Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2705

(03/2013)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

Réseaux de prochaine génération – Sécurité

Exigences minimales de sécurité de l'interconnexion pour le service de télécommunications d'urgence (ETS)

Recommandation UIT-T Y.2705

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
Télévision IP sur réseaux de prochaine génération	Y.1900–Y.1999
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Numérotage, nommage et adressage	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Réseaux de transmission par paquets	Y.2600–Y.2699
Sécurité	**Y.2700–Y.2799**
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999
RÉSEAUX FUTURS	Y.3000–Y.3499
INFORMATIQUE EN NUAGE	Y.3500–Y.3999

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

Recommandation UIT-T Y.2705

Exigences minimales de sécurité de l'interconnexion pour le service de télécommunications d'urgence (ETS)

Résumé

Le service de télécommunications d'urgence (ETS, *emergency telecommunications service*) est un service national, qui fournit des services de communication prioritaires aux utilisateurs autorisés en cas de catastrophe et dans les situations d'urgence. La Recommandation UIT-T Y.2705 établit les exigences minimales de sécurité de l'interconnexion inter-réseaux pour le service ETS, qui permettront à ce service de disposer du niveau de sécurité requis entre différents réseaux nationaux sur la base d'accords bilatéraux et/ou multilatéraux en cas de catastrophe et dans les situations d'urgence.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T Y.2705	2013-03-01	13

Mots clés

Sécurité dans les réseaux NGN, service de télécommunications d'urgence (ETS), services et capacités prioritaires.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) 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 développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

Le service de télécommunications d'urgence (ETS, *emergency telecommunications service*) est un service national, qui fournit des services de communication prioritaires aux utilisateurs autorisés en cas de catastrophe et dans les situations d'urgence. La mise en œuvre d'un service ETS relève de la compétence nationale. Toutefois, certaines catastrophes ou situations d'urgence peuvent dépasser les frontières géographiques et les pays/administrations peuvent donc conclure des accords bilatéraux ou multilatéraux pour relier leurs systèmes ETS respectifs. Ainsi, différents réseaux nationaux faisant l'objet d'accords bilatéraux et/ou multilatéraux pourraient prendre en charge des services de communication prioritaires (par exemple, téléphonie, messagerie, services de transmission vidéo et de données) dans le cadre du service ETS en cas de catastrophe et dans les situations d'urgence.

L'intégrité, la confidentialité et la disponibilité du service ETS entre les réseaux nationaux interconnectés dépendront de la sécurité de chacun des réseaux nationaux intervenant dans l'acheminement d'une communication de bout en bout. Pour que la sécurité du service ETS de bout en bout soit assurée entre différents réseaux nationaux (pays/administrations), des exigences de sécurité de l'interconnexion pour le service ETS sont nécessaires.

Recommandation UIT-T Y.2705

Exigences minimales de sécurité de l'interconnexion pour le service de télécommunications d'urgence (ETS)

1 Domaine d'application

La présente Recommandation établit les exigences minimales de sécurité de l'interconnexion inter-réseaux pour le service ETS. Les exigences de sécurité visent à protéger l'intégrité, la confidentialité et la disponibilité des communications ETS franchissant des limites de réseau (entre différents réseaux nationaux).

L'objet de la présente Recommandation est d'établir un ensemble minimal d'exigences de sécurité qui peuvent être utilisées pour faciliter la prise en charge du service ETS entre des réseaux interconnectés directement ou indirectement.

2 Références

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.

[UIT-T E.106] Recommandation UIT-T E.106 (2003), *Plan international de priorité en période de crise destiné aux opérations de secours en cas de catastrophe*.

[UIT-T E.107] Recommandation UIT-T E.107 (2007), *Service de télécommunications d'urgence (ETS) et cadre d'interconnexion des mises en œuvre nationales du service ETS*.

[UIT-T M.3342] Recommandation UIT-T M.3342 (2006), *Lignes directrices pour la définition des modèles de représentation des accords SLA*.

[UIT-T Y.2012] Recommandation UIT-T Y.2012 (2010), *Prescriptions et architecture fonctionnelles du réseau de prochaine génération*.

[UIT-T Y.2205] Recommandation UIT-T Y.2205 (2011), *Réseaux de prochaine génération – Télécommunications d'urgence – Considérations techniques*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes ci-après, qui sont définis ailleurs:

3.1.1 autorisation [b-UIT-T X.800]: attribution de droits, comprenant la permission d'accès sur la base de droits d'accès.

3.1.2 disponibilité [b-UIT-T X.800]: propriété d'être accessible et utilisable sur demande par une entité autorisée.

3.1.3 confidentialité [b-UIT-T X.800]: propriété d'informations qui ne sont pas mises à la disposition de personnes, entités ou processus non autorisés et qui ne leur sont pas divulguées.

3.1.4 intégrité des données [b-UIT-T X.800]: propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.

3.1.5 service de télécommunications d'urgence (ETS, *emergency telecommunications service*) [UIT-T E.107]: service national offrant des télécommunications prioritaires aux utilisateurs autorisés en cas de catastrophe et de situation d'urgence.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 fournisseur de services: le Fournisseur de services (initiale en majuscule) est un fournisseur de services de télécommunication publics autorisé à fournir le service de télécommunications d'urgence ETS.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes ci-après:

ANI interface application-réseau (*application network interface*)

CVE vulnérabilités et exposition courantes (*common vulnerabilities and exposure*)

CVSS système d'évaluation des vulnérabilités courantes (*common vulnerability scoring system*)

CWE liste des failles courantes (*common weakness enumeration*)

CYBEX échange d'informations de cybersécurité (*cybersecurity information exchange*)

DDoS déni de service réparti (*distributed denial of service*)

DNS serveur de noms de domaine (*domain name server*)

DoS déni de service (*denial of service*)

DSCP code Diffserv (*diffserv code point*)

ETS service de télécommunications d'urgence (*emergency telecommunications service*)

IDS système de détection des intrusions (*intrusion detection system*)

IEPS plan international de priorité en période de crise (*international emergency preference scheme*)

IP protocole Internet (*internet protocol*)

IPS système de prévention des intrusions (*intrusion prevention system*)

IPsec sécurité IP (*IP security*)

LAN réseau local (*local area network*)

NE élément de réseau (*network element*)

NGN réseau de prochaine génération (*next generation network*)

NNI interface réseau-réseau (*network-network interface*)

PII information d'identification personnelle (*personally identifiable information*)

RTPC réseau téléphonique public commuté

QoS qualité de service (*quality of service*)

SLA accord sur le niveau de service (*service level agreement*)

SNI interface service-réseau (*service network interface*)

UNI interface utilisateur-réseau (*user network interface*)

5 Conventions

Dans la présente Recommandation:

Le terme "Fournisseur de services" prend une majuscule lorsqu'il désigne un fournisseur de services de télécommunication publics autorisé à fournir le service ETS (voir le § 3.2.1).

L'expression "il est obligatoire" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

L'expression "il est recommandé" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "il est interdit" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

L'expression "peut, à titre d'option" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité.

Dans le corps de la présente Recommandation et dans ses annexes, on trouve parfois les expressions doit, ne doit pas, devrait et peut. Celles-ci doivent respectivement être interprétées comme correspondant aux expressions il est obligatoire, il est interdit, il est recommandé et peut, à titre d'option. Lorsque ces expressions apparaissent dans un appendice ou dans des parties dans lesquelles il est expressément indiqué qu'elles sont données à titre d'information, elles doivent être interprétées comme étant dépourvues d'intention normative.

6 Menaces et risques de sécurité

Les communications ETS peuvent être la cible d'attaques de cybersécurité en raison de leur grande importance. On trouvera des définitions et des informations relatives au service ETS dans les documents [UIT-T E.107], [UIT-T Y.2205] et [b-UIT-T Q-Sup.57]. Les menaces et les actions malveillantes visant à interrompre, utiliser abusivement ou manipuler le service ETS ou à nuire d'une autre manière au service ETS peuvent avoir diverses origines, en particulier les réseaux interconnectés. A titre d'exemple, le service ETS peut être la cible d'attaques de cybersécurité dans le but:

- d'empêcher le personnel chargé d'assurer le retour à la normale en cas de catastrophe de communiquer;
- d'obtenir des informations sensibles par une écoute clandestine au cours d'appels/de sessions ETS.

Une menace est considérée comme une faille de sécurité ou une vulnérabilité potentielle qui, si elle est exploitée, peut nuire à la disponibilité, à l'intégrité ou à la confidentialité des communications ETS.

Dans la présente Recommandation, on s'intéresse principalement aux menaces se rapportant à l'interconnexion des réseaux pour le service ETS, par exemple:

- Menace liée à l'interconnexion générale: faille de sécurité ou vulnérabilité potentielle associée au raccordement d'un réseau (par exemple, un réseau NGN) à d'autres réseaux gérés ou non, comme l'Internet public.

- Menace liée à la conception et à la mise en œuvre: faille de sécurité ou vulnérabilité potentielle dans la conception de l'architecture et de la mise en œuvre de l'interconnexion des réseaux.
- Menace liée à la gestion ou à l'exploitation ou menace interne: faille de sécurité ou vulnérabilité potentielle dans les fonctions de commande et de contrôle du service ETS et dans l'infrastructure sous-jacente.
- Menace liée au transport et aux installations: faille de sécurité ou vulnérabilité potentielle associée au réseau de transport sous-jacent (par exemple, routage, duplication de réseau, diversité, résilience), aux systèmes d'appui (par exemple, énergétique, environnemental) et à la protection physique des actifs des réseaux.

7 Architecture de référence concernant la sécurité de l'interconnexion pour le service ETS

La présente Recommandation repose sur l'architecture fonctionnelle et le modèle de connectivité de réseau définis dans la Recommandation [UIT-T Y.2012].

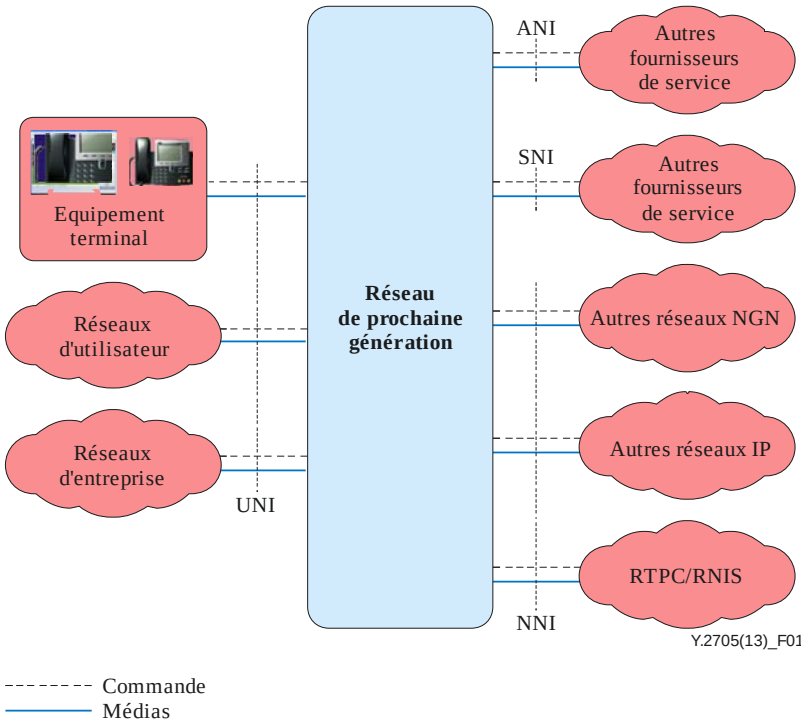


Figure 1 – Connectivité avec le réseau NGN [UIT-T Y.2012]

Les interfaces intervenant dans l'interconnexion des réseaux sont les suivantes:

- Interface application-réseau (ANI).
- Interface service-réseau (SNI).
- Interface réseau-réseau (NNI).

On trouvera une description des interfaces ANI, SNI et NNI dans la Recommandation [UIT-T Y.2012].

Pour permettre la prise en charge de communications ETS traversant différents réseaux, des mesures de sécurité particulières sont nécessaires afin de protéger l'intégrité, la confidentialité et la disponibilité des communications ETS à l'intérieur de chaque réseau national et entre les réseaux nationaux interconnectés.

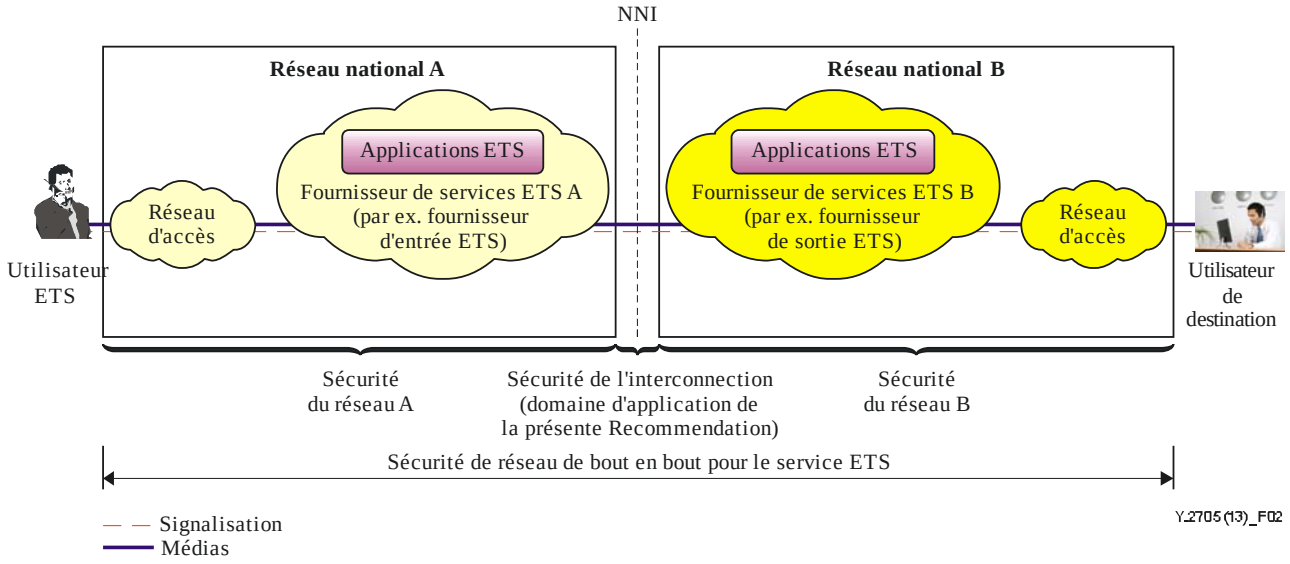


Figure 2 – Sécurité de réseau de bout en bout pour les applications ETS

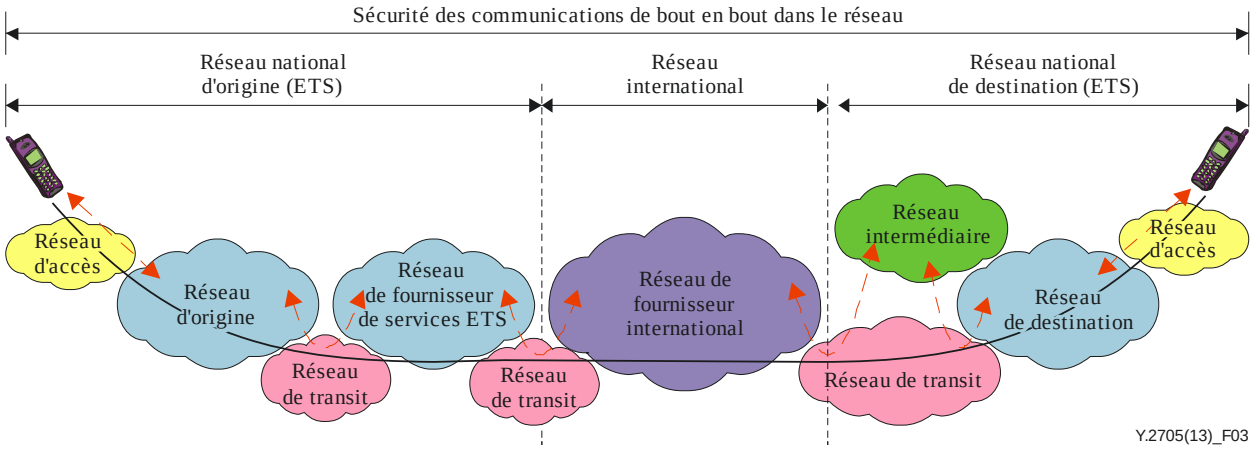
La Figure 2 montre que la sécurité de bout en bout d'une communication ETS traversant plusieurs réseaux (réseaux nationaux A et B) dépendra des mesures de sécurité appliquées dans chacun des réseaux et du niveau de sécurité de l'interconnexion entre les deux réseaux.

Comme indiqué sur la Figure 2, la présente Recommandation traite de la sécurité de l'interconnexion pour le service ETS.

8 Objectifs et lignes directrices concernant la sécurité de l'interconnexion pour le service ETS

8.1 Objectifs généraux

L'objectif général est de protéger la sécurité de réseau pour les communications ETS de bout en bout pouvant traverser différents domaines de réseaux nationaux ou internationaux (de différents pays/administrations), la sécurité étant assurée à l'intérieur du domaine de chacun des réseaux bond par bond.



Signalisation et commande (strate des services et de commande)
Trafic support ou de données (strate de transport)

NOTE – Le plan de gestion n'est pas représenté.

Figure 3 – Exemple de communications de bout en bout avec différentes mises en œuvre nationales du service ETS

La Figure 3 illustre des communications ETS de bout en bout (par exemple, des communications téléphoniques, vidéo, de données ou de messages prioritaires) ayant pour origine et pour destination deux réseaux nationaux différents. L'exemple montre qu'une communication ETS prioritaire de bout en bout peut traverser plusieurs segments de réseau et domaines administratifs (par exemple, réseau d'accès, réseau d'origine, réseau de fournisseur de services ETS, réseau de fournisseur international, réseau intermédiaire et réseau de destination). L'objectif général est que la sécurité soit protégée à l'intérieur du domaine de chaque réseau interconnecté le long du trajet de la communication ETS de bout en bout ainsi que pour l'interconnexion avec le réseau adjacent, afin que l'intégrité, la confidentialité et la disponibilité de la communication ETS de bout en bout ne soient pas compromises.

8.2 Lignes directrices générales

En ce qui concerne l'interconnexion de réseaux pour le service ETS, il convient d'établir et de mettre en œuvre une approche et une méthodologie structurées reposant sur des accords sur le niveau de service (SLA), avec les points suivants:

1) Evaluation des risques de sécurité: évaluation des risques pour les actifs ETS, analyse des menaces et des vulnérabilités liées à l'interconnexion pour le service ETS. Il est essentiel qu'une évaluation des risques de sécurité soit effectuée périodiquement ainsi que lorsque des modifications sont apportées et lorsque de nouvelles technologies, de nouveaux services ou de nouvelles applications sont mis en œuvre.

2) Architecture et solutions de sécurité: établissement de la politique de sécurité, conception de l'architecture de sécurité et spécification de solutions pour atténuer les effets des menaces identifiées pour le service ETS. Il s'agit notamment d'établir les accords SLA bilatéraux ou multilatéraux nécessaires pour la sécurité du service ETS (on trouvera des informations sur les accords SLA dans les documents [UIT-T M.3342] et [b-TMF GB917]). Les accords SLA pour l'interconnexion devront porter sur les politiques de sécurité, les exigences, la conception de l'architecture, les outils de prise en compte de la situation et d'investigation, et la sécurité de l'infrastructure.

3) Mise en œuvre de la sécurité: mise en œuvre et déploiement de l'architecture et des solutions de sécurité sur la base des accords SLA bilatéraux ou multilatéraux, selon le cas, pour assurer la sécurité de l'interconnexion pour le service ETS.

4) Opérations relatives à la sécurité: des mesures opérationnelles pour gérer les solutions de sécurité de l'interconnexion pour le service ETS doivent être spécifiées et mises en œuvre (par exemple, gestion des menaces internes, gestion des paramètres configurables et des valeurs par défaut, résilience et opérations de retour à la normale en cas de défaillance, tests de sécurité du service ETS, journalisation et audit des événements liés à la sécurité du service ETS).

8.3 Objectifs et exigences de base

Le présent paragraphe donne les exigences et les objectifs de base.

R-1 Le Fournisseur de services doit protéger les communications ETS contre les intrusions (par exemple, interception, détournement, répétition) qui compromettraient l'authenticité, l'intégrité, la confidentialité et la disponibilité du service ETS conformément aux bonnes pratiques disponibles sur le marché en termes de sécurité lorsque le trafic ETS traverse le domaine du Fournisseur de services.

Dans l'exigence ci-dessus, un domaine est un "segment de réseau" physique ou logique dont le contrôle administratif et opérationnel, la gestion, la maintenance et la sécurité relèvent entièrement du Fournisseur de services.

Les Fournisseurs de services devraient prendre en charge et utiliser un large éventail d'outils et de capacités de sécurité pour protéger le service ETS et l'intégralité du réseau ainsi que toutes les applications prises en charge. Il est important que des mesures appropriées soient prises pour faire en sorte que l'utilisation de ces capacités de sécurité ne nuise pas à la performance du service ETS et ne compromette pas involontairement la sécurité du service ETS.

R-2 L'utilisation par le Fournisseur de services de mécanismes de sécurité (par exemple, un système de détection et de prévention des intrusions [IDS/IPS] et un chiffrement) ne doit pas interférer avec les mécanismes de traitement prioritaire utilisés pour la prise en charge du service ETS (on trouvera la définition et la description des mécanismes de traitement prioritaire dans la Recommandation [UIT-T Y.2205]).

O-1 Il est souhaitable que, en ce qui concerne l'utilisation par le Fournisseur de services d'outils et de capacités de sécurité, des mesures appropriées soient prévues pour réduire le plus possible les incidences négatives sur la qualité du service ETS (par exemple, l'introduction de retards inutiles).

8.4 Authentification, autorisation et contrôle d'accès pour le service ETS

Le présent paragraphe englobe:

- l'authentification et l'autorisation des utilisateurs ETS;
- l'authentification et l'autorisation des fournisseurs ETS par les utilisateurs ETS;
- l'authentification des sources de données pour le service ETS;
- l'authentification et l'autorisation mutuelles des fournisseurs ETS.

8.4.1 Authentification mutuelle

L'authentification consiste à vérifier l'identité déclarée d'un participant à une communication. Elle permet de garantir la validité des identités déclarées des entités participant à une communication (par exemple, une personne, un dispositif, un service ou une application) et de garantir qu'une entité ne tente pas d'usurper l'identité d'une autre entité ou de répéter sans autorisation une communication précédente.

Une communication ETS de bout en bout peut faire intervenir plusieurs segments de réseau et domaines administratifs (par exemple, un réseau d'accès d'origine, un réseau de Fournisseur de services ETS, un réseau intermédiaire, un réseau d'accès de destination). Lors de la réception de trafic ETS, le Fournisseur de services doit vérifier la validité et l'autorisation de la source (par exemple, un réseau) du trafic reçu. Lors de l'envoi de trafic ETS, le Fournisseur de services doit vérifier la validité et l'autorisation de l'entité à laquelle il envoie le trafic NGN (par exemple, un réseau). Actuellement, les relations de confiance pour la sécurité de l'interconnexion ne peuvent être vérifiées que dans le cadre d'une interconnexion physique directe entre deux réseaux interconnectés.

R-3 Les Fournisseurs de services doivent s'authentifier mutuellement pour l'échange (c'est-à-dire l'envoi ou la réception) de trafic ETS, à savoir pour l'échange entre eux de tout trafic de signalisation ou de médias ETS via les interfaces NNI, ANI ou SNI.

Cette opération peut être accomplie par la vérification des interconnexions physiques directes et des accords sur le niveau de service (SLA).

NOTE – Le but ici n'est pas de procéder à une authentification pour chaque appel/session, mais d'introduire la notion de mécanismes permettant de procéder à une authentification en fonction des besoins ou périodiquement.

8.4.2 Contrôle d'accès

Des mesures de contrôle d'accès sont nécessaires pour assurer la protection contre l'utilisation non autorisée de ressources de réseau, y compris l'utilisation de ressources de manière non autorisée. Le contrôle d'accès garantit que seuls les utilisateurs ou les dispositifs autorisés peuvent accéder aux

éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications.

Par contrôle d'accès à l'interface NNI, on entend la capacité du réseau de réception d'accepter ou de rejeter un trafic spécifique provenant d'un réseau voisin et de restreindre l'accès des entités se trouvant en dehors du réseau aux ressources se trouvant à l'intérieur du réseau.

R-4 Le Fournisseur de services doit établir des règles et appliquer des mesures de contrôle d'accès pour assurer la protection contre les communications ETS non autorisées franchissant des interfaces NNI. En particulier, les Fournisseurs de services ne devraient autoriser le franchissement d'une interface NNI que par des communications entre des éléments de réseau qui ont été identifiés et préautorisés (par exemple par le biais d'accords SLA).

R-5 Lors de la réception de trafic de signalisation ETS provenant d'un autre fournisseur de services, le Fournisseur de services doit vérifier ses relations de confiance avec le fournisseur de services dont il reçoit le trafic.

R-6 Lors de la réception de trafic de médias ETS provenant d'un autre fournisseur de services, le Fournisseur de services doit vérifier ses relations de confiance avec le fournisseur de services dont il reçoit le trafic.

R-7 Lors de l'envoi de trafic de signalisation ETS à un autre fournisseur de services, le Fournisseur de services doit vérifier ses relations de confiance avec le fournisseur de services auquel il envoie le trafic.

R-8 Lors de l'envoi de trafic de médias ETS à un autre fournisseur de services, le Fournisseur de services doit vérifier ses relations de confiance avec le fournisseur de services auquel il envoie le trafic.

NOTE – Les dispositions ci-dessus ne visent pas à procéder à une vérification pour chaque appel/session.

L'autorisation est l'octroi de privilèges ainsi que l'octroi de l'accès sur la base de privilèges d'accès. L'autorisation est donnée à une entité après validation par un processus d'authentification et de contrôle d'accès.

R-9 Le Fournisseur de services doit protéger la sécurité afin d'empêcher tout accès non autorisé au service ETS.

Les moyens à utiliser pour respecter l'exigence R-9 peuvent notamment être les suivants (en fonction des besoins):

- Authentification et autorisation des utilisateurs finals et des dispositifs ETS.
- Authentification et autorisation des sources de données pour les communications ETS (par exemple, source de messages ou source de données).
- Capacités de sécurité pour assurer la protection contre l'accès non autorisé aux informations et ressources ETS (par exemple, les informations d'utilisateur dans les serveurs d'authentification et les systèmes de gestion).

Le contrôle d'accès aux systèmes repose sur l'utilisation de mesures de sécurité pour empêcher tout accès non autorisé aux éléments de réseau et aux systèmes et à leurs points d'accès associés. Il existe des menaces associées à l'accès non autorisé aux éléments de réseau et aux systèmes prenant en charge le service ETS. Il faut donc établir et appliquer des mesures de contrôle d'accès appropriées pour empêcher tout accès non autorisé.

R-10 Les Fournisseurs de services doivent établir des règles et appliquer des mesures de contrôle d'accès aux systèmes pour empêcher tout accès non autorisé aux éléments de réseau et aux systèmes prenant en charge le service ETS. Il s'agit notamment de protéger la sécurité à la fois pour l'accès logique et pour l'accès physique.

R-11 Le Fournisseur de services doit assurer la protection contre tout accès non autorisé aux données et ressources ETS (autrement dit, le Fournisseur de services ne doit permettre qu'aux administrateurs autorisés d'accéder aux données et ressources ETS [par exemple, fichiers, ensembles de commandes, logiciels] présents dans les éléments de réseau et les systèmes prenant en charge le service ETS).

8.5 Intégrité du service ETS

Le présent paragraphe traite de:

- la protection de l'intégrité de la signalisation ETS;
- la protection de l'intégrité des médias ETS.

8.5.1 Intégrité de la signalisation

La signalisation ETS inter-réseaux doit être protégée contre l'interception, la corruption et la manipulation (par exemple, suppression, création, ou répétition).

R-12 Les Fournisseurs de services doivent protéger l'intégrité de tout le trafic de signalisation ETS inter-réseaux passant par les interfaces NNI, ANI ou SNI.

Parmi les mesures qui pourraient être prises pour protéger l'intégrité du trafic de signalisation ETS, on peut notamment citer:

a) des mesures de sécurité physique (par exemple, la protection physique des éléments de réseau, des supports de transmission et des installations, et l'application de mesures de contrôle d'accès appropriées);

b) la protection cryptographique;

c) l'établissement et l'application d'exigences et d'objectifs appropriés en matière d'intégrité dans le cadre d'accords sur le niveau de service;

d) le contrôle de l'intégrité des configurations des interfaces NNI.

8.5.2 Intégrité des médias

Les médias associés aux communications ETS inter-réseaux doivent être protégés contre l'interception, la corruption et la manipulation (par exemple, suppression, création ou répétition).

R-13 Le Fournisseur de services doit protéger l'intégrité de tout le trafic de médias ETS inter-réseaux passant par les interfaces NNI ou SNI.

Parmi les mesures qui pourraient être prises pour protéger l'intégrité du trafic de médias, on peut notamment citer:

a) des mesures de sécurité physique (par exemple, la protection physique des éléments de réseau, des supports de transmission et des installations, et l'application de mesures de contrôle d'accès appropriées);

b) la protection cryptographique;

c) l'établissement et l'application d'exigences et d'objectifs appropriés en matière d'intégrité dans le cadre d'accords sur le niveau de service;

d) le contrôle de l'intégrité des configurations des interfaces NNI.

8.6 Confidentialité des communications ETS et protection des informations PII

Il faut protéger la confidentialité des communications ETS passant par les interfaces NNI, ANI et SNI afin d'empêcher les entités non autorisées d'obtenir des informations sensibles, et notamment protéger la confidentialité:

- de la signalisation et de la commande ETS;

- du trafic support ETS (par exemple, voix, vidéo ou données);
- des informations d'identification personnelle (PII).

8.6.1 Confidentialité de la signalisation

Les Fournisseurs de services doivent protéger la signalisation ETS inter-réseaux prise en charge aux interfaces NNI, ANI ou SNI contre tout accès non autorisé. Les informations de signalisation doivent être protégées contre l'écoute clandestine pour réduire le risque d'utilisation abusive d'informations sensibles révélées par une analyse du trafic de signalisation (par exemple, habitudes d'appel, informations de localisation et identité des utilisateurs).

R-14 Le Fournisseur de services doit protéger la confidentialité de toute la signalisation ETS inter-réseaux passant par les interfaces NNI, ANI ou SNI.

Parmi les mesures qui pourraient être prises pour protéger la confidentialité du trafic de signalisation et de médias, on peut notamment citer:

a) des mesures de sécurité physique (par exemple, la protection physique des éléments de réseau, des supports de transmission et des installations, et l'application de mesures de contrôle d'accès appropriées);

b) la protection cryptographique;

c) l'établissement et l'application d'exigences et d'objectifs appropriés en matière de confidentialité dans le cadre d'accords sur le niveau de service.

Si la protection de la confidentialité est souvent associée à des mécanismes de chiffrement, l'exigence énoncée dans le présent paragraphe relative à la protection de la confidentialité de la signalisation inter-réseaux ne vise pas à imposer l'utilisation de méthodes de chiffrement dans tous les scénarios ou pour tous les flux de signalisation de bout en bout, mais à obliger les Fournisseurs de services à prévoir et à mettre en œuvre les mesures nécessaires pour que les communications de signalisation passant par les interfaces NNI, ANI et SNI soient protégées contre l'écoute clandestine. Cela signifie que chaque interconnexion doit être examinée pour déterminer les mécanismes appropriés à utiliser pour protéger la confidentialité, comme demandé dans la politique de sécurité. On pourrait par exemple, protéger la confidentialité par des moyens physiques, compte tenu des configurations architecturales et physiques de l'interconnexion IP (par exemple, scénario avec une liaison physique dédiée).

8.6.2 Confidentialité des médias

Les flux de médias (par exemple, voix, vidéo et données) doivent être protégés contre l'accès non autorisé car l'écoute clandestine de flux de médias ETS pourrait révéler des informations de sécurité sensibles (acheminées dans la communication de médias).

R-15 Le Fournisseur de services doit protéger la confidentialité de tout le trafic de médias ETS inter-réseaux passant par les interfaces NNI ou SNI.

Parmi les mesures qui pourraient être prises pour protéger la confidentialité du trafic de signalisation et de médias, on peut notamment citer:

a) les mesures de sécurité physique (par exemple, la protection physique des éléments de réseau, des supports de transmission et des installations, et l'application de mesures de contrôle d'accès appropriées);

b) la protection cryptographique;

c) l'établissement et l'application d'exigences et d'objectifs appropriés en matière de confidentialité dans le cadre d'accords sur le niveau de service.

8.6.3 Protection des informations PII

Les informations d'identification personnelle (PII) associées au service ETS doivent être protégées contre toute observation ou divulgation non autorisée (par exemple, identités des utilisateurs finals ETS, identités des entités en communication, informations d'abonnement ETS, emplacement des utilisateurs finals ETS).

R-16 Le Fournisseur de services doit permettre à certains utilisateurs ETS d'utiliser le service ETS anonymement.

R-17 Le Fournisseur de services doit protéger la confidentialité des identités de certains utilisateurs ETS.

R-18 Le Fournisseur de services doit protéger la confidentialité de l'emplacement de certains utilisateurs ETS.

Il est nécessaire d'assurer la protection contre toute observation non autorisée des informations d'utilisation du service ETS (par exemple, données d'utilisation comme le volume de trafic ETS, les emplacements, la durée, la fréquence, etc.) et notamment de prendre en charge et d'utiliser des capacités de sécurité permettant de protéger les informations sensibles déduites de l'observation d'activités dans le réseau, comme les sites web visités par un utilisateur final, l'emplacement géographique d'un utilisateur final, ainsi que les adresses IP et les noms DNS des dispositifs dans le réseau d'un fournisseur de services.

O-2 Il est souhaitable que le Fournisseur de services assure la protection contre toute observation ou divulgation non autorisée des informations d'utilisation du service ETS (par exemple, observation d'activités dans le réseau, comme les sites web visités par un utilisateur ETS, les adresses IP des utilisateurs ETS, ou des données d'utilisation comme le volume de trafic ETS, les emplacements, la durée, la fréquence).

8.7 Transport IP inter-réseaux

8.7.1 Considérations générales

Il existe différentes possibilités d'interconnexion IP-IP entre deux Fournisseurs de services sur le plan de l'architecture et de la connectivité physique, avec des incidences différentes sur la sécurité.

L'intégrité et la disponibilité de l'interconnexion IP-IP entre deux Fournisseurs de services dépendront de facteurs comme l'architecture, la connectivité physique et les accords sur le niveau de service.

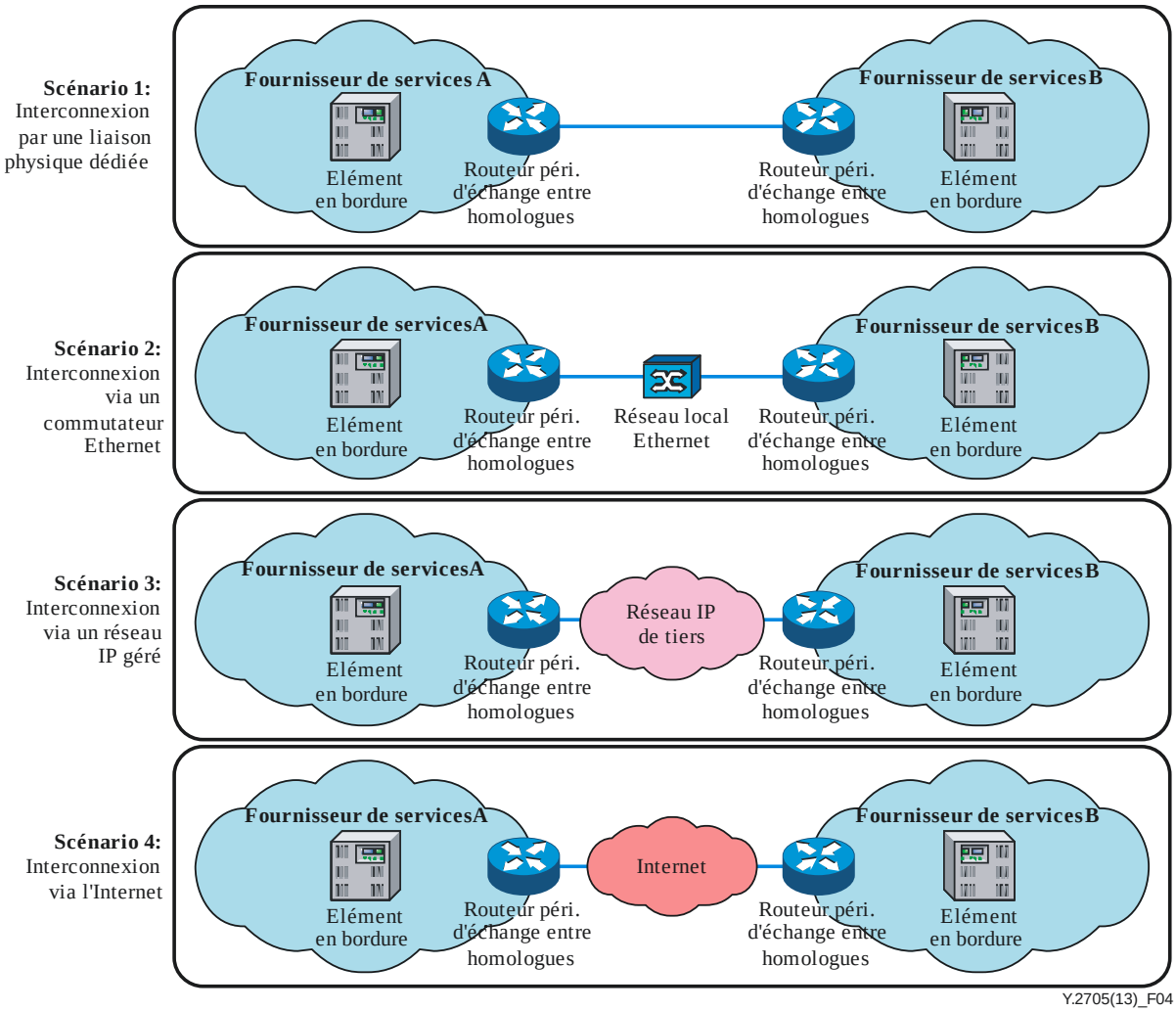


Figure 4 – Configurations d'interconnexion IP-IP

La Figure 4 représente un ensemble de configurations possibles d'interconnexion IP-IP:

1) Interconnexion par une liaison physique dédiée: dans cette configuration, on utilise une liaison physique dédiée pour raccorder entre eux les routeurs périphériques d'échange entre homologues des Fournisseurs de services A et B.

2) Interconnexion via un commutateur Ethernet: dans cette configuration, les routeurs périphériques d'échange entre homologues des Fournisseurs de services A et B sont raccordés physiquement via un commutateur Ethernet d'un réseau local (LAN).

3) Interconnexion via un réseau IP géré: dans cette configuration, l'interconnexion IP entre les Fournisseurs de services A et B a lieu via un réseau IP géré, par exemple, le réseau IP géré d'un fournisseur tiers.

4) Interconnexion via l'Internet: dans cette configuration, l'interconnexion IP entre les Fournisseurs de services A et B a lieu via l'Internet ouvert.

Les incidences sur la sécurité du service ETS sont différentes pour chacun des scénarios illustrés sur la Figure 4.

Le présent document n'énonce ni stipulations ni restrictions concernant l'interconnexion IP utilisée entre les Fournisseurs de services. L'objectif général est qu'il appartient aux Fournisseurs de services de prendre en charge et de mettre en œuvre, sur la base de la configuration IP-IP particulière, les mesures de sécurité appropriées pour protéger l'interconnexion et empêcher que les services soient impactés par des compromissions de l'interconnexion IP.

R-19 Le Fournisseur de services doit protéger le réseau de transport IP entre deux réseaux interconnectés de Fournisseur de services contre les intrusions (par exemple, interception, détournement et répétition) qui compromettraient l'authenticité, l'intégrité, la confidentialité et la disponibilité du service ETS conformément aux bonnes pratiques disponibles sur le marché en termes de sécurité.

Pour respecter cette exigence, le Fournisseur de services devrait établir et appliquer des règles de protection du réseau de transport IP entre les réseaux interconnectés de Fournisseur de services, et décrire les règles dans des accords SLA.

R-20 Le Fournisseur de services doit protéger l'intégrité des mécanismes et des capacités fonctionnelles de hiérarchisation des priorités du trafic IP ainsi que des données de protocole associées (par exemple, codes Diffserv) employés pour prendre en charge le service ETS via l'interconnexion de réseaux IP entre Fournisseurs de services.

NOTE – Il s'agit notamment de protéger l'intégrité des données configurées relatives au service ETS ou des paramètres relatifs à l'interconnexion IP ainsi que de tout mappage concerné (par exemple, le mappage de codes Diffserv sur la base du mécanisme utilisé par chaque Fournisseur de services participant à l'interconnexion).

CR-1 Si la signalisation ETS traverse un segment de réseau de transport IP non fiable (par exemple, réseau de transport IP de tiers), le Fournisseur de services doit utiliser un chiffrement (par exemple, IPsec) pour protéger l'intégrité et la confidentialité.

CR-2 Si les médias ETS traversent un segment de réseau de transport IP non fiable (par exemple, réseau de transport IP de tiers), le Fournisseur de services doit utiliser un chiffrement (par exemple, IPsec) pour protéger l'intégrité et la confidentialité.

8.7.2 Utilisation du chiffrement

L'utilisation de mécanismes de sécurité (par exemple, un chiffrement) ne doit pas interférer avec les mécanismes de traitement prioritaire ni dissimuler les informations nécessaires pour ces mécanismes.

L'exigence qui suit s'applique lorsque des tunnels IPsec sont utilisés pour le trafic ETS inter-réseaux (par exemple pour le franchissement d'interfaces NNI, ANI et SNI):

R-21 Le Fournisseur de services doit établir et appliquer des règles de prise en compte des informations de priorité et de protection de leur intégrité (par exemple des valeurs DSCP) lorsque des tunnels IPsec sont utilisés pour le trafic ETS inter-réseaux. Plus précisément, il convient d'établir dans des accords SLA des règles indiquant comment les valeurs de code Diffserv (DSCP) de l'en-tête interne sont prises en compte dans l'en-tête de tunnel IPsec au point d'entrée IPsec et d'appliquer ces règles afin de permettre un traitement prioritaire entre les points IPsec d'entrée et de sortie.

8.8 Disponibilité du service ETS

8.8.1 Objectif général

Pour garantir une disponibilité élevée du service ETS, il faut faire en sorte que les défaillances de chaque système (prenant en charge le service ETS) soient peu nombreuses, et le retour à la normale du service doit être rapide (après une interruption ou une défaillance). Les défaillances résultant de compromissions de sécurité devraient être prises en compte dans la planification et la conception d'ensemble de la disponibilité du service ETS. La disposition ci-après donne un objectif général pour la disponibilité du service ETS dans le contexte de la sécurité:

O-3 Il est souhaitable que les Fournisseurs de services tiennent compte des risques de défaillances ou d'interruptions de service dues aux événements affectant la sécurité des interconnexions inter-réseaux dans la planification et la conception d'ensemble de la

disponibilité de bout en bout du service ETS (c'est-à-dire pour des appels/sessions ETS traversant plusieurs réseaux de Fournisseur de services). Il convient aussi de prévoir des mesures pour assurer un retour à la normale rapide après les défaillances dues à des événements affectant la sécurité.

8.8.2 Protection de la disponibilité

Il faut protéger le service ETS contre le déni de service (DoS), le déni de service réparti (DDoS) et les autres types d'attaques susceptibles d'avoir une incidence sur la disponibilité du service ETS, notamment contre les attaques ayant une incidence sur la disponibilité du service ETS pour des utilisateurs ETS individuels, un groupe d'utilisateurs ETS, des utilisateurs ETS se trouvant à un emplacement ou sur un site particulier (par exemple, le site du réseau d'entreprise d'une agence publique), un utilisateur ETS se trouvant dans une zone géographique ou régionale cible ou la totalité des utilisateurs ETS.

R-22 Le Fournisseur de services doit protéger la disponibilité du service ETS (par exemple, protection contre les attaques DoS et DDoS et les autres types d'attaques ayant une incidence sur la disponibilité du service ETS) conformément aux bonnes pratiques disponibles sur le marché en termes de sécurité. Il s'agit notamment d'assurer une protection contre les attaques DoS et DDoS et les autres types d'attaques ayant une incidence sur la disponibilité du service ETS pour des utilisateurs ETS individuels, un groupe d'utilisateurs ETS, des utilisateurs ETS se trouvant à un emplacement ou sur un site particulier (par exemple, le site du réseau d'entreprise d'une agence publique), un utilisateur ETS se trouvant dans une zone géographique ou régionale cible ou la totalité des utilisateurs ETS.

Parmi les mesures qui pourraient être prises pour protéger la disponibilité du service ETS, on peut notamment citer:

a) l'utilisation de mécanismes de contrôle d'admission et de régulation;

b) l'utilisation d'outils et de fonctions d'atténuation des effets des attaques DoS et DDoS;

c) l'utilisation de systèmes de détection et de prévention des intrusions (IDS/IPS);

d) l'utilisation d'outils de contrôle de la sécurité;

e) l'utilisation d'outils de prise en compte de la situation.

R-23 Dans le cadre des outils et des capacités de sécurité utilisés par les Fournisseurs de services pour protéger la disponibilité (par exemple, mécanismes DoS et DDoS), il convient de prévoir des mesures appropriées pour empêcher tout déni involontaire d'appels/de sessions ETS légitimes (par exemple en bloquant un appel/une session ETS légitime ou en l'empêchant d'aboutir, ou en éliminant des paquets ETS légitimes).

8.9 Sécurité de la gestion et de l'exploitation

Le présent paragraphe traite de sujets liés:

- à la sécurité des opérations de gestion (par exemple, paramètres configurables et valeurs par défaut relatifs à l'approvisionnement de l'interconnexion pour le service ETS);
- à la journalisation des événements relatifs à la sécurité du service ETS;
- aux alertes et aux alarmes lorsqu'une atteinte à la sécurité s'est produite ou a pu se produire.

8.9.1 Intégrité des données ETS

Il faut protéger l'intégrité des données ETS stockées afin d'empêcher toute corruption ou manipulation des données ayant une incidence sur l'intégrité ou la disponibilité du service ETS.

R-24 Le Fournisseur de services doit protéger l'intégrité des données approvisionnées pour le service ETS, par exemple des données d'abonnement.

8.9.2 Paramètres configurables et valeurs par défaut

Il existe de nombreuses menaces de sécurité liées à la gestion des paramètres configurables et des valeurs par défaut fixés par les vendeurs et les fournisseurs d'équipements. Par exemple, les valeurs par défaut de divers paramètres configurables, telles qu'elles sont fournies par le vendeur, doivent être ajustées afin de respecter les exigences du Fournisseur de services. Les paramètres configurables doivent être attribués correctement et tenus à jour afin d'assurer un fonctionnement satisfaisant. L'administrateur humain doit être dûment autorisé à procéder à l'administration de la sécurité.

R-25 Le Fournisseur de services doit établir et appliquer des règles pour l'administration des paramètres configurables et des valeurs par défaut dans le contexte de la prise en charge du service ETS. Des mesures de contrôle d'accès doivent être mises en œuvre et appliquées afin que l'exécution des fonctions considérées soit réservée à l'administrateur autorisé (autrement dit, cette permission doit être refusée à tous les autres utilisateurs).

8.9.3 Gestion des menaces internes

Il se peut qu'un individu (par exemple, un employé, un contractuel ou un autre travailleur) obtienne un accès de gestion non autorisé ou utilise de manière abusive son accès de gestion aux éléments de réseau et aux systèmes prenant en charge le service ETS. Il est donc nécessaire de réduire le plus possible les menaces internes.

R-26 Le Fournisseur de services doit établir et mettre en œuvre des processus de sécurité pour réduire le plus possible les menaces internes visant le service ETS.

Comme exemples de méthodes qui pourraient être envisagées, on peut citer:

- Des contrôles d'authentification, l'attribution de privilèges en fonction du rôle, la séparation des fonctions, et des méthodes sécurisées d'accès aux systèmes pour l'accès à distance, sur console, de service, et automatique.
- La journalisation des événements affectant la sécurité liés aux actions de gestion.
- Le compartimentage des informations ETS, des applications, et de l'accès aux systèmes et applications utilisés en partage.
- L'audit des données configurées dans les éléments de réseau et les bases de données (par exemple, les profils d'abonnement) afin d'enregistrer et de révéler les modifications non autorisées.

8.9.4 Collaboration pour l'échange d'informations de cybersécurité

Les Fournisseurs de services devraient établir des relations de collaboration avec des partenaires en vue du partage d'informations au sujet des événements affectant la cybersécurité (y compris l'échange en temps réel d'informations pendant des attaques contre la cybersécurité). L'échange d'informations au sujet des incidents de cybersécurité peut offrir des avantages mutuels et peut servir à anticiper des menaces visant le service ETS en permettant au Fournisseur de services d'être à même de prévoir des contre-mesures efficaces.

O-4 Il est souhaitable que les Fournisseurs de services établissent et mettent en œuvre des processus de gestion et d'exploitation prévoyant la mise en place de relations de collaboration en vue du partage et de l'échange d'informations au sujet des événements affectant la cybersécurité. Dans ces processus, il convient de prévoir des fonctions d'analyse afin de pouvoir tirer parti des informations pour mettre en place des mesures et contre-mesures de sécurité afin de protéger le service ETS.

On pourra se reporter aux Recommandations UIT-T suivantes pour plus de précisions sur l'échange d'informations de cybersécurité:

- [b-UIT-T X.1500]

- [b-UIT-T X.1500.1]
- [b-UIT-T X.1520]
- [b-UIT-T X.1521]
- [b-UIT-T X.1524]
- [b-UIT-T X.1570]

8.9.5 Gestion de l'intervention en cas d'incident et du retour à la normale après un événement affectant la sécurité

La disponibilité du service ETS dépend des procédures opérationnelles en place pour le retour à la normale et le rétablissement du service après un événement affectant la sécurité. Il est essentiel que ces procédures soient clairement définies, décrites et mises en œuvre. Il s'agit notamment de prévoir les politiques et pratiques nécessaires pour le retour à la normale et le rétablissement du service à l'intérieur du domaine d'un Fournisseur de services et d'un domaine à l'autre pour l'interconnexion et les services inter-réseaux. Il est nécessaire de protéger la description et la mise en œuvre des procédures opérationnelles contre les intrus et les menaces internes.

R-27 Le Fournisseur de services doit disposer d'un plan détaillé pour l'intervention en cas d'incident et le retour à la normale, décrivant les politiques, la gestion, les étapes opérationnelles, les processus et les procédures concernant le retour à la normale et le rétablissement du service après un événement affectant la sécurité. Il s'agit notamment de prévoir les politiques et pratiques nécessaires pour le retour à la normale et le rétablissement du service à l'intérieur du domaine du Fournisseur de services et d'un domaine à l'autre pour l'interconnexion et les services inter-réseaux.

Bibliographie

[b-UIT-T Q-Sup.57] Recommandations UIT-T de la série Q – Supplément 57 (2008), *Spécifications de signalisation pour la prise en charge du service de télécommunications d'urgence (ETS) dans les réseaux IP*.

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[b-UIT-T X.1500] Recommandation UIT-T X.1500 (2011), *Techniques d'échange d'informations sur la cybersécurité*.

[b-UIT-T X.1500.1] Recommandation UIT-T X.1500.1 (2012), *Procédures d'enregistrement d'arcs sous l'arc d'identificateur d'objet aux fins de l'échange d'informations de cybersécurité*.

[b-UIT-T X.1520] Recommandation UIT-T X.1520 (2011), *Vulnérabilités et expositions courantes (CVE)*.

[b-UIT-T X.1521] Recommandation UIT-T X.1521 (2011), *Système d'évaluation des vulnérabilités courantes (CVSS)*.

[b-UIT-T X.1524] Recommandation UIT-T X.1524 (2012), *Liste des failles courantes*.

[b-UIT-T X.1570] Recommandation UIT-T X.1570 (2011), *Mécanismes de découverte dans le cadre de l'échange d'informations de cybersécurité*.

[b-TMF GB917] GB 917 (2012), *SLA Management Handbook, Release 3.1, TM Forum*.

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	Terminaux et méthodes d'évaluation subjectives et objectives
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, 2013