SPIE Communications

une offre globale du conseil à l'infogérance

David COJA

Responsable du Département Sécurité
Des Systèmes d'Information

Spie Communications

Tél : 04 72 81 10 51

david.coja@spie.com

Jacques VERDIER

Chef d'Agence
Secteur Alpes-Dauphiné

Spie Communications

Tél : 04 76 33 25 54

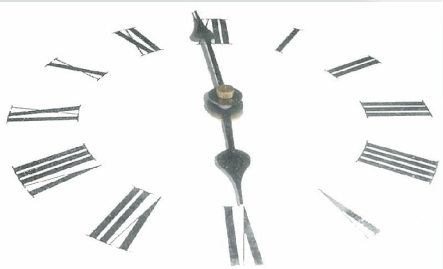
j.verdier@spie.com

Sécurité & ToIP

Réunion du CLUSIR – 09 juin 2008

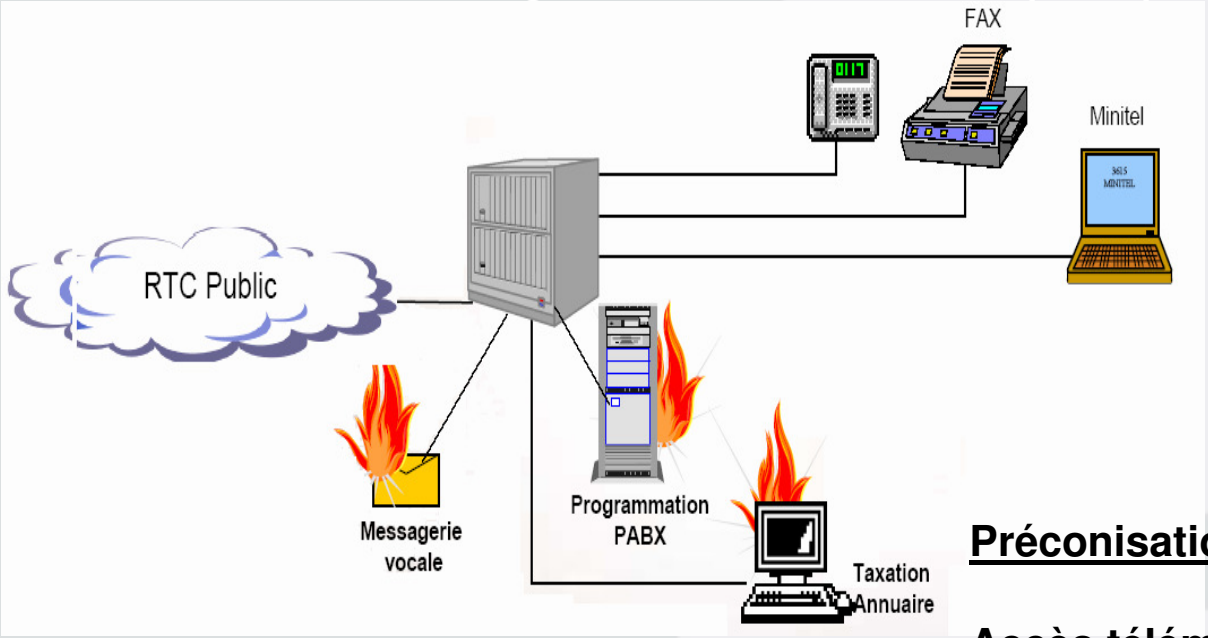
Agenda

- Quelques définitions et principes d'architectures
- Les Risques et les Vulnérabilités
- Quelques recommandations
- Récapitulatif en image
- Le Futur / Conclusion



La téléphonie, Hier

PABX : Private Automatic Branch Exchange / Autocommutateur téléphonique Privé



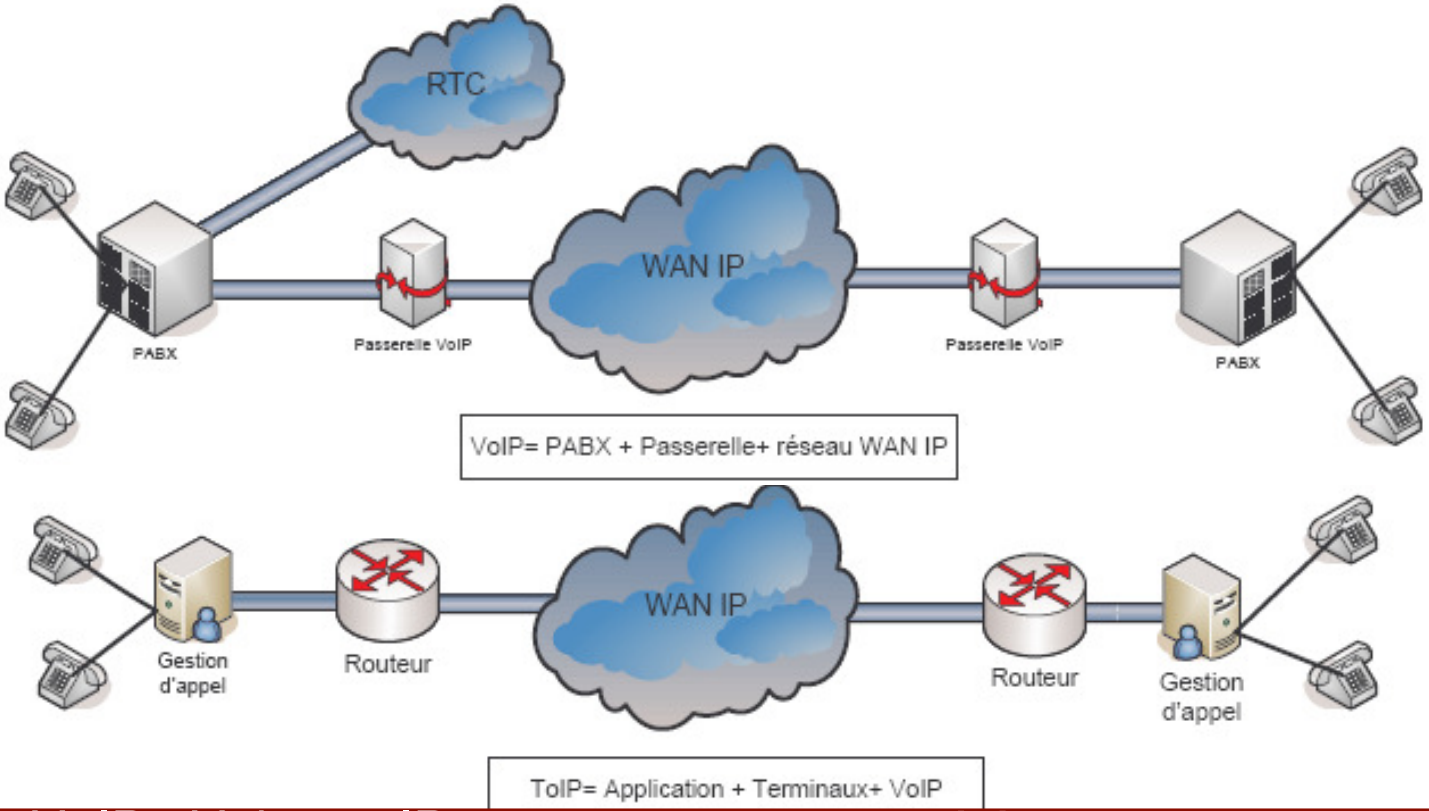
Menaces ;

Blocage de lignes / Usurpation de boites vocales
Écoutes / Modification configurations
Appels et taxation détournés / Etc..
Outils de piratage « simples »

Préconisations;

Accès télémaintenances- Modems
Messagerie vocale
Configurations : Ex fonction DISA
Taxation
Périphériques

VoIP vs ToIP



VoIP : Voix sur IP

Technologie de transport de la voix sur un réseau IP

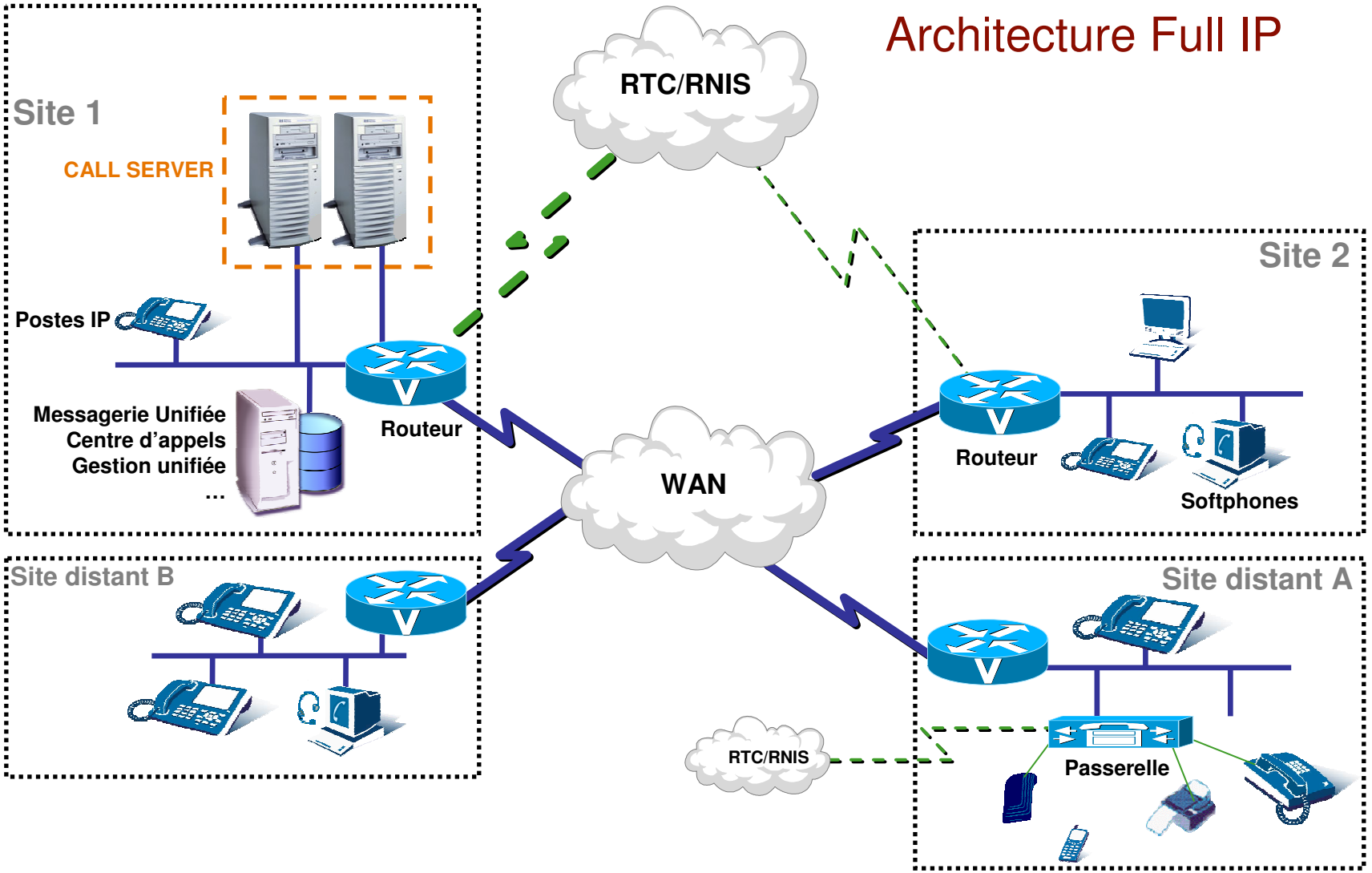
ToIP : Téléphonie sur IP

Ensemble des services de téléphonie en IP (terminaux et serveurs)

SPIE Communications

une offre globale du conseil à l'infogérance

Architecture Full IP



Les composants de la convergence

Gestion des appels

Serveur d'appels / IPBX

Terminaux

Postes IP, numériques, analogiques…

Softphones

Applications

Répondeur auto./IVR

Assistant personnel

Messagerie unifiée

Centre d'appels IP

Interfaces TAPI

Applications XML

Réseau de données avec la capacité voix

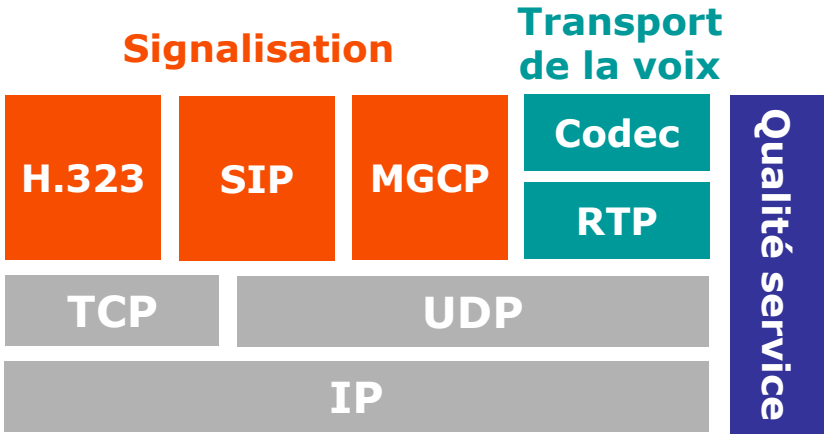
Commutateurs L2 avec QoS

Commutateurs L3 avec QoS

Routeurs

SPIE Communications

une offre globale du conseil à l'infogérance



Transport de la voix

- G.711 (sans compression)
- Compression quasi systématique pour le trafic WAN (G.729 ou G.723)

Codage	Qualité (MOS*)	Compression
G.711 / PCM	4,1	64 kbit/s
G.729 / CS-ACELP	3,92	8 kbit/s
G.723.1 / ACELP	3,65	5,3 kbit/s

* Mean Opinion Score

Signalisation

- **H.323 (ITU)**
  - Bonne réponse aux besoins télécoms et maturité
  - Protocole pénalisé par sa complexité et son manque de d'évolutivité
  - **Solution la plus supportée actuellement sur le marché**
- **SIP (IETF)**
  - Plus grande souplesse et évolutivité
  - Protocole jeune sujet à de nombreuses extensions propriétaires
  - **Fort engouement du marché**
- **MGCP/H.248 (IETF/ITU)**
  - Protocole de type maître/esclave complémentaire

  ➔**Particulièrement adapté pour les offres IP Centrex et résidentielles**

Vision et stratégie ToIP

- Le point de départ : la transition technologique IP
  - Protocole : du mode circuit au mode paquet
  - Réseau : de l'infrastructure TDM au LAN/WAN IP
  - Plateforme : du PABX dédié au PC standard
  - Interfaces : du propriétaire au standardisé
- La ToIP : une vision d'architecte
  - Séparation de la commutation et des services
  - Infrastructure voix et données commune
  - Les applications deviennent indépendantes de l'infrastructure
  - Centralisation des équipements, des données et de l'administration
  - Intégration des applications par les standards du Système d'Information

Risques

- Les risques sur les services de téléphonie
  - Disponibilité du système
    - Dénis de service
  - Confidentialité des conversations
    - Écoute téléphonique
  - Intégrité des conversations
    - Diffusion et modification de message
  - Fraude
    - Usurpation d'identité
  - Productivité individuelle
    - Spam vocal (SPIP)
  - Altération de la qualité des communications
    - Echo, coupure, hachage
- Les risques sur les services réseaux
  - Softphone
  - Messagerie unifiée, applications Voix/Data

Risques

- Les risques au niveau de l'application
  - Menaces et vulnérabilités liées à l'application
- Les risques au niveau IP
  - Interception des communications (écoute...)
  - Déni de service (avec ou sans spoofing)
  - Sur les équipements
  - Sur les flux
- Risques au niveau des protocoles
  - Surfacturation (par redirection)
  - Usurpation d'identité
  - Insertion, re-jeu,
  - Déni de service

Les vulnérabilités

- Vulnérabilité des protocoles
  - H323, SIP, …
- Vulnérabilité des systèmes
  - Call Manager (OS et menaces classiques)
  - Passerelle, SoftPhone, IP Phone
- Vulnérabilité des infrastructures
  - IP Phone (étanchéité voix/data)
  - Réseaux switchés / Pare-feu / accès Internet
- Vulnérabilité humaines
  - Organisation / formation
- Fortes contraintes de QoS
- Interactions avec le réseau Data

Risques & Vulnérabilités

Téléphonie Classique

- Équipements de piratage coûteux et difficilement accessibles
- Compétences en électronique nécessaires
- Protocoles peu enseignés, propriétaires, non documentés
- Exploitation des attaques sur place

VoIP

- Équipements de piratage accessibles à tous
  - Disponibles librement sur Internet
- Compétences d'informaticien suffisantes
- Protocoles enseignés et ouverts
- Exploitation des attaques à distance

Risques et Vulnérabilités

- Les vulnérabilités liées à la TOIP vont être issues du réseau téléphonique traditionnel, du réseau de données (IP), et des vulnérabilités propres aux spécificités des applications de téléphonie.
- La ToIP n'est pas équivalente à la téléphonie classique. La signalisation et le transport de la voix sont sur le même réseau et la notion de localisation géographique de l'appelant est donc perdue.
- Exigences câblage (cat6/7) – Appliquer 802.1&
  - ce n'est pas juste "une application en plus"
  - Application « temps réel », mobile, …
  - Exigeante (DCIP, … secours (flux, réseau, sauvegarde, ..))

Les objectifs

- Offrir la sécurité à laquelle les utilisateurs étaient habitués
  - Fiabilité du système téléphonique
  - Combien de pannes de téléphone / pannes informatique ?
  - Confidentialité des appels téléphoniques
  - Invulnérabilité du système téléphonique
    - Devenu un système susceptible d'intrusions, vers, etc
- Contraintes de la téléphonie appliquées au réseau
  - Taux d'indisponibilité téléphonie classique : 5 à 6 minutes d'interruption par an, 99,999 %
    - Disfonctionnement de la messagerie ➔ peu acceptable
    - Téléphone sonne occupé quand on veut appeler ➔ pas du tout envisageable

Qualité de service - les indicateurs

- **La qualité de la voix sur IP dépend principalement de 4 paramètres interdépendants :**
  - la latence (délai de transmission < 100ms)
  - la perte de paquets (<1%)
  - la gigue (variation du délai de transmission < 50 ms)
  - la bande passante

- **Problématique : Diffuser des Flux en Temps Réel**
  - Lors d'un Transfert de Vidéo ou de Voix seule importe la vitesse minimum garantie

    1mn à 8Mb/s ⇔ 30s à 4MB/s puis 30s à 12MB/s

    Premier cas : Ok
    Second : Le film est saccadé pendant les 30 premières Secondes

Qualité de service - les dérives

- Équipements réseaux
  - Temps de traitement des petits paquets voix → latence (ie Statefull, NAT)
- Chiffrement
  - Augmente la taille du paquet
    - La BP effective diminue
    - La gestion à travers les nœuds du réseau (routeur,FW) s'alourdit
    - AES répond au problème
  - Les moteurs de cryptographie non adaptés
    - Pas de prioritisation : les petits paquet voix attendent derrière les gros paquets Data;
    - Schéma type FIFO
    - Plus puissant et plus lourd : 3DES+SHA-1 > DES de 500 pps
  - Chiffrement et NAT incompatibles
    - @sources nattées : impossible d'authentifier l'émetteur

La sécurisation commence au niveau 1

- Câblage et LAN IEEE802.1
  - Cœur de réseau Gigabit cuivre ou fibre
  - Technologies switch 100Mb/s, câble UTP ou F2TP cat6/7
- Étiquetage des prises: Le service informatique doit savoir dans quelle pièce et sur quelle prise est chaque numéro de téléphone
  - N° de téléphone, @MAC, @IP et n° de prise Ethernet sont liés
- Si 802.1x → Capacité des postes téléphoniques de le gérer
- **Obligation** de créer des VLANs
- Intégrer la gestion de l'énergie
  - (PoE, Onduleurs, RPS sur les commutateurs qui ne peuvent délivrer de base la puissance pour alimenter un grand nombre de téléphones)

Exemple: gestion de la continuité GLOBALE

- Coupure de courant
  - Téléphone branché sur le secteur (pas PoE, pas secouru) ➔ plus de téléphone
  - Serveurs branchés sur le courant secouru mais pas le commutateur devant
- Retour du courant
  - Serveur de télé configuration des téléphones injoignable (DHCP,BOOTP pour le firmware, etc.) car commutateur pas encore redémarré
  - Les téléphones ont redémarré plus vite que le commutateur et se sont trouvés sans adresse IP, etc. et restent bloqués sur l'écran "Waiting for DHCP ..."
  - Pour une raison inconnue, une fois le serveur de télé configuration à nouveau joignable, les téléphones n'ont pas fonctionné
- → Seule solution trouvée : débrancher/rebrancher chaque téléphone un par un pour qu'ils se remettent en service

L'évolution des exigences sur le SI

- Services du réseau informatique qui deviennent des services critiques
  - DHCP
  - DNS
  - Commutateurs
  - QoS Réseau
  - WiFi / DECT
  - ...
- Mise en oeuvre de la Haute Disponibilité devenue obligatoire
  - Liaisons de secours éventuelles
  - Exploitation au quotidien
  - Évolution de la taille du réseau, du nombre d'équipements
  - Surveillance de la qualité de service
  - 24/7

Organisation

- L'organisation de l'Entreprise
  - Les organisations (conflit DSI, MG)
    - La téléphonie entre dans le giron de la Direction des Systèmes d'Information (DSI)
    - Les téléphonistes intègre la DSI
  - Compétences techniques
  - Les utilisateurs

- Extension des Politiques de sécurité
  - Adapter les méthodes
  - Adapter les outils
  - Adapter la formation et la sensibilisation

Sécurité ToIP - Principes techniques Pré-requis Sécurité

Haute disponibilité du service

- Redondance des équipements
  - Téléphonie : Serveur de contrôle et Passerelle
  - Mais aussi LAN et WAN (architecture en double étoile)
  - Avec des contraintes spécifiques (temps de convergence, distance)
- Sécurisation de l'alimentation électrique pour les sites sensibles
- Maintien de lignes analogiques en secours (appel d'urgence)
- Mesures nécessaires mais bénéficiant à l'ensemble du service data

Authentification et confidentialité

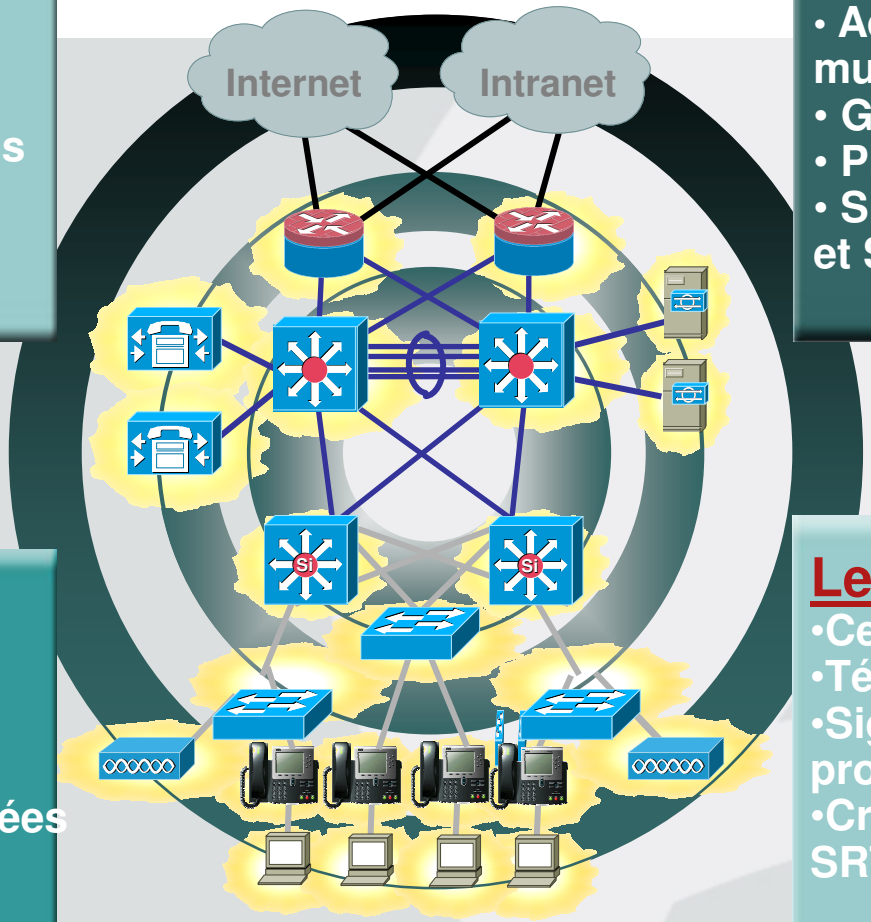
- Contrôle du téléphone IP (interdire l'accès aux équipements pirates)
- Chiffrement de la signalisation
- Chiffrement des communications (intégré au poste, IPSec, …)
- Authentification des utilisateurs

Protection face aux attaques réseau (déni de service, virus, intrusions)

- Durcissement des serveurs (OS allégé pour éviter les failles)
- Antivirus et contrôle de conformité
- Cloisonnement en zones en fonction de la criticité (Firewall, VLAN)
- Détection d'attaque (IDS, analyse de logs)
- Vulnérabilités plus importantes pour les softphones
- Sécuriser les flux d'administration
- Intégration de la téléphonie aux processus opérationnelles de gestion de la sécurité

Une stratégie globale de sécurité

Infrastructure
- Segmentation VLAN
- Protection de couche 2
- Pare-feu
- Détection des intrusions
- QoS et seuils
- VPN sécurisés
- Sécurité sans fil

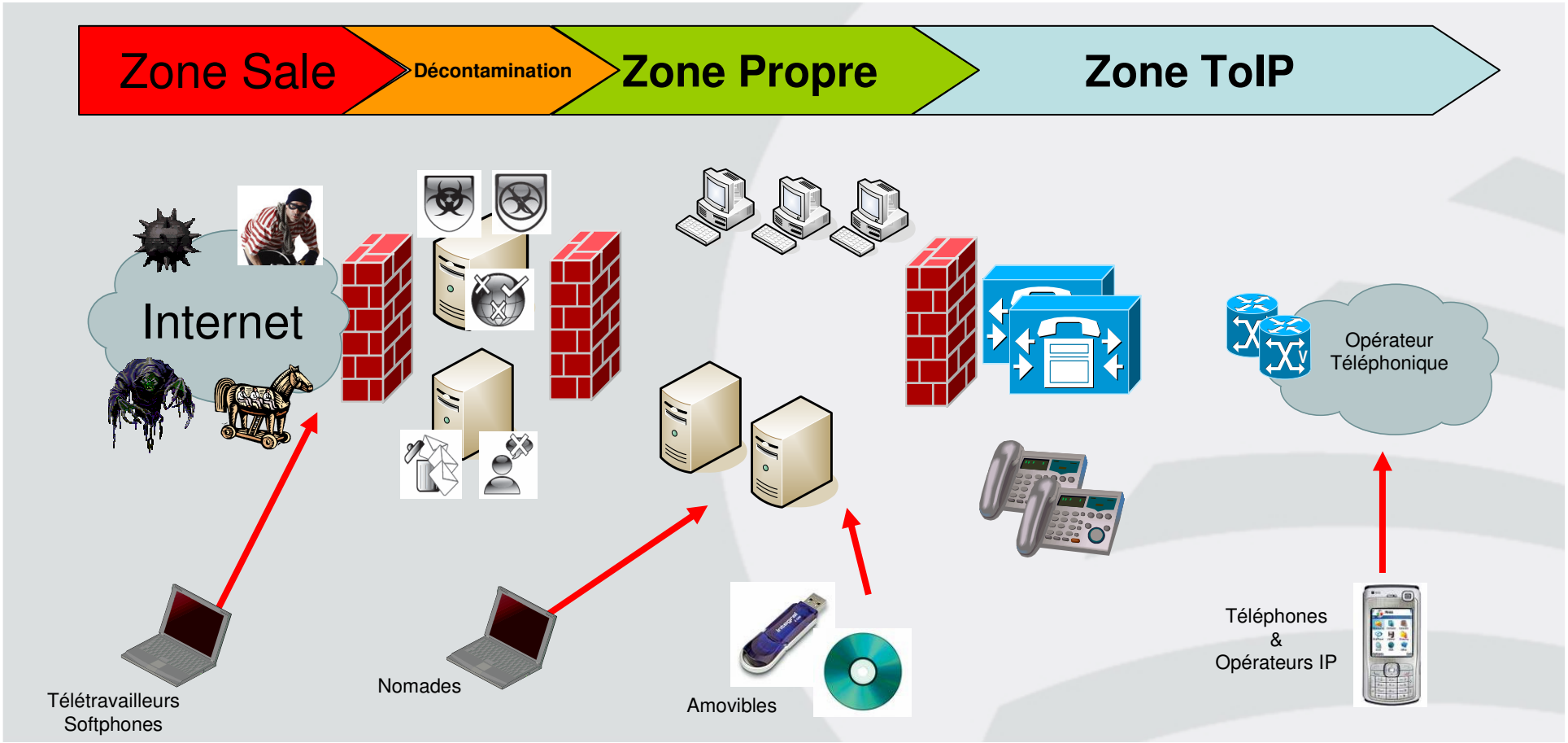


Applications
- Administration multi niveaux
- Gestion sécurisée
- Plates-formes renforcées
- Signalisation h.323 et SIP

Gestion d'appels
- Système d'exploitation renforcé
- Certificats numériques
- Images logicielles signées
- Signalisation TLS

Les terminaux
- Certificats numériques
- Téléphones authentifiés
- Signalisation TLS protégée
- Cryptage des supports SRTP

Schéma - Au niveau logique



L'évolution future de la ToIP

- Le futur, .., c'est la révolution de nos habitudes de travail
  - Mise en œuvre d'applicatifs ultra communicants (Exchange 2007 / Microsoft OCS ou leur(s) équivalent(s))
  - Banalisation des Softphones, des IMs, de la visioconférence
  - Globalisation du protocole IP, y compris chez les Opérateurs

Merci de votre attention.

Des questions?