Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

M.3016.3

(04/2005)

SÉRIE M: GESTION DES TÉLÉCOMMUNICATIONS Y COMPRIS LE RGT ET MAINTENANCE DES RÉSEAUX

Réseau de gestion des télécommunications

Sécurité pour le plan de gestion: mécanisme de sécurité

Recommandation UIT-T M.3016.3

Union internationale des télécommunications

RECOMMANDATIONS UIT-T DE LA SÉRIE M

GESTION DES TÉLÉCOMMUNICATIONS Y COMPRIS LE RGT ET MAINTENANCE DES RÉSEAUX

Introduction et principes généraux de maintenance et organisation de la maintenance	M.10–M.299
Systèmes de transmission internationaux	M.300–M.559
Circuits téléphoniques internationaux	M.560–M.759
Systèmes de signalisation à canal sémaphore	M.760–M.799
Systèmes internationaux de télégraphie et de phototélégraphie	M.800–M.899
Liaisons internationales louées par groupes primaires et secondaires	M.900–M.999
Circuits internationaux loués	M.1000–M.1099
Systèmes et services de télécommunication mobile	M.1100–M.1199
Réseau téléphonique public international	M.1200–M.1299
Systèmes internationaux de transmission de données	M.1300–M.1399
Appellations et échange d'informations	M.1400–M.1999
Réseau de transport international	M.2000–M.2999
Réseau de gestion des télécommunications	**M.3000–M.3599**
Réseaux numériques à intégration de services	M.3600–M.3999
Systèmes de signalisation par canal sémaphore	M.4000–M.4999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T M.3016.3

Sécurité pour le plan de gestion: mécanisme de sécurité

Résumé

La présente Recommandation définit les mécanismes de sécurité pour le plan de gestion dans le réseau de gestion des télécommunications (RGT). La présente Recommandation porte en particulier sur la question de la sécurité du plan de gestion pour les éléments de réseaux (NE, *network element*) et les systèmes de gestion (MS, *management system*), qui font partie de l'infrastructure de télécommunication.

Source

La Recommandation UIT-T M.3016.3 a été approuvée le 13 avril 2005 par la Commission d'études 4 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Introduction

L'infrastructure de télécommunication revêtant une importance fondamentale pour les communications et l'économie mondiales, une sécurité satisfaisante des fonctions de gestion régissant cette infrastructure s'impose. En dépit des nombreuses normes de sécurité applicables à la gestion des réseaux de télécommunication, peu d'entre elles sont effectivement appliquées et les applications sont incompatibles entre les divers équipements et logiciels de télécommunication. La présente Recommandation définit les mécanismes de sécurité permettant aux constructeurs, aux administrations et aux fournisseurs de services de mettre en place une infrastructure de gestion des télécommunications sécurisée. Bien que l'ensemble actuel des mécanismes de sécurité rende compte de l'état actuel des connaissances, les technologies continueront de progresser à mesure que les circonstances évolueront. Pour être utile, la présente Recommandation devra évoluer à mesure que les circonstances le justifieront. La présente Recommandation a pour objet de constituer un point de départ. Les fournisseurs de services peuvent y inclure des mécanismes de sécurité supplémentaires destinés à répondre à leurs besoins particuliers, en plus de ceux qui y figurent déjà.

La présente Recommandation constitue une des Recommandations UIT-T de la série M.3016.x visant à donner des indications et formuler des recommandations relatives à la sécurisation du plan de gestion de réseaux évolutifs:

Rec. UIT-T M.3016.0 – *Sécurité pour le plan de gestion: aperçu général*.

Rec. UIT-T M.3016.1 – *Sécurité pour le plan de gestion: prescriptions de sécurité*.

Rec. UIT-T M.3016.2 – *Sécurité pour le plan de gestion: services de sécurité*.

Rec. UIT-T M.3016.3 – *Sécurité pour le plan de gestion: mécanisme de sécurité*.

Rec. UIT-T M.3016.4 – *Sécurité pour le plan de gestion: formulaire de sécurité*.

Recommandation UIT-T M.3016.3

Sécurité pour le plan de gestion: mécanisme de sécurité

1 Domaine d'application

Les Recommandations UIT-T M.3016.1 à M.3016.3 définissent un ensemble de prescriptions, de services et de mécanismes permettant d'assurer dûment la sécurité des fonctions de gestion nécessaires à la prise en charge de l'infrastructure de télécommunication. Les administrations et organisations nécessitant des niveaux d'assistance variables sur le plan de la sécurité, les Recommandations UIT-T M.3016.1 à M.3016.3 ne précisent pas si une prescription, un service ou un mécanisme est obligatoire ou optionnel.

La présente Recommandation définit les mécanismes de sécurité pour le plan de gestion dans le réseau de gestion des télécommunications (RGT). La présente Recommandation porte en particulier sur la question de la sécurité du plan de gestion pour les éléments de réseaux (NE, *network element*) et les systèmes de gestion (MS, *management system*), qui font partie de l'infrastructure de télécommunication.

De caractère générique, la présente Recommandation ne définit ou n'aborde pas les mécanismes de sécurité applicables à telle ou telle interface du réseau de gestion des télécommunications (RGT).

Le formulaire défini dans la Rec. UIT-T M.3016.4 a pour objet d'aider les organisations, administrations et autres organismes nationaux ou internationaux à déterminer le caractère obligatoire ou optionnel de la prise en charge des prescriptions ainsi que les séries de valeurs et autres éléments qui faciliteront l'implémentation de leurs politiques de sécurité.

2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

– Recommandation UIT-T G.8080/Y.1304 (2001), *Architecture du réseau optique à commutation automatique (ASON)*, plus Amendement 2 (2005).

– Recommandation UIT-T M.3010 (2000), *Principes du réseau de gestion des télécommunications.*

– Recommandation UIT-T M.3016.0 (2005), *Sécurité pour le plan de gestion: aperçu général*.

– Recommandation UIT-T M.3016.2 (2005), *Sécurité pour le plan de gestion: services de sécurité*.

– Recommandation UIT-T M.3016.3 (2005), *Sécurité pour le plan de gestion: mécanisme de sécurité*.

– Recommandation UIT-T M.3016.4 (2005), *Sécurité pour le plan de gestion: formulaire de sécurité*.

– Recommandation UIT-T X.509 (2000), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*, plus Corrigendum 1 (2001), Corrigendum 2 (2002) et Corrigendum 3 (2004).

– Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*, plus Amendement 1 (1996).

– Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout*.

3 Définitions

La présente Recommandation ne définit aucun nouveau terme.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

CORBA architecture de courtier commun de requête d'objets (*common object request broker architecture*)

DoS refus de service (*denial of service*)

EMS système de gestion d'élément (*element management system*)

FTP protocole de transfert de fichiers (*file transfer protocol*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

IETF groupe de travail d'ingénierie Internet (*Internet engineering task force*)

IP protocole Internet (*Internet protocol*)

IPSec sécurité du protocole Internet (*Internet protocol security*)

ISO/CEI Organisation Internationale de Normalisation/Commission électrotechnique internationale

MS système de gestion: EMS, NMS ou OSS[1] (*management system*)

NE élément de réseau (*network element*)

NE/MS NE ou MS

NMS système de gestion de réseau (*network management system*)

NTP protocole relatif au temps dans le réseau (*network time protocol*)

NTPv3 NTP version 3

OAM&P exploitation, administration, maintenance et fourniture (*operations, administration, maintenance, and provisioning*)

OS système d'exploitation (*operating system*)

OSS système support d'exploitation (*operations support system*)

RFC demande de commentaires (*request for comments*)

RGT réseau de gestion des télécommunications

---

[1] Les systèmes support d'exploitation (OSS), en règle générale, peuvent être utilisés dans le même contexte que les systèmes de gestion (MS) dans n'importe quelle couche de la hiérarchie du réseau de gestion des télécommunications.

SAML langage de balisage d'assertion de sécurité (*security assertion markup language*)

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

SNMPv3 protocole simple de gestion de réseau, version 3 (*simple network management protocol version 3*)

SOAP protocole simple d'accès aux objets (*simple object access protocol*)

SSH protocole SSH (*secure shell*)

SSL protocole SSL (*secure socket layer*)

TCP protocole de commande de transmission (*transmission control protocol*)

TLS sécurité de la couche de transport (*transport layer security*)

UIT-T Union internationale des télécommunications – Secteur de la normalisation des télécommunications

XML langage de balisage extensible (*extensible markup language*)

5 Conventions

Dans les Recommandations UIT-T M.3016.1, M.3016.2 et M.3016.3, un descripteur est utilisé pour identifier les prescriptions, les services et les mécanismes. Ce descripteur consiste en l'une des étiquettes à trois lettres suivantes, suivie d'un numéro:

– REQ pour prescription;

– SER pour service;

– MEC pour mécanisme.

6 Mécanismes de sécurité

Le présent paragraphe énonce les mécanismes de sécurité propres aux systèmes d'exploitation, administration, maintenance et fourniture (OAM&P, *operations, administration, maintenance and provisioning*) et aux systèmes support d'exploitation (OSS, *operations support system*), applicables en particulier à la sécurité de l'infrastructure, des services et des applications dans le cadre du plan de gestion.

Le Tableau 1 reproduit de la Rec. UIT-T M.3016.0 reprend le Tableau 4 de la Rec. UIT-T M.3016.0. Ce tableau, qui donne un aperçu général de la relation entre les prescriptions et les services de sécurité, sert de point de départ pour l'organisation des autres documents de la série. Par exemple, la Rec. UIT-T M.3016.1 traite des prescriptions fonctionnelles de sécurité, la Rec. UIT-T M.3016.2 traite des services de sécurité et la présente Recommandation (Rec. UIT-T M.3016.3) traite des mécanismes de sécurité spécifiques correspondant aux services de sécurité.

Le présent paragraphe ne définit que les services de sécurité qui relèvent de solutions courantes; les autres services possibles (détection de refus de service, par exemple) ne sont pas abordés.

Tableau 1/M.3016.3 – Mappage entre prescriptions et services de sécurité

Prescription fonctionnelle de sécurité	Service de sécurité
Vérification d'identité	authentification de l'utilisateur authentification d'entité homologue authentification de l'origine des données
Contrôle d'accès et d'autorisation	contrôle d'accès
Protection de la confidentialité – données stockées	contrôle d'accès confidentialité
Protection de la confidentialité – données transférées	confidentialité
Protection de l'intégrité des données – données stockées	contrôle d'accès
Protection de l'intégrité des données – données transférées	intégrité
Responsabilité	non-répudiation
Journal d'activités	trace d'audit
Compte rendu d'alarme de sécurité	alarme de sécurité
Audit de sécurité	trace d'audit
Protection du réseau de communication de données (RCD)	contrôle des paquets

Le Tableau 2 ci-dessous indique sommairement la structure du présent paragraphe:

Tableau 2/M.3016.3 – Structure du présent paragraphe

Paragraphe	Contenu
6.1	Traite des mécanismes de sécurité d'authentification, parmi lesquels: authentification de l'utilisateur, authentification d'entité homologue.
6.2	Traite de l'authentification de l'origine des données.
6.3	Traite des mécanismes de sécurité de contrôle d'accès.
6.4	Traite des mécanismes de sécurité de confidentialité des données.
6.5	Traite des mécanismes de sécurité d'intégrité des données.
6.6	Traite des mécanismes de sécurité de trace d'audit.

6.1 Authentification de l'utilisateur

L'authentification de l'utilisateur consiste à vérifier l'identité déclarée par une personne. L'authentification de l'utilisateur peut être régie par différents mécanismes de sécurité, à savoir:

– combinaison d'une identité d'utilisateur et d'un mot de passe (suffisamment complexe) éventuellement à utilisation unique (identité sécurisée, par exemple);

– authentification à plusieurs facteurs;

– authentification par signature unique.

Les mécanismes de sécurité d'authentification de l'utilisateur sont examinés dans le présent paragraphe.

6.1.1 Authentification de l'identité d'utilisateur et des mots de passe

L'identité d'utilisateur et des mots de passe statiques peuvent être utilisés pour authentifier l'utilisateur. Cette opération exige de vérifier l'identité de l'utilisateur légitime du système et d'empêcher tout utilisateur illégitime d'usurper l'identité de celui-ci. Lorsqu'elle est dûment effectuée, l'authentification des utilisateurs permet de suivre les activités de ceux-ci et de leur

appliquer des restrictions d'accès les limitant à des activités ou des rôles préalablement autorisés, comme indiqué au § 6.2.

L'authentification de l'identité et du mot de passe des utilisateurs passe dans un premier temps par l'attribution d'une identité unique à chaque utilisateur, puis par l'attribution d'un mot de passe secret suffisamment complexe utilisé conjointement avec l'identité de l'utilisateur pour vérifier l'identité de celui-ci.

Les mots de passe doivent comporter suffisamment de caractères et autres éléments aléatoires pour éviter qu'ils puissent être extorqués par quiconque ou par des techniques automatisées. Comme exemples de mots de passe répondant à de telles caractéristiques de complexité, citons, entre autres:

MEC 1: mots de passe devant obligatoirement comporter un nombre minimal de caractères (huit caractères, par exemple).

MEC 2: mots de passe ne pouvant pas comporter certains caractères.

MEC 2a: mots de passe ne pouvant pas comporter une reprise dans le même ordre ou en ordre inverse de l'identité d'utilisateur associée.

MEC 2b: mots de passe ne pouvant pas comporter en aucune de leurs parties un ensemble de séquences de caractères configurés (mots d'un dictionnaire ou noms de produits, par exemple).

MEC 3: mots de passe ne pouvant pas comporter plus d'un certain nombre de caractères identiques consécutifs.

MEC 4: mots de passe devant obligatoirement comporter au moins un certain nombre de caractères alphabétiques minuscules et/ou majuscules.

MEC 5: mots de passe devant obligatoirement comporter au moins un certain nombre de caractères numériques.

MEC 6: mots de passe devant obligatoirement comporter au moins un certain nombre de caractères spéciaux.

La gestion des mots de passe contribue pour beaucoup à assurer un système d'authentification sécurisé. Par exemple, les capacités du système de gestion des mots de passe suivantes peuvent être souhaitées:

MEC 7: le système de gestion des mots de passe peut exiger la saisie de l'ancien mot de passe pour empêcher un autre utilisateur de modifier le mot de passe d'un utilisateur connecté à l'insu de celui-ci.

MEC 8: le système peut vérifier automatiquement que chaque nouveau mot de passe de connexion diffère du mot de passe précédent. (Les mots de passe étant généralement mémorisés par chiffrement unidirectionnel, la saisie de l'ancien mot de passe peut aussi être exigée pour permettre au système de déterminer le degré de différence entre l'ancien mot de passe et le nouveau[2]).

MEC 9: le système peut archiver les anciens mots de passe pour éviter qu'ils ne soient réutilisés.

MEC 10: le système peut imposer la modification des mots de passe à des intervalles de temps déterminés.

---

[2] Au lieu du chiffrement unidirectionnel, on peut recourir, à titre exceptionnel, au chiffrement symétrique pour les mots de passe qui doivent être déchiffrés pour usage transitoire interne dans une communication sécurisée de système à système ou dans une signature unique.

MEC 11: au bout d'un certain nombre de tentatives d'introduction d'un mot de passe invalide, le système peut limiter encore le nombre de nouvelles tentatives pendant un certain temps (60 minutes, par exemple) ou se verrouiller, interdisant ainsi l'accès aux utilisateurs concernés, qui pourront avoir à contacter le personnel chargé de la gestion de la sécurité pour mettre fin à l'état de verrouillage.

6.1.2 Authentification à plusieurs facteurs

Le terme "authentification à plusieurs facteurs" désigne un processus d'authentification nécessitant deux types d'information ou de facteurs différents ou plus pour établir l'identité de l'utilisateur aux fins de l'authentification de celui-ci. Le fait d'exiger plusieurs facteurs renforce la sécurité du système d'authentification en évitant de n'avoir à s'en remettre qu'à un seul facteur qui pourrait être plus facile à usurper.

Les facteurs d'authentification généralement utilisés dans les systèmes d'authentification de l'utilisateur à plusieurs facteurs sont notamment les suivants:

quelque chose que **connaît** l'utilisateur:	mot de passe secret ou phrase de passe secrète, par exemple.
quelque chose que **possède** l'utilisateur:	jeton, carte à puce, générateur de mot de passe à utilisation unique
quelque chose qui **caractérise en propre** l'utilisateur:	empreinte digitale ou autre mesure biométrique.

Un mécanisme courant d'authentification à plusieurs facteurs est l'authentification à deux facteurs, qui nécessite deux pièces d'identité pour l'authentification. Un exemple type d'authentification à deux facteurs nous est donné par le système des cartes bancaires dans lequel l'utilisateur doit, d'une part, être en possession de sa carte et, d'autre part, prouver qu'il connaît le numéro d'identification personnel (PIN, *personal identification number*) secret associé à la carte.

MEC 12: authentification à plusieurs facteurs avec indication du nombre de facteurs.

6.1.3 Authentification de l'utilisateur par signature unique

L'authentification de l'utilisateur peut mettre en œuvre les méthodes applicables à la signature unique sécurisée et à l'infrastructure des certificats de clé publique X.509. Dans le cas de la signature unique sécurisée, le protocole continue d'initier l'entité ou les entités concernées à produire des pièces d'identité; toutefois, un utilisateur peut ne pas avoir à les introduire du fait que celles-ci sont déjà stockées de manière sécurisée dans la mémoire cache d'une manière ou d'une autre (Kerberos, par exemple). Le recours aux techniques de la signature unique sécurisée permet d'éviter à l'utilisateur d'avoir à s'authentifier à maintes reprises auprès du système, ce qui risquerait de devenir contraignant.

MEC 13: authentification par signature unique.

6.2 Authentification de l'entité homologue et de l'origine des données

Le recours aux mécanismes d'authentification de l'entité homologue permet de vérifier l'identité déclarée par chacun des systèmes homologues. On recourt aux mécanismes de sécurité d'authentification de l'origine des données pour s'assurer que les messages reçus proviennent bien du système qui prétend les avoir envoyés. Etroitement liées entre elles, l'authentification de l'entité homologue et l'authentification de l'origine des données peuvent être régies, entre autres, par les mécanismes de sécurité suivants:

– mécanismes d'authentification cryptographique;

– mécanismes d'authentification par connexion sécurisée.

Ces mécanismes de sécurité d'authentification sont examinés dans le présent paragraphe.

6.2.1 Authentification cryptographique

Les mécanismes d'authentification cryptographique assurent l'authentification pendant les communications de données entre systèmes (de système à système ou d'application à application, par exemple) et sont à la base de l'établissement de communications privées avec intégrité des données. Pendant des communications de données, l'authentification cryptographique de l'entité émettrice permet au destinataire d'un message d'authentifier l'identité de l'expéditeur (authentification de l'entité homologue) et de déterminer l'origine du message (authentification de l'origine des données). Dans une voie de communication sécurisée, l'authentification de l'entité homologue et de l'origine des données peut reposer sur des informations cryptographiques associées à chaque message de manière à lier l'identité de l'entité émettrice au message. Le destinataire vérifiera les informations cryptographiques fournies avec le message pour confirmer la véracité de l'identité de l'entité émettrice.

Parmi les techniques cryptographiques qui peuvent être utilisées pour authentifier l'entité homologue et l'origine des données, citons: les techniques de chiffrement à clé publique ou à clé symétrique, les techniques à signatures numériques et les techniques de hachage numérique)[3]. L'authentification cryptographique peut être unidirectionnelle lorsqu'une seule extrémité de la conversation est authentifiée, ou bidirectionnelle lorsque les deux extrémités sont authentifiées. L'authentification bidirectionnelle est plus sûre et peut contribuer à prévenir des attaques actives.

MEC 14: authentification de l'entité homologue et de l'origine des données par chiffrement à clé publique.

MEC 15: authentification de l'entité homologue et de l'origine des données par chiffrement à clé symétrique.

MEC 16: authentification de l'entité homologue et de l'origine des données par signatures numériques.

MEC 17: authentification de l'entité homologue et de l'origine des données par des techniques de hachage numérique.

MEC 18: authentification cryptographique bidirectionnelle.

6.2.2 Authentification de l'utilisateur par connexion sécurisée

L'authentification par connexion sécurisée est un mécanisme de sécurité au moyen duquel les interactions d'authentification de système à système sont assurées sur une connexion sécurisée. Ce mécanisme ne peut être activé que par le système et est impossible à imiter. Une connexion sécurisée peut être une connexion physique dédiée (autrement dit une connexion directe entre un terminal et un système) ou une connexion chiffrée, sur laquelle protection de l'intégrité et protection "anti-rejeu" sont assurées (réseau privé virtuel IPSec, tunnel SSL/TLS (*secure socket layer/transport layer security*) ou protocole SSH (*secure shell*))[4]. Voir l'Appendice I pour une analyse des protocoles de sécurité IPSec, SSL/TLS et SSH.

MEC 19: authentification de l'entité homologue et de l'origine des données par connexion sécurisée.

6.3 Contrôle d'accès

Un réseau de gestion des télécommunications (RGT) peut faire en sorte que les parties intéressées ne puissent pas accéder aux informations ou ressources auxquelles elles ne sont pas autorisées à

---

[3] American National Standards Institute T1.243-1995, *Operations, Administration, Maintenance.*

[4] Selon le National Computer Security Center, NCSC-TG-004-88, *Glossary of Computer Security Terms*, octobre 1998 (peut être consulté à l'adresse suivante http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf.

accéder. Les mécanismes de sécurité de contrôle d'accès font que seuls les utilisateurs agréés sont autorisés à gérer les ressources de sécurité du système.

La mise en place de mécanismes de sécurité de contrôle d'accès peut être assurée par un système centralisé, souvent associé au système d'authentification. Ainsi, un serveur centralisé RADIUS système d'accès à distance (RADIUS, *remote access dial-in user system*) associé à une base de données LDAP protocole rapide d'accès à l'annuaire (LDAP, *lightweight directory access protocol*) peut être utilisé pour mettre en place un système centralisé d'authentification et de contrôle d'accès.

Les mécanismes de sécurité de contrôle d'accès peuvent présenter certaines des caractéristiques suivantes:

MEC 20: les différentes mesures administratives peuvent être liées à certaines personnes.

MEC 21: le mécanisme de sécurité de contrôle d'accès peut admettre la notion de "moindre privilège" (c'est-à-dire qu'une personne sera investie d'une mission et sera autorisée à consulter ou modifier des données ou à mettre en œuvre des mesures de gestion pour les seules fonctions autorisées dans le cadre de cette mission).

MEC 22: possibilité d'interdiction de verrouillage de plusieurs comptes d'administrateur au moins pour cause d'activités liées au mot de passe, telles que échecs ou délais d'attente de connexion.

MEC 23: plusieurs missions d'administrateur peuvent être définies, avec chacune des degrés variables de privilège afférents aux actions de gestion de sécurité essentielles. Ainsi, un système peut définir cinq missions d'administrateur alors qu'un autre système peut n'en définir que trois. Dans un cas comme dans l'autre, les missions peuvent être définies pour autoriser différents privilèges afférents aux actions de sécurité suivantes:

MEC 23a: définir et assigner des privilèges d'utilisateur

MEC 23b: ajouter et supprimer des identités d'utilisateur

MEC 23c: initialiser et réinitialiser des mots de passe de connexion

MEC 23d: initialiser et modifier des clés de chiffrement

MEC 23e: fixer, pour le système, la durée de validité des mots de passe de connexion

MEC 23f: fixer, pour le système, le nombre maximal d'échecs de connexion pour chaque identité d'utilisateur

MEC 23g: supprimer un verrouillage ou modifier, pour le système, la valeur de temporisation pour le verrouillage

MEC 23h: fixer, pour le système, la valeur de temporisation pour l'inactivité

MEC 23i: configurer une journalisation de sécurité et des alarmes de sécurité pour le système

MEC 23j: gérer les processus de journalisation de sécurité pour le système

MEC 23k: mettre à jour les logiciels de sécurité

MEC 23l: terminer les sessions d'utilisateur ou de système

MEC 23m: définir et assigner de nouveaux privilèges d'utilisateur ou de groupe au niveau de l'application

MEC 23n: conserver un enregistrement de toutes les demandes d'accès à l'application

MEC 23o: ajouter et supprimer des utilisateurs au niveau de l'application

MEC 23p: surveiller tous les journaux de sécurité de l'application

MEC 23q: configurer une journalisation de sécurité et des alarmes de sécurité pour l'application

MEC 23r: gérer les processus de journalisation de sécurité de l'application

MEC 23s: terminer les sessions d'application d'utilisateur.

6.4 Confidentialité des données

Les mécanismes de sécurité de confidentialité des données sont utilisés pour empêcher la réception non autorisée des données communiquées. Les mécanismes de sécurité cryptographiques permettant d'assurer la confidentialité des données sont examinés dans le présent paragraphe.

La confidentialité des données repose sur la cryptographie. Celle-ci utilise des algorithmes spéciaux basés sur des normes et accessibles au public, ce qui permet de les soumettre à un examen approfondi et de les mettre en œuvre facilement. La "force" de la cryptographie est fonction de l'algorithme cryptographique utilisé ainsi que de la longueur de clé utilisée (en d'autres termes, la force se mesure au temps nécessaire pour déterminer par ingénierie inverse (c'est-à-dire sur la base de constatations ou de conjectures) la ou les valeurs de clé utilisées avec un algorithme donné).

Les protocoles de sécurité (IPSec, SSL/TLS et SSH, par exemple) assurent généralement l'authentification de l'origine des données ainsi que l'intégrité et la confidentialité de celles-ci. (Voir l'Appendice I pour une analyse des protocoles de sécurité IPSec, SSL/TLS et SSH). Les extensions de sécurité à d'autres protocoles tels que le protocole simple de gestion de réseau, version 3 (SNMPv3)[5], l'architecture de courtier commun de requête d'objets (CORBA), le protocole de passerelle frontière (BGP, *border gateway protocol*) et le plus court chemin ouvert en premier (OSPF, *open shortest path first)* sont conçues pour assurer l'authentification de l'origine des données et l'intégrité des données.

Les méthodes utilisées pour produire, mémoriser, communiquer, détruire ou annuler des clés cryptographiques de confidentialité des données revêtent une importance cruciale. En outre, des facteurs tels que la longueur ou le choix des clés ainsi que le choix de l'algorithme ont une incidence directe sur la force de la sécurité d'un système cryptographique donné.

6.4.1 Confidentialité des données par clé symétrique

Le chiffrement à clé symétrique ou secrète s'applique à un système cryptographique dans lequel les clés de chiffrement et de déchiffrement sont identiques. Les systèmes cryptographiques à clé symétrique imposent la prise de dispositions initiales pour permettre aux différents utilisateurs de partager une clé secrète unique (la clé de chiffrement, par exemple). Cette clé doit être communiquée aux utilisateurs par des moyens sécurisés, ou produite à l'intérieur même du système (à partir d'une clé racine secrète partagée, par exemple) car connaître la clé de chiffrement ne va pas sans connaître la clé de déchiffrement, et vice versa.

Les mécanismes de sécurité de confidentialité des données peuvent utiliser des algorithmes cryptographiques symétriques tels que les algorithmes DES norme de chiffrement de données (DES, *data encryption standard*), AES norme de chiffrement évoluée (AES, *advanced encryption standard*), 3DES algorithme DES triple (3DES, *triple data encryption algorithm*) ou d'autres algorithmes.

L'algorithme DES, qui utilise le chiffrement à clé symétrique de 56 bits, est utilisé depuis de nombreuses années. Sa faible longueur de clé l'exposant à saturation lors de calculs parallèles massifs, l'algorithme DES est considéré aujourd'hui comme étant faible. Son utilisation est déconseillée par le *US National Institute of Standards and Technology* (NIST).

L'algorithme AES a été choisi par le NIST comme algorithme de chiffrement à clé symétrique normalisé en remplacement de l'algorithme DES pour les applications du secteur public aux Etats-Unis. L'algorithme AES utilise des longueurs de clé de 128, 192 et 256 bits.

L'algorithme 3DES n'est autre, somme toute, que l'algorithme DES appliqué à trois reprises, avec deux ou trois clés de 56 bits. L'algorithme 3DES est défini dans la Publication 46-3 de la Federal Information Processing Standard (FIPS), *Data Encryption Standard*, Octobre 1999, Appendice 2,

---

[5] Le protocole SNMPv3 peut aussi assurer la confidentialité.

Page 22 (qui peut être consultée à l'adresse suivante: http://csirc.nist.gov/publications/fips/fips46-3/fips46-3.pdf).

L'algorithme 3DES peut être mis en œuvre avec deux clés indépendantes de 56 bits ou trois clés indépendantes de 56 bits, censées correspondre respectivement à une force de 112 bits et de 168 bits. Toutefois, l'algorithme 3DES n'est pas à l'abri d'une attaque à texte clair connu, également dénommée attaque "meet in the middle", pouvant en ramener la force, pour deux clés indépendantes, à 57 bits seulement au lieu des 112 bits escomptés ou, pour trois clés indépendantes, à 112 bits seulement au lieu des 168 bits escomptés. En conséquence, pour une plus grande sécurité, il convient d'utiliser l'algorithme 3DES avec trois clés indépendantes, pour une force minimale, dans le cas le plus défavorable, de 112 bits.

Si l'algorithme DES peut être mis en œuvre relativement rapidement, en raison de sa faible longueur de clé de 56 bits, l'algorithme 3DES – qui, grosso modo, doit appliquer l'algorithme DES à trois reprises – est de ce fait beaucoup plus lent. L'algorithme AES, dont la longueur minimale de clé est de 128 bits, est plus fort sur le plan cryptographique que l'algorithme 3DES tout en pouvant être mis en œuvre très rapidement dans les équipements et les logiciels. Ainsi, une implémentation logicielle de l'algorithme AES peut être traitée pratiquement aussi rapidement que l'algorithme DES sur la même plate-forme, mais avec une force cryptographique bien supérieure à celle de l'algorithme DES.

MEC 24: confidentialité des données par clé symétrique selon l'algorithme cryptographique DES.

MEC 25: confidentialité des données par clé symétrique selon l'algorithme cryptographique AES.

MEC 26: confidentialité des données par clé symétrique selon l'algorithme cryptographique 3DES.

6.4.2 Confidentialité des données par clé asymétrique

Un système de chiffrement à clé asymétrique est un système dans lequel les clés de chiffrement et de déchiffrement sont interdépendantes tout en étant différentes. L'une est rendue publique, tandis que l'autre est tenue secrète. La clé publique est différente de la clé privée, et il passe pour être matériellement impossible d'obtenir la clé privée à partir de la clé publique. Si les clés publiques sont souvent communiquées, la clé privée est toujours tenue secrète.

Les mécanismes de sécurité de confidentialité des données peuvent utiliser des algorithmes cryptographiques asymétriques tels que l'algorithme RSA (*Rivest, Shamir, Adleman*), l'algorithme cryptographie à courbe elliptique (ECC, *elliptic curve cryptography*) ou d'autres algorithmes.

L'algorithme RSA est un algorithme asymétrique d'usage courant qui peut être utilisé à des fins de chiffrement ou pour des signatures numériques. L'algorithme RSA répond à la difficulté qu'il y a en mathématiques à factoriser les nombres premiers de grande taille. Les longueurs de clé courantes pour l'algorithme RSA sont de 1024 bits et 2048 bits. Notons qu'un algorithme RSA avec une longueur de clé de 2048 bits équivaut approximativement, en termes de force cryptographique, à un chiffrement symétrique de 128 bits.

La cryptographie à courbe elliptique (ECC) est une nouvelle méthode de mise en œuvre de la cryptographie à clé publique (comparable, en d'autres termes, à l'algorithme RSA). La cryptographie ECC permet de définir une courbe elliptique sur un certain champ, sur lequel on résoudra ensuite le problème dit du logarithme discret sur les courbes elliptiques. Le principal avantage de l'algorithme ECC par rapport aux autres algorithmes à clé publique, réside dans la longueur de la clé. Une clé d'algorithme ECC de 160 bits équivaut approximativement en termes de sécurité à une clé d'algorithme RSA de 1024 bits, et une clé d'algorithme ECC de 210 bits équivaut approximativement à une clé d'algorithme RSA de 2048 bits. Par sa longueur moindre, la clé de

l'algorithme ECC permet à la fois de réduire les coûts des calculs et de renforcer l'efficacité du système cryptographique[6].

MEC 27: confidentialité des données par clé asymétrique selon l'algorithme cryptographique RSA, avec indication de la longueur de clé.

MEC 28: confidentialité des données par clé asymétrique selon l'algorithme cryptographique ECC, avec indication de la longueur de clé.

6.4.3 Confidentialité des données – Résumé

Le Tableau 3 donne des exemples d'algorithmes qui peuvent être utilisés pour assurer la confidentialité des données. Il convient également d'examiner un certain nombre de points tels que le formatage, le bourrage, le traitement des erreurs, le choix de nombres entiers appropriés, la longueur de l'exposant public ainsi que, dans le cas de l'algorithme ECC, le champ et la courbe de base; toutefois, ces points ne relèvent pas du domaine d'application de la présente Recommandation.

Tableau 3/M.3016.3 – Exemples d'algorithmes cryptographiques utilisés pour assurer la confidentialité des données

Catégorie	Algorithme	Observations
Algorithmes de chiffrement symétrique	AES	Norme de chiffrement évoluée
	3-DES (triple DES)	Triple algorithme de chiffrement de données
	DES	Norme de chiffrement de données
Algorithmes de chiffrement asymétrique	RSA	Rivest, Shamir, Adleman
	ECC	Cryptographie à courbe elliptique

6.5 Intégrité des données

Les mécanismes de sécurité d'intégrité des données sont utilisés pour garantir que les données communiquées n'ont pas été modifiées.

L'intégrité des données repose sur la cryptographie. Celle-ci utilise des algorithmes spéciaux basés sur des normes et accessibles au public, ce qui permet de les soumettre à un examen approfondi et de les mettre en œuvre facilement. Les protocoles de sécurité (IPSec, SSL/TLS, SSH, par exemple) assurent généralement des services d'intégrité des données basés sur des algorithmes cryptographiques sous-jacents ainsi que d'autres services de sécurité tels que les services de confidentialité des données et d'authentification de l'origine des données. (Voir l'Appendice I pour une analyse des protocoles de sécurité IPSec, SSL/TLS et SSH).

Les méthodes utilisées pour produire, mémoriser, communiquer, détruire ou annuler des clés cryptographiques d'intégrité des données revêtent une importance cruciale. En outre, des facteurs tels que la longueur ou le choix des clés ainsi que le choix de l'algorithme ont une incidence directe sur la force de la sécurité d'un système cryptographique donné.

6.5.1 Intégrité des données par clé symétrique

L'intégrité des données par clé symétrique ou secrète s'applique à un système cryptographique dans lequel les clés utilisées pour l'intégrité des données sont les mêmes pour l'expéditeur et le destinataire des informations. Les systèmes cryptographiques à clé symétrique imposent la prise de dispositions initiales pour permettre aux différents utilisateurs de partager une clé secrète unique (la clé de chiffrement, par exemple). Cette clé doit être communiquée aux utilisateurs par des moyens

---

[6] Voir *Digital Signature Standard*, novembre 2002, (à l'adresse: http://csrc.nist.gov/cryptval/dss.htm) pour plus de précisions sur les algorithmes RSA, de Diffie-Hellman et ECC.

sécurisés, ou produite à l'intérieur même du système (à partir d'une clé racine secrète partagée, par exemple).

Les mécanismes de sécurité d'intégrité des données par clé symétrique pour des messages de longueur arbitraire peuvent utiliser des algorithmes de résumé de message chiffré associés à des fonctions de hachage. Comme exemples d'algorithmes de résumé de message chiffré, citons, entre autres, l'algorithme HMAC-MD5-96 (*hashed message authentication code with message digest 5*, code d'authentification de message haché avec résumé de message 5)[7] et l'algorithme HMAC-SHA-1-96 (*hashed message authentication code with secure hash algorithm 1*, code d'authentification de message haché avec l'algorithme de hachage sécurisé 1)[8].

MEC 29: intégrité des données par clé symétrique selon l'algorithme cryptographique HMAC-MD5-96.

MEC 30: intégrité des données par clé symétrique selon l'algorithme cryptographique HMAC-SHA-1-96.

6.5.2 Intégrité des données par clé asymétrique

Un système d'intégrité des données par clé asymétrique est un système dans lequel les clés de signature et de vérification sont interdépendantes, tout en étant différentes. La clé de vérification est rendue publique, tandis que la clé de signature est tenue secrète. La clé de signature est différente de la clé de vérification, et il passe pour être matériellement impossible d'obtenir la clé de vérification à partir de la clé de signature. Si les clés de vérification sont souvent communiquées, la clé de signature est toujours tenue secrète.

Les mécanismes de sécurité d'intégrité des données peuvent utiliser des algorithmes cryptographiques asymétriques tels que les algorithmes DSA, algorithme à signature numérique (DSA, *digital signature algorithm*) et RSA (*Rivest, Shamir, Adleman*).

Dans le cas des mécanismes de sécurité d'intégrité des données par clé asymétrique, l'expéditeur signe un résumé de message au moyen d'une clé de signature (privée), la clé de vérification (publique) étant utilisée par le destinataire pour vérifier que le résumé de message a bien été signé par l'expéditeur déclaré.

MEC 31: intégrité des données par clé asymétrique selon l'algorithme cryptographique DSA, avec indication de la longueur de clé.

MEC 32: intégrité des données par clé asymétrique selon l'algorithme cryptographique RSA, avec indication de la longueur de clé.

6.5.3 Intégrité des données – Résumé

Le Tableau 4 donne des exemples d'algorithmes qui peuvent être utilisés pour assurer l'intégrité des données. Il convient également d'examiner un certain nombre de points tels que le formatage, le bourrage, le traitement des erreurs et le choix de nombres premiers appropriés; toutefois, ces points ne relèvent pas du domaine d'application du présent document.

---

[7] Internet Engineering Task Force Request for Comment 2403, *The Use of HMAC-MD5-96 within ESP and AH*, C. Madson, R. Glenn, novembre 1998.

[8] Internet Engineering Task Force Request for Comment 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*, C. Madson, R. Glenn, novembre 1998.

Tableau 4/M.3016.3 – Exemples d'algorithmes cryptographiques utilisés pour assurer la confidentialité des données

Catégorie	Algorithme	Observations
Algorithmes de vérification de message par clé asymétrique	DSA	Algorithme à signature numérique.
Algorithmes de vérification de message par clé symétrique	HMAC-MD5-96	Code d'authentification de message haché avec résumé de message 5.
	HMAC-SHA-1-96	Code d'authentification de message haché avec algorithme de hachage sécurisé 1.

6.6 Trace d'audit

Les éléments de réseau et les systèmes de gestion doivent offrir des capacités adéquates autorisant la recherche et l'audit ainsi que des activités de détection, d'analyse et de protection en temps réel, afin que des mesures correctives adéquates puissent être prises. Le présent paragraphe traite des mécanismes de sécurité utilisés pour de tels journaux d'audit de sécurité. Les éléments du contenu et du format des journaux d'audit de sécurité ne relèvent pas du domaine d'application du présent document.

Les journaux d'audit de sécurité peuvent être conservés par les éléments de réseau et les systèmes de gestion. Ces journaux d'audit de sécurité peuvent être conservés au niveau local et peuvent être transmis à un référentiel centralisé ou un dispositif d'analyse de journaux.

Le mécanisme Syslog est communément utilisé pour transmettre des journaux d'audit de sécurité d'une mémoire locale à un référentiel centralisé de journaux.

Ce mécanisme peut généralement journaliser toute action ayant pour effet de modifier les attributs et services de sécurité, les contrôles d'accès ou d'autres paramètres de configuration des dispositifs, chaque tentative de connexion et son résultat et chaque déconnexion ou fin de session, que ce soit à distance ou à partir de la console. La journalisation de messages OAM & P non liés à la sécurité, parfois dénommés messages "nouvellement modifiés", est obligatoire pour toute action pouvant donner lieu à un audit.

Les entrées de journaux d'audit peuvent être envoyées à un serveur d'audit non modifiable après avoir été étiquetées séquentiellement et authentifiées (signées) par des moyens cryptographiques par l'élément de réseau ou le système de gestion. Les journaux d'audit de sécurité peuvent être envoyés à un référentiel central sur une connexion sécurisée. Pour que les actions puissent être correctement analysées, la date et l'heure des diverses sources des journaux doivent être rigoureusement synchronisées et sécurisées (par exemple, NTPv3).

MEC 33: journaux d'audit de sécurité établis sur la base du mécanisme Syslog.

MEC 34: entrée de journal d'audit de sécurité contenant les informations suivantes:

MEC 34a: description de l'action ou de l'action concrète en cours de journalisation.

MEC 34b: identité et niveau de sécurité de l'utilisateur ou du processus qui a déclenché l'action.

MEC 34c: date et heure auxquelles l'action s'est produite.

MEC 34d: informations d'origine et de destination du réseau, le cas échéant (par exemple, en cas de demande de connexion).

MEC 34e: indication de l'aboutissement ou de l'échec de l'activité.

MEC 34f: toute action devant faire l'objet d'un audit.

MEC 35: envoi de journaux d'audit de sécurité à un serveur d'audit non modifiable.

MEC 36: signature cryptographique de journaux d'audit de sécurité.

MEC 37: envoi de journaux d'audit de sécurité à un référentiel central sur une connexion sécurisée.

6.7 Echange de clés

Pour les applications assurant la confidentialité ou l'intégrité des données par clé symétrique, les clés cryptographiques doivent être échangées en toute sécurité entre les extrémités. Les clés de ces algorithmes symétriques doivent en principe être échangées selon un processus étroitement lié à l'authentification, au cas où un attaquant s'interposerait entre les processus d'authentification et de communication des clés.

Les méthodes utilisées pour produire, mémoriser, communiquer, détruire ou annuler ces clés cryptographiques revêtent une importance cruciale. En outre, des facteurs tels que la longueur ou le choix des clés ainsi que le choix de l'algorithme ont une incidence directe sur le niveau de sécurité qu'offre un système cryptographique.

Diverses méthodes peuvent être utilisées pour le dimensionnement et/ou l'échange des clés cryptographiques. Une méthode simple, en théorie, consiste à échanger des clés prépartagées émises hors bande et dimensionnées au niveau de chaque extrémité en fonction des besoins. Par exemple, le choix et la configuration des clés peuvent être effectués par les administrateurs de réseau lors de la mise en service. S'il peut se concevoir pour un petit nombre d'extrémités, l'échange de clés prépartagées n'est guère adapté en présence d'un grand nombre d'extrémités, la production et la configuration d'un grand nombre de clés devenant alors très compliquées.

Des algorithmes asymétriques tels que l'algorithme RSA peuvent être utilisés pour la prise en charge de services d'échange de clés. En cas d'utilisation de l'algorithme RSA, une extrémité sélectionne des clés cryptographiques symétriques et les répartit entre les autres extrémités, sous la protection de l'algorithme de chiffrement RSA. En cas d'utilisation de cette méthode, l'algorithme asymétrique doit utiliser une longueur de clé appropriée qui permette de protéger les clés symétriques émises. Pour protéger une clé symétrique de 128 bits, par exemple, l'algorithme RSA doit utiliser une longueur de clé de 2048 bits ou supérieure, ce qui équivaut approximativement en termes de force cryptographique à un chiffrement de clé symétrique de 128 bits.

L'algorithme de concordance de clés de Diffie-Hellman est une méthode de répartition de clés communément utilisée. En cas d'utilisation de l'algorithme de Diffie-Hellman, les extrémités calculent séparément les clés cryptographiques symétriques secrètes sur un réseau public. Seuls les résultats intermédiaires sont échangés entre les extrémités au cours du processus Diffie-Hellman, la clé secrète n'étant jamais révélée. Si le choix des nombres premiers de Diffie-Hellman est judicieusement effectué, il est impossible à tout attaquant de calculer la clé secrète à partir des résultats intermédiaires.

S'agissant des algorithmes RSA et de Diffie-Hellman, il convient également d'examiner des points tels que le choix de nombres premiers appropriés et d'exposants publics ainsi que le traitement des erreurs.

MEC 38: échange de clés cryptographiques sur la base de clés prépartagées.

MEC 39: échange de clés cryptographiques selon l'algorithme RSA asymétrique, avec indication de la longueur des clés RSA.

MEC 40: échange de clés cryptographiques selon l'algorithme de concordance de clés de Diffie-Hellman, avec indication d'un groupe de nombres premiers de Diffie-Hellman.

6.8 Envoi d'alarmes

Des alarmes de sécurité doivent être envoyées aux administrateurs en cas de détection de toute violation de sécurité ou d'impossibilité de continuer à remplir les journaux d'audit.

MEC 41: mécanismes d'envoi d'alarmes de sécurité de type X.736, par exemple.

6.9 Filtrage des paquets

Afin de protéger le réseau de communication de données (RCD) contre toute attaque et contre la perte d'informations relatives au RCD, il convient d'utiliser le filtrage des paquets pour les dispositifs avec connectivité en mode paquet.

MEC 42: filtrage des paquets axé sur un ou plusieurs des critères de contrôle suivants:

MEC 42a: adresse IP d'origine.

MEC 42b: adresse IP de destination.

MEC 42c: protocole.

MEC 42d: port d'origine.

MEC 42e: port de destination.

et assurant une ou plusieurs des actions suivantes:

MEC 42f: transmission.

MEC 42g: abandon.

MEC 42h: modification.

MEC 42i: redirection.

avec, éventuellement, la possibilité de tenir compte des décisions antérieures (c'est-à-dire en appliquant le filtrage stateful).

Appendice I

Mécanismes de sécurité utilisant les protocoles IPSec, SSL/TLS et SSH

I.1 Protocole IPSec

Le protocole IPSec assure la sécurité de la couche IP au moyen d'un ensemble de mécanismes de sécurité cryptographiques et protocolaires. Fonctionnant entre la couche Réseau (couche 3) et la couche Transport (couche 4), le protocole IPSec peut être utilisé pour protéger tout type de trafic de données (utilisant les protocoles TCP ou UDP) et est indépendant des applications. Il est conçu pour assurer la sécurité des versions 4 et 6 du protocole IP (IPv4 et IPv6) par des moyens cryptographiques interopérables de haute qualité. Il permet d'offrir, entre autres, les divers services de sécurité suivants:

a) intégrité des données.

b) authentification de l'origine des données selon l'adresse IP.

c) authentification machine-machine.

d) protection anti-rejeu.

e) confidentialité des données.

f) échange de clés cryptographiques.

Le recours à deux services de sécurité du trafic, à savoir les services AH (en-tête d'authentification) et ESP (charge utile d'encapsulation de sécurité), d'une part, ainsi qu'à des procédures et protocoles de gestion de clés cryptographiques, d'autre part, permet d'atteindre ces objectifs. Le service AH assure l'authentification de l'origine des données, l'authentification machine-machine et l'intégrité des données pour les paquets IP. Le service ESP assure la confidentialité des données ainsi que l'authentification de l'origine des données, l'authentification machine-machine et l'intégrité des

données pour les paquets IP. De plus, les mécanismes de sécurité utilisant le protocole IPSec sont conçus pour être indépendants des algorithmes cryptographiques afin de permettre la sélection de différents ensembles d'algorithmes sans que cela n'affecte les autres parties de l'application.

La gestion des clés est assurée par le protocole IKE échange de clés via Internet (IKE, *Internet Key Exchange*), qui offre des mécanismes manuel et automatique de négociation des clés entre extrémités. La négociation automatique de clés peut reposer sur des clés prépartagées (des mots de passe, par exemple) ou des certificats X.509.

Références [RFC 2401], [RFC 2402], [RFC 2403], [RFC 2404], [RFC 2405], [RFC 2406], [RFC 2407], [RFC 2408], [RFC 2409], [RFC 2410], [RFC 2411], [RFC 2412], [RFC 3602], [RFC 2451], [FIPS-197].

I.2 Protocole SSL/TLS

Le protocole de sécurité SSL couche de connecteurs sécurisée (SSL, *secure sockets layer*) assure le chiffrement des données, l'authentification du serveur, l'intégrité du message et l'authentification optionnelle du client pour une connexion TCP/IP dans la couche transport (couche 4). Le protocole SSL en est actuellement à la révision 3.0. Le protocole TLS (Transport Layer Security, *sécurité de la couche transport)* est la version IETF normalisée du protocole SSL qui comporte diverses améliorations de la sécurité par rapport au protocole SSL, parmi lesquelles:

- prise en charge obligatoire des algorithmes DSA (algorithme à signature numérique) et de Diffie-Hellman, avec prise en charge optionnelle de l'algorithme RSA;
- utilisation de l'algorithme HMAC code d'authentification de message haché (HMAC, *hashed message authentication algorithm*) fort au lieu de l'algorithme MAC défini selon un protocole SSL non normalisé;
- algorithme de production de clés modifié utilisant le mode résumé de message 5 (MD5) et l'algorithme SHA-1 (algorithme de hachage sécurisé 1) avec l'algorithme HMAC.

Le protocole SSL/TLS fonctionne au dessus de la couche réseau (couche 4) et est compatible avec le protocole de commande de transport (TCP) mais pas avec le protocole datagramme d'utilisateur (UDP, *user datagram protocol*). Les protocoles de la couche application qui fonctionnent communément au-dessus du protocole SSL/TLS sont notamment les suivants: le protocole de transport hypertexte (HTTP), le protocole rapide d'accès à l'annuaire (LDAP, *lightweight directory access protocol*) et le protocole d'accès à la messagerie Internet. Un protocole d'un niveau d'application supérieur peut fonctionner au-dessus du protocole SSL/TLS indépendamment de celui-ci; toutefois, le niveau d'application doit être lié au protocole SSL/TLS par l'utilisation de fonctions de rappel d'entrée ou de sortie.

Le protocole SSL/TLS assure trois fonctions de sécurité pour le trafic TCP: la confidentialité des données, l'intégrité des données et l'authentification.

L'architecture du protocole de sécurité SSL/TLS comporte deux couches fonctionnant sur le protocole TCP:

- les protocoles SSL/TLS de couche supérieure;
- le protocole SSL/TLS d'enregistrement.

Les protocoles SSL/TLS de couche supérieure comprennent notamment le protocole SSL/TLS de prise de contact, le protocole SSL/TLS de modification de chiffrement et le protocole SSL/TLS de notification d'alertes. Des sessions SSL/TLS sont établies, dans un premier temps, par le protocole SSL/TLS de prise de contact qui assure:

a) la négociation des mécanismes d'authentification et de sécurité;

b) l'authentification du client et du serveur (au moyen des clés publiques ou privées de ceux-ci);

c) l'établissement des clés de sécurité.

Une fois que la session SSL/TLS est établie, le protocole SSL/TLS d'enregistrement est utilisé pour assurer des services de transport d'un volume important de données. Le protocole SSL/TLS d'enregistrement assure:

a) l'authentification de l'origine des données selon les clés du serveur;

b) l'intégrité des données;

c) la confidentialité.

Notons que le protocole SSL en est actuellement à la version 3 (SSLv3), et le protocole TLS à la version 1. L'utilisation de versions antérieures de ces protocoles est déconseillée.

Le protocole SSL/TLS permet l'authentification unidirectionnelle, dans laquelle le serveur est authentifié auprès du client uniquement, ou l'authentification bidirectionnelle, dans laquelle le client et le serveur s'authentifient mutuellement l'un auprès de l'autre. L'authentification unidirectionnelle est la méthode généralement utilisée sur l'Internet public. Pour les applications de gestion de réseau, l'authentification bidirectionnelle est recommandée pour permettre aux deux parties de savoir qu'elles sont bien en communication avec l'extrémité souhaitée.

Références [RFC 2246], [RFC 3546], [SSL V3].

I.3 Protocole SSH

Le protocole SSH est un protocole de sécurité de la couche application (couche 7) communément utilisé pour remplacer directement les protocoles Telnet et de transfert de fichiers (FTP) non sécurisés. Les protocoles Telnet et FTP sont des protocoles non sécurisés qui transmettent les mots de passe et toutes les autres données sous forme de texte en clair. Le protocole SSH peut également être utilisé pour protéger d'autres protocoles grâce à l'utilisation de la redirection de ports, ce qui lui permet de faire fonction de protocole de sécurité de réseau général.

Le protocole SSH existe en deux versions (SSHv1 et SSHv2). Mise au point en 1998, la version SSHv1 est aujourd'hui considérée comme étant non sécurisée/obsolète.

Les fonctionnalités du protocole Secure Shell 2 sont les suivantes:

- remplacement intégral des protocoles Telnet, Rlogin, Rsh, Rcp et FTP pour assurer le transfert et la copie sécurisés de fichiers;
- authentification automatique des utilisateurs (aucun mot de passe envoyé sous forme de texte en clair);
- authentification bidirectionnelle (le serveur et le client sont tous deux authentifiés);
- tunnélisation d'applications arbitraires basées sur le protocole TCP/IP par l'utilisation de la redirection de ports;
- chiffrement des données pour assurer la confidentialité de celles-ci;
- diverses options d'authentification, parmi lesquelles l'authentification par mots de passe, par clé publique et par identificateur sécurisé;
- diverses suites de chiffres disponibles.

L'architecture du protocole SSHv2 comporte trois éléments principaux:

- le protocole de la couche Transport [SSH-TRANS], qui assure l'authentification du serveur ainsi que la confidentialité et l'intégrité des données. Il peut éventuellement assurer aussi la compression;
- le protocole d'authentification de l'utilisateur [SSH-USERAUTH], qui authentifie l'utilisateur côté client auprès du serveur;

- le protocole de connexion [SSH-CONNECT], qui assure le multiplexage du tunnel chiffré dans plusieurs voies logiques.

Le protocole de connexion établit des voies qui peuvent être utilisées à diverses fins. Des méthodes normalisées sont prévues pour l'établissement de sessions Shell interactives sécurisées et pour la redirection ("tunnélisation") de ports et de connexions TCP/IP arbitraires.

Le port numéro 22 a été enregistré auprès de l'IANA comme étant le port normalisé à utiliser pour les applications SSHv2.

Références [SSH-ARCH], [SSH-TRANS], [SSH-USERAUTH], [SSH-CONNECT].

Appendice II

La présente Recommandation définit un mécanisme de filtrage des paquets destiné à améliorer la sécurité du réseau de communication de données (RCD). Le RCD est utilisé pour connecter les applications de gestion (généralement situées dans les centres d'exploitation du réseau) aux éléments de réseau assurant la fourniture de services centralisés, la surveillance des alarmes, la réalisation d'essais, la facturation et d'autres activités de gestion du réseau. Les paragraphes 2.8 à 2.10 de la publication RFC 3871 définissent un ensemble de prescriptions de filtrage des paquets applicables aux grandes infrastructures de réseau IP des fournisseurs de services Internet. La présente contribution reprend certains éléments de la publication RFC 3871 pour définir les Recommandations relatives au filtrage des paquets applicable au RCD.

Le filtrage des paquets est le processus qui consiste à déterminer la disposition de chaque paquet traversant un élément de réseau en fonction de critères de correspondance déterminés[9]. Plusieurs dispositions sont possibles: transmission, abandon, redirection, etc. Le filtrage des paquets constitue le mécanisme de protection de base déterminant le volume de trafic entrant dans ou traversant l'élément de réseau ou le système de gestion.

L'objectif principal est de filtrer le trafic en provenance d'autres réseaux (réseaux écoulant le trafic client ou réseaux de gestion homologues, par exemple) à destination du RCD. En outre, il peut se révéler nécessaire d'isoler certains éléments du RCD des autres éléments. C'est pourquoi le filtrage peut être utilisé entre différents sous-réseaux (ou domaines) du RCD.

II.1 Objectifs

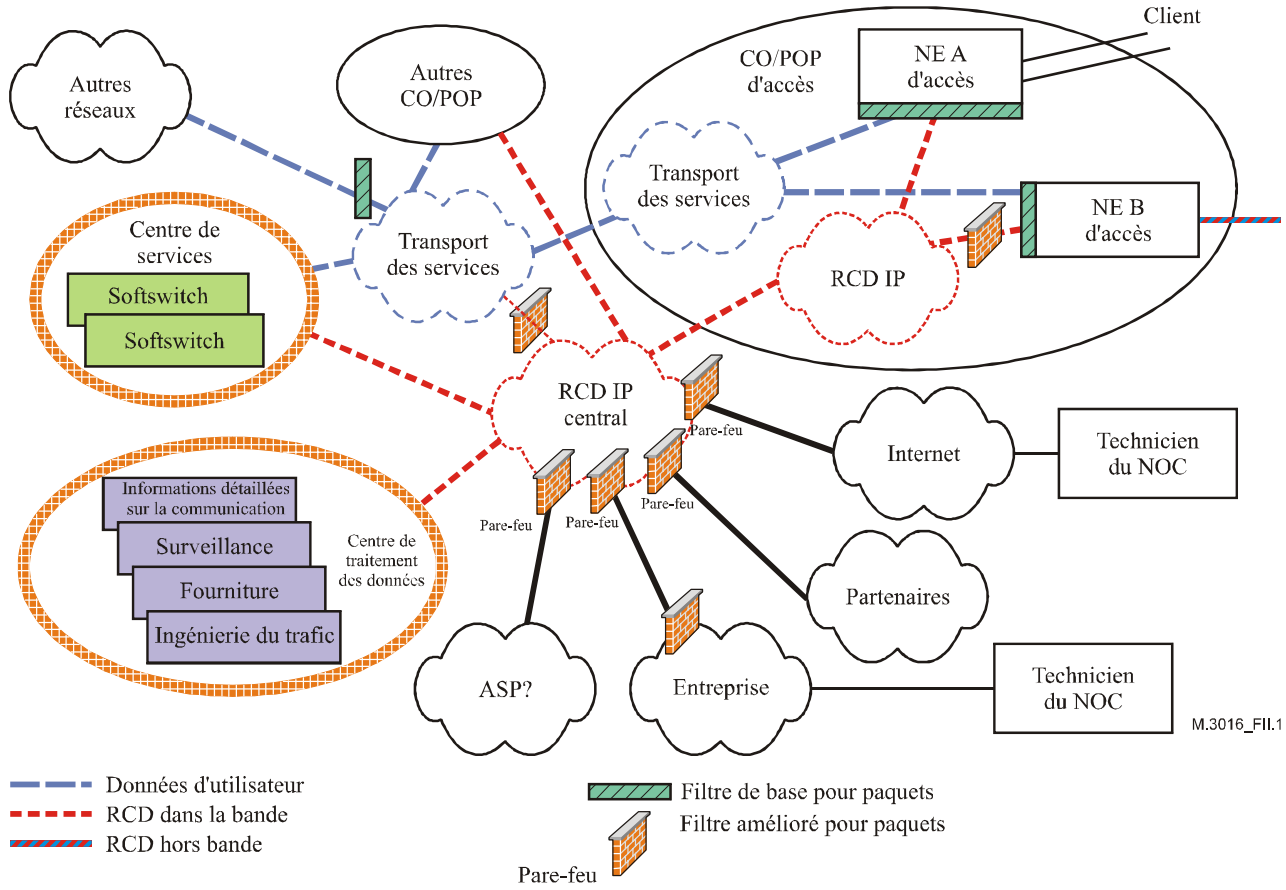
Le mécanisme de filtrage des paquets vise essentiellement à:

1) protéger l'infrastructure du RCD contre le trafic client. La protection doit prévoir un partage approprié des ressources communes pour éviter toute dégradation du service ou tout refus de service;
2) protéger l'infrastructure du RCD contre les réseaux homologues;
3) empêcher le trafic écoulé sur le RCD d'une manière non conforme à la politique de sécurité applicable de se propager dans l'infrastructure du RCD.

[9] Cette définition du filtrage des paquets s'apparente beaucoup à celle du routage des paquets; toutefois, le routage des paquets n'est pas abordé dans le présent appendice qui traite essentiellement du filtrage des paquets.

II.2 Considérations relatives à la conception du réseau ayant une incidence sur le filtrage des paquets

La présente Recommandation ne comporte pas de prescriptions applicables à la conception du RCD; néanmoins, la conception et la mise en place du RCD auront des incidences sur la mise en œuvre du filtrage des paquets dans le réseau et sur les prescriptions applicables à ce filtrage. La Figure II.1 représente un modèle de RCD de conception classique.



CO/POP	centre de commutation/point de présence
NE	élément de réseau
NOC	centre d'exploitation de réseau
Softswitch	plate-forme de commutation logicielle

Figure II.1/M.3016.3 – Exemple de RCD générique

On distingue généralement trois types de modèles de RCD:

- modèle avec gestion dans la bande: ce RCD utilise une largeur de bande réservée du réseau des services utilisé pour acheminer les données client. Par exemple, un réseau local virtuel (VLAN) sur une liaison Ethernet peut être dédié au trafic de gestion ou une connexion IPSec ou SSH peut être utilisée sur une connexion Internet (par exemple, dans le cas du technicien du centre d'exploitation de réseau (NOC) connecté sur l'Internet, représenté sur la Figure II.1);
- modèle avec gestion hors bande: le RCD est un réseau entièrement différent du réseau des services acheminant le trafic client. Ce réseau peut venir se superposer sur le réseau physique acheminant également le trafic de données d'utilisateur;
- modèle hybride: conjugue les méthodes de gestion dans la bande et hors bande;

L'étude comparative et générale de ces types d'architectures de gestion ne relève pas du domaine d'application de la présente Recommandation (voir RFC 3871, section 2.2). Toutefois, l'utilisation de l'une ou l'autre de ces méthodes aura des incidences sur les prescriptions de filtrage.

Les raisons invoquées pour créer des RCD varieront selon le type d'éléments de réseau pris en charge, les procédures et les préférences en matière d'exploitation, les topologies des réseaux, les conditions économiques, etc. La capacité, la robustesse et la sécurité des réseaux sont des éléments pris en considération pour chaque méthode.

Les offres de service de gestion de prochaine génération seront implémentées au moyen d'équipements de transport (à relais de trames, ATM, IP, MPLS, Ethernet, par exemple) en mode paquet. L'apparition de ces services rend nécessaire la gestion des équipements d'accès (CPE).

Il peut être nécessaire de recourir à un modèle hybride utilisant la gestion hors bande jusqu'aux points de présence (POP, *points-of-presence*) et la gestion dans la bande depuis les points POP jusqu'aux dispositifs d'accès CPE, du fait qu'il peut être matériellement impossible, économiquement parlant, d'utiliser la gestion hors bande sur toute la longueur du trajet jusqu'au dispositif d'accès CPE. Ce dispositif est représenté par l'élément de réseau (NE) d'accès B sur la Figure II.1. Dans ce cas, on peut recourir à un filtrage amélioré (pare-feu, par exemple) pour protéger le RCD contre le CPE. Comme autres exemples de l'utilisation d'une connexion dans la bande, citons la gestion d'un point de présence (POP) distant isolé où il est matériellement impossible de mettre en place un réseau séparé, ainsi que l'utilisation d'un réseau de services servant de réseau de secours pour le RCD.

En outre, le recours au filtrage des paquets suppose que l'espace adresse utilisé par le RCD soit séparé de l'espace adresse attribué aux clients et qu'il n'y ait pas lieu que le trafic s'écoule entre ces deux domaines. La séparation de l'espace adresse simplifie la mise au point de dispositifs de filtrage des paquets permettant d'empêcher le trafic client d'avoir accès aux ressources de gestion. La méthode la plus simple consiste à bloquer l'intégralité du trafic à destination du RCD, d'origine extérieure à celui-ci, de manière à protéger l'infrastructure de gestion contre le trafic client. Toutefois, un certain volume de trafic peut devoir être échangé entre des réseaux extérieurs et le RCD dans certains cas, aux fins, par exemple, de l'échange d'informations de gestion entre deux fournisseurs de services (le RCD mettant en relation deux fournisseurs de services en un point milieu, par exemple).

Il convient donc de prendre des dispositions pour autoriser la libre circulation d'un volume limité de trafic entre les domaines et de procéder à de plus nombreux contrôles (filtrage amélioré des paquets, par exemple) pour assurer de manière appropriée la sécurité du RCD.

La Figure II.1 représente un modèle de RCD axé sur les hypothèses susmentionnées. Le transport des services (en bleu) écoule le trafic client. Le RCD (en rouge) écoule le trafic de gestion. Le centre de services contient des serveurs, entre autres, qui assurent des services aux clients et auxquels ceux-ci ont accès (plates-formes de commutation logicielle Softswitch, par exemple). Le centre de traitement des données, qui contient des serveurs et d'autres systèmes d'exploitation utilisés pour assurer la gestion et la surveillance du réseau, n'est pas directement accessible aux clients. La connexion du RCD aux éléments de réseau peut utiliser les protocoles IP, X.25, async ou le service de réseau en mode sans connexion (CLNS) ISO.

La mise en œuvre du filtrage des paquets entrants à la limite entre le RCD et le réseau de services est une condition de base pour assurer la sécurité du RCD au niveau de l'élément de réseau (NE) d'accès. Toutefois, ce filtrage de base des paquets peut se révéler insuffisant, des attaques pouvant également émaner d'un élément de réseau ou d'un serveur interne du RCD en difficulté. En conséquence, des mécanismes appropriés de filtrage des paquets peuvent devoir être mis en place en différents points stratégiques du RCD pour faire en sorte que la politique de sécurité en vigueur soit appliquée. En outre, le filtrage amélioré des paquets peut être nécessaire lorsque le RCD est

relié à des réseaux externes (Internet, réseau d'entreprise d'un fournisseur de services, partenaires, par exemple).

Si le filtrage des paquets constitue un des aspects d'une stratégie de sécurité de réseau, il convient d'y recourir dans le cadre de l'ensemble des principes et des stratégies de sécurité de réseau parmi lesquels, par exemple, la compartimentation et la défense en profondeur. Ainsi, bien qu'une stratégie de sécurité satisfaisante englobera les prescriptions de sécurité relatives aux serveurs proprement dits (plates-formes de commutation logicielle Softswitch, par exemple) et la compartimentation du réseau, celles-ci ne relèvent pas du domaine d'application de la présente Recommandation.

Pour protéger l'infrastructure de gestion, ainsi que le RCD de manière générale, il serait bon que l'opérateur de réseau rejette certains paquets provenant de l'extérieur du périmètre du RCD (c'est-à-dire d'opérateurs homologues et de clients). Ainsi, les paquets ayant des adresses IP d'origine non valables et les paquets destinés à des adresses IP utilisées exclusivement sur le RCD ne devraient pas être autorisés à l'intérieur du périmètre du RCD. Cette fonction est appelée filtrage à l'entrée. Ces prescriptions sont tirées de [RFC 3871] et [RFC 2827].

Il existe deux catégories de filtrage des paquets:

- le filtrage de base des paquets, qui utilise l'information d'en-tête de paquet et qui permet notamment de détecter et de bloquer les paquets dont l'adresse d'origine est usurpée;
- le filtrage amélioré des paquets, comportant notamment les opérations suivantes:
  - examen de tous les états des paquets (*stateful inspection*) dont l'information de contexte ou d'état est également utilisée dans la prise des décisions de filtrage;
  - filtrage dynamique de certains protocoles dont les filtres s'ouvrent dynamiquement selon l'information acheminée dans la charge utile de ces protocoles;
  - contrôle approfondi des paquets donnant lieu à un examen des protocoles du niveau application afin d'y déceler tout élément anormal, insolite ou suspect.

II.3 Filtrage de base des paquets

L'équipement assurant le raccordement au RCD doit pouvoir, en option, abandonner les paquets reçus en provenance d'interfaces tournées vers l'extérieur (clients et homologues, par exemple) et contenant des adresses IP d'origine non valables. De telles adresses peuvent être:

- des adresses Bogon (voir RFC 3871, section 1.8);
- des adresses Martians (voir RFC 3871, section 1.8);
- des adresses IP non attribuées au client (ou non valables et ne pouvant pas être envoyées par l'homologue).

Le mécanisme de filtrage des paquets doit être en mesure de filtrer le trafic à destination des blocs d'adresse attribués au RCD et en provenance de l'extérieur (de clients, par exemple) compte tenu des attributs définis en MEC 42.

Le mécanisme de filtrage des paquets doit produire des statistiques relatives au trafic précises, par interface. Le niveau de granularité des statistiques peut varier en fonction du mécanisme de filtrage des paquets.

L'équipement doit être en mesure de filtrer le trafic en provenance du RCD (de clients, par exemple) et à destination directe d'un élément de réseau via l'une quelconque de ses interfaces (interfaces de bouclage comprises) compte tenu des attributs définis en MEC 42.

Le mécanisme de filtrage de paquets peut prendre en charge le concept de domaines de sécurité multiples du modèle de RGT dans lequel tous les éléments d'un domaine de sécurité ont reçu mandat de suivre une politique de sécurité commune.

L'équipement peut avoir la capacité de produire des alarmes appropriées en fonction du trafic, de situations d'exception et de ses conditions d'exploitation.

II.4 Filtrage amélioré des paquets

L'application des Recommandations relatives au filtrage amélioré des paquets doit être envisagée dans les cas où il existe un degré important de chevauchement entre le trafic utilisateur et le trafic de gestion, c'est-à-dire lorsque la ligne de démarcation entre ces deux trafics ne correspond pas exactement à la limite du réseau et lorsque le RCD est directement relié à d'autres réseaux. En outre, ces capacités de filtrage doivent être mises en œuvre aux limites des sous-réseaux protégés (entre le RCD et le centre de traitement des données, par exemple).

Le mécanisme doit examiner les protocoles d'application utilisés sur le RCD en vue de déceler toute anomalie ou comportement anormal de ces protocoles et doit bloquer de manière appropriée le trafic qui subirait de telles perturbations.

Le mécanisme doit examiner le contenu du trafic sur le RCD pour y déceler tout élément malveillant tel que virus, vers, cheval de Troie (Trojans), etc., s'il y a lieu.

Le mécanisme doit assurer la protection, le cas échéant, des types d'attaques de refus de service (DoS, *denial of service*).

Le mécanisme doit pouvoir assurer le filtrage stateful, dans lequel les informations de session sont utilisées pour le filtrage des paquets. La transmission du trafic retour d'une session doit toujours être autorisée.

Le mécanisme doit prendre en charge la fonction de micro-ouverture dynamique pour tous les protocoles utilisés dans le réseau acheminant l'information de port dans leur charge utile (protocole de transfert de fichiers (FTP), protocole d'ouverture de session (SIP), par exemple). Le mécanisme de filtrage des paquets doit examiner l'information de port dans la charge utile et ouvrir la communication sur le port considéré (micro-ouverture dynamique) pendant la durée de la session. En cas d'interruption brusque de la session, un mécanisme de temporisation approprié doit être prévu pour clore le port.

Le mécanisme doit prendre en charge les fonctions protocolaires d'exécution forcée parmi lesquelles l'abandon des paquets mal configurés ou l'ouverture de session indue, etc.

Les autres capacités de filtrage recommandées sont indiquées aux sections 2.7 à 2.10 de la publication RFC 3871.

BIBLIOGRAPHIE

[RFC 2827] IETF RFC 2827 (2000), *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*.

[RFC 2401] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*, http://www.ietf.org/rfc/rfc2401.txt?number=2401

[RFC 3704] IETF RFC 3704 (2004), *Ingress Filtering for Multihomed Networks*.

[RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure*.

[NDS/IP] 3GPP TS 33.210 (2001), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security*.

[RFC 2402] IETF RFC 2402 (1998), *IP Authentication Header*, http://www.ietf.org/rfc/rfc2402.txt?number=2402

[RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*, http://www.ietf.org/rfc/rfc2403.txt?number=2403

[RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH*, http://www.ietf.org/rfc/rfc2404.txt?number=2404

[RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm with Explicit IV*, http://www.ietf.org/rfc/rfc2405.txt?number=2405

[RFC 2406] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*, http://www.ietf.org/rfc/rfc2406.txt?number=2406

[RFC 2407] IETF RFC 2407 (1998), *The Internet IP Security Domain of Interpretation for ISAKMP*, http://www.ietf.org/rfc/rfc2407.txt?number=2407

[RFC 2408] IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*, http://www.ietf.org/rfc/rfc2408.txt?number=2408

[RFC 2409] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*, http://www.ietf.org/rfc/rfc2409.txt?number=2409

[RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use with IPsec*, http://www.ietf.org/rfc/rfc2410.txt?number=2410

[RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap*, http://www.ietf.org/rfc/rfc2411.txt?number=2411

[RFC 2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*, http://www.ietf.org/rfc/rfc2412.txt?number=2412

[RFC 3602] IETF RFC 3602 (2003), *The AES-CBC Cipher Algorithm and Its Use with IPsec*, http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-aes-cbc-04.txt

[RFC 2451] IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms*, http://www.ietf.org/rfc/rfc2451.txt

[RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol, Version 1.0*, ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt

[RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*, ftp://ftp.rfc-editor.org/in-notes/rfc3546.txt

[SSL V3] *Secure Socket Layer Version 3.0 Specification*, Netscape Communications. http://wp.netscape.com/eng/ssl3/

[SSH-ARCH] YLONEN (T.): *SSH Protocol Architecture*, I-D draft-ietf-architecture-15.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-15.txt

[SSH-TRANS] YLONEN (T.): *SSH Transport Layer Protocol*, I-D draft-ietf-transport-17.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-transport-17.txt

[SSH-USERAUTH] YLONEN (T.): *SSH Authentication Protocol*, I-D draft-ietf-userauth-18.txt, September 2002. http://www.ietf.org/internet-drafts/draft-ietf-secsh-userauth-18.txt

[SSH-CONNECT] YLONEN (T.): *SSH Connection Protocol*, I-D draft-ietf-connect-18.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-connect-18.txt

[FIPS-46-3] Data Encryption Standard. (Describes both DES and 3DES). http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[FIPS-197] Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[RFC 2437] IETF RFC 2437 (1998), *PKCS #1: RSA Cryptography Specifications Version 2.0*, http://www.ietf.org/rfc/rfc2437.txt?number=2437

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	**Gestion des télécommunications y compris le RGT et maintenance des réseaux**
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2005