serveurs de la Toile.

Avertissement : aucun.

### 2.8.4 Capacité de filtrage sur les entrées et les sorties

Exigence : Il DOIT être possible de filtrer le trafic entrant et sortant sur toutes les interfaces.

Justification : Cette exigence permet une souplesse dans l'application de filtres aux endroits où ils ont le plus de sens. Elle permet que le trafic invalide ou malveillant soit éliminé aussi près de la source que possible.

Exemples : Il peut être souhaitable sur un routeur bordure, par exemple, d'appliquer un filtre de sortie sur l'interface qui connecte un site à son FAI externe pour éliminer le trafic sortant qui n'a pas une adresse de source interne valide. En entrée, il peut être souhaitable d'appliquer un filtre qui bloque tout le trafic provenant d'un site connu pour transmettre ou générer des quantités de pourriels.

Avertissement : aucun.

## 2.9 Exigence d'un compteur de filtrage de paquet

### 2.9.1 Capacité à compter précisément les touches de filtre

Exigence : l'appareil DOIT fournir une facilité pour compter précisément toutes les touches de filtre.

Justification : un comptage précis de correspondance de règle de filtre est important parce qu'il montre la fréquence des tentatives de violation de la politique. Cela permet de concentrer les ressources sur les zones de plus grand besoin.

Exemple : supposons par exemple, que le réseau d'un FAI mette en œuvre des filtres de sortie anti fraude (voir la [RFC2827]) sur les interfaces de ses routeurs de bordure qui prennent en charge des réseaux de bout à un seul rattachement. Les compteurs pourraient permettre au FAI de détecter les cas où de grands nombres de paquets falsifiés sont envoyés. Cela peut indiquer que le client est en train d'effectuer des actions potentiellement malveillantes (éventuellement en violation de la politique d'utilisations acceptables du FAI) ou que le ou les systèmes sur le réseau du client ont été "appropriés" par des pirates et sont utilisés abusivement pour lancer des attaques.

Avertissement : aucun.

### 2.9.2 Capacité à afficher des compteurs de filtre

Exigence : L'appareil DOIT fournir un mécanisme pour afficher les compteurs de filtres.

Justification : les informations qui sont collectées ne sont utiles que si elles peuvent être affichées de façon utile.

Exemples : supposons qu'il y a un routeur avec quatre interfaces. Une est une liaison avec un FAI qui fournit des chemins pour l'Internet. Les trois autres connectent à des réseaux internes séparés. Supposons qu'un hôte sur un des réseaux internes ait été compromis par un pirate et envoi du trafic avec des adresses de source boguées. Dans une telle situation, il serait souhaitable d'appliquer des filtres d'entrée à chacune des interfaces internes. Une fois que les filtres sont en place, les compteurs peuvent être examinés pour déterminer la source (interface entrante) des paquets bogués.

Avertissement : aucun.

### 2.9.3 Capacité à afficher des compteurs de filtre par règle

Exigence : L'appareil DOIT fournir un mécanisme pour afficher les compteurs de filtre par règle.

Justification : cela rend possible de voir quelles règles sont touchées et à quelle fréquence.

Exemples : Supposons qu'un filtre a été défini avec deux règles, une qui permet tout le trafic SSH (tcp/22) et la seconde qui élimine tout le trafic restant. Si trois paquets sont dirigés vers/à travers le point auquel le filtre est appliqué, l'un à l'accès 22, les autres à des accès différents, l'affichage du compteur devrait montrer un paquet correspondant à la règle 'permet tcp/22' et deux paquets correspondant à la règle 'rejeter tous les autres'.

Avertissement : aucun.

### 2.9.4 Capacité à afficher des compteurs de filtre par application de filtre

Exigence : Si il est possible d'appliquer un filtre plus d'une fois au même moment, l'appareil DOIT alors fournir un mécanisme pour afficher les compteurs de filtre par application de filtre.

Justification : Il peut y avoir un sens à appliquer la même définition de filtre simultanément plus d'une fois (à des interfaces différentes, etc.). Si c'est le cas, il serait beaucoup plus utile de savoir quelle instance d'un filtre correspond plutôt que de savoir qu'une certaine instance a correspondu quelque part.

Exemples : Une façon de mettre en œuvre cette exigence serait d'avoir le mécanisme d'affichage du compteur qui montre l'interface (ou une autre entité) à laquelle le filtre a été appliqué, ainsi que le nom (ou une autre désignation) du filtre. Par exemple si un filtre nommé "desktop\_outbound" appliqué à deux interfaces différentes, dit, "ethernet0" et "ethernet1", l'affichage devrait indiquer quelque chose comme "correspondance de filtre 'desktop\_outbound' sur ethernet0 ..." et "correspondance de filtre 'desktop\_outbound' sur ethernet1 ..."

Avertissement : aucun.

### 2.9.5 Capacité à remettre à zéro les compteurs de filtre

Exigence : Il DOIT être possible de remettre à zéro les compteurs pour chaque filtre. Pour les besoins de cette exigence, il serait acceptable que le système tienne deux compteurs : un "compteur absolu", C[maintenant], et un compteur de "réinitialisation", C[reset]. Le compteur absolu tiendrait le compte qui augmente de façon monotone jusqu'à revenir à zéro ou à

déborder le compte. Le compteur reset recevrait une copie de la valeur courante du compteur absolu lorsque la fonction de réinitialisation a été fournie pour ce compteur. Les fonctions qui affichent ou restituent le compteur pourraient alors afficher le delta ( $C[\text{maintenant}] - C[\text{reset}]$ ).

Justification : cela permet aux opérateurs d'avoir une vision actuelle du trafic qui correspond à des filtres de règles particulières.

Exemples : Supposons que les compteurs de filtre sont utilisés pour détecter des hôtes internes qui sont infectés par un nouveau ver. Une fois qu'on pense que tous les hôtes infectés ont été nettoyés et que le ver a été retiré, l'étape suivante serait de le vérifier. Une façon de le faire serait de remettre à zéro les compteurs de filtre et de voir si le trafic indicatif du ver a cessé.

Avertissement : aucun.

### 2.9.6 Les compteurs de filtre doivent être précis

Exigence : Les compteurs de filtre DOIVENT être précis. Ils DOIVENT refléter le nombre réel de paquets correspondants depuis la dernière remise à zéro du compteur. Les compteurs de filtre DOIVENT être capables de contenir jusqu'à  $2^{32} - 1$  valeurs sans déborder, et DEVRAIENT être capables de contenir jusqu'à  $2^{64} - 1$  valeurs.

Justification : on ne peut pas s'appuyer sur des données imprécises pour une action. Des données mal rapportées peuvent dissimuler l'ordre de grandeur d'un problème.

Exemples : Si N paquets correspondants à un filtre sont envoyés à travers un appareil, le compteur devrait montrer N correspondances.

Avertissement : aucun.

## 2.10 Autres exigences de filtrage de paquets

### 2.10.1 Capacité de spécifier la granularité de l'enregistrement du filtre

Exigence : Il DOIT être possible d'activer/désactiver l'enregistrement sur la base de la règle.

Justification : La capacité de régler la granularité de l'enregistrement permet à l'opérateur de n'enregistrer que les informations qu'il désire. Sans cette capacité, il est possible que des données supplémentaires (ou pas du tout) soient enregistrées, rendant plus difficile de trouver les informations pertinentes.

Exemples : si un filtre est défini avec plusieurs règles, et si une des règles refuse les connexions telnet (tcp/23) il devrait alors être possible de spécifier que seules les correspondances à cette règle qui refusent telnet devraient générer un message d'enregistrement.

Avertissement : aucun.

## 2.11 Exigence d'enregistrement des événements

### 2.11.1 La facilité d'enregistrement utilise des protocoles soumis à révision ouverte

Exigence : L'appareil DOIT fournir une facilité d'enregistrement qui se fonde sur des protocoles soumis à révision ouverte. Voir au paragraphe 1.8. Des protocoles personnalisés ou propriétaires PEUVENT être mis en œuvre pourvu que les mêmes informations soient rendues disponibles.

Justification : l'utilisation d'enregistrements fondés sur des protocoles soumis à révision ouverte permet à l'opérateur d'effectuer l'archivage et l'analyse des enregistrements sans s'appuyer sur un logiciel et des serveurs fournis par le fabricant.

Exemples : Cette exigence peut être satisfaite par l'utilisation d'un ou plusieurs de syslog [RFC3164], syslog avec livraison fiable [RFC3195], TACACS+ [RFC1492] ou RADIUS [RFC2865].

Avertissements : Bien que la [RFC3164] satisfasse cette exigence, elle pose de nombreux problèmes de sécurité et par elle même ne satisfait pas aux exigences du paragraphe 2.1.1. Voir la section Considérations pour la sécurité de la [RFC3164] pour la liste des problèmes. La [RFC3195] donne des solutions à la plupart de ces problèmes, cependant, au moment de la rédaction du présent document, il y a peu de mises en œuvre. D'autres solutions possibles seraient de tunneler syslog sur un transport sûr,

mais cela soulève souvent des problèmes difficiles de gestion de clé et d'adaptabilité.

La meilleure solution actuelle semble être la suivante :

- \* mettre en œuvre la [RFC3164],
- \* envisager la mise en œuvre de la [RFC3195].

### 2.11.2 Enregistrements envoyés à un serveur distant

Exigence : L'appareil DOIT prendre en charge la transmission à un ou plusieurs appareils distants d'enregistrements de sécurité se rapportant aux événements. Il DOIT y avoir des réglages de configuration sur l'appareil qui permettent le choix du serveur.

Justification : ceci est important parce que cela prend en charge l'identification individuelle. Il est important de les mémoriser sur un serveur séparé pour les préserver en cas d'échec ou de compromission de l'appareil géré.

Exemples : Cette exigence peut être satisfaite par l'utilisation d'un ou plusieurs de syslog [RFC3164], syslog avec livraison fiable [RFC3195], TACACS+ [RFC1492] ou RADIUS [RFC2865].

Avertissements : Noter qu'il peut y avoir des considérations de confidentialité ou juridiques sur les activités d'enregistrement/surveillance d'utilisateurs. De forts volumes d'enregistrements peuvent générer un trafic réseau excessif et/ou entrer en concurrence pour des ressources rares de mémoire et de CPU sur l'appareil.

### 2.11.3 Capacité de choisir une livraison fiable

Exigence : Il DEVRAIT être possible de choisir une livraison fiable des messages d'enregistrement.

Justification : la livraison fiable est importante dans la mesure où ces données enregistrées conditionnent des décisions et des analyses opérationnelles. Sans livraison fiable, les données enregistrées deviennent une collection d'indications.

Exemples : un exemple de livraison fiable de syslog est définie dans la [RFC3195]. Syslog-ng donne un autre exemple, bien que le protocole n'ait pas encore été normalisé.

Avertissement : aucun.

### 2.11.4 Capacité d'enregistrer en local

Exigence : Il DEVRAIT être possible d'enregistrer en local sur l'appareil lui-même. L'enregistrement local DEVRAIT être écrit sur un support de mémoire non volatile.

Justification : l'enregistrement local des tentatives échouées d'authentification sur un support de mémorisation non volatile est critique. Cela donne le moyen de détecter les attaques lorsque l'appareil est isolé de ses interfaces d'authentification et attaqué sur la console. L'enregistrement local est important pour voir les informations quand on est connecté à l'appareil. Cela fournit une sauvegarde des données d'enregistrement au cas où la connexion à distance échoue. Cela donne un moyen pour voir les enregistrements pertinents pour un appareil sans avoir à trier dans un ensemble éventuellement grand d'enregistrements provenant d'autres appareils.

Exemples : un exemple d'enregistrement local serait une mémoire tampon qui recevrait des copies des messages envoyés au serveur d'enregistrement distant. Un autre exemple pourrait être un serveur syslog local (en supposant que l'appareil soit capable de faire fonctionner syslog et ait une mémorisation locale).

Avertissements : La mémorisation sur l'appareil peut être limitée. De gros volumes d'enregistrements peuvent rapidement remplir la mémoire disponible, auquel cas il y a deux options : les nouveaux enregistrements écrasent les vieux (éventuellement via l'utilisation d'une mémoire tampon circulaire ou d'une rotation des fichiers d'enregistrement) ou bien l'enregistrement s'arrête.

### 2.11.5 Capacité de maintenir une heure système précise

Exigence : L'appareil DOIT maintenir une heure système précise, de "haute résolution" (voir la définition au paragraphe 1.8).

Justification : une heure précise est importante pour la génération de données d'enregistrement fiables. Une heure précise est aussi importante pour le fonctionnement correct de certains mécanismes d'authentification.

Exemples : Cette exigence peut être satisfaite par la prise en charge du protocole de l'heure du réseau (NTP), du protocole simple d'heure du réseau (SNTP), ou via une connexion directe à une source horaire précise.

Avertissements : Les processeurs d'horloge système sont imprécis à des degrés divers. L'heure système ne devrait pas être considérée comme fiable si elle n'est pas régulièrement vérifiée et synchronisée avec une source horaire externe précise connue comme un serveur NTP de couche 1). Noter aussi que si la synchronisation à l'heure du réseau est utilisée, un attaquant peut être capable de manipuler l'horloge sauf si l'authentification cryptographique est utilisée.

### **2.11.6 Affichage de la zone horaire et du décalage par rapport à l'UTC**

Exigence : tous les affichages et les enregistrements de l'heure système DOIVENT inclure une zone horaire ou un décalage par rapport à l'UTC.

Justification : connaître la zone horaire ou les décalages à l'UTC rend possible la corrélation des données et la coordination avec les données dans d'autres zones horaires.

Exemples : Bob est à Terre-Neuve, Canada qui est à UTC -3,30. Alice est quelque part en Indiana, USA. Certaines parties de l'Indiana passent à l'heure d'hiver alors que d'autres ne le font pas. Un utilisateur sur le réseau de Bob attaque un usager du réseau d'Alice. Tous deux utilisent des enregistrements avec des zones horaires locales et pas d'indication de décalage à l'UTC. Corréler ces enregistrements sera difficile et enclin à l'erreur. Inclure la zone horaire, ou mieux, le décalage à l'UTC, élimine ces difficultés.

Avertissement : aucun.

### **2.11.7 La zone horaire par défaut devrait être l'UTC**

Exigence : La zone horaire par défaut pour afficher et enregistrer DEVRAIT être UTC. L'appareil PEUT prendre en charge un mécanisme pour permettre à l'opérateur de spécifier l'affichage et l'enregistrement des heures dans une zone horaire autre que l'UTC.

Justification : connaître la zone horaire ou le décalage à l'UTC rend possibles la corrélation de données et la coordination avec les données dans d'autres zones horaires.

Exemples : Bob à Terre-Neuve (UTC -3,30) et Alice dans l'Indiana (UTC -5 ou UTC -6 selon la période de l'année et le comté exact de l'Indiana) travaillent ensemble sur un incident en utilisant leurs enregistrements. Tous deux ont laissé les réglages par défaut, qui étaient l'UTC, de sorte qu'il n'y a pas de traduction d'heure nécessaire pour corréler les enregistrements.

Avertissement : aucun.

### **2.11.8 Les enregistrements doivent être horodatés**

Exigence : par défaut, l'appareil DOIT horodater tous les messages d'enregistrement. l'horodatage DOIT être précis à la seconde ou moins. L'horodatage DOIT inclure une zone horaire. Il PEUT y avoir un mécanisme pour désactiver la génération des horodatages.

Justification : des horodatages précis sont nécessaires pour corréler les événements, en particulier à travers plusieurs appareils ou avec d'autres organisations. Cela s'applique lorsque il est nécessaire d'analyser les enregistrements.

Exemples : Cette exigence PEUT être satisfaite en écrivant les horodatages dans les messages syslog.

Avertissements : Il est difficile de corréler les enregistrements provenant de zones horaires différentes. Les événements de sécurité sur l'Internet impliquent souvent des machines et des enregistrements provenant de localisations physiques diverses. Pour cette raison, l'UTC est préféré, toutes choses égales par ailleurs.

### **2.11.9 Les enregistrements contiennent des adresses IP non traduites**

Exigence : Les messages d'enregistrement NE DOIVENT PAS faire la liste des adresses traduites (noms DNS) associées aux adresses sans faire la liste des adresses IP non traduites lorsque l'adresse IP est disponible pour l'appareil qui génère le message d'enregistrement.

Justification : Inclure l'adresse IP des tentatives de violations de liste d'accès, d'authentification, les allocations de prêt

d'adresse et des événements similaires dans les journaux d'événements permet un niveau d'identification individuelle et organisationnelle et est nécessaire pour permettre l'analyse des événements de réseau, des incidents, des violations de politique, etc.. Les entrées du DNS tendent à changer plus rapidement que les allocations de blocs IP. Cela rend l'adresse plus fiable pour l'analyse des données. Les recherches dans le DNS peuvent être lentes et consomment des ressources.

Exemples : Un échec de connexion réseau devrait générer un enregistrement avec l'adresse de source de la tentative de connexion.

Avertissements :

- \* Les adresses de source peuvent être falsifiées. Les attaques fondées sur le réseau utilisent souvent des adresses de source falsifiées. Les adresses de source ne devraient pas être crues a priori sauf à être vérifiées par d'autres moyens.
- \* Les adresses peuvent être réallouées à différents individus, par exemple, dans un environnement d'ordinateurs portables utilisant DHCP. Dans de tels cas, l'identification de l'individu visée par cette exigence est faible. Avoir une heure précise dans l'enregistrement augmente les chances que l'utilisation d'une adresse puisse être corrélée à un individu.
- \* Les topologies de réseau peuvent changer. Même en l'absence d'allocation dynamique d'adresse, les topologies de réseau et les allocations de bloc d'adresses changent. Les enregistrements d'une attaque d'il y a un mois peuvent ne pas donner une indication précise de l'hôte, du réseau ou de l'organisation qui possédait le ou les systèmes en question à ce moment.

#### **2.11.10 Les enregistrements contiennent les événements de sécurité**

Exigence : L'appareil DOIT être capable d'envoyer un enregistrement d'au moins les événements suivants :

- \* réussites d'authentification,
- \* échecs d'authentification,
- \* terminaison de session,
- \* changements d'autorisation,
- \* changements de configuration,
- \* changements d'état d'appareil.

L'appareil DEVRAIT être capable d'envoyer un enregistrement de tous les autres événements en rapport avec la sécurité.

Justification : ceci est important parce que cela prend en charge l'identification des individus. Voir le paragraphe 4.5.4.4 de la [RFC2196].

Exemples : Les exemples d'événements pour lesquels il doit y avoir un enregistrement incluent les connexions des usagers, les mauvaises tentatives de connexion, les fins de connexion, les changements de niveau de privilège d'utilisateur, les commandes de configuration individuelles produites par les usagers et les événements de démarrage/fermeture de système.

Avertissements : cette liste est loin d'être complète.

Noter qu'il peut y avoir des considérations juridiques ou de confidentialité lors de l'enregistrement/surveillance des activités des utilisateurs.

#### **2.11.11 Les enregistrements ne contiennent pas de mot de passe**

Exigence : Les mots de passe DEVRAIENT être exclus de tous les enregistrements d'audit, y compris des enregistrements de tentatives d'authentification réussies ou non.

Justification : les exigences de contrôle d'accès et d'autorisation diffèrent pour les enregistrements comptables (les journaux d'événements) et pour les bases de données d'autorisation (mots de passe). Enregistrer les mots de passe peut accorder un accès non autorisé aux individus qui ont accès aux journaux d'enregistrement. L'enregistrement des échecs de mots de passe peut donner des indications sur les mots de passe réels. Voir au paragraphe 4.5.4.4 de la [RFC2196].

Exemples : un usager peut faire de petites fautes en entrant un mot de passe comme d'utiliser une casse incorrecte ("mon mot de passe" au lieu de "Mon mot de Passe").

Avertissement : il peut y avoir des situations où il est approprié/exigé d'enregistrer les mots de passe.

### **2.12 Exigences d'authentification, autorisation, et comptabilité (AAA)**

#### **2.12.1 Authentifier tous les accès d'utilisateur**

Exigence : L'appareil DOIT fournir une facilité d'effectuer l'authentification de tous les accès d'utilisateur au système.

Justification : cette fonctionnalité est exigée afin que l'accès au système puisse être restreinte au personnel autorisé.

Exemples : Cette exigence PEUT être satisfaite en mettant en œuvre un système d'authentification centralisé. Voir au paragraphe 2.12.5. Elle PEUT aussi être satisfaite en utilisant une authentification locale. Voir au paragraphe 2.12.6.

Avertissement : aucun.

### **2.12.2 Prise en charge de l'authentification d'utilisateurs individuels**

Exigence : Les mécanismes utilisés pour authentifier l'accès interactif pour la configuration et la gestion DOIVENT prendre en charge l'authentification d'utilisateurs individuels distincts. Cette exigence PEUT être atténuée pour prendre en charge l'installation de système du paragraphe 2.4.5 ou la récupération de l'accès autorisé du paragraphe 2.12.15.

Justification : l'utilisation de comptes individuels, en conjonction avec la connexion, promeut l'identification. L'utilisation de comptes de groupe ou par défaut compromet l'identification individuelle.

Exemples : un usager peut avoir besoin de se connecter à l'appareil pour accéder à des fonctions de CLI pour la gestion. L'authentification des usagers individuels pourrait être fournie par un serveur d'authentification centralisé ou une base de données de noms d'utilisateur/mots de passe mémorisée sur l'appareil. Ce serait une violation de cette règle pour l'appareil de ne prendre en charge qu'un seul "compte" (avec ou sans nom d'utilisateur) et un seul mot de passe partagé par tous les usagers pour obtenir l'accès administratif.

Avertissements : cela exige simplement que le mécanisme de prise en charge des usagers individuels soit présent. Une politique (par exemple, interdire les comptes partagés par un groupe) et sa mise en application sont aussi nécessaires mais sortent du domaine d'application du présent document.

### **2.12.3 Prise en charge de connexions simultanées**

Exigence : L'appareil DOIT prendre en charge plusieurs connexions simultanées par des utilisateurs distincts, éventuellement à des niveaux d'autorisation différents.

Justification : cela permet à plusieurs personnes d'effectuer des fonctions de gestion autorisées simultanément. Cela signifie aussi que des tentatives de connexions par des usagers non autorisés ne bloquent pas automatiquement les utilisateurs autorisés.

Exemple : aucun.

Avertissement : aucun.

### **2.12.4 Capacité de désactiver tous les comptes locaux**

Exigence : L'appareil DOIT fournir un moyen pour désactiver tous les comptes locaux y compris :

- \* les utilisateurs locaux,
- \* les comptes par défaut (fabricant, maintenance, invités, etc.),
- \* les comptes privilégiés et non privilégiés.

Un compte local est défini comme celui où toutes les informations nécessaires pour l'authentification de l'utilisateur sont mémorisées dans l'appareil.

Justification : les comptes par défaut, les comptes bien connus, et les vieux comptes, sont des cibles faciles pour quelqu'un qui tente d'obtenir l'accès à un appareil. Il doit être possible de les désactiver pour réduire la vulnérabilité potentielle.

Exemples : la mise en œuvre dépend des types d'authentification pris en charge par l'appareil.

Avertissement : aucun.

### **2.12.5 Prise en charge de méthodes d'authentification d'utilisateur centralisée**

Exigence : L'appareil DOIT prendre en charge une méthode d'authentification centralisée de tous les accès d'utilisateur via des protocoles d'authentification standard.

Justification : la prise en charge de l'authentification centralisée est particulièrement importante dans les grands

environnements où le réseau d'appareils est largement réparti et où de nombreuses personnes y ont accès. Cela réduit la quantité d'efforts pour réduire efficacement et retracer les accès au système par le personnel autorisé.

Exemples : Cette exigence peut être satisfaite par l'utilisation de DIAMETER [RFC3588], TACACS+ [RFC1492], RADIUS [RFC2865], ou Kerberos [RFC1510]. Les exigences de gestion sécurisée (paragraphe 2.1.1) s'appliquent à l'AAA. Voir dans la [RFC3579] une discussion des questions de sécurité relatives à RADIUS.

Avertissement : aucun.

### **2.12.6 Prise en charge d'une méthode d'authentification de l'utilisateur local**

Exigence : L'appareil DEVRAIT prendre en charge une méthode d'authentification locale. Si elle est mise en œuvre, la méthode NE DOIT PAS exiger d'interaction avec quelque chose d'externe à l'appareil (comme un serveur AAA distant) et DOIT fonctionner en conjonction avec le paragraphe 2.3.1 (prendre en charge une interface de 'console') et le paragraphe 2.12.7 (prendre en charge la configuration de l'ordre des méthodes d'authentification).

Justification : la prise en charge de l'authentification locale peut être exigée dans de plus petits environnements où il peut n'y avoir que peu d'appareils et un nombre de personnes limité qui ont accès. Le surcoût de la maintenance de serveurs d'authentification centralisée peut n'être pas justifié.

Exemples : l'utilisation de noms d'utilisateur et mots de passe locaux, par appareil donne un moyen pour mettre en œuvre cette exigence.

Avertissements : les informations d'authentification doivent être protégées partout où elles résident. Avoir, par exemple, des noms d'utilisateur et des mots de passe locaux mémorisés sur cent appareils réseau signifie qu'il y a un potentiel de cent points de fuite par où les informations pourraient être compromises au lieu de mémoriser les données d'authentification dans des serveurs centralisés, ce qui réduirait les points de fuite potentiels au nombre de serveurs et permet de focaliser les efforts de protection (renforcement du système, audits, etc.) sur au plus quelques serveurs.

### **2.12.7 Prendre en charge la configuration de l'ordre des méthodes d'authentification**

Exigence : L'appareil DOIT prendre en charge la capacité de configurer l'ordre dans lequel sont tentées les méthodes d'authentification prises en charge. L'authentification DEVRAIT "fermer par défaut", c'est-à-dire, l'accès devrait être refusé si aucune des méthodes d'authentification énumérées ne réussit.

Justification : cela permet à l'opérateur la souplesse de mettre en œuvre les politiques de sécurité appropriées qui équilibrent les besoins de fonctionnement et de sécurité.

Exemples : si, par exemple, un appareil prend en charge l'authentification RADIUS et les noms d'utilisateur et mots de passe locaux, il devrait être possible de spécifier que l'authentification RADIUS devrait être tentée si les serveurs sont disponibles, et que les noms d'utilisateur et mots de passe locaux devraient être utilisés pour l'authentification seulement si les serveurs RADIUS ne sont pas disponibles. De façon similaire, il devrait être possible de spécifier que seule l'authentification RADIUS ou seule l'authentification locale est utilisée.

Avertissement : aucun.

### **2.12.8 Capacité d'authentification sans mot de passe en clair**

Exigence : L'appareil DOIT prendre en charge des mécanismes qui n'exigent pas la transmission de mots de passe en clair dans tous les cas qui exigent la transmission des informations d'authentification à travers les réseaux.

Justification : les mots de passe en clair peuvent être facilement observés en utilisant des renifleurs de paquet sur des réseaux partagés. Voir la [RFC1704] et la [RFC3631] pour un exposé complet.

Exemples : la connexion à distance exige la transmission d'informations d'authentification à travers les réseaux. Telnet transmet des mots de passe en clair. SSH ne le fait pas. Telnet échoue à cette exigence. SSH réussit.

Avertissement : aucun.

### 2.12.9 Pas de mot de passe par défaut

Exigence : la configuration initiale de l'appareil NE DOIT PAS contenir de mots de passe par défaut ou d'autres jetons d'authentification.

Justification : les mots de passe par défaut fournissent un moyen facile aux agresseurs pour obtenir un accès non autorisé à l'appareil.

Exemples : des mots de passe comme le nom du fabricant, de l'appareil, "par défaut", etc. sont faciles à deviner. Les chaînes de communauté SNMP "public" et "privée" sont bien connues comme mots de passe par défaut qui donnent un accès en lecture et écriture aux appareils.

Avertissements : des listes de mots de passe par défaut pour divers appareils sont directement disponibles sur de nombreux sites de la Toile.

### 2.12.10 Les mots de passe doivent être explicitement configurés avant l'utilisation

Exigence : L'appareil DOIT exiger que l'opérateur configure explicitement les "mots de passe" avant l'utilisation.

Justification : Cette exigence est destinée à empêcher un accès non autorisé à la gestion. Exiger que l'opérateur configure explicitement les mots de passe tendra à avoir pour effet d'assurer une diversité de mots de passe. Il fait aussi glisser la responsabilité du choix des mots de passe à l'utilisateur.

Exemples : Supposons qu'un appareil vienne avec un accès de console pour la gestion et un compte administratif par défaut. Cette exigence jointe à celle d'exclusion des mots de passe par défaut dit que le compte administratif devrait venir sans mot de passe configuré. Une façon de satisfaire cette exigence serait que l'appareil exige de l'opérateur qu'il choisisse un mot de passe pour le compte administratif au titre du dialogue la première fois que l'appareil est configuré.

Avertissements : Bien que cet appareil exige de l'opérateur qu'il établisse les mots de passe, cela ne les empêche pas de faire des choses comme l'utilisation de scripts pour configurer des centaines d'appareils avec le même mot de passe facile à deviner.

### 2.12.11 Capacité de définir des niveaux de privilège

Exigence : Il DOIT être possible de définir des sous ensembles arbitraires de toutes les fonctions de gestion et de configuration et de les allouer à des groupes ou "niveaux de privilège", qui peuvent être alloués aux utilisateurs conformément au paragraphe 2.12.12. Il DOIT y avoir au moins trois niveaux de privilège possibles.

Justification : Cette exigence prend en charge la mise en œuvre du principe de "moindre privilège", qui déclare qu'un individu ne devrait avoir que les privilèges nécessaires pour exécuter les opérations qu'il est obligé d'effectuer.

Exemples : des exemples de niveaux de privilège pourraient inclure celui de "usager" qui ne permet que l'initiation d'une session PPP ou telnet, "lecture seule", qui permet l'accès en lecture seule à la configuration de l'appareil et aux statistiques de fonctionnement, "racine/super utilisateur/administrateur" qui permet l'accès et la mise à jour de tous les paramètres configurables, et "opérateur" qui permet les mises à jour à un ensemble de paramètres limité, défini par l'utilisateur. Noter que les niveaux de privilège peuvent être définis en local sur l'appareil ou sur des serveur d'authentification centralisés.

Avertissement : aucun.

### 2.12.12 Capacité d'allouer des niveaux de privilège aux utilisateurs

Exigence : L'appareil DOIT être capable d'allouer un ensemble défini de fonctions autorisées, ou "niveaux de privilège", pour chaque utilisateur une fois qu'ils se sont authentifiés auprès de l'appareil. Le niveau de privilège détermine quelles fonctions un utilisateur est autorisé à exécuter. Voir aussi au paragraphe 2.12.11.

Justification : Cette exigence prend en charge la mise en œuvre du principe de "moindre privilège", qui déclare qu'un individu devrait seulement avoir les privilèges nécessaires pour exécuter les opérations qu'il est obligé d'effectuer.

Exemples : la mise en œuvre de cette exigence va évidemment être étroitement couplée avec le mécanisme d'authentification. Si on utilise RADIUS, un attribut pourrait être établi dans le profil RADIUS de l'usager qui peut être utilisé pour transposer l'identifiant à un certain niveau de privilège.

Avertissement : aucun.

### 2.12.13 Le niveau de privilège par défaut doit être 'aucun'

Exigence : Le niveau de privilège par défaut NE DEVRAIT PAS permettre d'accès aux fonctions de gestion ou de configuration. Il PEUT permettre l'accès aux fonctions de niveau utilisateur (par exemple, commencer PPP ou telnet). Il DEVRAIT être possible d'allouer un niveau de privilège différent comme niveau par défaut. Cette exigence PEUT être atténuée pour prendre en charge l'installation de système selon le paragraphe 2.4.5 ou la récupération d'un accès autorisé selon le paragraphe 2.12.15.

Justification : Cette exigence prend en charge la mise en œuvre du principe de "moindre privilège", qui déclare qu'un individu devrait seulement avoir les privilèges nécessaires pour exécuter les opérations qu'il est obligé d'effectuer.

Exemples : des exemples de niveaux de privilège pourraient inclure celui de "usager" qui ne permet que l'initiation d'une session PPP ou telnet, "lecture seule", qui permet l'accès en lecture seule à la configuration de l'appareil et aux statistiques de fonctionnement, "racine/super utilisateur/administrateur" qui permet l'accès et la mise à jour de tous les paramètres configurables, et "opérateur" qui permet les mises à jour à un ensemble de paramètres limité, défini par l'utilisateur. Noter que les niveaux de privilège peuvent être définis en local sur l'appareil ou sur des serveurs d'authentification centralisés.

Avertissements : Il peut être exigé que soient apportées des exceptions à la prise en charge de l'exigence de soutien de la récupération de l'accès privilégié (paragraphe 2.12.15) et de prendre en charge l'installation et la configuration du système d'exploitation (paragraphe 2.4.5). Par exemple, si le système d'exploitation et/ou de configuration est devenu plus ou moins corrompu, un individu autorisé avec accès physique peut avoir besoin d'avoir l'accès de niveau "racine" pour effectuer une installation.

### 2.12.14 Le changement de niveau de privilège exige la ré authentification

Exigence : L'appareil DOIT ré authentifier un usager avant d'accorder tout changement d'autorisation d'utilisateur.

Justification : Cette exigence assure que les utilisateurs sont capables d'effectuer des actions autorisées.

Exemples : Cette exigence pourrait être mise en œuvre par l'allocation des niveaux de base de privilège à tous les utilisateurs et en permettant à l'usager de demander des privilèges supplémentaires, avec des demandes validées par le serveur AAA.

Avertissement : aucun.

### 2.12.15 Prise en charge de la récupération d'accès privilégié

Exigence : L'appareil DOIT prendre en charge un mécanisme pour permettre aux individus autorisés de récupérer les pleins privilèges d'accès administratif dans l'éventualité d'une perte de l'accès. L'utilisation du mécanisme DOIT exiger un accès physique à l'appareil. Il PEUT y avoir un mécanisme pour désactiver le dispositif de récupération.

Justification : Il arrive que les mots de passe administratifs locaux soient perdus, quand la seule personne qui les connaît quitte la société, ou quand des pirates ont établi ou changé le mot de passe. Dans tous ces cas, l'accès administratif légitime à l'appareil est perdu. Il devrait y avoir un moyen pour récupérer l'accès. Exiger l'accès physique pour invoquer la procédure rend moins vraisemblable qu'il en soit fait un usage abusif. Des organisations peuvent vouloir un niveau de sécurité encore plus fort et vouloir risquer la perte totale d'accès autorisé en désactivant le dispositif de récupération, même pour ceux avec accès physique.

Exemples : des exemples des façons de satisfaire cette exigence sont d'avoir l'appareil qui donne à l'usager une chance d'établir un nouveau mot de passe administratif lorsque :

- \* l'usager établit une bretelle sur le tableau système pour une position particulière,
- \* l'usager envoie une séquence particulière à l'accès console RS232 durant la séquence d'amorçage initial,
- \* l'usager établit "un registre d'amorçage" à une valeur particulière.

Avertissements : ce mécanisme, par conception, donne une "porte de derrière" pour réaliser le contrôle administratif de l'appareil et peut n'être pas approprié pour des environnements où ceux qui ont l'accès physique à l'appareil peuvent ne pas être de confiance. Voir aussi l'avertissement du paragraphe 2.3.1 (Prise en charge de l'interface 'console').

### 2.13 Les appareils de couche 2 doivent satisfaire les exigences des couches supérieurs

Exigence : Si un appareil fournit des services de couche 2 qui dépendent de services de couche 3 ou plus, les portions qui opèrent à la couche 3 ou au dessus DOIVENT se conformer aux exigences décrites dans le présent document.

Justification : Tous les appareils de couche 3 ont des besoins de sécurité similaires et devraient être soumis à des exigences similaires.

Exemples : les protocoles de signalisation exigés pour la commutation de couche 2 peuvent échanger des informations avec les autres appareils en utilisant des communications de couche 3. Dans de tels cas, l'appareil doit fournir une facilité de couche 3 sûre. Aussi, si des capacités de couches supérieures (disons, SSH ou SNMP) sont utilisées pour gérer un appareil de couche 2, le reste des exigences du présent document s'applique à ces capacités.

Avertissement : aucun.

### 2.14 Les dispositifs de sécurité ne devraient pas causer de problème de fonctionnement

Exigence : L'utilisation de dispositifs de sécurité spécifiés par les exigences du présent document NE DEVRAIENT PAS causer de problèmes de fonctionnement sévères.

Justification : les dispositifs de sécurité qui causent des problèmes de fonctionnement ne sont pas utiles et peuvent laisser l'opérateur sans mécanisme pour appliquer la politique appropriée.

Exemples : certains exemples de problèmes sévères de fonctionnement incluent :

- \* l'arrêt de l'appareil,
- \* l'appareil devient ingérable,
- \* les données sont perdues,
- \* l'utilisation du dispositif de sécurité consomme des ressources excessives (CPU, mémoire, bande passante).

Avertissements : La détermination de la conformité à cette exigence implique un niveau de jugement. Qu'est ce qui est "sévère" ? Certainement l'arrêt du fonctionnement est sévère, mais qu'en est-il de 5 % de perte de débit lorsque la connexion est activée ? On devrait aussi noter qu'il peut y avoir des limitations physiques inévitables, comme la capacité totale d'une liaison.

### 2.15 Les dispositifs de sécurité devraient avoir un impact minimal sur les performances

Exigence : Les dispositifs de sécurité spécifiés par les exigences du présent document DEVRAIENT être mis en œuvre avec un impact minimal sur les performances. D'autres paragraphes du présent document peuvent spécifier des exigences de performances différentes (par exemple, des "DOIT").

Justification : Les dispositifs de sécurité qui ont un impact significatif sur les performances peuvent laisser l'opérateur sans mécanisme pour appliquer la politique appropriée.

Exemples : Si l'application de filtres est connue pour avoir un potentiel de réduction significative du débit pour le trafic non filtré, il y aura une tendance, ou dans certains cas une politique, de non utilisation de filtres. Supposons par exemple, qu'un nouveau ver soit lâché qui examine au hasard les adresses IP à la recherche d'écoutes de services sur l'accès TCP 1433. Un opérateur peut vouloir faire des investigations pour voir si des hôtes de son réseau ont été infectés et essayent de répandre le ver. Une façon de le faire serait d'établir des filtres non bloquants qui comptent et enregistrent le nombre de connexions 1433 sortantes, et de bloquer ensuite les demandes dont il est déterminé qu'elles viennent des hôtes infectés. Si une de ces capacités (filtrage, comptage, enregistrement) a le potentiel d'imposer de sévères réductions de performances, ce cours d'action par ailleurs rationnel pourrait n'être pas possible.

Avertissements : Les exigences pour lesquelles les performances sont un souci particulier incluent le filtrage, la limitation de débit, les compteurs, l'enregistrement et l'anti falsification.

## 3. Exigences de documentation

Les exigences de cette section sont destinées à faire la liste des informations qui vont aider les opérateurs à évaluer et faire fonctionner en toute sécurité un appareil.

### 3.1 Identifier les services autorisés à écouter

Exigence : Le fabricant DOIT fournir une liste de tous les services qui peuvent être actifs sur l'appareil. La liste DOIT identifier les protocoles et les accès par défaut (si c'est applicable) sur lesquels les services écoutent. Elle DEVRAIT fournir des références à la documentation complète qui décrit le service.

Justification : Ces informations sont nécessaires pour permettre une évaluation précise des risques potentiels de sécurité associés au fonctionnement de chaque service.

Exemples : La liste va probablement contenir des protocoles réseau et de transport tels que IP, ICMP, TCP, UDP, des protocoles d'acheminement tels que BGP et OSPF, des protocoles d'application tels que SSH et SNMP ainsi que des références aux RFC ou autre documentation qui décrivent les versions des protocoles mis en œuvre.

Les serveurs de la Toile écoutent "usuellement" sur l'accès 80. Dans la configuration par défaut de l'appareil, il peut y avoir un serveur de la Toile qui écoute sur l'accès 8080. Dans le contexte de cette exigence "identifier ...l'accès par défaut" signifierait "l'accès 8080".

Avertissements : Il peut y avoir des raisons valides, non techniques pour ne pas divulguer les spécifications des protocoles propriétaires. Dans ce cas, tout ce qui doit être divulgué est l'existence du service et les accès par défaut (si applicable).

### 3.2 Documenter les valeurs par défaut du service

Exigence : Le fabricant DOIT fournir une liste de l'état par défaut de tous les services.

Justification : Comprendre les risques exige de comprendre l'exposition. Chaque service activé présente un certain niveau d'exposition. Avoir une liste des services qui sont activés par défaut rend possible d'effectuer une analyse des risques significatifs.

Exemples : La liste peut n'être rien de plus que le résultat d'une commande qui mette en œuvre le paragraphe 2.5.1.

Avertissement : aucun.

### 3.3 Documenter le processus d'activation du service

Exigence : Le fabricant DOIT documenter brièvement les dispositifs qui activent et désactivent les services.

Justification : Une fois le risque évalué, cette liste donne à l'opérateur un moyen rapide pour comprendre comment désactiver (ou activer les services non désirés (ou désirés).

Exemples : Ce peut être une liste de commandes pour activer/désactiver les services un par un ou une seule commande qui active/désactive des groupes de commandes "standard".

Avertissement : aucun.

### 3.4 Documenter l'interface de ligne de commande

Exigence : Le fabricant DOIT fournir une documentation complète de l'interface de ligne de commande avec chaque livraison du logiciel. La documentation DEVRAIT inclure un précis des changements depuis les versions précédentes. La documentation DEVRAIT faire la liste du résultat potentiel de chaque commande.

Justification : La compréhension des entrées et de leur résultat est nécessaire pour la prise en charge des descriptifs. Voir au paragraphe 2.4.2.

Exemples : Une documentation séparée devrait être fournie pour chaque commande en donnant la liste de la syntaxe, des paramètres, des options, etc. ainsi que du résultat attendu (état, tableaux, etc.).

Avertissement : aucun.

### 3.5 Documentation du profil de communication 'Console' par défaut

Exigence : Le profil console par défaut des paramètres de communications DOIT être publié dans la documentation du système.

Justification : La publication dans la documentation du système rend les réglages accessibles. Manquer à les publier pourrait obliger l'opérateur à devoir les deviner.

Exemple : aucun.

Avertissement : aucun.

## 4. Exigences d'assurance

Les exigences de cette section sont destinées à :

- o identifier les comportements et les informations qui vont accroître la confiance que l'appareil va satisfaire les exigences fonctionnelles de sécurité ;
- o fournir des informations qui vont aider à effectuer les évaluations de la sécurité.

### 4.1 Identifier l'origine de la pile IP

Exigence : Le fabricant DEVRAIT divulguer l'origine ou les bases de la pile IP utilisée sur le système.

Justification : Ces informations sont exigées pour mieux comprendre les possibles faiblesses de la sécurité qui peuvent être inhérentes à la pile IP.

Exemples : "La pile IP a été déduite de BSD 4.4", ou "La pile IP a été mise en œuvre à partir de rien."

Avertissements : De nombreuses piles IP font des hypothèses simplificatrices sur la façon dont un paquet IP devrait être formé. Un paquet mal formé peut causer un comportement inattendu dans l'appareil, comme une panne du système ou un débordement de mémoire tampon qui peut résulter en un accès non autorisé au système.

### 4.2 Identifier l'origine du système d'exploitation

Exigence : Le fabricant DEVRAIT divulguer l'origine ou la base du système d'exploitation (OS, *operating system*).

Justification : Cette information est exigée pour mieux comprendre les faiblesses de la sécurité qui peuvent être inhérentes à l'OS sur la base de son origine.

Exemples : "Le système d'exploitation se fonde sur le noyau Linux 2.4.18."

Avertissement : aucun.

## 5. Considérations sur la sécurité

Générales

La sécurité est le sujet du présent mémoire. La section des justifications de chaque exigence individuelle fait la liste des implications pour la sécurité de la satisfaction ou de la non satisfaction de l'exigence.

SNMP

Les versions de SNMP avant SNMPv3 n'incluaient pas une sécurité adéquate. Même si le réseau lui-même est sûr (par exemple en utilisant IPsec) il n'y a même alors pas de contrôle sur qui est admis à accéder au réseau sûr et à obtenir ou régler avec les commandes GET/SET (lire/changer/créer/supprimer) les objets dans la MIB.

Il est recommandé que les mises en œuvre envisagent les caractéristiques de sécurité comme fournies par le cadre de SNMPv3 (voir la [RFC3410], section 8) incluant la pleine prise en charge des mécanismes de chiffrement de SNMPv3 (pour l'authentification et la protection de la confidentialité).

De plus, le déploiement des versions de SNMP antérieures à SNMPv3 N'EST PAS RECOMMANDÉ. À la place, il est RECOMMANDÉ de déployer SNMPv3 et d'activer la sécurité cryptographique. Il est alors de la responsabilité du consommateur/opérateur de s'assurer que l'entité SNMP qui donne accès aux objets de la MIB est configurée de façon appropriée pour donner accès aux objets seulement aux principaux (usagers) qui ont des droits légitimes à exécuter sur eux les commandes GET ou SET (changer/créer/supprimer).

## 6. Références

- [ANSI.X9-52] American National Standards Institute, "Triple Data Encryption Algorithm Modes of Operation", ANSI X9.52, 1998.
- [bmwg-acc] Poretzky, S., "Framework for Accelerated Stress Benchmarking", Travail en cours, octobre 2003.
- [FIPS.197] National Institute of Standards et Technology, "Advanced Encryption Standard", FIPS PUB 197, novembre 2001, < <http://csrc.nist.gov/publications/fips/fips197/fips-197.ps> >.
- [PKCS.3] RSA Laboratories, "Diffie-Hellman Key-Agreement Standard, Version 1.4", PKCS 3, novembre 1993.
- [RFC1208] O. Jacobsen et D. Lynch, "[Glossaire des termes de réseautage](#)", mars 1991. (*Info*)
- [RFC1321] R. Rivest, "Algorithme de [résumé de message MD5](#)", avril 1992. (*Information*)
- [RFC1492] C. Finseth, "Un protocole de contrôle d'accès, parfois appelé TACACS", juillet 1993. (*Information*)
- [RFC1510] J. Kohl et C. Neuman, "Service Kerberos d'authentification de réseau (v5)", septembre 1993. (*Obsolète, voir RFC6649*)
- [RFC1704] N. Haller et R. Atkinson, "[Authentification sur l'Internet](#)", octobre 1994. (*Information*)
- [RFC1812] F. Baker, "[Exigences pour les routeurs IP](#) version 4", juin 1995. (*MàJ par les RFC2644, RFC6633*)
- [RFC1918] Y. Rekhter et autres, "Allocation d'[adresse pour les internets privés](#)", BCP 5, février 1996.
- [RFC2026] S. Bradner, "Le processus de [normalisation de l'Internet](#) -- Révision 3", ([BCP0009](#)) octobre 1996. (*Remplace RFC1602, RFC1871*) (*MàJ par RFC3667, RFC3668, RFC3932, RFC3979, RFC3978, RFC5378, RFC6410*)
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
- [RFC2196] B. Fraser, "[Manuel de la sécurité des sites](#)", septembre 1997. ([FYI0008](#)) (*Information*)
- [RFC2246] T. Dierks et C. Allen, "[Protocole TLS version 1.0](#)", janvier 1999.
- [RFC2385] A. Heffernan, "Protection des sessions de BGP via l'option de signature MD5 de TCP", août 1998. (*P.S. (MàJ par la RFC6691)*) (*Remplacée par RFC5925*)
- [RFC2401] S. Kent et R. Atkinson, "[Architecture de sécurité](#) pour le protocole Internet", novembre 1998. (*Obsolète, voir RFC4301*)
- [RFC2631] E. Rescorla, "Méthode d'[accord de clé Diffie-Hellman](#)", juin 1999. (*P.S.*)
- [RFC2827] P. Ferguson, D. Senie, "[Filtrage d'entrée de réseau](#) : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP", mai 2000. (*MàJ par RFC3704*) ([BCP0038](#))
- [RFC2865] C. Rigney et autres, "Service d'[authentification à distance de l'utilisateur appelant](#) (RADIUS)", juin 2000. (*MàJ par RFC2868, RFC3575, RFC5080*) (*D.S.*)
- [RFC3013] T. Killalea, "[Services et procédures de sécurité recommandés](#) pour les fournisseurs de service Internet",

novembre 2000. ([BCP0046](#))

- [RFC3164] C. Lonvick, "Protocole BSD de Syslog", août 2001. (*Information*)
- [RFC3174] D. Eastlake 3 et P. Jones, "[Algorithme US de hachage](#) sécurisé n° 1 (SHA1)", sept. 2001. (*Info, MàJ par 4634 et 6234*)
- [RFC3195] D. New, M. Rose, "[Livraison fiable pour syslog](#)", novembre 2001. (*P.S.*)
- [RFC3309] J. Stone, R. Stewart, D. Otis, "Changement de somme de contrôle du protocole de transmission de commandes de flux (SCTP)". septembre 2002. (*Obsolète, voir [RFC4960](#)*) (*P.S.*)
- [RFC3330] IANA, "Adresses IPv4 d'usage particulier", septembre 2002. (*Information*) (*Remplacée par [RFC5735](#)*)
- [RFC3360] S. Floyd, "[Réinitialisations inappropriées de TCP](#) considérées comme dommageables", août 2002. ([BCP0060](#))
- [RFC3410] J. Case et autres, "Introduction et déclarations d'applicabilité pour le cadre de gestion standard de l'Internet", décembre 2002. (*Information*)
- [RFC3411] D. Harrington, R. Presuhn, B. Wijnen, "[Architecture de description des cadres de gestion](#) du protocole simple de gestion de réseau (SNMP)", décembre 2002. (*MàJ par [RFC5343](#)*) ([STD0062](#))
- [RFC3447] J. Jonsson et B. Kaliski, "[Normes de cryptographie à clés publiques](#) (PKCS) n° 1 : Spécifications de la cryptographie RSA version 2.1", février 2003.
- [RFC3562] M. Leech, "Considérations sur la gestion de clés pour l'option de signature MD5 dans TCP", juillet 2003. (*Information*)
- [RFC3579] B. Aboba, P. Calhoun, "Prise en charge du protocole d'authentification extensible (EAP) par RADIUS", septembre 2003. (*MàJ par [RFC5080](#)*) (*Information*)
- [RFC3588] P. Calhoun et autres, "Protocole fondé sur Diameter", septembre 2003. (*Remplacée par la [RFC6733](#)*) (*P.S.*)
- [RFC3631] S. Bellovin, J. Schiller et C. Kaufman, éd., "[Mécanismes de sécurité pour l'Internet](#)", décembre 2003. (*Information*)
- [RFC3704] F. Baker, P. Savola, "[Filtrage d'entrée pour réseaux à rattachement multiples](#)", mars 2004. ([BCP0084](#))
- [RFC3766] H. Orman, P. Hoffman, "[Détermination de la force des clés publiques](#) utilisées pour l'échange de clés symétriques", avril 2004. ([BCP0086](#))
- [Schneier] Schneier, B., "Applied Cryptography", 2nd Ed., Publisher John Wiley & Sons, Inc., 1996.

## Appendice A Profils d'exigences

Cet Appendice énumère différents profils. Un profil est une liste d'exigences qui s'appliquent à une classe particulière d'appareils. Le profil d'exigences minimum s'applique à tous les appareils.

### A.1 Profil minimum d'exigences

Les fonctionnalités citées ici représentent un ensemble minimum des exigences auxquelles l'infrastructure gérée des grands réseaux IP devrait adhérer.

Le profil minimal des exigences vise les fonctionnalités qui vont fournir des capacités raisonnables pour gérer les appareils dans l'éventualité d'attaques, simplifier les dépannages, garder trace des événements qui affectent l'intégrité du système; aider à analyser les causes des attaques, ainsi qu'à fournir aux administrateurs le contrôle sur les adresses IP et les protocoles pour aider à atténuer les attaques et exploitations les plus courantes.

- o Prise en charge de canaux sûrs pour la gestion
- o Utiliser des protocoles soumis à révision ouverte pour la gestion
- o Utiliser des algorithmes de chiffrement soumis à révision ouverte

- o Utiliser un chiffrement fort
- o Permettre le choix des paramètres de chiffrement
- o Les fonctions de gestion devraient avoir une priorité accrue
- o Prise en charge d'une interface de 'console'
- o Le profil de communication de 'console' doit prendre en charge la réinitialisation
- o Le profil de communication de 'console' est documenté
- o La 'console' exige les fonctions minimales des appareils rattachés
- o Prise en charge d'interfaces IP de plan de gestion séparés
- o Pas de transmission entre plan de gestion et les autres interfaces
- o La 'CLI' donne accès à toutes les fonctions de configuration et de gestion
- o La 'CLI' prend en charge l'inscription des configurations
- o La 'CLI' prend en charge la gestion sur des liaisons 'lentes'
- o Documenter l'interface de ligne de commande
- o Prise en charge de l'installation de logiciel
- o Prise en charge de la sauvegarde de configuration à distance
- o Prise en charge de la restauration de configuration à distance
- o Prise en charge des fichiers de configuration de texte
- o Capacité à identifier tous les services écoutants
- o Capacité à désactiver tout et tous services
- o Capacité à contrôler les liens de service pour les services écoutants
- o Capacité à contrôler les adresses de source de service
- o Capacité à filtrer le trafic
- o Capacité à filtrer le trafic vers l'appareil
- o Prise en charge du filtrage de chemin
- o Capacité de spécifier des actions de filtrage
- o Capacité à enregistrer des action de filtrage
- o Capacité à filtrer sans dégradation significative des performances
- o Capacité à spécifier la granularité des enregistrements de filtre
- o Capacité à filtrer sur les protocoles
- o Capacité à filtrer sur les adresses
- o Capacité à filtrer sur les champs d'en-tête de protocole
- o Capacité à filtrer en entrée et en sortie
- o Exigences de compteur de filtre de paquets
- o Exigence de comptages des paquets filtrés
- o Capacité à afficher les compteurs de filtre par règle
- o Capacité à afficher les compteurs de filtre par application de filtre
- o Capacité à remettre à zéro les compteurs de filtre
- o Les compteurs de filtre doivent être précis
- o Les facilités d'enregistrement utilisent des protocoles soumis à révision ouverte
- o Les enregistrements sont envoyés à des serveurs distants
- o Capacité à enregistrer en local
- o Capacité à maintenir une heure réseau précise
- o Affichage de la zone horaire et du décalage à l'UTC
- o La zone horaire par défaut devrait être l'UTC
- o Les enregistrements doivent être horodatés
- o Les enregistrements contiennent des adresses IP non traduites
- o Les enregistrements contiennent les événements de sécurité
- o Authentifier tous les accès d'utilisateur
- o Prise en charge de l'authentification des utilisateurs individuels
- o Prise en charge des connexions simultanées
- o Capacité à désactiver tous les comptes locaux
- o Prise en charge centralisée des méthodes d'authentification d'utilisateur
- o Prise en charge locale de la méthode d'authentification d'utilisateur
- o Prise en charge de la configuration de l'ordre des méthodes d'authentification
- o Capacité à authentifier sans mot de passe en clair
- o Les mots de passe doivent être explicitement configurés avant utilisation
- o Pas de mot de passe par défaut
- o Capacité à définir des niveaux de privilège
- o Capacité à allouer des niveaux de privilège aux utilisateurs
- o Le niveau de privilège par défaut doit être 'aucun'
- o Le changement de niveau de privilège exige la ré-authentification
- o Prise en charge de la récupération de l'accès privilégié
- o Les enregistrements ne contiennent pas de mot de passe

- o Les dispositifs de sécurité ne doivent pas causer de problème de fonctionnement
- o Les dispositifs de sécurité devraient avoir un impact minimal sur les performances
- o Identifier les services qui peuvent être en écoute
- o Documenter les services par défaut
- o Documenter le processus d'activation de service
- o Identifier l'origine de la pile IP
- o Identifier l'origine du système d'exploitation
- o Identifier l'origine de la pile IP
- o Les appareils de couche 2 doivent satisfaire les exigences des couches supérieures

## A.2 Profil de bordure réseau de couche 3

Ce paragraphe s'appuie sur la liste des exigences de A.1 et ajoute des fonctions de sécurité plus rigoureuses spécifiques des appareils de couche 3 qui font partie de la bordure du réseau. La bordure du réseau est normalement l'endroit où sont mises en œuvre la plupart des politiques de filtrage et de contrôle du trafic.

Un appareil de bordure se définit comme un appareil qui constitue l'infrastructure du réseau et se connecte directement aux abonnés ou aux homologues. Cela va inclure les routeurs connectés aux points d'échange, aux commutateurs qui se connectent aux hôtes des abonnés, etc.

- o Prise en charge de l'anti falsification automatique pour les réseaux à un seul rattachement
- o Prise en charge de l'élimination automatique des bogons et des martiens
- o Prise en charge de compteurs de paquets éliminés
- o Prise en charge de la limitation de débit
- o Prise en charge de l'application directionnelle de la limitation de débit par interface
- o Prise en charge de la limitation de débit fondée sur l'état
- o Capacité à filtrer le trafic à travers l'appareil.

## Appendice B. Remerciements

Le présent document se fonde sur un document sur les exigences de sécurité internes utilisé par UUNET pour vérifier les appareils qui étaient proposés pour connexion au cœur de réseau.

L'éditeur remercie de leurs contributions : Greg Sayadian, auteur d'un prédécesseur du présent document, Eric Brandwine, comme source majeure d'idées et de critiques, la corporation MITRE pour son soutien continu au développement de ce document.

Note : l'affiliation de l'éditeur à The MITRE Corporation n'est donnée qu'à des fins d'identification, et n'est pas destinée à porter ou impliquer la concurrence ou le soutien de MITRE avec les positions, opinions ou points de vue exprimés par l'éditeur.

L'ancienne équipe de sécurité réseau de UUNET : Jared Allison, Eric Brandwine, Clarissa Cook, Dave Garn, Tae Kim, Kent King, Neil Kirr, Mark Krause, Michael Lamoureux, Maureen Lee, Todd MacDermid, Chris Morrow, Alan Pitts, Greg Sayadian, Bruce Snow, Robert Stone, Anne Williams, Pete White.

D'autres qui ont fourni des retours significatifs à divers stades de la vie de ce document sont : Ran Atkinson, Fred Baker, Steve Bellovin, David L. Black, Michael H. Behringer, Matt Bishop, Scott Blake, Randy Bush, Pat Cain, Ross Callon, Steven Christey, Owen Delong, Sean Donelan, Robert Elmore, Barbara Fraser, Barry Greene, Jeffrey Haas, David Harrington, Dan Hollis, Jeffrey Hutzelman, Merike Kaeo, James Ko, John Kristoff, Chris Lonvick, Chris Liljenstolpe, James W. Laferriere, Jared Mauch, Perry E. Metzger, Mike O'Connor, Alan Paller, Rob Pickering, Pekka Savola, Gregg Schudel, Juergen Schoenwaelder, Don Smith, Rodney Thayer, David Walters, Joel N. Weber II, Russ White, Anthony Williams, Neal Ziring.

Madge B. Harrison et Patricia L. Jones, ont effectué la relecture technique. Cette liste est destinée à reconnaître les contributions, et non à impliquer que les individus ou organisations approuvent le contenu de ce document. Mes excuses à ceux qui ont commenté ou ont contribué au document et ne sont pas cités.

## Adresse de l'auteur

George M. Jones  
The MITRE Corporation  
7515 Colshire Drive, M/S WEST  
McLean, Virginia 22102-7508  
U.S.A.

téléphone : +1 703 488 9740  
mél : [gjm3871@pobox.com](mailto:gjm3871@pobox.com)

## Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2004). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de droits de reproduction ci-dessus et le présent paragraphe soient inclus dans toutes telles copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de droits de reproduction ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour le besoin du développement des normes Internet, auquel cas les procédures de droits de reproduction définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou ses successeurs ou ayant droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

### Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr>.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

### Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.