

## Audit de réseaux VoIP

### 4 – Vulnérabilités

<b>Project phase</b>	WP6
<b>Author</b>	Juergen Ehrensberger, Alistair Doswald
<b>Document creation</b>	10 octobre 2006
<b>Version</b>	1.0
<b>Latest modification</b>	10 octobre 2006
<b>Version control path</b>	

#### Résumé

*Ce document fait partie de la méthodologie d'audit de réseaux VoIP du projet Vadese. Il fournit les checklists pour la collecte d'informations pour la 4ème étape de l'audit, le test des vulnérabilités du système.*

© 2006 HES-SO

#### Relation avec les documents de l'audit VoIP

Ce document contient les checklists pour la collecte d'informations de la première étape de l'audit VoIP. La méthodologie d'audit générale est décrite dans le document « Audit sécurité VoIP » [1]. L'analyse des informations collectées et les instructions pour la rédaction du rapport d'audit sont traitées dans le document « Caractérisation – Analyse » [2].

#### Structure du document

La première partie du document décrit les composants de réseaux VoIP. La deuxième partie fournit les checklists qui permettent de collecter les informations qui caractérisent le réseau VoIP et qui délimitent l'envergure de l'audit.

## 1 Composants de réseaux VoIP

Cette section décrit brièvement les différents composants qui forment un réseau VoIP. D'après [1], les composants de réseaux VoIP comprennent :

- le matériel (serveurs, dispositifs de réseau),
- les logiciels,
- les services,
- les contrôles (méthodes de sécurisation),

- les données gérées.

Un service est réalisé par un logiciel spécifique qui fonctionne sur un ou plusieurs serveurs ou dispositifs de réseau. Certains services gèrent des données, p.ex. pour l'authentification des utilisateurs ou le routage d'appels. Les données sont donc liées aux services.

Les contrôles sont les méthodes de sécurisation du réseau, comme l'authentification des utilisateurs ou un firewall. Ils sont traités dans l'étape 3 de la méthodologie d'audit.

## 1.1 Serveurs et dispositifs de réseaux

---

<b>Back-to-back user agent (B2BUA)</b>	
<b>Description</b>	Un « back-to-back user agent » (B2BUA) est un dispositif qui doit faire des opérations plus compliquées que celles d'un simple proxy. D'après la RFC il doit agir comme un UAS pour recevoir les requêtes, pouvoir déterminer comment la requête doit être traitée en maintenant l'état du dialogue, et pouvoir répondre comme un UAC. Un Session Border Controller (SBC) est un exemple d'un B2BUA.
<b>Services</b>	Nombreux services possible
<b>Protocoles</b>	SIP, potentiellement de nombreux autres.
<b>Réalisation</b>	Logiciel commercial : - Logiciel open source : - Matériel : -
<b>Références</b>	<ul style="list-style-type: none"><li>• 3261: Session Initiation Protocol</li></ul>

<b>Client Hardphone</b>	
<b>Description</b>	Un hardphone ressemble à un téléphone traditionnel, mais se branche sur un réseau IP. De plus, il peut intégrer de nombreux services supplémentaires rendus possibles par le modèle SIP. La description du fonctionnement d'un client SIP est décrite dans la RFC 3261, mais une définition des exigences d'un téléphone SIP se trouve dans la RFC 4504.

<b>Services</b>	Téléphonie, vidéophonie, conférence, présence (ou état), authentification, sécurisation des messages et flux média, mis en attente, transfert d'appel, information sur l'appelant, itinérance, messagerie instantanée, comptes multiples, e-mail, voice-mail, messagerie instantanée off-line
<b>Protocoles</b>	SIP, DHCP, SNTP, DNS, ENUM, RTP, RTCP, SRTP, SRTCP, SIMPLE, SNMP, HTTP, HTTPS, TFTP, UPnP, STUN, TURN
<b>Réalisation</b>	Matériel : Cisco Unified IP phones, snom VoIP Phone, Sipura IP phones
<b>Références</b>	<ul style="list-style-type: none"> <li>• RFC 3261: Session Initiation Protocol</li> <li>• RFC 4504 : SIP Telephony Device Requirements and Configuration</li> </ul>

<b>Client Softphone</b>	
<b>Description</b>	Un softphone est un logiciel qui fournit les services VoIP. La description donnée dans la RFC 4504 pour les hardphones est aussi valide pour les softphones (bien qu'une partie ne soit pas utile). Par contre, plusieurs protocoles ne seront pas pris en charge directement par le logiciel, mais plutôt par l'OS sous-jacent. Quelques versions offrent des services et protocoles supplémentaires.
<b>Services</b>	Téléphonie, vidéophonie, conférence, présence (ou état), authentification, sécurisation des messages et flux média, mis en attente, transfert d'appel, information sur l'appelant, itinérance, messagerie instantanée, comptes multiples, e-mail, voice-mail, messagerie instantanée off-line
<b>Protocoles</b>	SIP, DHCP, SNTP, DNS, ENUM, RTP, RTCP, SRTP, SRTCP, SIMPLE, SNMP, HTTP, HTTPS, TFTP, UPnP, STUN, TURN

<b>Réalisation</b>	Logiciel commercial : Snom 360 softphone, AGEphone, Vphone Logiciel open source : Ekiga, KPhone, Minisip, Twinkle, TudoMais (multiplateforme), Wengophone (multiplateforme)
<b>Références</b>	<ul style="list-style-type: none"> <li>• RFC 3261: Session Initiation Protocol</li> <li>• RFC 4504 : SIP Telephony Device Requirements and Configuration</li> </ul>

<b>Contrôleur de session (SBC)</b>	
<b>Description</b>	Le but d'un contrôleur de session (session controller ou session border controller, SBC) est de permettre la communication interactive à travers les frontières de différents réseaux IP. Pour ce faire, cet équipement travail soit avec (devant, pour être plus précis) les « softswitchs », les firewalls et les NATs, soit tout seul, en intégrant ces fonctions. Le contrôleur de session traite non seulement le trafic SIP, mais également le trafic média. En plus des fonctions permettant de traverser les frontières d'un réseau, il peut également avoir des fonctionnalités supplémentaires comme gateway ou contrôle de sécurisation.
<b>Services</b>	Transport, sécurisation, filtrage d'appel, authentification, transport vers d'autres protocoles
<b>Protocoles</b>	SIP, RTP, RTCP, H.323, protocoles de communication PSTN et ISDN
<b>Réalisation</b>	Logiciel commercial : Data connection's SBC, RapidFLEX™ Session Border Control Server Logiciel open source : OpenSBC Matériel : Cisco Multiservice IP-to-IP Gateway, Newport networks 1460 Session Border Controller
<b>Références</b>	<ul style="list-style-type: none"> <li>• Wikipedia, 'Session border Controller', <a href="http://en.wikipedia.org/wiki/Session_Border_Controller">http://en.wikipedia.org/wiki/Session_Border_Controller</a></li> <li>• Session Controller Forum, <a href="http://www.sessioncontrollerforum.org/">http://www.sessioncontrollerforum.org/</a></li> <li>• Newport Networks, 'SIP, Security and Session Border Controllers', 2005 <a href="http://www.newport-networks.com/whitepapers/security1.html">http://www.newport-networks.com/whitepapers/security1.html</a></li> </ul>

<b>Firewall</b>	
<b>Description</b>	<p>Un firewall est un dispositif situé entre deux réseaux et qui filtre certaines communications entre les réseaux. Principalement on distingue des firewalls sans état et des firewalls avec état. Un firewall sans état traite chaque paquet de manière indépendante, sans garder de traces de paquets observés ou de décisions prises précédemment.</p> <p>Un firewall avec état mémorise certaines informations et est capable d'associer les paquets à des connexions. Un firewall avec état peu p.ex bloquer une réponse HTTP, si aucune requête n'a été observée précédemment.</p> <p>On distingue également des firewalls au niveau réseau et des firewalls applicatifs.</p>

	<p>Un firewall au niveau réseau ne connaît que les couches OSI 1-4 et base sa décision de bloquer ou faire passer un paquet sur</p> <ul style="list-style-type: none"> <li>• les adresses IP sources et destination,</li> <li>• le protocole de transport (UDP, TCP)</li> <li>• les ports TCP/UDP source et destination,</li> <li>• les informations de routage (interface d'entrée et de sortie),</li> <li>• l'état de la communication, pour un firewall avec états.</li> </ul> <p>Les firewalls applicatifs ou ALG (Application Layer Gateways) connaissent les protocoles supérieurs (couches OSI 5-7) et sont capables d'utiliser les informations contenus dans les messages de ces protocoles afin de prendre la décision de bloquer ou laisser passer les paquets. En particulier, un ALG permet de tenir compte de numéro de ports négociés dynamiquement, de session impliquant plusieurs connexions et du contenu des messages au niveau application. Un SBC (contrôleur de session) est un ALG spécifique à la VoIP.</p> <p>Souvent, le même dispositif combine des fonctions de firewall/ALG et NAT.</p>
<b>Services</b>	Filtrage de paquets
<b>Protocoles</b>	UPnP
<b>Réalisation</b>	<p>Logiciel commercial : Cisco IOS Firewall (SIP aware), Logiciel open source : Shoreline Firewall, Bastion firewall IP Filter Matériel : Borderware SIPassure (SIP aware), Ingate Firewall (SIP aware), Cisco PIX firewall</p>
<b>Références</b>	<ul style="list-style-type: none"> <li>• Lisa Hallingström, Janne Magnusson, <i>'The SIP Protocol and Firewall Traversal'</i>, 2005 <a href="http://www.intertex.se/upfiles/IntertexSIPWhitePaper.pdf">http://www.intertex.se/upfiles/IntertexSIPWhitePaper.pdf</a></li> <li>• TERENA, <i>'IP Telephony Cookbook'</i>, 2004, <a href="http://www.terena.nl/activities/iptel/contents1.html">http://www.terena.nl/activities/iptel/contents1.html</a></li> </ul>

<b>Gateway PSTN, H.323, ...</b>	
<b>Description</b>	Les gateways les plus courants sont ceux pour relier une communication SIP avec les réseaux PSTN et ISDN, mais c'est aussi possible de trouver des portails qui font la traduction vers d'autres normes VoIP (comme H.323).
<b>Services</b>	Transport vers d'autres protocoles
<b>Protocoles</b>	SIP, H.323, protocoles de communication PSTN et ISDN
<b>Réalisation</b>	<p>Logiciel commercial : Cisco Voice Gateways Logiciel open source : aucun logiciel spécifique, il faut utiliser un IPBX comme Asterisk Matériel : Datang MG3000-T32 Trunk Gateway, YuXIN YGW30 Gateway</p>
<b>Références</b>	<ul style="list-style-type: none"> <li>• TERENA, <i>'IP Telephony Cookbook'</i>, 2004, <a href="http://www.terena.nl/activities/iptel/contents1.html">http://www.terena.nl/activities/iptel/contents1.html</a></li> </ul>

IPBX	
<b>Description</b>	Pour SIP, un IPBX est une réunion de ses divers services. En particulier : un proxy, un registrar, un service de localisation, et éventuellement un ou plusieurs portails. Des IPBX tel qu'Asterisk incorporent tous ces services et plus encore, par exemple celles proposés par un système de messagerie unifiée.
<b>Services</b>	Routage, transport, transport vers d'autres protocoles, authentification, enregistrement, localisation
<b>Protocoles</b>	SIP, DNS, H.323, protocoles de communication PSTN et ISDN
<b>Réalisation</b>	Logiciel commercial : Cisco Unified CallManager, Cisco Unified CallManager Express, pbxnsip, Microsoft Office Unified Communications Logiciel open source : Asterisk, SipX PBX, Open PBX, SIPexchange PBX Matériel : -
<b>Références</b>	-

NAT	
<b>Description</b>	<p>Un NAT permet de faire la traduction depuis des adresses privées non routable, vers une ou plusieurs adresses IP publique. L'avantage est double : on permet aux systèmes avec les adresses routables d'accéder à Internet, et on cache la topologie du réseau local derrière une seule adresse IP. Pour SIP ceci pose un problème étant donné qu'il a été élaboré sans prendre en compte les NAT, et le protocole utilise les ports et adresses IP locaux à la couche application. Il faut donc mettre en place des mécanismes tels que STUN, TURN, UPnP ou ICE pour traverser ces NATs.</p> <p>Il existe plusieurs catégories de NATs :</p> <ul style="list-style-type: none"> <li>• Full Cone : Toutes les requêtes d'une même adresse interne et même port sont mappé vers le même adresse et port externe. Un système externe peut contacter un système interne via cette adresse et port.</li> <li>• Restricted Cone : Idem que le full cone, sauf qu'un système externe ne peut contacter un système interne (via mapping) que s'il a été contacté en premier.</li> <li>• Port Restricted Cone : Idem que le restricted cone, à part qu'un système externe ne peut envoyer un paquet vers un port sur un système interne (via mapping) que s'il a été contacté depuis ce port.</li> <li>• Symmetric : Les requêtes d'une adresse et port interne vers un système externe sont mappées vers une même adresse et un même port externe. Par contre, les requêtes depuis ce port et cette adresse interne vers une autre destination seront mappées différemment.</li> </ul>
<b>Services</b>	Translation d'adresses
<b>Protocoles</b>	uPnP

<b>Réalisation</b>	Logiciel commercial : Cisco IOS NAT, Wingate Logiciel open source : IP Filter, natd Matériel : Draytek V2900VG Broadband VoIP Security Router (SIP-aware)
<b>Références</b>	<ul style="list-style-type: none"> <li>• Wikipedia, '<i>Network Address Translation</i>', <a href="http://en.wikipedia.org/wiki/Network_address_translation">http://en.wikipedia.org/wiki/Network_address_translation</a></li> <li>• TERENA, '<i>IP Telephony Cookbook</i>', 2004, <a href="http://www.terena.nl/activities/iptel/contents1.html">http://www.terena.nl/activities/iptel/contents1.html</a></li> </ul>

<b>Serveur de conférence</b>	
<b>Description</b>	Le serveur de conférence est l'élément adressé (via URI) par les participants pour rejoindre ou créer une conférence. Il est ensuite responsable de maintenir une signalisation SIP avec ces participants ainsi que de s'assurer qu'ils reçoivent le media. Le serveur est aussi responsable d'implémenter les politiques de conférences. Le serveur peut contenir des modules supplémentaires : des mixeurs, qui reçoivent plusieurs flux média d'un même type, les combinant avant de les envoyer, et un <i>serveur de protocole de conférence</i> , qui peut retenir et manipuler la politique, et qui n'est pas forcément spécifique à SIP.
<b>Services</b>	Conférence
<b>Protocoles</b>	SIP, RTP, RTCP
<b>Réalisation</b>	Logiciel commercial : Cisco Unified MeetingPlace, Cisco Unified MeetingPlace Express, FirstHand Audio Conferencing Server Logiciel open source : Coolcollaborator, Vovida VOCAL Matériel : Cisco Unified MeetingPlace, Cisco Unified MeetingPlace Express
<b>Références</b>	<ul style="list-style-type: none"> <li>• RFC 4353 : A Framework for Conferencing with SIP</li> </ul>

<b>Serveur ENUM</b>	
<b>Description</b>	Dans un réseau VoIP, ce type de serveur sert à faire la traduction d'un numéro du PSTN vers une adresse SIP (peut aussi servir à faire la traduction vers une autre adresse web, comme un e-mail). Le serveur ENUM est en fait un serveur DNS qui accepte une demande de résolution d'adresse dans le domaine E.164 et qui rend un ou plusieurs enregistrements NAPTR.
<b>Services</b>	Traduction PSTN vers adresse web (SIP)
<b>Protocoles</b>	DNS, ENUM
<b>Réalisation</b>	Logiciel commercial : Lucent Technologies VitalQIP ENUM Manager, PowerDNS, Incognito Software ENUM commander Logiciel Open Source : MaraDNS Matériel : -

<b>Références</b>	<ul style="list-style-type: none"> <li>• RFC 3761 : The E.164 to URI DDDS Application (ENUM)</li> <li>• Lucent Technologies, "<i>ENUM Use and Management for the Successful Deployment of ENUM-Enabled Services</i>", <a href="http://www.lucent.com/livelihood/09009403800937d7_White_paper.pdf">http://www.lucent.com/livelihood/09009403800937d7_White_paper.pdf</a></li> <li>• IETF Internet draft : Session Peering Use Case for Cable</li> </ul>
-------------------	--

<b>Serveur de localisation</b>	
<b>Description</b>	Ce serveur est capable de fournir la localisation courante (ou les localisations courantes possibles) d'un appelé. Bien que la RFC demande un tel service, elle ne fournit aucun mécanisme particulier avec lequel il doit être implémenté.
<b>Services</b>	Localisation
<b>Protocoles</b>	Typiquement LDAP. N'importe quel protocole de communication compris par les proxys, serveur de redirection et registrar locaux.
<b>Réalisation</b>	Logiciel commercial : Indigo SIP Server & SDK Logiciel open source : OpenSER Matériel : -
<b>Références</b>	<ul style="list-style-type: none"> <li>• 3261: Session Initiation Protocol</li> </ul>

<b>Serveur de présence</b>	
<b>Description</b>	Un serveur de présence peut agir selon deux fonctions : soit comme un proxy pour router les messages de présence, soit pour retenir les informations de présence et d'état pour les clients. Dans ce cas ce serveur sera responsable d'informer ses clients des divers changements d'états qu'il reçoit.
<b>Services</b>	Transport, Routage, Présence/Etat
<b>Protocoles</b>	SIP, SIMPLE, protocole de communication avec le service de localisation (p. ex LDAP).
<b>Réalisation</b>	Logiciel commercial : Cisco Unified presence Server, RADVISION SIP Server Logiciel open source : OpenSER Matériel : -
<b>Références</b>	<ul style="list-style-type: none"> <li>• RFC 3856: A Presence Event Package for SIP</li> <li>• RFC 3903: Extension for Event State Publication</li> </ul>

<b>Serveur de redirection</b>	
<b>Description</b>	Lorsqu'il reçoit une requête, ce serveur renvoie une liste des emplacements courants de l'utilisateur demandé, ou du proxy à contacter.
<b>Services</b>	Redirection
<b>Protocoles</b>	SIP, protocole de communication avec le service de localisation (p. ex LDAP)

<b>Réalisation</b>	Logiciel commercial : Cisco proxy server, Indigo SIP Server & SDK, RADVISION SIP Server Logiciel open source : OpenSER Matériel : -
<b>Références</b>	<ul style="list-style-type: none"> <li>• 3261: Session Initiation Protocol</li> </ul>

<b>Serveur registrar</b>	
<b>Description</b>	Le registrar est un serveur qui accepte les requêtes d'enregistrement, puis place cette information dans le service de localisation de son domaine.
<b>Services</b>	Enregistrement
<b>Protocoles</b>	SIP, protocole de communication avec le service de localisation (p. ex LDAP)
<b>Réalisation</b>	Logiciel commercial : Cisco proxy server, Indigo SIP Server & SDK, RADVISION SIP Server Logiciel open source : OpenSER, Obelisk SIP proxy Matériel : -
<b>Références</b>	<ul style="list-style-type: none"> <li>• 3261: Session Initiation Protocol</li> </ul>

<b>Serveur proxy à états</b>	
<b>Description</b>	Le proxy à états a les mêmes fonctions que le proxy sans état, mais fait des traitements supplémentaires avec les messages qu'il reçoit, tel que valider les messages, multiplier un message ou absorber les messages retransmis. Un serveur proxy peut également utiliser des méthodes plus compliquées pour trouver un utilisateur, comme essayer un lieu possible, puis un autre s'il n'y a pas de réponse. Pour accomplir ses fonctions, ce type de proxy peut également générer certains messages SIP en plus de les router. Bien que ça ne fasse pas partie de la RFC, d'autres fonctionnalités avancées sont souvent incluses dans (ou avec) les proxys à état.
<b>Services</b>	Routage, transport, authentification
<b>Protocoles</b>	SIP, DNS, protocole de communication avec le service de localisation (p. ex LDAP)
<b>Réalisation</b>	Logiciel commercial : Cisco proxy server, Indigo SIP Server & SDK, RADVISION SIP Server Logiciel open source : OpenSER, PartySIP Matériel : -
<b>Références</b>	<ul style="list-style-type: none"> <li>• 3261: Session Initiation Protocol</li> </ul>

<b>Serveur proxy sans état</b>	
<b>Description</b>	<p>Le but du proxy sans état est simplement de router les messages SIP, c'est à dire vérifier qu'un message est correctement formé (selon certain critères), et déterminer la prochaine machine à qui il faut envoyer ce message. Le proxy peut également modifier les parties de l'entête du message qui concernent le chemin effectué.</p> <p>Afin de traiter le routage, le proxy doit également communiquer avec le service de localisation pour connaître l'emplacement des utilisateurs, mais peut également utiliser des tables statiques.</p>
<b>Services</b>	Transport de signalisation, routage de signalisation
<b>Protocoles</b>	SIP, DNS, protocole de communication avec le service de localisation (p. ex LDAP)
<b>Réalisation</b>	<p>Logiciel commercial : Cisco proxy server, Indigo SIP Server &amp; SDK, RADVISION SIP Server</p> <p>Logiciel open source : OpenSER, PartySIP, Obelisk SIP proxy</p> <p>Matériel : -</p>
<b>Références</b>	<ul style="list-style-type: none"> <li>• 3261: Session Initiation Protocol</li> </ul>

<b>Serveur STUN/TURN</b>	
<b>Description</b>	<p>Les serveurs STUN et TURN ont pour but de permettre à la communication SIP de traverser un NAT. Il faut noter que les deux types de serveurs doivent se trouver dans le réseau public.</p> <p>Un client SIP muni de STUN peut contacter un serveur pour connaître l'adresse publique du NAT. La réponse du serveur permettra également au client de connaître le type de NAT (cf. 1.1, NAT). Il est à noter que les serveurs STUN ne permettent pas de traverser un NAT symétrique.</p> <p>Un serveur TURN agit comme un relais pour les messages de signalisation et des messages de media. Le client a donc une adresse de transport pour pouvoir contacter l'extérieur avec une adresse routable, et se faire contacter en retour. Il est intéressant de noter que la combinaison d'un serveur TURN et d'un NAT symétrique agit comme un NAT à adresses restreint.</p>
<b>Services</b>	Transport à travers NAT, Transport (pour TURN)
<b>Protocoles</b>	STUN/TURN, pour TURN: SIP, RTP, RTCP
<b>Réalisation</b>	<p>Logiciel commercial : Eyeball Any-Firewall™ Server (STUN &amp; TURN)</p> <p>Logiciel open source : STUN server</p> <p>Matériel : -</p>
<b>Références</b>	<ul style="list-style-type: none"> <li>• RFC 3489: STUN</li> <li>• Draft-rosenberg-midcom-tun-08 : TURN</li> <li>• Newport Networks, '<i>NAT Traversal for Multimedia over IP Services</i>'; <a href="http://www.newport-networks.com/whitepapers/nat-traversal1.html">http://www.newport-networks.com/whitepapers/nat-traversal1.html</a></li> </ul>

<b>Système de messagerie unifiée (UM)</b>	
<b>Description</b>	Ce service doit seulement pouvoir communiquer avec le réseau téléphonique SIP via un moyen ou un autre (VoIP ou via PSTN/ISDN). Du côté du téléphone SIP, la seule chose qui est fait est une simple re-direction vers le service UM. Les seules contraintes que l'UM sont de diriger correctement le média vers le bon compte (boite e-mail/voix), et de fournir au propriétaire de ce compte la capacité de récupérer ce média.
<b>Services</b>	E-mail, voice-mail, messagerie instantanée offline, système de réponse interactive
<b>Protocoles</b>	SIP, RTP, RTCP, H.323, protocole de communication PSTN ou ISDN
<b>Réalisation</b>	Logiciel commercial : Cisco Unity, Cisco Unity Express, Mitel NuPoint Messenger IP Logiciel open source : Lintad, OpenUMS Matériel : Adomo Voice messaging, Nortel CallPilot 150,
<b>Références</b>	<ul style="list-style-type: none"><li>• RFC 4458 : SIP URIs for Applications such as Voicemail and Interactive Voice Response (IVR)</li></ul>

## 2 Références

---

- [1] Projet VaDeSe : « Audit de la sécurité de réseaux VoIP » ; Version 1.0 ; Octobre 2006 ; HES-SO.
- [2] Projet VaDeSe : « Audit de la sécurité de réseaux VoIP - Caractérisation du système – Checklists » ; Version 1.0 ; Octobre 2006 ; HES-SO.
-

## 4 – Vulnérabilités

Collecte d'informations

Description de l'audit :

---

---

---

Auditeurs :

---

Date début de l'audit :

---

Date fin de l'audit :

---

Client Hardphone			
Vulnérabilité		Procédure suggérée	Résultats
1	Services et configuration	a	Vérifier que le hardphone ne propose pas de services à risque. OK N/A
		b	Vérifier que les services non supportés par le réseau sont désactivés OK N/A
		c	Vérifier que les ports supplémentaires du hardphone soient désactivés, ou utilisent le 802.1Q VLAN tagging (s'ils sont nécessaires) OK N/A
2	Contenu des messages	a	Vérifier les messages sortant pour des anomalies. Utiliser un logiciel, ou vérifier pour : des messages de signalisation vers des proxys hors du réseau local, des valeurs inconsistantes avec les appels faits, ou des champs contenant des valeurs non-standard. OK N/A
		b	Vérifier que des modifications faites au message par le hardphone ne révèlent pas des informations sensibles OK N/A
		c	Vérifier si l'on peut déterminer d'avance les identifiants (Call-ID, To, From, Cseq) des messages générés par le hardphone. Il faut voir si 1) les parties « random » sont en fait tirés des autres champs de la conversation 2) si ce sont des suites logiques qu'on peut déduire de l'historique. OK N/A
3	Session	a	Déterminer si une information de session peut être réutilisée sur cette machine ou d'autres hardphones (session replay). OK N/A
		b	Essayer de faire du vol de session. Sniffer et insérer un message de type « Refer » avec les bons paramètres. OK N/A
		c	Manipuler les messages pour tromper ou modifier la logique du hardphone. Tester pour des vulnérabilités connues, ou essayer de modifier des champs soit de manière logique, soit de manière à provoquer des erreurs (fuzzing). OK N/A

<b>Client Softphone</b>			
Vulnérabilité		Procédure suggérée	
1	Services et configuration	a	b
		Faire une liste des services que le softphone propose	Liste des services du softphone
		Vérifier que les services non supportés par le réseau soient désactivés	OK Pas OK N/A
		Regarder si le softphone interagit correctement avec le système de sécurité de la station.	OK Pas OK N/A
		Vérifier que le softphone ne comporte pas de systèmes qui envoient des données personnelles. Faire du sniffing (mais nécessite p-t de capturer et regarder BCP de messages), et rechercher sur le net si ce logiciel est connu pour venir avec du spyware.	OK Pas OK N/A
2	Placement réseau	a	b
		Regarder si la machine sur laquelle est installée le softphone fait un pont entre le réseau de données et le réseau voix	OK Pas OK N/A
		La confidentialité est elle importante sur ce réseau VoIP ?	oui non N/A
3	Session	a	b
		Déterminer si une information de session peut être réutilisée sur cette machine ou d'autres softphones.	OK Pas OK N/A
		Essayer de faire du vol de session. Sniffer et insérer un message de type « Refer » avec les bons paramètres.	OK Pas OK N/A
		Manipuler les messages pour tromper ou modifier la logique du softphone. Tester pour des vulnérabilités connues, ou essayer de modifier des champs soit de manière logique, soit de manière à provoquer des erreurs (fuzzing).	OK Pas OK N/A
4	Contenu des messages	a	b
		Vérifier les messages sortant pour des anomalies. Utiliser un logiciel, ou vérifier pour : des messages de signalisation vers des proxys hors du réseau local, des valeurs inconsistantes avec les appels faits, ou des champs contenant des valeurs non-standard.	OK Pas OK N/A
		Vérifier que des modifications faites au message par le softphone ne révèlent pas d'informations sensibles	OK Pas OK N/A

		c	<p>Vérifier si l'on peut déterminer d'avance les identifiants (Call-ID, To, From, Cseq) des messages générés par le softphone. Il faut voir si 1) les parties « random » sont en fait tirés des autres champs de la conversation 2) si ce sont des suites logiques qu'on peut déduire de l'historique.</p>	OK	Pas OK	N/A
--	--	---	--	----	--------	-----

<b>Contrôleur de session</b>			
Vulnérabilité		Procédure suggérée	Résultats
1	Installation dans le réseau	a Si le SBC prend la place d'un firewall, utiliser l'OSSTMM section C module 8 – Access control testing	Résultats de l'OSSTMM
2	Epuisement de ressources	a Vérifier le nombre de sessions que le SBC peut maintenir b Vérifier que le trafic SIP par session est limité c Vérifier que le trafic de signalisation par utilisateur est limité d Vérifier que le trafic par réseau relié est limité e Vérifier que la signalisation globale est limitée de manière à ce que ça ne puisse pas épuiser les ressources du matériel du réseau f Tester s'il est possible d'épuiser les ressources du SBC avec un grand nombre de sessions	Nombre de sessions OK Pas OK N/A OK Pas OK N/A OK Pas OK N/A OK Pas OK N/A OK Pas OK N/A
3	Session	a Tester si le portail est susceptible à un épuisement de ressources par une inondation de messages « INVITE ». b Déterminer si une information de session peut être réutilisée sur cette machine (session replay). c Essayer de faire du vol de session. Sniffer et insérer un message de type 3xx avec les valeurs appropriés en début de session. d Manipuler les messages pour tromper ou modifier la logique du SBC. Tester pour des vulnérabilités connues, ou essayer de modifier des champs soit de manière logique, soit de manière à provoquer des erreurs (fuzzing).	OK Pas OK N/A OK Pas OK N/A OK Pas OK N/A OK Pas OK N/A

## Gateway

Vulnérabilité		Procédure suggérée	Résultats		
1	Routeage	a	Vérifier la table de routage pour vérifier qu'il n'y ait pas d'adresses non-nécessaires ou suspectes	Table de routage	
		b	Dans le cas d'un service de localisation interrogé via le réseau, vérifier si le protocole a des vulnérabilités connus	Protocole utilisé N/A	
2	Contenu des messages	a	Vérifier les messages sortant pour des anomalies. Utiliser un logiciel, ou vérifier pour : des adresses hors du réseau local (pour le coté SIP qui devrait être interne), des valeurs inconsistantes avec les appels faits, ou des champs contenant des valeurs non-standard.	OK Pas OK N/A	
		b	Vérifier que des modifications faites au message par le gateway ne révèlent pas des informations sensibles	OK Pas OK N/A	
		c	Vérifier si l'on peut déterminer d'avance les identifiants (Call-ID, To, From, Cseq) des messages générés par le gateway. Il faut voir si 1) les parties « random » sont en fait tirés des autres champs de la conversation 2) si ce sont des suites logiques qu'on peut déduire de l'historique.	OK Pas OK N/A	
3	Session	a	Vérifier le nombre de sessions concurrents que le portail peut supporter	Nombre de sessions	
		b	Tester si le portail est susceptible à un épuisement de ressources par une inondation de messages « INVITE ».	OK Pas OK N/A	
		c	Déterminer si une information de session peut être réutilisée sur cette machine ou sur d'autres gateways (session replay)	OK Pas OK N/A	
		d	Essayer de faire du vol de session. Sniffer et insérer un message de type 3xx avec les valeurs appropriées en début de session.	OK Pas OK N/A	
		e	Manipuler les messages pour tromper ou modifier la logique du Gateway. Tester pour des vulnérabilités connues, ou essayer de modifier des champs soit de manière logique, soit de manière à provoquer des erreurs (fuzzing).	OK Pas OK N/A	

Audit de réseaux VoIP - Vulnérabilités - Tests

4	Vol de service	a	Vérifier les logs du portail pour des appels anormalement longs, en particulier vers des destinations distantes. Vérifier si ce type d'appel est répété. Vérifier contre la politique d'appel de l'entreprise.	Logs du portail et politique d'appels de l'entreprise
		b	Vérifier que les logs du trafic du portail et les logs du trafic du serveur de comptabilité soient en accord	Log du serveur de comptabilité
		c	Si le portail est connecté sur un PBX appartenant à l'entreprise, vérifier le log des appels du portail contre celui du PBX	Log du PBX

<b>Serveur de conférence</b>						
Vulnérabilité		Procédure suggérée	Résultats			
1	Confidentialité et politique de conférence	a	Vérifier les politiques de conférence pour des anomalies (modifications, entrées non-logiques).	OK	Pas OK	N/A
		b	Vérifier que les politiques de conférence permettent seulement des utilisateurs de confiance de créer/superviser des conférences	OK	Pas OK	N/A
		c	Vérifier que l'information d'une conférence ne peut seulement être obtenue par des adresses locales (ou par des utilisateurs de confiance)	OK	Pas OK	N/A
2	Session	a	Vérifier qu'il n'est pas possible de d'épuiser les ressources en créant un grand nombre de conférences	OK	Pas OK	N/A
		b	Tester si le serveur de conférences est vulnérable à un épuisement de ressources par une inondation de messages « INVITE ».	OK	Pas OK	N/A
		c	Déterminer si une information de session peut être réutilisée sur cette machine ou une autre des serveurs de conférence (session replay).	OK	Pas OK	N/A
		d	Essayer de faire du vol de session. Sniffer et insérer un message de type « Refer » avec les bons paramètres.	OK	Pas OK	N/A
		e	Manipuler les messages pour tromper ou modifier la logique du serveur de conférence. Tester pour des vulnérabilités connues, ou essayer de modifier des champs soit de manière logique, soit de manière à provoquer des erreurs (fuzzing).	OK	Pas OK	N/A

<b>Serveur de présence</b>			
Vulnérabilité		Procédure suggérée	Résultats
1	Communication et traitement des messages	a	Si le serveur utilise le registrar pour les présences, déterminer le protocole de communication, et regarder s'il comporte des vulnérabilités  N/A
		b	Vérifier que le service de présence n'accepte pas de demande d'enregistrement vers une adresse non-locale ou non de confiance  OK Pas OK N/A
2	Informations transmises	a	Vérifier que le serveur de présence ne divulgue pas de l'information sensible dans ses messages  OK Pas OK N/A
		b	Vérifier que les règles d'affichage de présence soient respectées. Se procurer la politique de l'entreprise à ce propos au préalable.  OK Pas OK N/A
3	Tables de présence	a	Vérifier la table des présences pour des entrées malicieuses  Table de présences
		b	Vérifier la capacité de la table des présences  Nombre d'entrées possible
		c	Vérifier si le serveur est vulnérable à l'épuisement de ressources (entrées excessifs)  OK Pas OK N/A
4	Routage - si le serveur de présence est utilisé pour router les messages de présence	a	Vérifier la table de routage pour vérifier qu'il n'y ait pas d'adresses non-nécessaires ou suspectes  Table de routage

## Serveur proxy sans état

Vulnérabilité		Procédure suggérée		Résultats	
1	Routage	a	Vérifier la table de routage pour vérifier qu'il n'y ait pas d'adresses non-nécessaires ou suspectes	Table de routage	
		b	Dans le cas d'un service de localisation sur le réseau, vérifier si le protocole à des vulnérabilités connus	Protocole utilisé	N/A
2	Contenu des messages	a	Vérifier les messages sortant pour des anomalies. Utiliser un logiciel, ou vérifier pour : des adresses hors du réseau local (sauf en cas d'un proxy de bordure de réseau), des valeurs inconsistantes avec les appels faits, ou des champs contenant des valeurs non-standard.	OK	Pas OK N/A
		b	Vérifier que des modifications faites au message pas le proxy ne révèlent pas des informations sensibles (par exemple la structure du réseau)	OK	Pas OK N/A

<b>Serveur proxy à états</b>			
Vulnérabilité		Procédure suggérée	Résultats
1	Routage	a	Vérifier la table de routage pour vérifier qu'il n'y ait pas d'adresses non-nécessaires ou suspectes  Table de routage
		b	Dans le cas d'un service de localisation interrogé via le réseau, vérifier si le protocole a des vulnérabilités connus  Protocole utilisé N/A
		d	Vérifier que le proxy impose soit une limite sur le nombre de sauts (max-forwards), soit détecte les boucles  OK Pas OK N/A
2	Contenu des messages	a	Vérifier les messages sortant pour des anomalies. Utiliser un logiciel, ou vérifier pour : des adresses hors du réseau local (sauf en cas d'un proxy de bordure de réseau), des valeurs inconsistantes avec les appels faits, ou des champs contenant des valeurs non-standard.  OK Pas OK N/A
		b	Vérifier que des modifications faites au message par le proxy ne révèlent pas des informations sensibles  OK Pas OK N/A
		c	Vérifier si l'on peut déterminer d'avance les identifiants (Call-ID, To, From, Cseq) des messages générés par le proxy. Il faut voir si 1) les parties « random » sont en fait tirés des autres champs de la conversation 2) si ce sont des suites logiques qu'on peut déduire de l'historique.  OK Pas OK N/A
3	Session	a	Vérifier le nombre de sessions concurrentes que le proxy peut supporter  Nombre de sessions
		b	Tester si le proxy est susceptible à un épuisement de ressources par une inondation de messages « INVITE ».  OK Pas OK N/A
		c	Déterminer si une information de session peut être réutilisée sur cette machine ou sur d'autres proxys à états (session replay).  OK Pas OK N/A
		d	Essayer de faire du vol de session. Sniffer et insérer un message de type 3xx avec les valeurs appropriés en début de session.  OK Pas OK N/A
		e	Manipuler les messages pour tromper ou modifier la logique du  OK Pas OK N/A



<b>Serveur de redirection</b>			
Vulnérabilité		Procédure suggérée	
1	Routage	a	Vérifier la table de routage pour vérifier qu'il n'y ait pas d'adresses non-nécessaires ou suspectes
		b	Dans le cas d'un service de localisation sur le réseau, vérifier si le protocole a des vulnérabilités connues
		d	Vérifier que le serveur de redirection ne permette pas de rediriger vers une adresse externe
2	Contenu des messages	a	Vérifier les messages sortant pour des anomalies. Utiliser un logiciel, ou vérifier pour : des adresses hors du réseau local (vérifier avec un administrateur réseau pour ne pas avoir de faux positifs), des valeurs inconsistantes avec les appels fait, ou des champs contenant des valeurs non-standard.
		Résultats	
		Table de routage	
		Protocole utilisé	N/A
		OK	Pas OK
		OK	N/A
		OK	Pas OK
		OK	N/A

<b>Serveur Registrar</b>				
Vulnérabilité		Procédure suggérée		
Information traité		a	b	c
1		Vérifier que le registrar traite correctement une inondation de messages qui paraissent légitime (surtout depuis la même source).	OK	N/A
		Vérifier si le registrar refuse les valeurs possibles, mais absurdes, dans les champs du message (p.ex 0 dans expires)	OK	N/A
		Vérifier que l'application refuse les valeurs possibles, mais absurdes, dans les champs du message (p.ex 0 dans expires)	OK	N/A
2		Vérifier que le registrar n'accepte pas un enregistrement forgé	OK	N/A
		Dans le cas d'un service de localisation interrogé via le réseau, vérifier si le protocole à des vulnérabilités connues.	OK	N/A
			Protocole utilisé	N/A

## Service de localisation

Vulnérabilité		Procédure suggérée	Résultats		
1	Communication et traitement des messages	a	Déterminer le protocole de communication via le réseau, et regarder s'il comporte des vulnérabilités	Protocole utilisé	
		b	Vérifier que le service de localisation n'accepte pas d'entrées vers une adresse externe	OK	Pas OK N/A
		c	Vérifier que le service n'est pas susceptible à l'injection de SQL : vérifier en premier que le service utilise SQL, puis envoyer des messages SQL en essayant de tromper le service.	OK	Pas OK N/A
	Tables d'adresses	a	Vérifier les tables d'adresses pour des entrées malicieuses (cf.: Best Practices A.15, A.16, A.17, A.18)	Table d'adresses	
		b	Vérifier la capacité de la table d'enregistrement	Nombre d'entrées possible	
		c	Vérifier si le serveur est vulnérable à l'épuisement de ressources (entrées excessifs)	OK	Pas OK N/A

<b>Système de messagerie unifiée</b>					
Vulnérabilité		Procédure suggérée		Résultats	
1	Sécurité des comptes	a	Appliquer l'OSSTMM section D méthode 2 - Voicemail Testing	Résultats de l'OSSTMM	
		b	Vérifier que les comptes ne soient accessibles que depuis des stations ou adresses de confiance	OK	Pas OK N/A
2	Epuisement de ressources	a	Vérifier que la taille de la communication par message soit limitée	OK	Pas OK N/A
		b	Vérifier que les comptes aient une taille limitée ou un nombre de messages limités	OK	Pas OK N/A
		c	Vérifier qu'un avertissement soit donné si le système est à court de ressources	OK	Pas OK N/A