Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 23 décembre 2013

N° DAT-NT-14/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 29

Note technique

Recommandations de sécurisation d'une architecture de téléphonie sur IP

Public visé:

Développeur	
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	

Informations

Avertissement

Ce document rédigé par l'ANSSI présente les « **Recommandations de sécurisation d'une architecture de téléphonie sur IP** ». Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (`www.etalab.gouv.fr`). Il est par conséquent diffusable sans restriction.

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

Personnes ayant contribué à la rédaction de ce document:

Contributeurs	Rédigé par	Approuvé par	Date
BPR, BAI, MRR, LRP, BAS, BSC	BSS	SDE	23 décembre 2013

Évolutions du document :

Version	Date	Nature des modifications
1.0	23 décembre 2013	Version initiale

Pour toute remarque:

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

Table des matières

1 Préambule

La téléphonie sur IP (ou ToIP) est une évolution majeure récente dans le monde des télécommunications. Cette technologie consiste à utiliser le protocole de transfert de données IP pour acheminer des communications téléphoniques numérisées sur des réseaux privés ou publics. La mise en place de ce type de technologie au sein d'une entreprise ou d'une administration implique des modifications profondes du système d'information (remplacement des *PABX*[1], installation de serveurs applicatifs, changement des postes téléphoniques, câblage, etc.), et doit à ce titre être conduite comme un projet à part entière. L'utilisation de la ToIP a souvent pour objectif d'apporter des gains en terme de coûts, de souplesse de déploiement et de fonctionnalités offertes aux usagers. La ToIP reposant sur une infrastructure IP, elle rapproche deux types de réseaux historiquement disjoints : les réseaux de données et les réseaux de téléphonie. Ce rapprochement accroît les risques auxquels sont exposés les services de téléphonie (fraude, écoute, intrusion, usurpation d'identité, etc.).

Ce document a pour objectifs de présenter ces risques ainsi que les mesures de sécurisation qui doivent accompagner la mise en œuvre d'une infrastructure de téléphonie sur IP. Il s'adresse à un public très large mais il n'a pas pour but de présenter en détail le fonctionnement de la téléphonie sur IP. Il suppose que le lecteur dispose de connaissances minimales sur le sujet pour comprendre les recommandations de sécurité présentées.

La responsabilité de la mise en œuvre des recommandations proposées dans ce document incombe au lecteur. Il pourra s'appuyer sur la politique de sécurité du système d'information existante et sur les résultats d'une analyse de risques[2] pour déterminer les recommandations les plus pertinentes dans le contexte auquel il est soumis. Des tests pourront aussi être réalisés afin d'apprécier l'impact lié à la mise en œuvre de ces recommandations. Étant donnée la nature évolutive des systèmes d'information et des menaces portant sur ceux-ci, ce document présente un savoir-faire à un instant donné et a pour ambition d'être régulièrement amélioré et complété.

2 Généralités

2.1 Écosystème de la téléphonie sur IP

La mise en œuvre d'une infrastructure de téléphonie sur IP, au sein d'une entreprise ou d'une administration, nécessite généralement l'usage de plus d'équipements centraux que la téléphonie traditionnelle (utilisation de nombreux serveurs applicatifs : standard, messagerie, enregistrement, etc.). En outre, chaque éditeur de solution de téléphonie sur IP dispose de son propre écosystème, les briques nécessaires au fonctionnement de l'infrastructure de ToIP ne sont pas toujours portées par les mêmes équipements. La répartition des fonctionnalités dépend de la logique retenue par l'éditeur, des orientations technologiques, des services offerts par la solution, etc. Il est impératif de bien comprendre le rôle de chaque équipement et d'identifier l'ensemble des échanges au sein de l'écosystème de téléphonie sur IP, mais également entre l'infrastructure de téléphonie et l'extérieur (opérateur, autres réseaux).

Voici une description synthétique des principaux composants spécifiques à une architecture de téléphonie sur IP :

- les serveurs d'appels (*PABX IP* ou *IPBX*) : ils sont en charge de la gestion des flux de signalisation échangés entre les différents composants du système de téléphonie (passerelles, serveurs applicatifs, téléphones, etc.) ;

1. *Private Automatic Branch eXchange* ou autocommutateur téléphonique privé.
2. La méthode d'analyse de risques EBIOS peut par exemple être utilisée. L'ensemble des informations relatives à cette méthode est disponible sur le site de l'ANSSI dans la section intitulée « EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité ».

– les passerelles : elles sont utilisées principalement pour raccorder l'infrastructure de téléphonie sur IP aux opérateurs de télécommunication ;
– les serveurs applicatifs : ils hébergent des services téléphoniques tels que la messagerie vocale, l'annuaire, etc. ;
– les téléphones IP.

2.2 Logique de déploiement

La mise en place d'une infrastructure de téléphonie sur IP au sein d'une entreprise ou d'une administration peut être réalisée selon plusieurs logiques parmi lesquelles :

1. ToIP internalisée utilisant des liens opérateurs traditionnels : selon cette logique, les communications téléphoniques transitent sur des réseaux IP uniquement au sein du système d'information interne. Le lien avec l'opérateur de télécommunication ne repose pas sur IP, il utilise des modes de communications traditionnels (*TDM*[3] par exemple). L'ensemble des composants de l'architecture de ToIP, en particulier les passerelles qui sont en charge de la conversion des communications entrantes et sortantes, est hébergé au sein du système d'information interne ;
2. ToIP internaliseé utilisant des liens opérateurs IP : selon cette logique, l'infrastructure de téléphonie est directement reliée à l'opérateur via une liaison IP sur laquelle transitent les flux de téléphonie (trunk *SIP*[4]). L'ensemble des composants de l'architecture de ToIP est hébergé au sein du système d'information interne, mais il ne comprend plus de passerelles liées au changement de médium. Cependant, l'établissement du canal de communication sur IP avec l'opérateur peut nécessiter l'emploi de dispositifs spécifiques pour assurer une meilleure isolation entre le système d'information interne et celui de l'opérateur (se référer au paragraphe 6.3.3) ;
3. ToIP externalisée : selon cette logique, les équipements centraux de l'infrastructure de ToIP sont hébergés chez un prestataire de service spécialisé qui joue également le rôle d'opérateur. L'ensemble des échanges réalisés entre le système d'information interne (les téléphones IP) et le prestataire transite sur des liens IP (*SIP*) et est donc soumis aux mêmes contraintes que celles présentées dans la logique détaillée au point 2.

Le choix d'une logique est dépendant de plusieurs facteurs : le coût, la solution de téléphonie retenue, les possibilités d'intégration au sein du système d'information existant, etc. À la date de rédaction de ce document, il est recommandé d'opter d'abord pour la première logique de déploiement car elle permet d'éviter d'être confronté à un certain nombre de problèmes de sécurité (se référer au paragraphe 6.3.3.2) qui doivent être correctement appréhendés. En effet, les autres logiques ne permettent pas toujours d'être déployées dans des conditions de sécurité acceptables. Il est cependant préférable d'opter pour une technologie de téléphonie supportant les liaisons opérateurs sur IP (en vue d'une évolution future).

2.3 Les acteurs spécifiques de la téléphonie

Certaines particularités des systèmes de téléphonie (IP ou non) induisent l'intervention d'acteurs spécifiques lors de leurs exploitations :

– les télémainteneurs : l'administration à distance (permanente ou ponctuelle) d'une infrastructure de téléphonie par un tiers est une pratique très ancrée dans le monde de télécom, et ce bien avant l'arrivée de la ToIP. La plupart des solutions de téléphonie intègrent nativement des fonctions de prise en main à distance. La mise en place de ce type d'accès présente des risques (intrusion, fraude, vol de données). Si un service de télémaintenance est activé, il convient de respecter les recommandations spécifiques présentées dans le paragraphe 6.3.6 ;

3. Time Division Multiplexing.
4. Session Initiation Protocol.

– les postes opérateurs sur PC (ou POPC) : leur rôle consiste à mettre en relation des personnes au niveau d'un standard à l'aide d'applicatifs spécifiques à la solution de ToIP employée. Ces postes disposent ainsi de certains privilèges et interagissent directement avec les équipements centraux de l'architecture de téléphonie, ce qui peut présenter des risques (indisponibilité, écoute, vol de données). Au même titre que les postes en charge de l'administration de l'infrastructure de téléphonie, les POPC doivent faire l'objet d'une attention particulière. Le paragraphe 6.3.5 présente les recommandations associées à cette population spécifique.

3 Risques associés à une infrastructure de ToIP

3.1 Les besoins de sécurité

Une infrastructure de téléphonie sur IP est un système d'information particulier ; il est dédié à un usage spécifique. À ce titre il est soumis aux besoins de sécurité habituels d'un système d'information auxquels s'ajoutent des besoins spécifiques de la téléphonie fixe.

3.1.1 Disponibilité

Un défi majeur de la téléphonie sur IP est d'être en mesure de satisfaire un taux de disponibilité très élevé, équivalent à celui fourni par les systèmes de téléphonie traditionnelle. Atteindre cet objectif est d'autant plus difficile que l'écosystème nécessaire au fonctionnement d'une infrastructure de téléphonie sur IP est beaucoup plus étendu. Il est également davantage exposé car accessible en IP. Le téléphone est un élément critique de la sécurité au sens large, indépendamment des pertes de production ou de données qui résultent de l'indisponibilité des lignes téléphoniques : un dysfonctionnement peut occasionner, par exemple, l'impossibilité de joindre les secours en cas d'accident sur le lieu de travail.

R1

Les mécanismes à mettre en œuvre pour atteindre le taux de disponibilité visé sont dépendants des résultats de l'analyse de risque menée. Voici une liste des mesures qu'il est conseillé de mettre en œuvre pour renforcer la disponibilité du service de téléphonie :

– au niveau géographique : si l'architecture de téléphonie est répartie sur plusieurs sites physiques, les équipements centraux (serveurs d'appel, serveurs de messagerie, etc.) doivent être présents sur différents sites pour que le service de téléphonie soit disponible lorsqu'un site n'est plus accessible ;
– au niveau opérateur : prévoir plusieurs points de raccordements au réseau opérateur, si possible répartis sur plusieurs sites physiques distincts ;
– au niveau électrique : plusieurs sources d'énergie doivent être présentes pour alimenter les équipements. Ces machines doivent également disposer de plusieurs blocs d'alimentation ;
– au niveau réseau : les équipements d'interconnexion tels que les commutateurs, les routeurs et les pare-feux doivent être redondés ;
– au niveau applicatif : mettre en place des mécanismes de haute disponibilité au niveau des applicatifs de téléphonie.

3.1.2 Intégrité

Le besoin en intégrité d'un système de téléphonie concerne en particulier :

- les communications entre les personnes : porter atteinte à l'intégrité des communications téléphoniques nécessite une modification en temps-réel des conversations ; si l'objectif est la désinformation d'un interlocuteur, il pourra plus simplement être réalisé par l'usurpation d'identité en empruntant son poste, ses accès ou par des techniques d'ingénierie sociale. Il existe cependant un risque d'atteinte plus important au niveau des méta-données qui accompagnent les appels téléphoniques (ex : identité de l'appelant). Une modification de ces données peut poser des problèmes de sécurité (ex : usurpation d'identité) ;
- la configuration des équipements : porter atteinte à l'intégrité de la configuration des équipements peut engendrer de graves problèmes de sécurité, par exemple, en modifiant des droits utilisateurs, en activant des fonctionnalités à risques (se référer au paragraphe 6.5.1) ou encore en changeant certains paramètres des téléphones. Un audit régulier doit être mené pour mesurer les écarts entre une configuration théorique et la réalité « terrain ».

3.1.3 Confidentialité

La principale atteinte au besoin de confidentialité est la possibilité d'écouter des communications téléphoniques. Qu'il s'agisse d'une conversation dite « privée » ou « professionnelle », la perte de confidentialité d'une communication téléphonique reste une menace aux multiples enjeux dont une responsabilité juridique au regard de l'article 323-1 et suivant du code pénal relatif aux communications électroniques et aux services de communications audiovisuelles. Au-delà de l'aspect légal, des informations sensibles peuvent être interceptées en temps réel dans une communication téléphonique (et dans les méta-données associées), mais également en différé par l'écoute des messages vocaux par exemple (qui relève donc du même cadre juridique).

3.2 Menaces et impacts

Les systèmes de téléphonie sont sujets aux mêmes types de menaces que les systèmes d'information classiques (déni de service, intrusion, vol de données, etc.), celles-ci sont simplement adaptées aux spécificités du service de téléphonie [5]. Mais la principale motivation des attaquants de ces systèmes est la possibilité d'utiliser abusivement les ressources téléphoniques, soit pour pouvoir passer des appels téléphoniques aux frais de l'entité compromise, soit pour couvrir des actions illégales [6]. Au-delà des impacts financiers, les attaques menées à l'encontre des systèmes de téléphonie peuvent donc avoir des conséquences d'ordre juridique et peuvent engendrer un déficit d'image de l'entité compromise.

R2

La mise en place d'un suivi régulier de la facturation du système de téléphonie est un moyen permettant de détecter les fraudes à but lucratif. Il est important de prêter attention aux indicateurs suivants :

- les appels surtaxés ;
- les appels à l'étranger ;
- les appels réalisés en dehors des horaires métier ;
- les appels de longue durée ;
- les statistiques d'appels.

5. Citons par exemple, les attaques de type TDOS (Telephony Denial Of Service) qui consistent à rendre indisponible un système de téléphonie en le surchargeant d'appels initiés à l'aide d'outils automatiques.

6. Par le passé, des systèmes de téléphonie compromis appartenant à des sociétés françaises ont été employés pour déclencher des dispositifs utilisés dans le cadre d'actions terroristes (Source : CLUSIF).

4 Respect des principes fondamentaux de la SSI

Une architecture de téléphonie sur IP est un système d'information particulier qui nécessite la mise en place de mesures de sécurité spécifiques. Cependant, au préalable, les principes fondamentaux de sécurisation d'un système d'information doivent être respectés.

4.1 Défense en profondeur

Le principe de défense en profondeur [7] appliqué aux systèmes d'information consiste à mettre en œuvre des protections à tous les niveaux où il est possible d'agir (physique, réseau, système, applicatif, etc.). La présence de ces lignes de défense successives obligera un attaquant à passer outre chacune d'entre elles pour compromettre le système d'information cible. Ces protections doivent être indépendantes et l'ensemble doit être cohérent pour que le niveau de sécurité fourni soit homogène. L'application de ce principe à une architecture de téléphonie sur IP signifie que l'ensemble des briques qui composent l'infrastructure (téléphones, serveurs d'appel, équipements réseau, passerelles, applications, etc.) doivent disposer de leur propre moyen de protection.

4.2 Principe du moindre privilège

Le principe du moindre privilège vient en complément de la défense en profondeur, il s'applique au niveau des bases de comptes du système d'information. Ce principe vise à s'assurer que chacun des comptes ne dispose que des droits qui lui sont strictement nécessaires pour effectuer les actions correspondant à son rôle. L'objectif est de se prémunir contre les incidents de sécurité déclenchés par des modifications de configuration (volontaires ou non) résultant de l'affectation d'un niveau de privilège trop important à certaines personnes.

Ce principe s'applique à l'ensemble des populations disposant de privilèges sur les composants de l'infrastructure de ToIP, parmi lesquelles :
- les administrateurs système ;
- les administrateurs réseau ;
- les administrateurs sécurité ;
- les télémainteneurs ;
- les postes opérateurs sur PC (POPC).

Il s'applique également aux comptes qui ne sont pas nominatifs (démons par exemple) ainsi qu'aux comptes utilisateurs des postes téléphoniques. En effet les solutions de téléphonie offrent un large éventail de fonctionnalités aux usagers, certaines d'entre elles peuvent présenter des risques si elles ne sont pas correctement assignées (se référer au paragraphe 6.5.1).

La mise en œuvre du principe du moindre privilège impose :
- la définition précise de l'ensemble des rôles auxquels les personnes peuvent être associées ;
- la mise en place d'audits réguliers afin de s'assurer que l'affectation des rôles correspond toujours à un réel besoin.

4.3 Réduction de la surface d'attaque

La réduction de la surface d'attaque est un principe fondamental de sécurisation, il vise à réduire au maximum les points d'entrées qui pourraient être utilisés pour compromettre un système d'information. La mise en œuvre de ce principe se traduit par l'application de mesures logiques ou physiques

7. Le concept de défense en profondeur est détaillé dans le document « La défense en profondeur appliquée aux systèmes d'information » disponible sur le site de l'ANSSI.

au niveau de l'ensemble des composants de l'architecture à sécuriser. L'application de ce principe à une infrastructure de téléphonie sur IP revêt un caractère particulier lorsqu'il s'agit de l'appliquer directement aux postes téléphoniques (se référer au paragraphe 6.1).

5 Mesures de sécurité d'ordre général

5.1 Bonnes pratiques

Pour répondre aux principes présentés précédemment, une infrastructure de téléphonie sur IP doit être sécurisée en appliquant d'abord les bonnes pratiques générales de sécurisation. Celles-ci ne seront pas détaillées dans ce document, il est possible de s'appuyer sur le « Guide d'hygiène informatique » disponible sur le site de l'ANSSI pour déterminer les principales mesures à mettre en place. Pour mémoire, voici une liste non exhaustive des thématiques à prendre en considération lors de la sécurisation d'un système d'information :

- authentification des utilisateurs/administrateurs (comptes nominatifs, utilisation d'annuaires, politique de mot de passe, etc.) ;
- durcissement des systèmes ;
- application des correctifs de sécurité ;
- journalisation ;
- surveillance (sondes, supervision, etc.) ;
- sauvegarde ;
- sécurité physique ;
- établissement de PCA [8]/PRA [9] ;
- documentation ;
- audit.

5.2 Utilisation de mécanismes cryptographiques

La sécurisation d'une architecture de téléphonie sur IP nécessite l'emploi de nombreux mécanismes cryptographiques (algorithmes de chiffrement, fonctions de hachage, etc.). Il est ainsi nécessaire d'identifier précisément l'ensemble de ces usages afin de s'assurer que les configurations mises en œuvre sont en accord avec les exigences de sécurité résultant de l'analyse de risques. Quels que soient les mécanismes cryptographiques employés, il est nécessaire de s'assurer qu'ils respectent également les recommandations détaillées dans l'annexe B1 du « Référentiel Général de Sécurité (RGS) » disponible sur le site de l'ANSSI.

Les fonctionnalités qui peuvent nécessiter l'usage de mécanismes cryptographiques au sein d'une architecture de téléphonie sur IP concernent entre autres :

- la sécurisation des communications téléphoniques ;
- l'administration des équipements ;
- la sécurisation des échanges entre les différents équipements qui composent l'architecture de téléphonie ;
- le contrôle d'accès au réseau ;
- la vérification de signature de fichiers.

Des précisions relatives à ces différents cas d'usage sont apportées dans la suite de ce document (paragraphes 5.5.5, 6.1.7, 6.2.4, 6.3.6.3, 6.4).

8. Plan de Continuité d'Activité.
9. Plan de Reprise d'Activité.

5.3 Isolation de l'infrastructure de téléphonie

5.3.1 Isolation physique totale

R3

> Si l'analyse de risques a mis en évidence un besoin élevé en disponibilité du système de téléphonie ou en intégrité/confidentialité des communications, une séparation physique totale de l'architecture ToIP par rapport aux infrastructures de données (internes et externes) doit être retenue.

Afin d'assurer une sécurité maximale de l'infrastructure de téléphonie sur IP, il est recommandé de pratiquer une isolation complète de celle-ci par rapport aux réseaux de données existants. Ce choix implique que l'infrastructure de téléphonie sur IP ne soit pas connectée à des réseaux de données internes (bureautique, serveur) ou externes (Internet) à l'entreprise/l'administration. Si cette séparation est mise en œuvre, les échanges de données réalisés entre l'infrastructure de téléphonie et les réseaux de données doivent être effectués à l'aide de procédures organisationnelles documentées (utilisation de médias amovibles, serveurs de mises à jour hors ligne, etc.). Cette séparation doit intervenir à tous les niveaux :

- réseau : l'ensemble des équipements réseau utilisés dans l'architecture de téléphonie doit être dédié (commutateurs, routeurs, pare-feux, etc.) ;
- système : l'ensemble des machines utilisées (serveurs et postes de travail) dans l'architecture de téléphonie doit être dédié à ce besoin ; y compris les serveurs hébergeant des machines virtuelles si l'architecture de téléphonie en fait usage ;
- données : l'ensemble des données relatives à l'architecture de téléphonie doit être stocké sur des supports physiques dédiés ;

et a pour objectifs :

- d'assurer la très forte disponibilité du service de téléphonie : les équipements qui composent l'architecture de téléphonie n'étant pas mutualisés avec d'autres services, le risque de surcharge est limité ;
- d'assurer la confidentialité et l'intégrité des données relatives à la téléphonie : les données utilisateurs, les communications, les messages vocaux, les configurations ne sont pas accessibles à partir d'équipements qui n'appartiennent pas à l'infrastructure de téléphonie sur IP ;
- de minimiser les risques d'attaques à partir des postes informatique internes : il existe néanmoins des postes informatiques autorisés à se connecter à l'infrastructure de téléphonie, les postes administrateurs et les POPC, dont la sécurisation doit être assurée au même titre qu'un poste bureautique classique (les mesures de sécurisation des POPC sont détaillées dans le paragraphe 6.3.5) ;
- de minimiser les risques d'attaques à partir de sources externes : une infrastructure de ToIP non dédiée à un usage interne est toujours exposée car elle conserve nécessairement un lien avec l'extérieur pour que les communications externes puissent être acheminées. L'absence de raccordement à Internet diminue de façon significative les risques d'attaques externes.

5.3.2 Mesures de cloisonnement minimales

Si, pour des raisons techniques ou fonctionnelles ou économiques, il n'est pas possible de pratiquer une isolation physique complète de l'infrastructure de téléphonie , certaines mesures de cloisonnement minimales doivent être mises en œuvre en plus des recommandations de sécurisation mentionnées dans la suite de ce document.

R4

Si l'isolation physique totale du système de téléphonie n'est pas réalisée, certaines mesures d'isolation doivent être mises en œuvre pour assurer un niveau sécurité minimal :

- cloisonnement logique des réseaux : les équipements qui composent l'infrastructure de téléphonie doivent se situer *a minima* dans des réseaux logiques (*VLAN*) distincts de ceux utilisés pour les réseaux de données. Cette préconisation s'applique aussi bien au niveau des équipements centraux (serveur d'appel, passerelle, etc.) qu'au niveau des téléphones IP ;
- filtrage réseau : si des réseaux appartenant à l'infrastructure de téléphonie sont directement interconnectés à des réseaux de données, il est impératif de réaliser un filtrage précis des flux réseaux échangés à l'aide de pare-feux à état (*stateful*) afin de n'autoriser que les échanges strictement nécessaires. Le nombre de points d'interconnexion entre les réseaux de données et les réseaux de téléphonie doit être limité afin de conserver un meilleur contrôle des échanges entre les deux environnements ;
- maîtrise des échanges : la communication entre deux serveurs est à privilégier au maximum par rapport à des communications clients vers serveurs en ce qui concerne les échanges entre les architectures de téléphonie et de données. En effet, l'accès aux équipements de l'infrastructure de téléphonie par de nombreux clients rend plus difficile la maîtrise des flux et expose davantage les équipements qui la constituent ;
- contrôle applicatif : pour les échanges entre les réseaux de téléphonie et les réseaux de données (annuaire, mise à jour, etc.), il est recommandé de mettre en place en place des passerelles applicatives afin de contrôler la conformité des données transmises et des protocoles employés. Le cas échéant, pour des environnements très sensibles, il peut être fait usage de « diodes » pour renforcer le contrôle des informations échangées.

Les infrastructures de téléphonie et de données sont deux systèmes d'information à part entière, plus il existe d'adhérences entre eux, plus ils deviennent tributaires du niveau de sécurité de l'autre partie. Le risque d'attaque par rebond est important si les deux systèmes sont interconnectés sans précaution. L'exploitation d'une vulnérabilité de l'infrastructure de téléphonie peut permettre de porter atteinte au système d'information de données et réciproquement.

5.4 Sécurisation des services réseaux

5.4.1 Service DNS

R5

Un service DNS ne doit être mis en œuvre que si cela est réellement nécessaire au fonctionnement de l'infrastructure de téléphonie sur IP. Dans ce cas, il doit être dédié à l'infrastructure de ToIP.

5.4.2 Service DHCP

R6

L'utilisation du service DHCP pour attribuer les adresses IP aux téléphones est acceptable si des mesures de protection complémentaires sont mises en œuvre. En particulier celles qui visent à protéger l'accès au réseau.

L'utilisation du service DHCP pour attribuer les adresses IP aux téléphones facilite le déploiement et la gestion du parc. Cependant son usage peut présenter un risque, une personne malveillante peut

facilement disposer d'une connectivité IP à partir d'un équipement tiers connecté au réseau volontairement pour mener une attaque. Néanmoins, l'emploi de DHCP dans ce cas d'usage est acceptable si les mesures suivantes sont respectées :

- l'activation des mécanismes de protection de niveau 2 (se reporter au paragraphe 6.2.3) ;
- la mise en place du contrôle d'accès au réseau (se reporter au paragraphe 6.2.4) ;
- la désactivation de l'inscription automatique des téléphones auprès des serveurs centraux une fois la phase de déploiement terminée (se reporter au paragraphe 6.1.8).

5.4.3 Service de temps

R7

> Synchroniser les horloges de l'ensemble des équipements de l'architecture de ToIP sur des sources de temps internes cohérentes, elles-mêmes pouvant être synchronisées sur des sources de temps extérieures (serveurs publics, signaux radio/satellitaires).

La synchronisation des horloges des systèmes (téléphones, serveurs d'appels, etc.) à l'aide du protocole *NTP*[10] est importante à la fois pour conserver la cohérence des services de téléphonie (journal d'appels, taxation, etc.) mais également pour assurer le bon fonctionnement de certains mécanismes de sécurité (journalisation, vérification de certificats, etc.).

5.5 Administration

5.5.1 Postes d'administration dédiés

R8

> Utiliser des postes de travail dédiés pour administrer les équipements de l'infrastructure de ToIP.

Les postes de travail utilisés pour administrer les applicatifs et les systèmes installés sur les équipements de l'infrastructure de téléphonie sur IP doivent être dédiés à ce besoin et doivent respecter en particulier les exigences suivantes :

- les postes d'administration ne doivent pas disposer d'accès à Internet ;
- les postes d'administration doivent être mis à jour régulièrement avec les derniers correctifs de sécurité ;
- seuls les applicatifs strictement nécessaires à l'administration de l'infrastructure de téléphonie doivent être présents sur les postes d'administration.

5.5.2 Réseaux d'administration dédiés

R9

> Idéalement, utiliser des réseaux d'administration physiquement dédiés pour assurer l'exploitation des équipements de l'infrastructure de ToIP (usage de commutateurs dédiés en particulier), dans tous les cas distincts de ceux employés pour l'administration des réseaux de données. *A minima* ces réseaux doivent être isolés logiquement (*VLAN*).

10. Network Time Protocol.

5.5.3 Interface d'administration

R10

Il est recommandé de dédier une interface réseau physique (logique *a minima*) à l'administration sur chacun des équipements de l'infrastructure de ToIP (hors téléphones).

L'ensemble des équipements (hors téléphones) qui composent l'infrastructure de téléphonie doivent idéalement disposer d'une interface réseau physique dédiée et connectée au réseau d'administration qui leur est associé. S'il n'est pas possible de disposer d'une interface physique, un cloisonnement logique (*VLAN*) doit être réalisé *a minima* sur les équipements. Dans ce cas, une interface physique unique portera deux interfaces logiques : une interface de production et une interface d'administration.

5.5.4 Comptes d'administration

R11

Les comptes utilisés pour l'administration des systèmes ou des applicatifs doivent respecter les recommandations suivantes :
- les comptes d'administration doivent être nominatifs ;
- les comptes d'administration présents par défaut doivent être supprimés (si cela n'est pas possible, leur mot de passe doit être modifié *a minima*) ;
- les comptes utilisés sur les postes d'administration ne doivent pas disposer de droits d'administration locaux ;
- le mode d'authentification par certificat ou par bi-clé doit être privilégié par rapport à l'utilisation de mots de passe. La solution idéale consiste à utiliser un mode d'authentification à deux facteurs (carte à puce associée à un code d'accès utilisateur par exemple) ;
- chaque compte d'administration ne doit disposer que des droits qui lui sont strictement nécessaires (utilisation de rôles) en application du principe de « moindre privilège » ;
- les comptes d'administration doivent être régulièrement audités (vérification de la légitimité des comptes, vérification des droits effectifs par rapport aux droits théoriques, etc.).

5.5.5 Protocoles d'administration

R12

Utiliser des protocoles sécurisés pour administrer à distance les équipements de l'infrastructure de ToIP.

Les protocoles employés pour l'administration à distance des équipements de l'infrastructure de téléphonie doivent être sécurisés, ils doivent notamment apporter des mécanismes de chiffrement et d'authentification (mutuelle si possible). Les protocoles SSH [11] et HTTPS doivent par exemple être utilisés en remplacement de TELNET et HTTP.

11. Une note technique intitulée « Recommandations pour un usage sécurisé d'(Open)SSH » est disponible sur le site de l'ANSSI.

6 Mesures de sécurité spécifiques à la téléphonie sur IP

6.1 Téléphones IP

Il est crucial d'appliquer le principe de défense en profondeur directement au niveau des téléphones. Ces équipements peuvent être source de nombreuses vulnérabilités pour les raisons suivantes :

- le système d'exploitation qu'ils utilisent peut être atypique ;
- leur nombre peut être très important au sein d'un même parc ;
- ils peuvent être répartis sur des sites géographiquement très éloignés ;
- ils ne sont pas nécessairement placés dans des lieux dont la sécurité physique est assurée ;
- le parc déployé peut être très hétérogène (différents modèles installés) ;
- le renouvellement du parc n'est pas aussi fréquent que pour des postes informatiques.

6.1.1 Modes de déploiement

Les téléphones IP peuvent être déployés de différentes manières. Le choix s'opère souvent en fonction des besoins et des contraintes métier de l'organisme. La première solution consiste à attribuer nominativement un téléphone à chaque usager, cela suppose que les personnes ne sont pas mobiles dans les locaux et qu'elles disposent d'un espace physique de travail qui leur est propre. La seconde option vise à banaliser les postes téléphoniques, un poste n'est pas affecté à un usager, il peut être utilisé par n'importe quel abonné dès lors qu'il s'est correctement authentifié sur l'équipement. Ce mode de déploiement est généralement désigné par le terme de *free seating*.

Les deux modes de déploiement peuvent être utilisés dans une même architecture de téléphonie sur des périmètres géographiques ou fonctionnels distincts mais, les mesures de sécurisation des téléphones IP doivent être appliquées de façon homogène à l'ensemble du parc.

6.1.2 Codes d'accès utilisateur

R13

> Quelle que soit la logique de déploiement retenue, il est recommandé de protéger les téléphones IP à l'aide de codes d'accès spécifiques à chaque utilisateur.

La saisie sur le poste, par l'usager, de son identifiant et de son code personnel (ou *PIN*[12]) lui permet d'accéder à son environnement personnel et de profiter de l'ensemble des services téléphoniques qui ont été affectés à son profil.

12. Personnal Identification Number.

R14

Voici quelques recommandations à respecter dans la gestion des codes *PIN* :
- à l'installation, un code *PIN* aléatoire doit être généré pour remplacer celui présent par défaut sur les postes. Ce code est communiqué à l'utilisateur pour qu'il puisse le modifier ;
- chaque utilisateur doit être contraint de modifier son code personnel lors du premier accès au service de téléphonie. L'idéal est d'activer une mesure technique obligeant l'utilisateur à changer son *PIN*. Si la solution de téléphonie employée ne dispose pas d'une telle fonctionnalité, une contrainte organisationnelle doit être mise en œuvre pour s'assurer que chaque usager a personnalisé son code d'accès ;
- l'usage de codes *PIN* triviaux doit pouvoir être bani (00000, 12345, etc.) ;
- une politique de gestion des codes d'accès doit être définie (complexité : *a minima* 5 caractères pour les codes *PIN*, fréquence de renouvellement, nombre de tentatives avant verrouillage du compte, etc.) ;
- l'ensemble des actions relatives à la modification des codes *PIN* doit être journalisé.

6.1.3 Codes d'accès administrateur

Les solutions de téléphonie offrent généralement la possibilité de configurer un code d'accès administrateur sur les postes afin de permettre la modification de certains éléments de configuration directement à partir de l'équipement (configuration du réseau, des services actifs, etc.). L'idéal est de désactiver ce type d'accès une fois le déploiement terminé et de permettre la modification des paramètres des téléphones uniquement au niveau des serveurs de configuration centraux à partir desquels les postes téléchargent leur configuration. S'il n'est pas possible de désactiver les accès administrateur au niveau des téléphones, les recommandations de sécurité relatives à la génération des mots de passe doivent être appliquées [13] lors de la configuration des postes.

6.1.4 Interfaces de communication

R15

Désactiver l'ensemble des interfaces de communications non utilisées par les téléphones IP.

La surface d'attaque des téléphones IP doit être réduite au strict minimum, aussi bien au niveau physique qu'au niveau logiciel. Au niveau physique, l'ensemble des connectiques présentes sur les téléphones sont des vecteurs potentiels d'attaques. À ce titre l'ensemble des interfaces de communication non utilisées doivent être désactivées, par exemple :
- port Ethernet additionnel : certains modèles de téléphones IP disposent d'un port Ethernet supplémentaire permettant de raccorder un autre équipement au réseau via la fonctionnalité de commutateur intégré au poste. En application du principe de séparation des réseaux de téléphonie et de données, il est recommandé de désactiver le port Ethernet additionnel afin d'éviter tout raccordement (volontaire ou non) d'un équipement non autorisé aux réseaux de téléphonie. Si malgré cette recommandation le port Ethernet est utilisé, il est nécessaire de cloisonner logiquement (*VLAN*) les réseaux de téléphonie et de données. Les mécanismes de contrôle d'accès au réseau (se référer au paragraphe 6.2.4) doivent également être activés au niveau du téléphone et de l'équipement « chaîné » ;
- port USB : certains modèles de téléphones IP disposent d'un port USB, celui-ci peut être utilisé pour ajouter des fonctionnalités (connexion d'une caméra par exemple) ou pour réaliser des opérations de maintenance spécifiques. Il est recommandé de désactiver ce port qui pourrait être

13. Se reporter au document intitulé « Recommandations de sécurité relatives aux mots de passe » disponible sur le site de l'ANSSI.

employé par une personne mal intentionnée pour installer, par exemple, un système d'exploitation piégé sur les équipements ;
– connectivité sans fil (Bluetooth par exemple) : ce type d'interface est parfois présent pour permettre l'usage de kits mains libres sans fil. Il est recommandé de désactiver ces moyens de communication sans fil car ils sont des vecteurs d'attaques fréquemment utilisés. L'usage de kits mains libres filaires est préférable, il est généralement possible de raccorder ces dispositifs aux téléphones à l'aide d'une connectique spécifique.

6.1.5 Services non essentiels

R16

> Désactiver l'ensemble des services qui ne sont pas strictement nécessaires au fonctionnement des téléphones IP ; en particulier les services non sécurisés et les mécanismes de prise de contrôle à distance des postes (web services, telnet, etc.).

La présence de services d'administration à distance est rarement nécessaire à la bonne marche des postes, l'administration peut généralement être réalisée à partir des équipements de gestion centralisée. Les services non sécurisés doivent également être désactivés et remplacés par d'autres utilisant des mécanismes cryptographiques robustes, s'ils sont nécessaires au fonctionnement des téléphones. Certaines solutions de téléphonie proposent des services spécifiques de prise en main à distance, il est préconisé de désactiver ces fonctions qui peuvent être utilisées à des fins malveillantes.

6.1.6 Informations techniques

R17

> Masquer aux utilisateurs les informations techniques superflues affichées sur les postes téléphoniques.

Les informations techniques affichées sur les postes téléphoniques, lors de la séquence de démarrage ou via des menus, peuvent faciliter la mise au point de scénarios d'attaques par des personnes mal intentionnées. À ce titre, il est préférable de masquer aux utilisateurs les informations techniques qui ne leur sont pas utiles pour un usage quotidien (version logicielle, plan d'adressage, etc.).

6.1.7 Sécurisation des données « techniques »

6.1.7.1 Signature des firmwares

R18

> Utiliser des mécanismes cryptographiques robustes de vérification de signatures afin de s'assurer que seuls les binaires signés par une autorité de confiance puissent s'installer sur les téléphones IP.

La vérification de la signature des firmwares téléchargés par les téléphones permet de s'assurer que le système d'exploitation installé sur les postes provient bien de l'éditeur de la solution de téléphonie. En effet, si aucun mécanisme de vérification n'est en place, une personne mal intentionnée peut tenter d'installer un système piégé pour procéder à l'écoute des communications téléphoniques (par exemple). L'utilisation de routines permettant un simple calcul de sommes de contrôle (*checksum*) des fichiers n'est pas suffisant car elles permettent de vérifier uniquement que les données n'ont pas été altérées durant le transfert, elles ne sont pas en mesure de s'assurer de la provenance des données. Il est recommandé d'utiliser une solution qui repose sur des mécanismes de signature numérique s'appuyant sur des suites

cryptographiques robustes. Seuls les binaires signés par une autorité de certification de confiance (liée à l'éditeur ou si c'est possible au système de téléphonie lui même) pourront alors s'installer sur les téléphones. Cette autorité de confiance doit être connue des postes, ils doivent donc disposer de la clef publique de celle-ci pour pouvoir effectuer la vérification de la signature des fichiers téléchargés. Cette solution ajoute à la vérification de l'intégrité des données la validation de la provenance de celles-ci.

6.1.7.2 Sécurisation des flux « techniques »

R19

> Utiliser des protocoles de communication sécurisés pour protéger les flux « techniques » entre les téléphones IP et les équipements centraux de l'architecture de téléphonie.

Les téléphones IP téléchargent régulièrement (au démarrage notamment) des fichiers mis à disposition par les équipements centraux de l'architecture de téléphonie. La nature de ces fichiers dépend de la solution de téléphonie employée. Voici une liste non exhaustive des types de fichiers qui peuvent être téléchargés par les téléphones :

- firmware ;
- fichier de configuration du système ;
- fichier de configuration de l'interface utilisateur ;
- certificat ;
- fichier de langue ;
- fichier de licence .

Certains de ces fichiers peuvent contenir des informations confidentielles (login/mot de passe) ou des éléments (version logicielle) qui peuvent faciliter l'action d'une personne malveillante si celle-ci a la possibilité d'intercepter la communication entre les téléphones et les équipements centraux. L'usage de protocoles non sécurisés ou non authentifiés tels que TFTP ou FTP est à proscrire pour transférer ces données entre les composants de l'infrastructure de téléphonie. Il est recommandé d'utiliser des protocoles sécurisés (HTTPS, IPsec) pour assurer la protection des flux « techniques » échangés entre les téléphones IP et les équipements centraux. Ces protocoles doivent assurer le chiffrement des données et si possible une authentification mutuelle des parties à l'aide de certificats issus d'une autorité de certification de confiance.

6.1.8 Inscription des téléphones

R20

> La fonctionnalité d'inscription automatique des téléphones auprès des équipements centraux peut être employée mais, celle-ci doit être désactivée une fois le déploiement initial achevé.

Les solutions de téléphonie sur IP offrent généralement la possibilité d'inscrire automatiquement les postes téléphoniques, auprès des serveurs centraux, lors de leur installation. Cette fonctionnalité permet le déploiement rapide d'un parc composé de plusieurs centaines d'équipements, mais elle comporte des risques si elle reste activée après la phase de déploiement. Une personne mal intentionnée peut par exemple tenter de connecter au réseau un téléphone IP de modèle identique mais provenant de l'extérieur. Si l'inscription du poste réussit, l'attaquant pourrait bénéficier de l'accès à de nombreux services et pourrait même compromettre entièrement l'infrastructure de téléphonie, voire l'ensemble du système d'information. L'inscription automatique des postes n'est pas déconseillée lors du déploiement d'un parc important, mais uniquement si des mécanismes de contrôle d'accès au réseau sont correctement mis en œuvre en complément (se référer au paragraphe 6.2.4). Il est par contre recommandé de désactiver la fonctionnalité d'inscription automatique des postes une fois la phase d'installation du parc

terminée. L'ajout d'un nouveau poste ou le remplacement d'un équipement défectueux devra ensuite être réalisé en suivant un processus d'inscription manuel.

6.2 Commutateurs

Cette section ne détaille que les mesures de sécurisation spécifiques au cas d'usage de commutateurs de desserte dans une architecture de téléphonie sur IP. Néanmoins les recommandations de sécurisation habituelles d'équipements de niveau 2 doivent également être mises en œuvre au niveau de l'ensemble des commutateurs de l'architecture de téléphonie (commutateurs de cœur de réseau et de desserte).

6.2.1 Utilisation de commutateurs POE

L'usage de commutateurs supportant la norme POE[14] peut faciliter le déploiement d'un parc de téléphones IP. Cette mesure ne permet pas de renforcer directement la sécurité d'une installation, mais l'emploi ou non de cette norme est un élément structurant dans le choix des modèles de commutateurs de desserte utilisés au sein de l'infrastructure de ToIP.

R21

> Lorsqu'il est envisagé d'utiliser des commutateurs POE, il est indispensable de retenir ceux permettant de fixer de manière statique la puissance électrique fournie à chacun de leurs ports.

6.2.2 Ports de commutateur non utilisés

R22

> Désactiver les ports Ethernet non utilisés sur les commutateurs destinés à accueillir les téléphones IP.

Il est recommandé de désactiver les ports inutilisés sur les commutateurs de desserte afin d'éviter le raccordement volontaire (ou non) d'équipements non autorisés à l'infrastructure de téléphonie. La mise en œuvre de cette recommandation oblige ainsi une modification manuelle de la configuration des commutateurs lorsqu'un téléphone est ajouté ou retiré de la production.

6.2.3 Mécanismes de protection de niveau 2

Plusieurs mécanismes de protection doivent être mis en œuvre au niveau des commutateurs de desserte et des téléphones afin de limiter certains types d'attaques au niveau 2 (usurpation, empoisonnement de cache par exemple) :

- limitation du nombre d'adresses MAC : il est généralement possible de définir, au niveau des ports de commutateurs de désserte, le nombre d'adresses MAC autorisées à accéder au réseau. Cependant il n'est pas recommandé de définir explicitement sur chaque port de commutateur l'adresse MAC du téléphone normalement connecté à ce port, cela n'apporte pas de réelle sécurité supplémentaire et induit des coûts d'exploitation importants (maintien à jour des adresses MAC dans la configuration des commutateurs). Le renforcement du niveau de sécurité des ports de commutateurs implique la mise en œuvre des mécanismes de contrôle d'accès au réseau détaillés dans le paragraphe suivant ;

14. Power Over Ethernet : Alimentation électrique des équipements via Ethernet.

R23

> Si les architectures de téléphonie et de données sont correctement séparées, chaque port de commutateur ne doit autoriser qu'une seule adresse MAC (seul un téléphone sera raccordé à chaque port).

– requêtes ARP gratuites : il est essentiel que la prise en compte d'informations de mises à jour ARP non sollicitées (utilisées en cas d'attaque de type *Man in the Middle*) soit évitée ;

R24

> Il est recommandé de désactiver la prise en compte des requêtes ARP gratuites au niveau des ports de commutateurs mais également au niveau des téléphones.

– inspection ARP en environnement DHCP : il est important d'avoir des protections permettant de contrôler l'émission de requêtes DHCP et de vérifier la validité de la correspondance adresse MAC/adresse IP dans les trames ARP et ainsi limiter les risques d'usurpation d'adresses au niveau 2 en bloquant les trames incohérentes. Cette recommandation s'applique difficilement dans un contexte d'attribution statique des IP car elle obligerait à maintenir manuellement une base de données de correspondance adresse MAC/adresse IP au niveau des commutateurs ;

R25

> Si les adresses IP des téléphones sont attribuées via DHCP, il est recommandé d'activer, au niveau des commutateurs de desserte, les deux mécanismes *DHCP Snooping* et *Dynamic ARP Inspection*.

– isolation des téléphones IP : si le modèle d'architecture retenu n'autorise pas les échanges directs entre les téléphones IP (se reporter au paragraphe 6.3.1 relatif à la centralisation des flux), des protections complémentaires peuvent être ajoutées au niveau des ports de commutateurs afin d'interdire les échanges directs inter-postes ;

R26

> L'usage de VLAN privés (*PVLAN*[15]) ou la configuration des ports de commutateurs en mode *protected* sont des moyens supplémentaires à mettre en œuvre pour assurer un cloisonnement bas niveau entre les téléphones IP .

– autres : les différentes technologies de commutateurs et de téléphones IP peuvent disposer d'autres mécanismes de protection niveau 2 qu'il est conseillé de mettre en œuvre en complément des mesures énoncées ci-dessus.

6.2.4 Contrôle de l'accès au réseau

R27

> Au niveau des commutateurs de desserte, contrôler l'accès au réseau à l'aide du protocole EAP-TLS. Si cela n'est pas possible, EAP-MD5 doit être mis en place *a minima*.

La sécurisation du niveau 2 n'est pas suffisante pour s'assurer que seuls les postes téléphoniques légitimes se connectent à l'infrastructure de ToIP. Il est recommandé de contrôler l'accès au réseau en utilisant le standard 802.1x. Le protocole EAP [16] permet la mise en œuvre de ce standard, il est

15. *Private VLAN*.
16. Extensible Authentication Protocol.

supporté par la majorité des solutions de téléphonie du marché. Sa configuration nécessite l'installation de serveurs d'authentification (RADIUS [17] par exemple) et de commutateurs de desserte disposant des fonctionnalités d'authentification 802.1x.

Il existe plusieurs méthodes supportées par le protocole EAP, parmi lesquelles :

- EAP-TLS : cette méthode peut apporter un bon niveau de sécurité si elle est correctement configurée. EAP-TLS repose sur l'utilisation de certificats et permet l'authentification mutuelle des clients (les téléphones) et du serveur d'authentification (serveur RADIUS). La mise en œuvre de cette méthode d'authentification nécessite l'emploi d'une IGC [18]. Il est recommandé d'utiliser des gabarits de certificats respectant les préconisations mentionnées dans l'annexe B1 du référentiel général de sécurité (RGS) ;
- EAP-MD5 : cette méthode apporte un niveau de sécurité moins élevé, elle repose sur un challenge-réponse utilisant la fonction de hachage MD5 vulnérable aux attaques par force brute ou par dictionnaire. De plus, ce mécanisme ne permet pas une authentification mutuelle des deux parties ; seul le client s'authentifie auprès du serveur. L'utilisation de cette méthode n'est donc préconisée que si l'emploi d'EAP-TLS n'est pas possible. Des mesures de protection complémentaires doivent également être configurées, en particulier celles activant le blocage des ports de commutateur après plusieurs échecs d'authentification. Les mots de passe employés dans les configurations de type EAP-MD5 doivent respecter *a minima* les recommandations mentionnées dans le document « Recommandations de sécurité relatives aux mots de passe » disponible sur le site de l' ANSSI et leur taille doit être d'au moins 25 caractères pour assurer une robustesse minimale dans ce cas d'usage.

6.3 Architecture réseau

6.3.1 Centralisation des flux de téléphonie

R28

> Centraliser les flux de communication échangés entre les téléphones IP (flux de signalisation et flux média) afin d'accroître le niveau de sécurité de l'architecture de ToIP.

En fonction du type d'architecture de ToIP retenu et des protocoles de téléphonie employés, il est possible que les téléphones échangent certains flux directement entre eux sans passer par un équipement intermédiaire (flux média notamment). Cette communication pair à pair directe peut poser des problèmes de sécurité ; une personne mal intentionnée pourrait piéger un téléphone pour mener différents types d'attaques dirigées contre les autres postes téléphoniques du parc (prise de contrôle à distance, écoute à distance, déni de service, etc.). La possibilité de centraliser des flux de communication dépend de la solution de téléphonie employée, cette fonctionnalité est généralement portée par les passerelles. Si la centralisation des flux est mise en œuvre, elle doit s'accompagner de mesures complémentaires de cloisonnement de niveau 2 (se reporter au paragraphe 6.2.3) afin d'assurer une isolation maximale entre les téléphones IP.

6.3.2 Segmentation des réseaux et filtrage inter-zone

R29

> Segmenter l'architecture de ToIP en zones logiques et filtrer les flux inter-zones à l'aide de pare-feux à état (*stateful*).

17. Remote Authentication Dial-In User Service.
18. Infrastructure de Gestion de Clés.

Voici une liste des zones pouvant être distinguées dans une architecture de ToIP :
- zone accueillant les téléphones IP ;
- zone hébergeant les serveurs d'appels ;
- zone hébergeant les serveurs applicatifs (messagerie, standard, etc.) ;
- zone hébergeant les passerelles ;
- zone hébergeant les postes d'administration dédiés à la ToIP ;
- zone hébergeant les postes opérateurs dédiés à la ToIP (POPC) ;
- zone hébergeant les équipements dédiés à la télémaintenance .

Deux publications, disponibles sur le site Internet de l'ANSSI, peuvent aider à la mise en œuvre de cette segmentation :
- le guide intitulé « Définition d'une architecture de passerelle d'interconnexion sécurisée » ;
- la note technique intitulée « Recommandations pour la définition d'une politique de filtrage ».

Lors du choix de la technologie de pare-feu utilisée pour réaliser la segmentation de l'architecture de téléphonie sur IP, il est judicieux de valider au préalable la compatibilité entre ces équipements de filtrage et les flux de téléphonie. En effet, certaines spécificités propres aux protocoles (utilisation de ports sources aléatoires par exemple) utilisés au sein des architectures de téléphonie peuvent ne pas être correctement comprises par certaines technologies de pare-feux et entraîner le blocage des flux.

6.3.3 Interconnexions

Par essence, une architecture de téléphonie est destinée à être raccordée à d'autres réseaux pour que les communications téléphoniques avec des entités extérieures soient possibles. Il faut cependant veiller à ce que ces canaux soient correctement sécurisés pour que l'infrastructure de téléphonie ne soit pas exposée inutilement.

6.3.3.1 Interconnexions avec d'autres réseaux de téléphonie IP

R30

Utiliser des équipements de protection périmétrique (de type *SBC*[19] ou *BG*[20]) pour renforcer la sécurité de l'architecture de ToIP et des communications IP échangées avec les réseaux extérieurs de ToIP.

R31

Placer les équipements de protection périmétrique *SBC*/*BG* dans une zone dédiée.

L'utilisation d'IP et les possibilités de connectivité associées rendent plus aisées l'interconnexion des réseaux de téléphonie entre eux mais, cette facilité présente des risques. Il est recommandé d'utiliser des équipements spécifiques pour assurer la sécurité à la périphérie des infrastructures de téléphonie sur IP. Les équipements de type *SBC*/*BG* sont employés à la frontière des architectures de téléphonie pour apporter des fonctions de sécurité périmétriques utiles dans la protection de l'infrastructure de ToIP mais également au niveau des communications téléphoniques échangées avec l'extérieur. Ces équipements peuvent offrir de nombreux services en matière de sécurité, mais également dans d'autres domaines : connectivité, optimisation, etc.

19. Session Border Controller.
20. Border Gateway.

Voici une liste non exhaustive des fonctions de sécurité que peut apporter un équipement de type *SBC/BG* :

- chiffrement des flux média et des flux de signalisation ;
- *B2BUA* [21] ;
- analyse protocolaire ;
- prévention des attaques en déni de service ;
- masquage de la topologie des réseaux internes/NAT ;
- limitation du trafic .

6.3.3.2 Interconnexions opérateurs

R32

> Pour renforcer la disponibilité du service de téléphonie, raccorder l'infrastructure de ToIP à plusieurs liens opérateurs répartis si possible sur des sites physiques distincts.

R33

> Utiliser de préférence des liens *TDM* pour raccorder l'infrastructure de ToIP à celles des opérateurs.

R34

> Si des trunks *SIP* sont utilisés pour raccorder une architecture de téléphonie aux opérateurs (non recommandé), il est impératif d'utiliser des équipements de sécurité périphériques (*SBC/BG* par exemple) pour sécuriser les échanges avec l'extérieur et protéger le système d'information.

Le raccordement opérateur peut s'effectuer à l'aide de différents type de liens :

- *TDM* : ce type de lien est utilisé historiquement pour raccorder les infrastructures de téléphonie classiques (non IP) aux opérateurs et nécessite l'utilisation de cartes spécifiques sur certains équipements centraux (cartes T0, T2). L'usage de liens *TDM* est toujours recommandé pour interconnecter une infrastructure de téléphonie sur IP car il assure une rupture protocolaire entre le monde IP utilisé en interne et le monde extérieur non IP. Ce type de lien assure une ligne de démarcation claire entre le système d'information interne et les infrastructures des opérateurs externes. Les liens *TDM* facilitent également le diagnostic des problèmes de qualité de service et délimitent avec précision les domaines de responsabilité. Il est également recommandé de mettre en place des liens opérateurs unidirectionnels, certains dédiés aux appels sortants et d'autres dédiés aux appels entrants. En cas d'attaque venant de l'extérieur, seules les communications entrantes seront ainsi perturbées ;
- IP (Trunk *SIP*) : ce type de lien est plus récent, il permet le raccordement d'une infrastructure de téléphonie aux opérateurs directement en IP via l'utilisation de trunks *SIP*. Si cette solution offre une certaine souplesse à l'usage et peut aider à réduire les coûts, elle ne permet pas de rupture protocolaire (tout IP) entre les réseaux IP internes et l'extérieur. La démarcation est moins nette entre les réseaux non maîtrisés (côté opérateur) et le système d'information interne. L'usage de trunks *SIP* n'est donc actuellement pas recommandé pour interconnecter une infrastructure de téléphonie sur IP aux réseaux des opérateurs. Si malgré tout, ce type de lien est utilisé, il est préconisé de mettre en place des mécanismes de sécurité adéquates pour protéger l'infrastructure interne ainsi que les communications téléphoniques. Les équipements de type *SBC/BG* doivent

21. *Back to Back User Agent* : Cette fonctionnalité permet au *SBC/BG* de se placer en coupure de l'ensemble des flux de téléphonie (signalisation et média), évitant par exemple les connexions directes entre deux postes. Si cette fonctionnalité est nécessaire, il convient de prévoir un autre *SBC/BG* pour assurer la protection périmétrique.

être mis en œuvre pour sécuriser les trunk *SIP*. Il est également recommandé de mettre en place des liens *TDM* de secours pour renforcer la résilience du service en cas d'indisponibilité des liaisons IP.

6.3.4 Qualité de service (QoS)

R35

Marquer les flux de téléphonie permet d'améliorer la qualité des communications téléphoniques et de renforcer la disponibilité du service.

La nature temps réel des flux de voix les rend particulièrement sensibles aux perturbations du réseau. Ces flux peuvent être perturbés par d'autres types de trafic, en particulier lorsque les équipements réseaux sont mutualisés avec des réseaux de données (déconseillé). Il est ainsi recommandé de marquer au plus tôt les flux de téléphonie pour qu'ils soient correctement priorisés tout au long de leur parcours, et ce quelle que soit l'architecture retenue. Les possibilités de marquage sont dépendantes de la solution de téléphonie employée ainsi que des technologies utilisées au niveau des équipements réseaux. Il est possible de différencier les flux de téléphonie à l'aide de marqueurs positionnés à différents niveaux (niveau 2 : 802.1p, niveau 3 : DSCP [22], etc.). Il existe pour chacun d'entre eux des classes de services adaptées aux communications temps réel ; au lecteur de déterminer la ou les technologies de QoS qu'il est possible d'utiliser dans son contexte.

6.3.5 Postes opérateurs sur PC (POPC)

Les POPC sont des postes informatiques spécifiques utilisés par des personnes disposant de privilèges sur des applicatifs de l'infrastructure de téléphonie. À ce titre, ils doivent être sécurisés comme les postes d'administration.

R36

A minima, les préconisations suivantes sont à respecter pour les POPC :
- ils doivent être hébergés sur des réseaux différents des réseaux d'administration ;
- ils ne doivent pas disposer d'accès à Internet ;
- les comptes utilisateurs locaux aux POPC ne doivent pas disposer de droits d'administration locaux ;
- les comptes utilisateurs employés sur les applicatifs de téléphonie doivent disposer des droits strictement nécessaires au rôle d'opérateur (respect du principe de moindre privilège) ;
- seuls les applicatifs utiles au rôle d'opérateur doivent être présents sur les POPC.

6.3.6 Télémaintenance

Certains mainteneurs ou certains éditeurs imposent la mise en place de liens de télémaintenance pour accéder à distance aux équipements de l'infrastructure de téléphonie sur IP installés chez leurs clients. La mise à disposition d'un service de ce type comporte des risques, il convient donc d'être rigoureux lors de sa mise en œuvre pour ne pas exposer inutilement le système d'information.

22. Differentiated Services Code Point.

R37

La télémaintenance par des mainteneurs ou des éditeurs externes est déconseillée. Si elle est indispensable, il est primordial de s'assurer contractuellement que les opérations de télémaintenance seront effectuées depuis les locaux du contractant, situés de préférence sur le territoire national.

6.3.6.1 Cloisonnement des équipements de télémaintenance

R38

Les opérations d'assistance menées par le télémainteneur doivent être réalisées uniquement à partir d'un serveur de rebond dédié à la ToIP dont l'accès nécessite une authentification préalable des intervenants extérieurs.

L'ensemble des équipements qui composent l'infrastructure de téléphonie ne doit pas être accessible directement via le lien de télémaintenance. Il est recommandé de disposer d'une machine de rebond placée dans une DMZ spécifique dédiée à la télémaintenance de la téléphonie sur IP (se référer au paragraphe 6.3.2). Cet équipement est un point de passage obligatoire pour les demandes de connexions provenant du télémainteneur. L'accès à cette machine doit nécessiter une authentification, elle est la seule autorisée à accéder aux équipements de l'infrastructure de ToIP normalement accessible au télémainteneur.

6.3.6.2 Liaison temporaire

R39

Définir une procédure manuelle d'établissement de la liaison de télémaintenance de l'infrastructure de ToIP. Ce lien ne doit être fonctionnel que le temps des opérations réalisées à distance par le tiers.

Si le prestataire en charge de l'assistance à distance ne réalise pas l'infogérance [23] au quotidien de l'infrastructure de téléphonie, la liaision de télémaintenance établie entre celui-ci et l'entité cliente ne doit être activée que temporairement. Il est recommandé d'établir la liaison manuellement (branchement d'un câble par exemple) via une procédure de contre-appel. L'accès à distance aux équipements de l'infrastructure de téléphonie ne doit être opérationnel que le temps nécessaire à l'intervention du tiers, il doit être désactivé une fois les opérations terminées.

6.3.6.3 Liaison sécurisée et dédiée

R40

Utiliser une liaison réseau sécurisée et dédiée pour l'accès à distance à la zone réservée à la télémaintenance de l'infrastructure de ToIP. Ce lien peut être sécurisé à l'aide du protocole IPsec [24] par exemple.

23. Les problématiques associées à l'infogérance sont présentées dans le document intitulé « Guide de l'externalisation » disponible sur le site de l'ANSSI.
24. Le document intitulé « Recommandations de sécurité relatives à IPsec » est disponible sur le site de l'ANSSI.

6.3.6.4 Traçabilité

R41

> Utiliser des comptes d'administration spécifiques pour la télémaintenance. Ces comptes, activés temporairement, ne doivent disposer que de privilèges strictement nécessaires à la réalisation des opérations d'assistance.

R42

> Journaliser l'ensemble des actions réalisées par les télémainteneurs au même titre que pour n'importe quel compte disposant d'un accès sur l'infrastructure de ToIP. En fonction du niveau de sensibilité de l'entité, il est recommandé de journaliser l'ensemble des actions à l'aide d'un dispositif qui n'est pas accessible par le télémainteneur.

6.3.6.5 Architecture de télémaintenance type

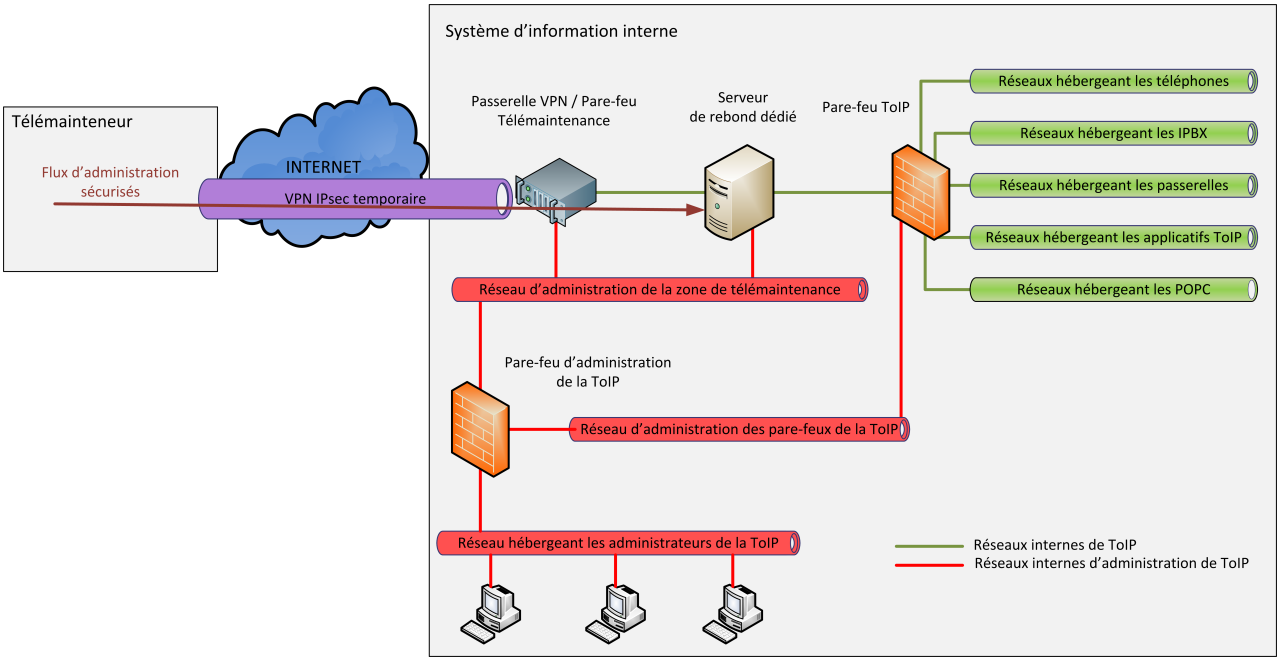

FIGURE 1 – Architecture de télémaintenance type.

Cette illustration reprend les principes énoncés précédemment :
- utilisation d'un serveur de rebond dédié à la ToIP ;
- établissement d'une liaison de télémaintenance temporaire ;
- sécurisation de la liaison à l'aide de mécanismes robustes (IPsec).

6.4 Protection des communications téléphoniques

R43

> Sécuriser les flux média et les flux de signalisation pour assurer la protection des communications téléphoniques et des données associées.

R44

> L'emploi ou non du service de sécurisation des communications doit être visible de l'utilisateur (affichage d'un symbole spécifique sur l'écran de l'usager).

La sécurisation des communications téléphoniques nécessite généralement la protection de deux types de flux réseau :

- les flux média : ces flux sont utilisés pour transporter la voix. Le protocole *SRTP*[25] correspond à la déclinaison sécurisée du protocole *RTP* généralement utilisé pour transporter la voix dans les architectures de téléphonie sur IP ;
- les flux de signalisation : ces flux sont utilisés pour gérer les échanges entre les différents composants de l'architecture de téléphonie. Ils permettent en particulier l'établissement des communications téléphoniques et peuvent véhiculer des informations sensibles. Le protocole sécurisé *SIP-TLS* (par exemple) correspond à la déclinaison sécurisée du protocole de signalisation *SIP*.

La mise en œuvre de ces protocoles doit s'accompagner de l'utilisation de mécanismes cryptographiques robustes (algorithmes, fonctions de hachage, etc.) qui respectent les recommandations décrites dans l'annexes B1 du Référentiel Général de Sécurité (RGS), en particulier lorsqu'il est fait usage de certificats.

L'activation des mécanismes de protection des communications téléphoniques induit un surplus de consommation de bande passante ainsi qu'une consommation plus élevée des ressources des équipements en charge des opérations cryptographiques. Les éditeurs de solutions de téléphonie sont normalement en mesure d'estimer les surcoûts engendrés afin de dimensionner correctement les équipements de l'infrastructure de téléphonie.

6.5 Maîtrise des fonctionnalités téléphoniques

6.5.1 Fonctionnalités à risque

La téléphonie sur IP permet d'offrir aux usagers un nombre toujours croissant de fonctionnalités accessibles à partir de leur terminal. Parmi les services offerts, un certain nombre d'entre eux peut présenter des risques de différentes natures (perte de confidentialité, perte financière). La maîtrise des fonctionnalités mises à disposition aux utilisateurs permet de limiter ces risques.

Voici quelques fonctionnalités téléphoniques « à risque » qu'il est recommandé de ne pas activer :

- poste fictif ;
- substitution ;
- entrée en tiers discrète ;
- écoute discrète ;
- DISA[26] ;

et celles pour lesquelles une attention particulière doit être portée lors de leur activation :

- appel à l'international ;
- transfert d'appels ;
- conférence avec enregistrement.

R45

> Il est recommandé de désactiver les fonctionnalités « à risque » pour l'ensemble des usagers avant d'associer à chacun, à l'aide d'un nombre réduit de rôles, les services de téléphonie qui leur sont strictement nécessaires.

25. Secure Real-Time Transport Protocol.
26. Direct Inward System Access : Cette fonctionnalité permet à l'usager de bénéficier de fonctionnalités internes du service de téléphonie à partir d'un appel émis de l'extérieur.

Voici la méthode qu'il est recommandé de mettre en œuvre pour garder le contrôle des fonctionnalités identifiées comme « à risque » :

1. désactiver les fonctionnalités pour l'ensemble des usagers ;
2. créer des groupes spécifiques pour chacune des fonctionnalités ;
3. associer aux utilisateurs les groupes qui leur sont strictement nécessaires.

6.5.2 Restriction d'accès à certaines fonctionnalités

R46

> Mettre en œuvre des restrictions d'usage si des fonctionnalités « à risque » sont activées.

Au-delà des services accordés aux utilisateurs, il est recommandé de prévenir l'utilisation abusive ou frauduleuse des fonctionnalités permises. Les solutions de téléphonie offrent généralement la possibilité de configurer des mécanismes permettant de restreindre l'usage des fonctionnalités autorisées. La définition précise des restrictions à mettre en place est dépendante des besoins métiers et des possibilités qu'offrent la solution de téléphonie employée. Il convient donc d'étudier avec précision ces deux aspects.

Voici, par exemple, quelques restrictions qu'il est possible de mettre en place pour les appels à l'étranger :

- restrictions horaires : les appels à l'étranger sont ils autorisés la nuit ? Si oui, le code *PIN* pourra être demandé au préalable à l'utilisateur avant de pouvoir composer ce type de numéro en dehors des horaires métiers ;
- restriction des pays de destination : les appels vers le pays X sont-ils nécessaires au métier de l'entité ? Si non, il est possible de l'interdire totalement. Si oui, il est recommandé de n'accorder le droit qu'aux groupes de personnes susceptibles d'en avoir un usage professionnel.

6.6 Convergence

La convergence appliquée au domaine de la téléphonie sur IP a pour objectif de rendre accessible des services de téléphonie à partir d'équipements/de réseaux tiers ou d'enrichir le service de téléphonie à l'aide de services extérieurs. Cela peut se traduire par exemple par la mise à disposition d'un accès web à la messagerie (messagerie unifiée) ou encore l'usage de *softphone* (cf. paragraphe suivant).

L'ouverture de ce type de service implique des interactions directes entre l'infrastructure de téléphonie et les réseaux de données internes ou externes, ce qui est déconseillé (cf. 5.3.1). Si malgré tout, ce type de service est proposé, il est impératif de respecter les recommandations de cloisonnement minimales présentées dans le paragraphe 5.3.2. À ce titre, les équipements centraux qui participent à la mise à disposition de services associés à la convergence doivent être placés dans une zone dédiée.

6.6.1 Softphone

R47

> L'usage de *softphones* en lien avec l'infrastructure de téléphonie est déconseillé.

Les *softphones* sont des logiciels qui permettent d'utiliser le service de téléphonie depuis un ordinateur connecté à un réseau de données (interne ou externe). Ces applicatifs peuvent s'avérer pratiques et économiques mais ils exposent davantage l'infrastructure de téléphonie (perte de confidentialité, intrusion etc.). Ils sont aujourd'hui connus comme pouvant être des vecteurs d'attaques des postes

sur lesquels ils sont installés [27]. Si malgré cette recommandation, des *softphones* sont employés il est impératif de cloisonner les réseaux hébergeant les postes informatiques qui en font usage.

6.6.2 Technologies sans fil

R48

> L'usage de téléphones IP basés sur des technologies sans fil est déconseillé (DECT, Wifi, Wimax..).

Si malgré cette recommandation la technologie Wifi est utilisée, sa mise en œuvre doit respecter *a minima* les recommandations détaillées dans la note technique intitulée « Recommandations de sécurité relatives aux réseaux Wifi » disponible sur le site de l'ANSSI.

6.7 Divers

6.7.1 Équipements analogiques persistants

R49

> Identifier les équipements analogiques persistants et prendre les mesures adéquates pour assurer leur fonctionnement après le passage en IP de l'infrastructure de téléphonie.

Lors de la mise en œuvre d'une architecture de téléphonie sur IP, il est important de déterminer les équipements analogiques qui ne seront pas migrés en IP pour des questions fonctionnelles ou techniques. Cela peut concerner par exemple des fax ou des postes téléphoniques réservés à un usage spécifique (gardiennage par exemple). Il existe des solutions permettant de faire transiter les fax sur des réseaux IP [28] mais elles ne sont pas détaillées dans ce document. Si des équipements persistants sont identifiés, il convient de prendre les dispositions adéquates pour qu'ils puissent continuer à communiquer après le passage en IP de l'infrastructure de téléphonie (conservation de lignes analogiques dédiées, ajout de cartes analogiques sur certains équipements centraux, etc.).

27. Voir par exemple la publication http://cs.gmu.edu/~xwangc/Publications/Securecom13-VDOS.pdf.
28. protocole T38/ RFC 3362.