White Paper

La sécurité des communications unifiées et la collaboration

Welcome to the Human Network

Contact :

Fabien MEDAT

Solutions et Technologies

Communications unifiées et Collaboration

fmedat@cisco.com - +33 6 34 04 16 84

En quelques mots

Le contexte de sécurité a beaucoup évolué ces dernières années, tant du point de vue des menaces que du point de vue des usages : L'explosion de la mobilité et des nouveaux outils de communication rend la notion de périmètre de l'entreprise de plus en plus floue. L'information à protéger est désormais distribuée et mobile, avec de plus en plus d'applications temps-réel, tels les outils de collaboration. Le piratage informatique, quant à lui, est aujourd'hui réalisé par des professionnels, avec une véritable motivation financière derrière les attaques. Enfin, l'adoption de nouvelles règles de conformité dans un contexte de contrôle des coûts impacte l'élaboration de la stratégie de sécurité, et l'on recherche efficacité opérationnelle et optimisation des coûts.

L'approche CISCO

Cisco propose une approche de la sécurité des communications unifiées basée grâce à des fonctions réparties dans les différents équipements,

- **Les commutateurs**
- **Les routeus**
- **Les serveurs d'infrastructure**
- **Les applications**
- **Les IP Phones**
- **Les clients de communications**
- **Les pare-feu**
- **Les sondes IDS**

Les solutions de sécurité doivent répondre aux problématiques rencontrées sur les réseaux de voix, de vidéo et de données, à savoir :

- Déni de Service (DoS)
- Violation de Confidentialité
- Usurpation d'identité
- Manipulation de l'information
- Fraude à l'usage

La réponse CISCO pour sécuriser les communications unifiées et la collaboration dans l'entreprise est basée sur quatre piliers :

- L'infrastructure
- Le traitement d'appel
- Les terminaux
- Les applications

Cette approche permet aujourd'hui de garantir une sécurité globale apportant disponibilité, confidentialité, authenticité des communications.

Agenda

1 Introduction et menaces

Initialement les réseaux voix étaient séparés du monde IP. Cela était valable au niveau des infrastructures mais également au niveau des organisations dans les entreprises. Il y avait les services généraux qui géraient la voix et les services informatiques pour les serveurs et les postes utilisateurs.
L'arrivée de la téléphonie sur IP a quelque peu perturbé ce mode de fonctionnement en unifiant les communications autour d'IP et donc du réseau d'entreprise.
Pour beaucoup le réseau est encore synonyme de vulnérabilités potentielles et après avoir unifié voix et données autour d'IP on cherche de nouveaux à créer des domaines voix et données séparés tout en permettant les communications d'un domaine à l'autre de manière Sécurisé.

Les menaces potentielles sur un réseau de Communications Unifiées sont familières aux professionnels de la voix comme à ceux de la donnée :

- Déni de Service (DoS)
- Violation de Confidentialité
- Usurpation d'identité
- Manipulation de l'information
- Fraude à l'usage

Les professionnels de la voix ont eu à faire à ces risques depuis longtemps, les professionnels de la donnée aussi. Les fonctions étudiées dans ce qui suit visent à contrer ces différentes menaces. Les fraudeurs sont à l'affût et nul ne conteste aujourd'hui que la protection de la voix et de la donnée sur le réseau est critique pour l'entreprise.

2 La réponse CISCO

Cisco c'est employé ces dernières années à apporter une solution complète de sécurité (Self Defending Network) permettant d'assurer ces nouveaux modes de communications sans prendre de risque pour l'intégrité des systèmes.

Cisco vous propose aujourd'hui de sécuriser votre réseau de Communications Unifiées dans le cadre d'une approche système exhaustive. Les produits et technologies de Cisco garantissent un niveau de sécurité maximum à tous les niveaux de la solution de Communications Unifiées :

- L'infrastructure
- Le traitement d'appel
- Les terminaux
- Les applications

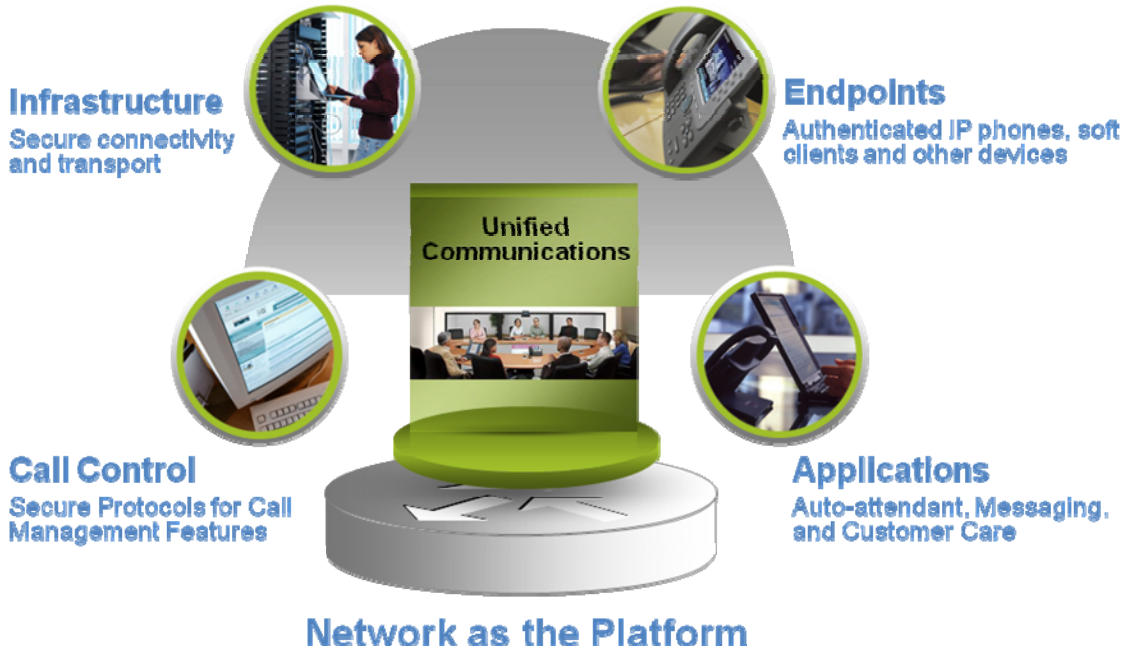

Figure 1 Les quatre piliers de la sécurité CISCO

Pour que votre réseau de Communications Unifiées puisse être considéré comme vraiment sécurisé, la sécurité de chacun de ces niveaux doit être adressée dans le cadre d'une approche système où tous les composants sont conçus pour travailler ensemble, mettant en commun leurs moyens pour lutter efficacement contre les attaques déclenchées depuis l'extérieur comme depuis l'intérieur, dans un contexte qui inclut également la composante mobilité. Chaque composant doit certes offrir des services qui lui permettent de se protéger, mais il doit aussi contribuer à la sécurité de l'ensemble du système. Cette approche, beaucoup plus efficace que la technique du point par point qui consiste à insérer des composants spécifiques pour résoudre des problèmes ponctuels (pare-feu à la frontière avec Internet, boîtier de chiffrement en coupure…) offre des avantages considérables sur les plans de :

- La simplification de l'environnement pour une administration plus facile
- L'intégration plus forte pour une réaction plus rapide face aux menaces
- La visibilité bien meilleure sur le fonctionnement de l'ensemble de la solution
- Du déploiement, des opérations et de l'optimisation plus aisés
- Du coût de possession réduit

L'architecture de sécurité proposée par Cisco dans le cadre des Communications Unifiées tire parti des fonctions de sécurité intégrées dans tous les produits et technologies mis en œuvre dans la solution, de façon à garantir des Communications Unifiées sécurisées et fiables.

Nous allons passer en revue dans ce qui suit l'ensemble des fonctions de sécurité intégrées dans les différents produits qui constituent la solution de Communications

Unifiées commercialisée par Cisco dont un résumé des fonctions est donné ci-dessous regroupées dans les quatre catégories présentés ci-dessus.

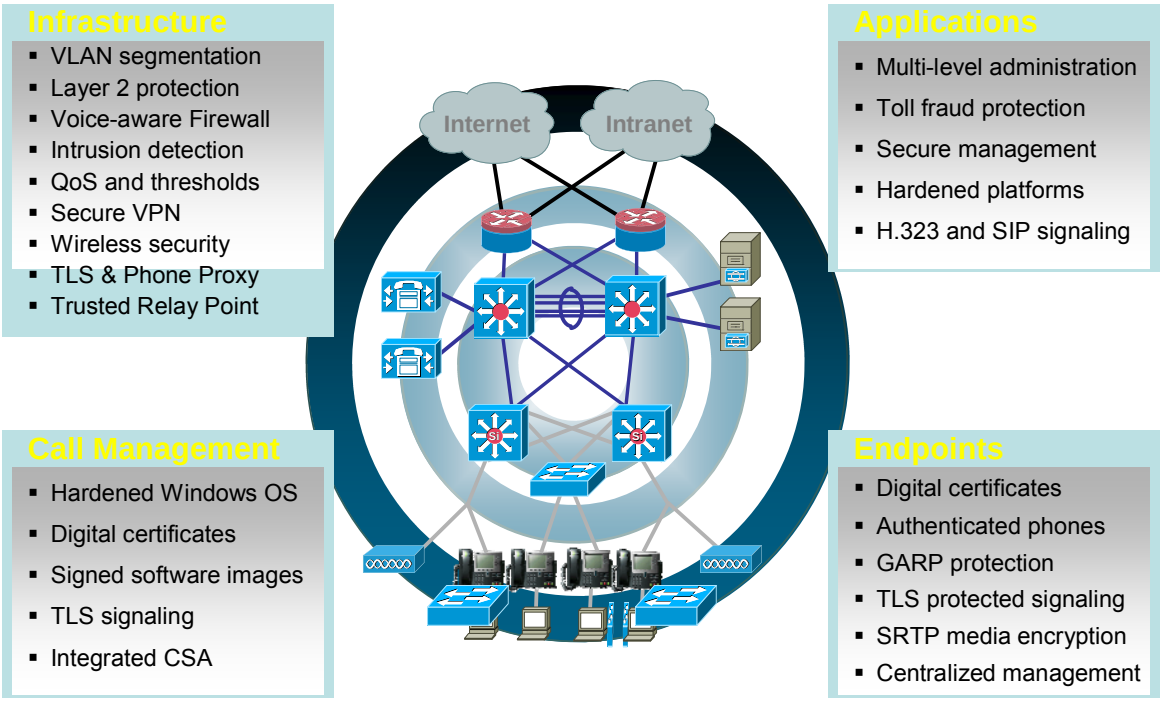

Figure 2 Les quatre piliers de la sécurité CISCO en détail

3 Les éléments de sécurité

3.1 Infrastructure

3.1.1 Sa propre protection

L'infrastructure doit bien sûr elle-même se protéger ce qui renforce la sécurité globale et la disponibilité du système. Chaque équipement, du commutateur Ethernet sur lequel est connecté le téléphone, en passant les commutateurs de cœur de réseau, les routeurs et par les pare-feu, doit être sécurisé pour éviter une prise de contrôle malveillante. Ceci est assuré par la protection des accès aux équipements en mode administrateur (mots de passe forts, liste restreinte d'adresses autorisées, chiffrement SSL des connexions, authentification RADIUS des utilisateurs).

L'infrastructure réseau apporte également un certain nombre de fonctions qui doivent être activées par configuration pour renforcer la sécurité des communications:

Les fonctionnalités de pare-feu ou de routeur filtrant, de détection et de prévention d'intrusion doivent être réparties sur le réseau. Cisco propose soit d'ajouter des équipements de type ASA (« Adaptive Security Appliance »), remplaçant du PIX bien connu sur le marché de la sécurité), soit d'intégrer ces fonctionnalités dans les routeurs à intégration de services (ISR) ou dans les commutateurs. En ce qui concerne la fonction de pare-feu hébergée par l'ASA ou les ISR, elle supporte :

- L'inspection des protocoles de signalisation : SIP, H.323 et MGCP
- L'écoulement du trafic inspecté sans ralentissement
- La qualité de service (QoS)
- La mise en œuvre d'un système redondant

3.1.2 Gestion de l'accès à l'infrastructure

Nous cherchons ici a construire une infrastructure qui permet d'assurer une séparation des flux tout en mutualisant cette dernière.

L'isolation des flux voix et données sur la même infrastructure grâce aux VLANs (réseaux locaux) ou aux technologies de virtualisation de l'infrastructure de type VRF (réseaux locaux et étendus).

Nous apportons donc le support du Vlan Voix avec plusieurs mécanismes de contrôle d'accès :

- Les protocoles LLDP-MED et CDP permettent de réaliser l'auto-configuration mais également de contrôler l'entrée d'un périphérique dans le Vlan Voix, ainsi le commutateur n'autorisera l'entrée dans le Vlan Voix qu'à condition qu'un terminal voix de type « IP Phone » soit reconnu sur le port.
- La gestion d'accès au réseau par des technologies d'authentification répondant au standard IEEE 802.1x, à la fois pour les téléphones mais aussi pour les postes informatiques connectés sur ces téléphones (qui hébergent un micro-commutateur). Les commutateurs Ethernet supportent la technologie « MDA » Multi Domain Authentication » pour permettre une gestion indépendante de contrôle d'accès au Vlan Voix et Données. (basé sur 802.1X, identification par adresse MAC, …)
  A noter dans ce chapitre que les Téléphones IP supportent la fonction EAPOL Logoff qui évite à un PC qui vient se connecter derrière un téléphone, de bénéficier de la connexion ouverte par le PC précédemment connecté et déconnecté de manière « brutale ». Le déploiement des UC ne remet donc pas en cause les choix de stratégie de sécurité de l'entreprise.

Cette isolation ne peut être totale, en effet certains flux média (Voix et Vidéo) doivent pouvoir transiter entre les segments voix et données. Des fonctions de type TRP (« Trusted Relay Point ») ou Phone Proxy dans l'ASA permettent de terminer, de manière transparente, les flux voix et vidéo provenant par exemple des téléphones logiciels sur PC appartenant au segment « données » et de les relayer vers les Téléphones IP qui appartiennent au segment « voix », et réciproquement.

3.1.3 Fonction dans les commutateurs

La mise en place sur les commutateurs de mécanismes permettant de parer des attaques de type :

- Saturation de la table d'adresses MAC d'un commutateur visant à le transformer en un simple répéteur (« hub ») de façon à récupérer des flux sur des interfaces où ils ne sont théoriquement pas attendus. Appelée « MAC flooding », cette attaque est parée par l'activation de la fonctionnalité de « port security ».
- Ecoute et capture de trafic basés sur le vol d'adresses IP obtenues par émission de trames GARP (« gratuitous ARP »). Appelées « ARP spoofing », ces attaques sont contrées par deux techniques au choix :
- L'activation de la fonction DAI (Dynamic ARP Inspection) sur les commutateurs
- L'activation de rejet des trames GARP sur les téléphones
- Déni de service sur les serveurs DHCP soit par introduction (parfois involontaire…) d'un second serveur DHCP dans le réseau ou par saturation des plages d'adresses par inondation de requêtes factices. On se protège contre ces attaques grâce à deux techniques au choix :
    - Activation de la fonction « DHCP snooping » sur les commutateurs
    - Limitation (« rate limiting ») du nombre de requêtes par seconde émises vers un port du commutateur
- Fonction de type « VLAN Access-lists » qui permet d'interdire plein de flux autre que le RTP entre les IP Phones, diminuer les risques d'attaque au sein des Vlans Voix.
- Fonction de renforcement d'accès au réseau : Support de 802.1X sur le Vlan Voix ou Données
- Support des Vlans et du « Multi Domain Authentication » 802.1X permettant de gérer indépendamment une politique d'accès au Vlan Voix et Données.
- -Port Security permettant de limiter le nombre d'adresses MAC par port détectées.

Tous les commutateurs CISCO supportent le cumul de ces fonctionnalités simultanément.

3.1.4 Le réseau sans fils « Wifi »

La mobilité intra-entreprise autour du WiFi doit également être prise en compte. Si la securité proposée dans ce cadre (authentification forte IEEE 802.1x / EAP et chiffrement TKIP – WPA – ou AES – WPA2 - conformes à la norme IEEE 802.11i) est utilisée par nos clients pour les postes de travail informatiques, elle est applicable et doit aussi être mise en oeuvre pour les Communications Unifiées.

Il est fortement recommandé de choisir une infrastructure et des terminaux qui supportent les fonctionnalités suivantes afin de ne pas diminuer la sécurité globale

- Choisir une méthode d'authentification de chaque utilisateur, et ce par session

- Ne pas déployer WPA-PSK plutôt utilisé dans un environnement personnel.

Réauthentification rapide lors de roaming entre bornes. Pour cela, nous apportons également une solution de « Fast Secure Roaming » en attendant l'intégration de 802.11r fast secure roaming à une norme dite « Voice Enterprise » de la Wifi Alliance.

- Management Frame Protection afin d'éviter l'envoi d'éventuelles trames de désassociassions provoquant un déni de services.

3.1.5 Les fonctions dans les routeurs multi-services Voix/Vidéo

Les routeurs ISR sont utilisés pour les fonctions suivantes dans les UC :

- Passerelles Voix
- Secours SRST sur site distant
- Fonctionnalités UC de type : messagerie, serveur de Fax, …

Les fonctionnalités suivantes sont disponibles et recommandés

- Les fonctionnalités d'IOS Firewall disponibles sur les routeurs ISR sont recommandées lors du déploiement de ces routeurs multiservices afin d'améliorer la disponibilité de la solution en évitant des dénis de service.
- Fonction IDS/IPS locale au routeur
- Fonction « Trusted Relay Point » : abordé dans le chapitre segmentation

3.2 Clients

3.2.1 Les téléphones

Les images logicielles opérationnelles des téléphones, ainsi que les fichiers de configuration téléchargés sur les terminaux sont signés, et les fichiers de configuration sont chiffrés pour éviter toute attaque en déni de service.

Les terminaux téléphoniques supportent l'authentification conforme au standard IEEE 802.1x, permettant de contrôler leur accès au réseau local, aussi bien que l'accès des postes informatiques connectés derrière eux via le micro-commutateur, ceci dans les mêmes conditions de sécurité que si le poste informatique était connecté directement sur le port Ethernet du commutateur d'infrastructure. A noter dans ce chapitre que les Téléphones IP supportent la fonction EAPOL Logoff qui évite à un PC qui vient se connecter derrière un téléphone, de bénéficier de la connexion ouverte par le PC précédemment connecté et déconnecté de manière « brutale ».

Les téléphones supportent également nativement les fonctionnalités suivantes :

- Client 802.1x pour accéder au Vlan Voix
- Support du 802.1x avec fonction EAP-LOGOFF pour assurer déconnexion du poste de travail
- Renforcement de la sécurité en désactivant des services
- Désactivation des gratuitous ARP pour éviter des attaques de type « Man in the Middle ».

3.2.2 Les postes informatiques

Les communications unifiées et la collaboration impliquent de plus en plus les postes de travail informatique comme composante client. Ces derniers bénéficient des services suivants :

- des outils d'analyse comportementale, comme CSA (Cisco Security Agent), permettant de renforcer la sécurité du système d'exploitation
- des outils comme CCAA (Cisco Clean Access Agent), permettant de vérifier la posture du poste de travail avant de l'accepter sur le réseau.
- -Client 802.1x pour accéder au Vlan Data
- -Accès distants par Tunnel SSL, IPSEC ou par chiffrement signalisation+média
- -Support de NAC pour vérifier la posture du poste de travail

3.2.3 Fonctionnalités communes à tous les terminaux

Les téléphones et les serveurs applicatifs supportent nativement le chiffrement et l'authentification des flux de signalisation (SIP/TLS) grâce au serveur de communications CUCM.
Le chiffrement des communications(SRTP) est supporté par les passerelles voix, par les téléphones ainsi que par les serveurs applicatifs afin de garantir la confidentialité des données. Cette fonctionnalité est offerte pour les appels internes, externes et les conférences et est mis en œuvre par simple activation logicielle sans surcoût.

Il est intéressant de noter aussi que ces flux chiffrés peuvent traverser les pare-feu grâce à l'utilisation de la fonction ASA TLS Proxy. Dans ce mode de fonctionnement, l'ASA est intégré dans le processus de distribution de clé de la plateforme de traitement d'appel (CUCM), (intégration sans laquelle l'analyse des flux chiffrés est impossible) et s'insère dans le flux sécurisé. Ainsi le flux chiffré est traduit en clair dans l'ASA pour analyse protocolaire, puis est rechiffré pour reprendre son chemin sur le réseau.

3.3 Serveurs applicatifs

3.3.1 Généralités

- OS Durci :
  Les systèmes d'exploitation sur base Linux distribués par Cisco pour supporter les plateformes de traitement d'appel (et les applications de Communications Unifiées en général) sont « durcis » pour augmenter leur résistance aux attaques (désactivation des services et fermeture des ports réseau non indispensables au bon fonctionnement).Les accès à l'OS sont également restreints afin de réduire les moyens d'attaque.

- CSA :
  Quel que soit le système d'exploitation utilisé (base Linux en mode « appliance » ou base Microsoft Windows Server), Cisco fournit gratuitement le client Cisco

Security Agent (CSA) d'analyse comportementale. De type « Host IDS », CSA permet de renforcer la sécurité du système d'exploitation par :

- Détection et protection contre les tentatives d'intrusion ou d'installation de logiciel malicieux.
- Protection contre les débordements de mémoire tampon (« buffer overflow »)
- Protection contre les vers (« worms ») réseau
- Protection du serveur Web d'administration
- Protection des fichiers système et de la base de registre

- Intégration dans la PKI de l'entreprise :

Les différents certificats utilisés par les serveurs applicatifs et les équipements réseaux peuvent être signés localement ou dépendre de la PKI de l'entreprise.

3.3.2 Serveurs de traitement des communications (CUCM)

Les serveurs de traitement des communications (CUCM) offrent une panoplie de services permettant de déployer un environnement de communications unifiées sécurisé. Il fournit :

- Chiffrement et authentification de la signalisation & CTI (SIP/TLS ou IPSEC).
- Distribution dynamique des clés de chiffrement et authentification pour que les terminaux et les serveurs puissent générer un flux Média chiffré (SRTP)
- Intégration dans la PKI de l'entreprise avec des fonctionnalités d'automatisation de distribution des certificats aux terminaux.
- Mécanismes de classes de restrictions d'appels (voix/vidéo) permettant d'éviter les usages abusifs du système de communications.
- Administration multi-niveaux et délégation avec gestion des droits et stockage des mots de passe avec mécanismes de sécurité forts.
- Télédistribution des mises à jour de microcodes signées et chiffrées
- Télédistribution des fichiers de configuration signés et chiffrés
- -Administration sécurisée : SSH / SFTP / SNMPv3 / HTTPS

Vos responsables sécurité ont déjà amorcé une réflexion sur la protection des serveurs du Système d'Information vis a vis des utilisateurs internes. Il est également recommandé de placer les serveurs de traitement d'appel, comme d'ailleurs les autres serveurs applicatifs du réseau de Communications Unifiées, en salle informatique derrière l'infrastructure de sécurité mutualisée.

Les serveurs de traitement d'appel Cisco (Cisco Unified Communications Manager – CUCM) formant des grappes (ou « clusters ») peuvent être répartis sur plusieurs salles informatiques, apportant d'une part la redondance et améliorant d'autre part la sécurité en rendant plus difficile une attaque ciblée de type DoS.

3.3.3 Serveurs applicatifs tiers

Les autres serveurs applicatifs (SVI, Messagerie, …) fournis par Cisco dans le cadre de son offre de communications unifiées, fournissent les services suivants afin de garantir la meilleure sécurité du système :

- Chiffrement et authentification de la signalisation (SIP/TLS ou IPSEC)
- Chiffrement et authentification du flux Média (SRTP)
- Chiffrement pendant le stockage (messagerie Unifiée Unity)
- Conservation des messages vocaux dans l'entreprise
- OS Renforcé
- Logiciel d'analyse comportementale (CSA)
- Administration multi-niveaux

3.3.4 Cas de la messagerie

La sécurité également se prolonge dans le comportement de l'application elle-même. La messagerie permet par exemple de chiffrer le message audio stocké dans le serveur de messagerie électronique d'entreprise (pour de la messagerie unifiée) ou sur le serveur de messagerie vocale (pour de la messagerie vocale ou intégrée).
Seul le destinataire du message vocal est habilité à l'écouter. Il est donc déchiffré à la volée par le serveur (cas de l'écoute par téléphone) ou par le client (cas de l'écoute depuis l'interface Web avec un plugin téléchargé localement) ou grâce à un plugin téléchargé dans le client de messagerie électronique (par exemple Cisco View Mail pour Outlook).

La notion de message audio privé permet au système d'interdire son transfert vers l'extérieur de l'entreprise pour éviter les fuites d'informations.

3.4 Confidentialité des communications

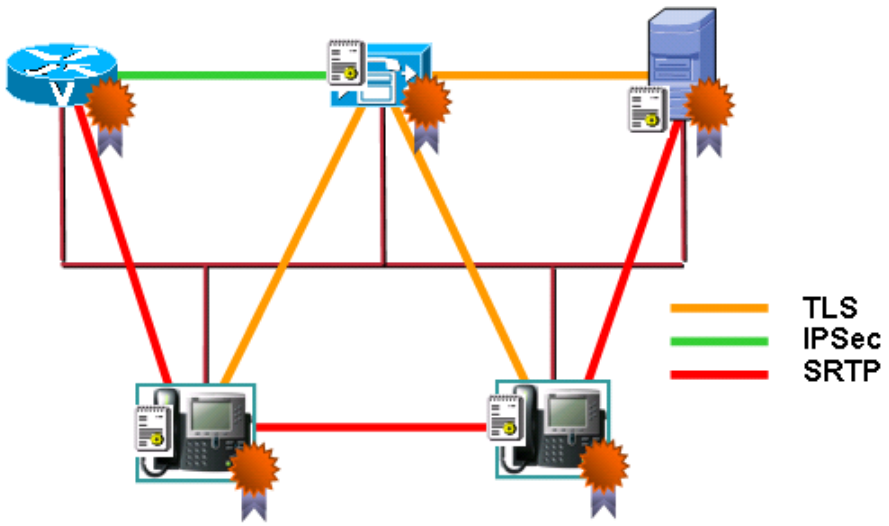

Figure 3 L'authentification et le chiffrement des communications
[2]

Nativement et avec un impact très faible (inférieure à 10%) sur les performances du CUCM, le chiffrement et authentification de la signalisation et du média peuvent être activés.
Les appels internes entre téléphones et téléphones logiciels, les conférences mais aussi les appels externes vers le RTP au travers des passerelles ou d'un SBC SIP (Session Border Controller) peuvent être authentifiés et chiffrés.

Les certificats utilisés pour ces échanges peuvent avoir été signés par CISCO en usine ou bien être intégrés à la PKI de l'entreprise par l'utilisation d'une fonction de proxy de certification sur le CUCM.

Le CUCM a pour but de gérer :

- L'authentification des terminaux qui s'enregistrent
- Le chiffrement de la signalisation vers les terminaux
- Le chiffrement de la signalisation vers les passerelles et vers les ressources de conférence
- Le chiffrement de la signalisation vers les serveurs applicatifs
- La distribution dynamique des clés a chaque appel pour chiffrer le flux média vers les terminaux, les passerelles, les serveurs applicatifs et les ressources de conférences.
- La génération des certifications avec une fonction de « Proxy » à destination des terminaux
- La maintenance des certificats dans les terminaux (distribution, mise à jour, suppression, …)
- La gestion et la distribution d'une « CTL », liste de confiance de certificats pour les terminaux, garantissant que la communication est autorisée à destination d'un équipement reconnu.

Deux technologies sont mises en œuvre pour ce faire :

- IPSEC pour le chiffrement et l'authentification à destination des terminaux H323
- Une technlogie autour de TLS pour SIP, SCCP et les protocoles CTI

Le chiffrement de la signalisation et des communications entraine par défaut l'impossibilité pour un pare-feu de continuer son rôle d'inspection applicative. Cisco répond à ce problème en fournissant un module dit « Proxy TLS » qui est décrit plus loin dans ce document.

3.5 Gestion des mises à jours et alertes de sécurité

Pour préserver cette résistance accrue, leur mise à jour ne se fait que par application de « patches » et « hot fix » préalablement testés par Cisco et distribués par le canal du site Web de Cisco, sur lequel vous pouvez vous abonner de façon à être notifié par e-Mail de l'apparition d'un nouveau correctif :

- **Cisco CallManager Notification Tool:** Notifications automatique relatives aux produits voix Cisco que vous sélectionnez : http://www.cisco.com/pcgi-bin/Software/Newsbuilder/Builder/VOICE.cgi

- **Cisco PSIRT Advisory Notification Tool**: Notification automatique de tous les Cisco Security Advisories publiés par le Cisco Product Security Incident Response Team (PSIRT). Les Security Advisories, qui décrivent les problèmes de sécurité concernant les produits Cisco, fournissent l'ensemble des actions requises pour réparer ces produits :

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html - SecurityInfo

Il est également recommandé, comme expliqué plus loin que les équipements de communication unifiée soient protégées par des fonctionnalités d'IDS/IPS afin de minimiser les impacts d'un éventuel problème de sécurité. Puisque sans qu'une mise à jour sur un serveur incriminé soit nécessaire, la fonction d'IDS/IPS pourra bloquer la tentative d'attaque.

4 Sécurité entre zones internes

4.1 Définition

Un des principaux challenges pour les responsables de la sécurité c'est de pouvoir autoriser les communications unifiées entre le mode de la téléphonie et du poste de travail tout en garantissant des échanges sécurisés entre ces domaines de confiances.

4.1.1 La segmentation voix/données

Le service de segmentation et virtualisation a commencé dés les premiers déploiements de ToIP grâce à la notion de Vlan Voix séparé.
Il s'étend aujourd'hui au delà du domaine Ethernet afin de prolonger cette segmentation du réseau dans tout ou partie de l'entreprise.

L'isolation sur le réseau local se réalise grâce au Vlan voix. Son extension sur un réseau de Campus de niveau 3 peut être réalisé grâce à la technologie de VRF.
La notion de VRF présente sur les équipements de type routeur ou commutateur permet de conserver l'étanchéité du flux Voix en traversant une infrastructure de niveau 3. Ainsi étendu, le nombre de points de passage entre les domaines Voix et Data peut être réduit afin notamment de mutualiser les équipements permettant de gérer la sécurité notamment des routeurs filtrants, des pare-feu ou sondes IPS/IDS.

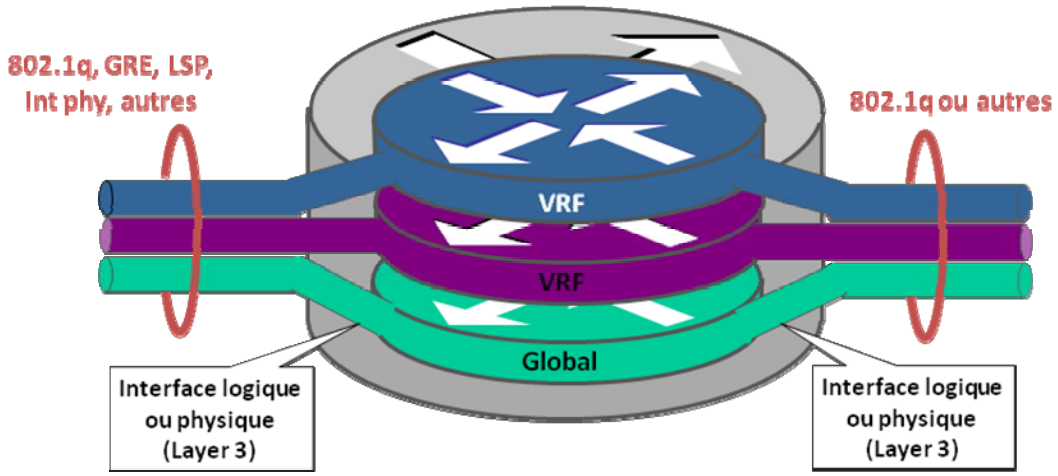

Figure 4 La notion de VRF

Ainsi une même infrastructure véhicule de manière étanche les flux par profil ou par type dans l'entreprise.

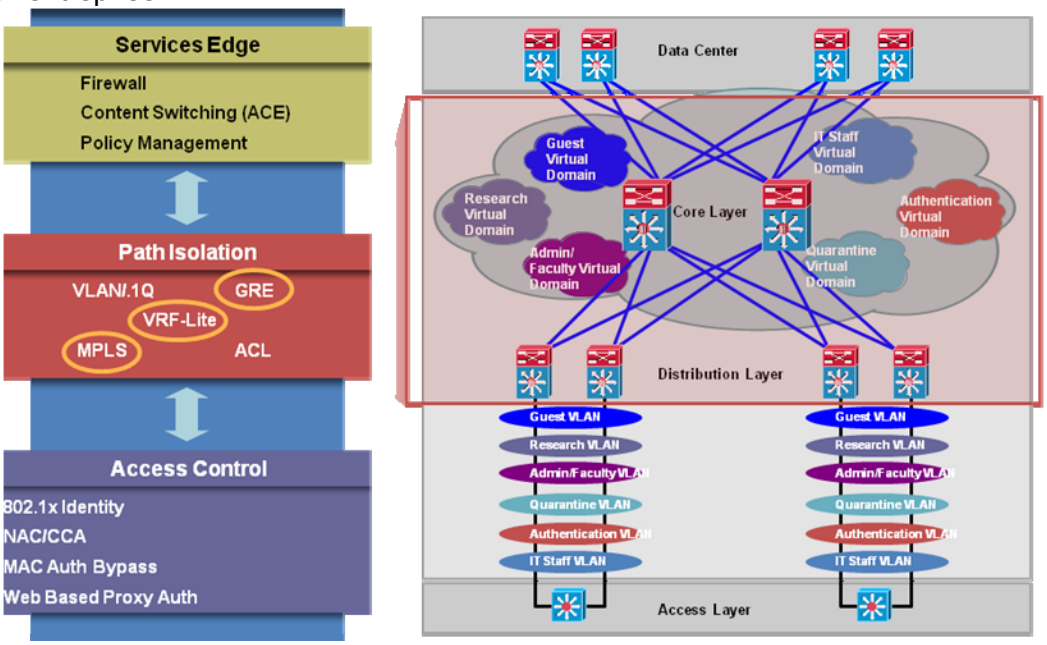

Figure 5 L'extension de la segmentation par les VRF

Plusieurs technologies permettent d'étendre cette segmentation au delà du réseau local pour par exemple la conserver entre sites distants et le site principal.

- Utilisation des VRFs de bout en bout par un mécanisme de type VRF-Lite (utilisation d'un Vlan par VRF et par lien routé)
- Aboutement des VRFs sur différents VPN/MPLS privés ou opérateurs
- Aboutement des VRFs sur tunnels GRE ou mGREs

La encore, cette isolation permet de gérer de manière centralisée des points de passage entre les zone afin d'en garantir la meilleure sécurité et d'en réduire la complexité.

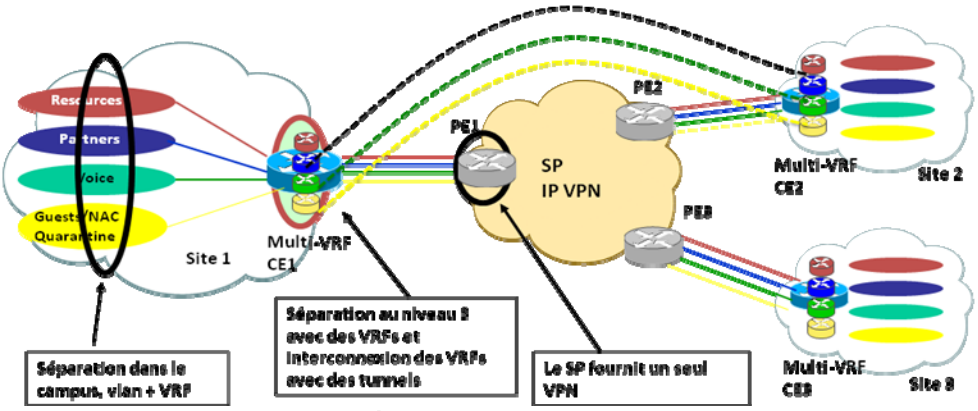

Figure 6 Extension d'une VRF au delà du Campus

4.1.2 Identification des zones

Cela passe généralement par une phase initiale qui consiste à définir les différents domaines de confiance. On retrouve ainsi une mise en place de segmentation sous forme de vlans différents, voir de VRF avec par exemple les domaines suivants :

- Services d'appels (CUCM)
- Applications unifiées et applications tierces (Unity, enregistrement des appels, Facturation…)
- Supervision
- Réseaux utilisateurs voix (téléphones)
- Réseaux utilisateurs data (PCs)
- Eventuellement une zone pour les passerelles
- Réseau VoiP externe (opérateurs ou réseau voix tiers ou autres entreprises)

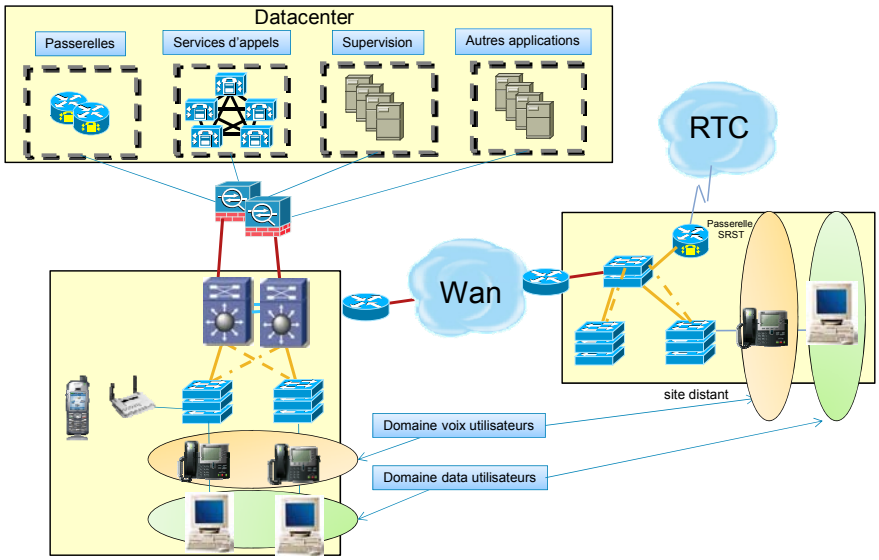

Figure 7 Exemple de définition des domaines de confiances

4.1.3 Les flux entre domaines de confiance

La phase suivante s'avère souvent plus complexe car elle consiste à définir une matrice des flux afin de bien comprendre quels sont les protocoles que l'on devra inspecter entre les domaines de confiances.

Cette matrice devra prendre en compte les spécificités des protocoles utilisées dans le cadre des communications unifiées. A savoir de la signalisation basée essentiellement sur des ports TCP fixes qui aura pour rôle d'autoriser les communications (RTP) basés sur de l'UDP avec au passage une négociation dynamique des ports UDP.

	Services d'appels	Passerelles	Applications tierces	Supervision	Vlans voix	Data users
Services d'appels	Informix (intra-cluster), H323, SIP (inter-clusters)	MGCP, H323	CTI, SIP, SCCP	SNMP, HTTPS, SCP, SFTP, SSH	SCCP, SIP, TFTP	SCCP, SIP, CTI-QBE, JTAPI, etc ….
Passerelles	MGCP, H323	RTP, SRTP, SIP	Dépend des applications	SSH, SCP, HTTPS	RTP, SRTP	
Applications tierces	CTI, SIP, SCCP	Dépend des applications	Dépend des applications	SNMP, HTTPS, SCP, SFTP, SSH	DHCP, HTTP, DNS	Dépend des applications
Supervision	SNMP, HTTPS, SCP, SFTP, SSH	SSH, SCP, HTTPS	SNMP, HTTPS, SCP, SFTP, SSH	X	HTTP, ICMP	X
Vlans voix	SCCP, SIP, TFTP	RTP, SRTP	DHCP, HTTP, DNS	HTTP, ICMP	RTP, SRTP	RTP, SRTP
Data users	SCCP, SIP, CTI-QBE, JTAPI, etc …	RTP, SRTP	Dépend des applications	X	RTP, SRTP	RTP, SRTP

Figure 8 Exemple de matrice des communications entre domaines

4.2 Site principal : Mécanismes de sécurité entre zones de confiance

4.2.1 Sécurité par filtrage statique entre domaines de confiance

Il est possible de positionner des listes de contrôle d'accès statiques de niveau 3 ou 4 sur les commutateurs niveau 3 ou sur les routeurs entre les zones. Il est cependant impossible d'assurer une sécurité forte au cause de l'aspect dynamique des protocoles mis en jeu (exemple : négociation de ports dynamiques RTP).

4.2.2 Firewall ASA avec inspection applicative ou FWSM

C'est dans cet environnement complexe que l'on doit positionner les fonctions de sécurité avec comme critères pour la sélection d'un Firewall :

- Le bon dimensionnement de l'équipement pour pouvoir tenir la charge en termes de débit, de connexions par secondes et de sessions simultanées.
- La prise en compte de la QoS pour les flux temps réels

- Sa capacité à interpréter et à filtrer les signalisations utilisées (SIP, H323, MGCP, SCCP ….)
- Sa capacité à offrir des services de haute disponibilité (Failover)

Les flux voix et vidéo bénéficient d'un traitement poussé en matière de protection au sein des plateformes ASA, avec notamment le support de :

- Ouverture Dynamique des ports pour les applications voix et vidéo
- Vérification de la conformité au standard pour les protocoles SIP, SCCP, H.323, MGCP
- Inspection applicative et contrôle des messages SIP envoyés aux CUCMs
- Qos : LLQ et Rate limiting (gestion de files d'attentes prioritaires pour le trafic temps réel)
- Filtrage avancé des listes blanches / Noir, numéros appelant et appelés, URI SIP
- Autorisation uniquement des téléphones enregistrés à passer des appels
- Inspection des flux encryptés (voir paragraphe suivant)

4.2.1 La gestion de l'inspection applicative des flux signalisation et média chiffrées

Dans le cadre d'une communication entre deux équipements voix sur IP, la partie confidentialité avec l'encryption de la signalisation et des flux RTP (SRTP) est souvent un challenge pour les équipements de filtrage. Disponible depuis plus d'un an l'ASA offre une fonction unique sur le marché : TLS-Proxy, il va ainsi décrypter la signalisation à la volée que ce soit du SIP ou du SCCP.

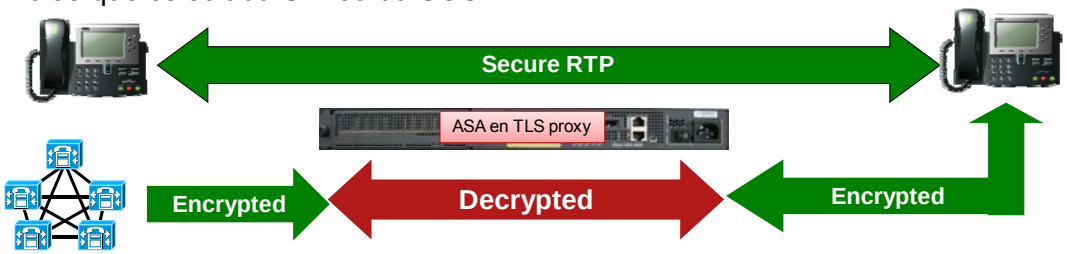

Figure 9 TLS-Proxy : Filtrage de la voix encryptée

Cela implique une très forte intégration entre l'ASA et les CUCM avec entre autre une intégration dans la CTL (Certificate Trusted List) de l'ASA.
L'ASA ouvrira dynamiquement les ports RTP en fonction de ce qui sera négocié par la signalisation, cela évite ainsi d'autoriser statiquement un range de port RTP et donc de laisser passer les potentielles failles de sécurités.
Cette fonction permettra aussi d'appliquer des fonctions de translation (NAT) et bien sur une analyse et un filtrage approfondie des messages de la signalisation.
Dans ce domaine également l'ASA offre des fonctions avancées avec des moteurs d'inspections très poussé sur SCCP et SIP ainsi que pour H323v1 à v4 et MGCP.

Avec ses fonctions uniques dans le domaine des communications unifiées la gamme ASA renforce considérablement la sécurité des échanges entre les différents domaines de confiances. Ils permettent ainsi la mise en place de ces nouveaux outils de communications dans les entreprises sans craintes pour l'intégrité des systèmes.

4.2.2 Fonction d'IDS/IPS

Il est également recommandé d'ajouter des fonctions de type IPS avec signature pour lutter contre d'éventuelles vulnérabilités des protocoles ou des applications.

Toute attaque connue au niveau de l'équipement IDS sera alors stoppée par le moteur d'inspection de l'IDS.

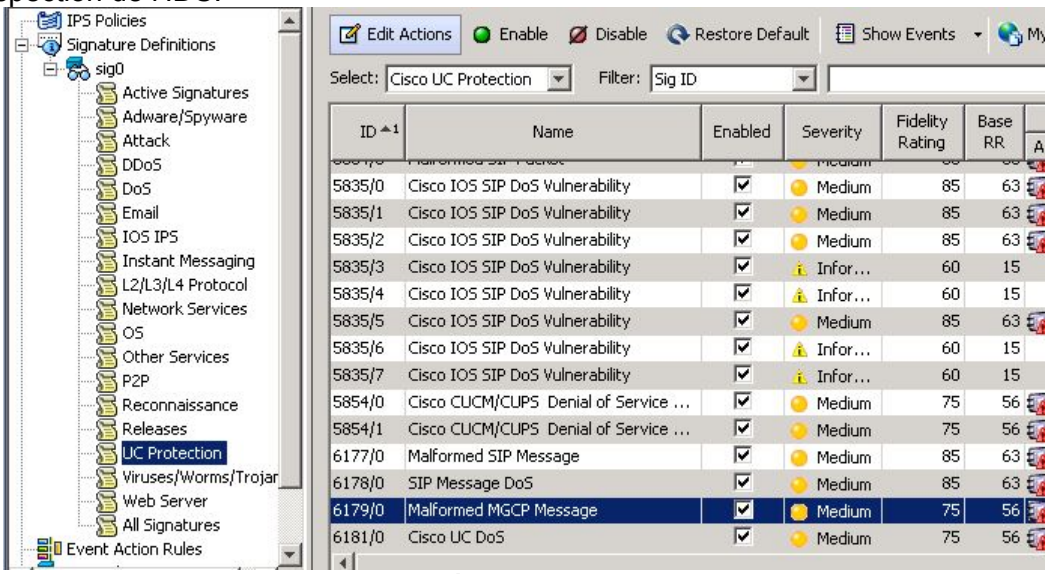

Figure 10 Quelques signatures IPS protégeant les UC dans l'ASA

4.2.3 Fonction de type « ASA Phone Proxy »

L'ASA phone proxy offre également la possibilité d'une segmentation entre les vlans data et les vlans voix en assurant une fonction proxy pour les soft phones (Cisco IP Communicator).
Cela répond à une demande récurrente des entreprises d'assurer les communications entre un soft phone installé sur les PC des utilisateurs et les téléphones IP tout en garantissant qu'une vulnérabilité du monde PC ne viendra pas contaminer la téléphonie.

Cette fonction permet aussi de déployer des IP Phones ou des téléphones logiciels sur une zone de défiance (Vlan Guest par exemple).

Pour réaliser cette fonction, les softphones devront s'authentifier sur l'ASA en TLS avant de pouvoir communiquer avec de domaine voix. L'ASA en profitera au passage assurer la fonction proxy et l'inspection de la signalisation.

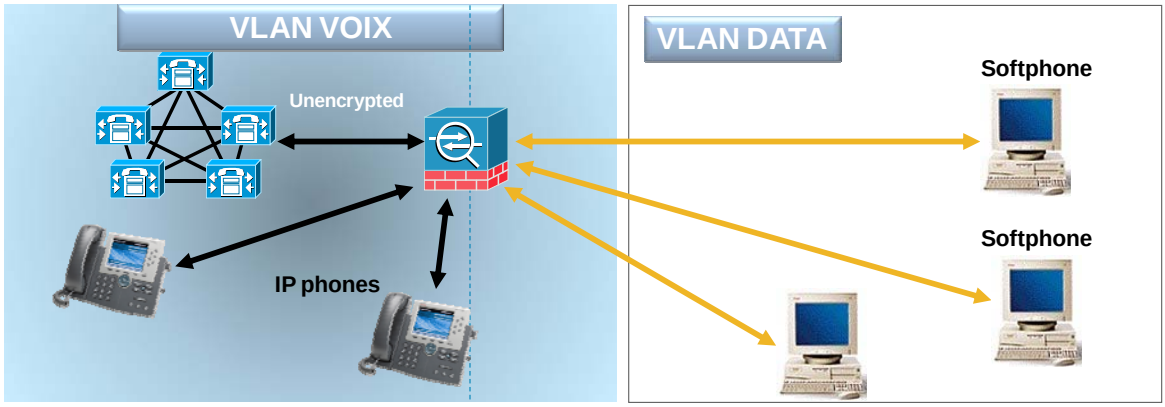

Figure 11 Phone proxy : Segmentation des domaines Data et voix

4.2.4 Fonction de type « IOS TRP »

La fonction d'IOS TRP (Trusted Relay Point) permet au CUCM de manière transparente de terminer les flux Média (Voix et Vidéo) sur un routeur ISR plutôt que de les faire transiter nativement entre les équipements.
Cette fonction permet de grandement simplifier la sécurité entre les segments voix et data sur le réseau puisque seul l'équipement ISR choisi ne doit être autorisé à transiter entre ces deux segments.
L'intelligence du CUCM permet de choisir le meilleur ISR pour réaliser ce service en fonction de la charge, la disponibilité et la localisation des clients.

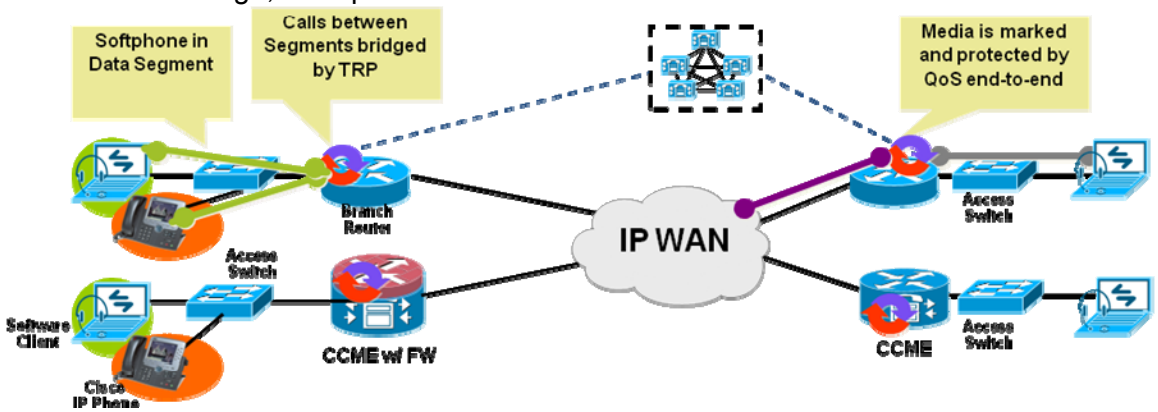

Figure 12 IOS TRP : Segmentation des domaines Data et voix

5 Sécurité vis-à-vis de l'extérieur et de la mobilité

En plus des organes de sécurité traditionnels que Cisco propose pour connecter le réseau interne de l'entreprise au monde extérieur (Internet ou réseau d'un partenaire), Cisco propose également des solutions dites de « Session Border Controller » (SBC) qui permettent de relayer les flux voix et vidéo du réseau IP interne de l'entreprise vers l'extérieur. Ces solutions sont notamment proposées pour véhiculer des flux IP de manière sécurisée vers des opérateurs de téléphonie IP, depuis des clients distants sur Internet mais aussi entre entités d'une entreprises ou entre entreprises partenaires. Ces fonctions sont par exemple disponibles pour l'entreprise, dans la gamme des routeurs à intégration de services (ISR).

Le déploiement de terminaux (téléphones ou téléphones logiciels) distants (par exemple sur Internet) est également possible grâce à la fonctionnalité Cisco Phone Proxy intégrée dans les pare-feu Cisco ASA et qui permet :

De télécharger les images logicielles opérationnelles des téléphones, ainsi que les fichiers de configuration de manière sécurisée.
De relayer les flux de signalisation et de voix sur IP vers les téléphones distants de manière sécurisée

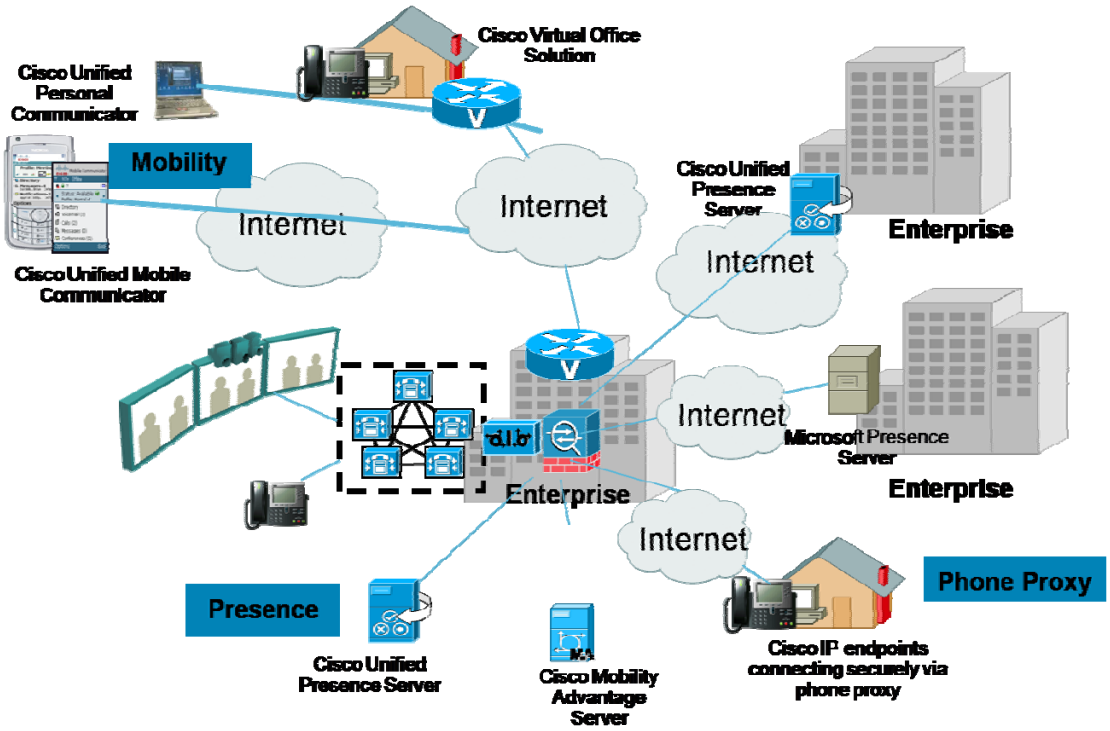

Figure 13 Les besoins de sécurité vers l'extérieur de l'entreprise

5.1 En situation de mobilité

5.1.1 Solution de Tunneling IPSEC ou SSL

Il n'est plus possible aujourd'hui de raisonner en termes de périmètre (interne, externe), chaque utilisateur pouvant être indifféremment à l'intérieur de l'entreprise puis à l'extérieur en situation de mobilité.

La mobilité des utilisateurs change l'approche sécurité dans l'entreprise puisque nous abordons la sécurité également sous l'angle :

- de la fourniture d'accès distants sécurisés au travers de technologies de tunnel IPSec ou SSL depuis tous types de terminaux

- de la protection des postes de travail des utilisateurs nomades (CSA – Cisco Security Agent, CCAA – Cisco Clean Access Agent) pour une vérification de posture de ces terminaux (mise à jour du logiciel d'exploitation ou de l'anti-virus par exemple) au moment de la connexion au réseau de l'entreprise.

5.1.2 Les fonctions de l'ASA vis-à-vis

Indépendamment des fonctions spécifiques aux communications unifiées, l'ASA supporte simultanément les fonctions suivantes :

- Pare Feu pour sécurité périmètrique
- Fonctions embarquées d'IDS/IPS
- Fonctions de filtrage d'URL et Filtrage d'emails
- Terminaison de tunnels IPSEC Site-à-site
- Terminaison de tunnels IPSEC/SSL de nomades
- ASA : « IP Phone Proxy » pour téléphones IP + CIPC distants
- ASA : Mobility Proxy » pour les terminaux « CU Mobile Communicator » distants
- ASA : Presence Proxy pour la fédération de présence

5.1.3 ASA : Mobility Proxy

L'ASA prend en compte les nomades. L'ASA permet de terminer les sessions TLS des clients unifiés dédiés aux mobiles (CUMC).
Un utilisateur peux ainsi utiliser disposer de CUMC sur son GSM (Symbian, Backberry, Windows Mobile), et à travers un réseau 3G, un Hotspot ou n'importe quel accès internet pouvoir se connecter de manière sécurisée en TLS à son entreprise.

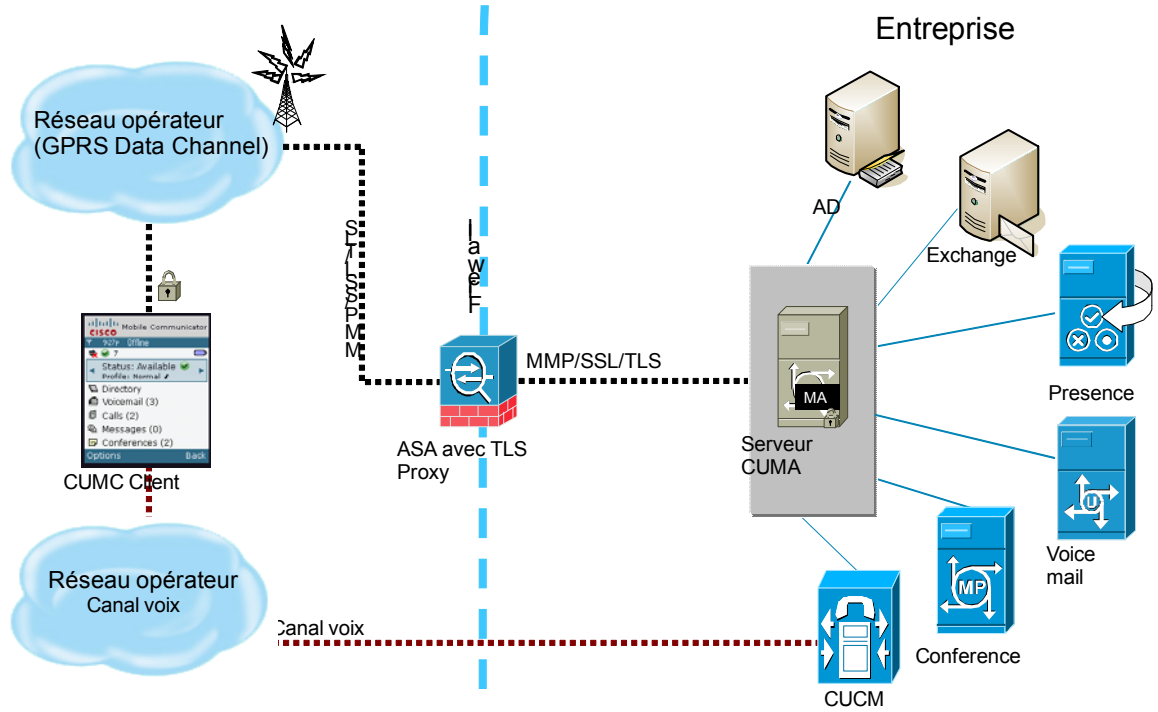

Figure 14 Mobile Proxy : Les services unifiés pour les nomades

5.1.4 ASA : Phone Proxy

Cette nouvelle fonction a pour objectif d'offrir aux entreprises la possibilité de connecter un Téléphone IP Cisco sur un réseau non sécurisé avec une liaison TLS entre le téléphone et l'ASA. L'ASA se positionne ainsi comme un point de terminaison des sessions de signalisations (SIP ou SCCP) encryptées en TLS.

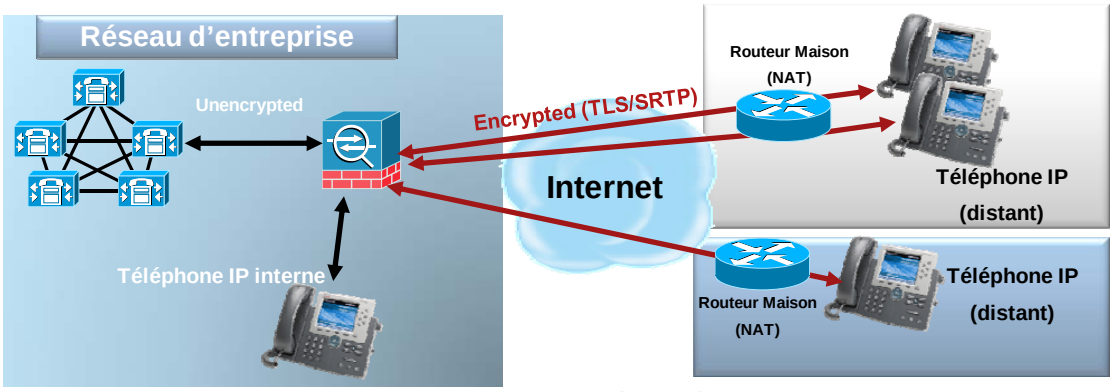

Figure 15 Phone proxy : connexions des postes sécurisés

C'est ainsi qu'une entreprise peut par exemple proposer à ses collaborateur des postes téléphoniques qu'ils pourront utiliser à leur domicile tout en garantissant la confidentialité et l'intégrité des appels via l'asa en Phone proxy. Ces postes communiqueront avec l'ASA qui se chargera des communications avec le cluster de serveurs d'appels (CUCM)

5.2 La fédération de présence grâce à l'ASA

Parmi les innovations qui ont étés introduites par cisco dans le domaine des communications unifiées il y a les informations de présences entre les téléphones IP et les clients unifiées que l'on trouve sur les PC.

Pour fédérer ces informations de présences et de messagerie instantanée, l'infrastructure Cisco s'appuie sur des clusters de serveurs CUP (Cisco unified Presence server). Ces serveurs offrent la possibilité d'interconnexion vers des domaines de présences externes que ce soit d'autres domaines Cisco CUP ou Microsoft OCS.

Que ce soit au sein d'une même entreprise ou entre entités différentes. Cette fonction garantie l'intégrité des différents domaines avec au passage l'inspections et le filtrage des informations de présence.

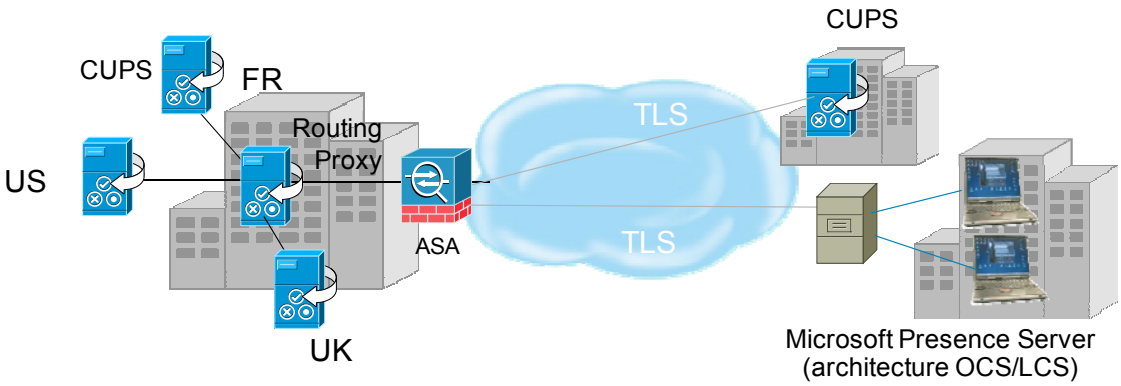

Figure 16 Présence proxy : Interconnexion des domaines de présences

5.2.1 Les fonctions de SBC : inter entreprise ou « collecte IP »

Les fonctions de SBC (session border Controller) SIP/H323 d'entreprise sont disponibles sur les plateformes ISR et se nomment « Cisco Unified Border Element ».

Cela permet de proposer des solutions d'interconnexion native en IP pour les flux Voix et Vidéo :

- A destination d'un opérateur dans le cadre de la collecte IP qui permet d'avoir un point de passage unique entre les réseaux IP de l'entreprise et de l'opérateur. Le flux de signalisation ainsi que le flux média sont relayés afin d'apporter une isolation complète
- A destination d'une autre entreprise pour une connexion B to B afin d'activer les échanges de voix et de vidéo au travers d'un réseau entre entreprise. Outre les fonctions de sécurité, le CUBE dans ce cas peut apporter le chiffrement de la signalisation et des communications si les équipements dans les entreprises ne le supportent pas.

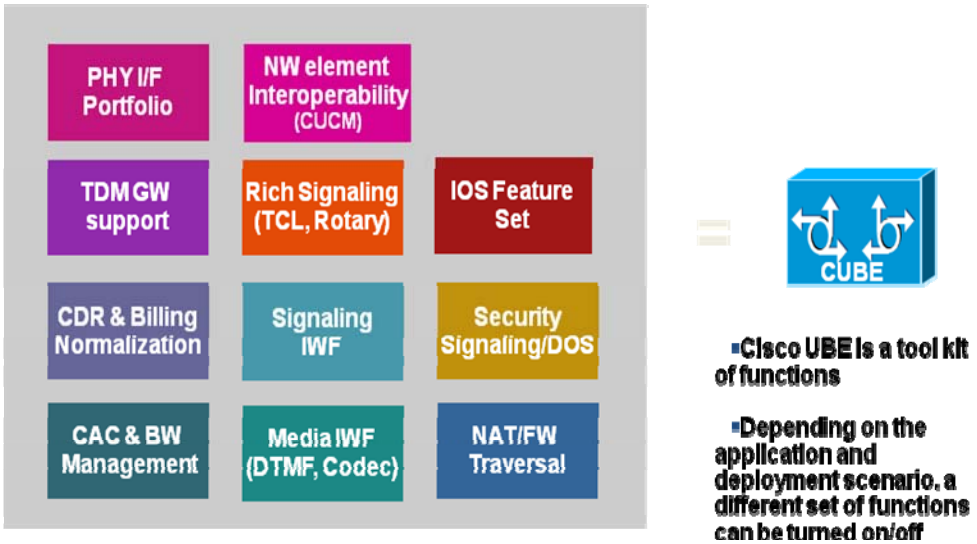

Figure 17 Les composants du SBC Cisco

Les fonctions proposées sur le SBC CUBE :

- Interopérabilité H323/SIP Le SBC permet de se connecter entre un monde SIP et un monde H323.
- Gatekeeper H323 : Fonctions en co-résidence avec des fonctions de proxy et de SBC.
- Interconnexion des appels VoIP et visioconférence en B to B
- Interconnexion des appels Telepresence
- Chiffrement et authentification de la signalisation (SIP/TLS ou IPSEC) Chiffrement et authentification du flux Média (SRTP)
- Inspection protocolaire sur règles de Pare-feu applicatif
- Récriture des paquets SIP grâce au SBC B2BUA et RTP
- Renforcement du SBC par un pare-feu (IOS Firewall) et IPS intégré à l'équipement.
- Services de transcoding de flux audio ainsi que d'adaptation DTMF entre les entités.

Il est à noter qu'une passerelle RTC peut évoluer vers une fonction de SBC CUBE sans remise en cause de l'investissement par une simple reconfiguration.

6 Conclusion

La relation étroite entre l'infrastructure, la sécurité et les services de Communications Unifiées est fondamentale et c'est ce que Cisco propose dans sa stratégie « réseau en temps que plateforme ».

La sécurité des Communications Unifiées doit faire partie intégrante de la sécurité globale de l'entreprise. Par exemple, l'activation de la sécurité des communications téléphoniques peut s'appuyer sur des certificats provenant de la PKI existant dans l'entreprise.

Cisco propose également des outils d'administration permettant d'assurer la cohérence entre tous les éléments cités plus haut et qui contribuent à la sécurité globale du réseau de l'entreprise et donc à sa disponibilité.

Il est important de noter enfin que la sécurité proposée dans le cadre des Communications Unifiées Cisco s'entend bien sur sans remise en cause du choix des protocoles de signalisation normalisés tels que H.323 et SIP, et ceci que l'infrastructure fonctionne en mode nominal ou bien en mode secours (dans lequel on utilise la fonction SRST embarquée dans les routeurs ISR à services intégrés et qui supporte toutes les fonctions de sécurité disponibles sur la plateforme CUCM opérationnelle en mode nominal).