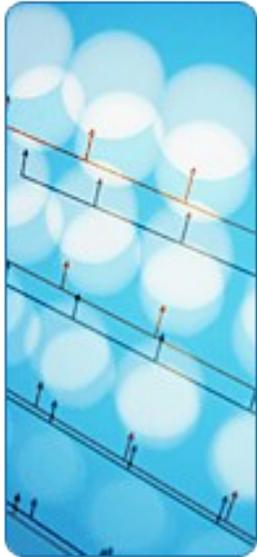


# CheckPhone



Analyser, contrôler  
et sécuriser vos  
applications  
téléphoniques



- ◉ **ELEMENTS DE CONTEXTE**
  - ▶ Présentation société
  - ▶ Les Grandes familles d'attaques
- ◉ **L'OFFRE TECHNIQUE**
- ◉ **MENACES ET CONTRE-MESURES**
- ◉ **CONCLUSION ET PERSPECTIVES**

# CheckPhone en deux mots

## Créateur d'innovations :

- ▶ Aujourd'hui 40 personnes dont 17 en R&D
- ▶ Un investissement permanent en R&D (1M€ en 2005)
- ▶ Une politique de dépôt de brevets : 3 brevets déposés en 2005
- ▶ Lauréat 2005 « entreprise INNOVANTE » concours ANVAR & Lauréat 2005 « Tremplin Entreprise » concours SENAT
- ▶ Label Jeune Entreprise Innovante



## Référencement Application Partner Program



## Référencement Hipath Advanced Partner

## Référencement Partner Program



## Partenariat technologique

## Partenariat technologique : « Fireconverge »



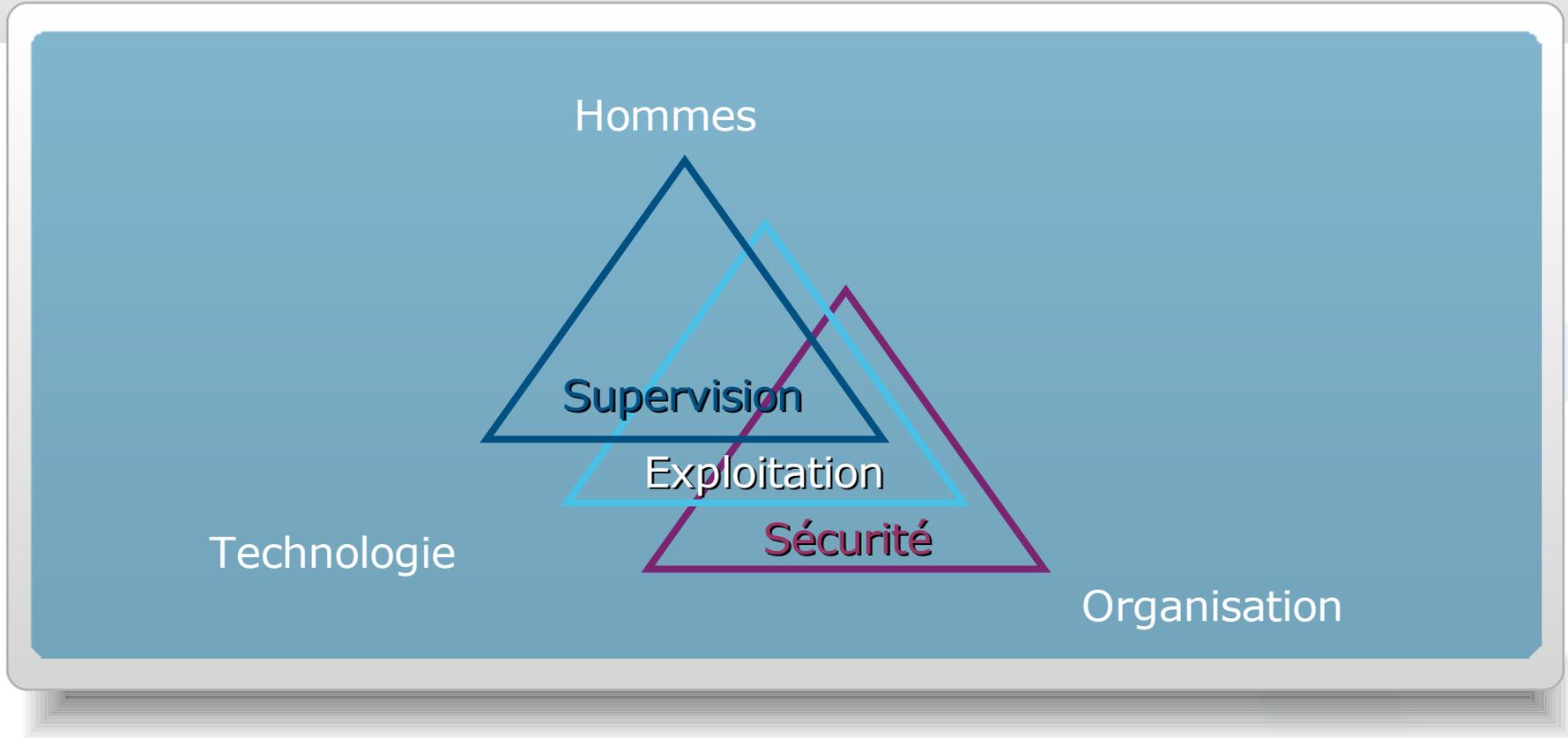
## Référencement OPSEC

## Référencement en cours avec Cisco et Nortel



# La VoIP, une rupture technologique, ...

Mais également organisationnelle ...



- ▶ Infiltration de la téléphonie dans l'ensemble des organes du SI (PABX, IPBX, PROXY, Firewall, switchs, ...)
- ▶ Pas d'outil de supervision global dédié à la voix
- ▶ Pas de contrôle centralisé de la sécurité
- ▶ Pas de visibilité globale pour les RSSI et DSI
- ▶ Pas de visibilité globale pour les directions Télécoms

# Les Problématiques de Piratage

## En France :

Source CERTA (Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques)

- ▶ 16 500 attaques de systèmes téléphoniques (SIT) estimées
- ▶ L'augmentation annuelle moyenne est de 50 % en France
- ▶ Taxonomie des attaques éditée par le VoIPSA en 2005

## Déstabilisation de l'entreprise & Maîtrise de l'information :

- ▶ Consommation : risque sanitaire ....
- ▶ Finance : communication financière sensible ....
- ▶ Social : restructuration, licenciements ...
- ▶ Juridique : confidentialité de procédures ....
- ▶ Industrie sensible : propriété industrielle, intelligence économique ...
- ▶ Pertes Financières directes : fraudes à la facturation / Phreaking

# Quelques exemples & Impacts

- « **Cour d'appel de Caen** - Les magistrats de la cour d'appel de Caen avaient dénoncé les écoutes téléphoniques dont ils pensaient avoir été victimes de la part de leur hiérarchie

En 1999, Jean-Claude Chilou, 1<sup>e</sup> président de la cour et Michel Julien auraient demandé de pouvoir intercepter les communications dans la cour d'appel, une fonction du central téléphonique. La fonction « entrée tiers » a été activée.

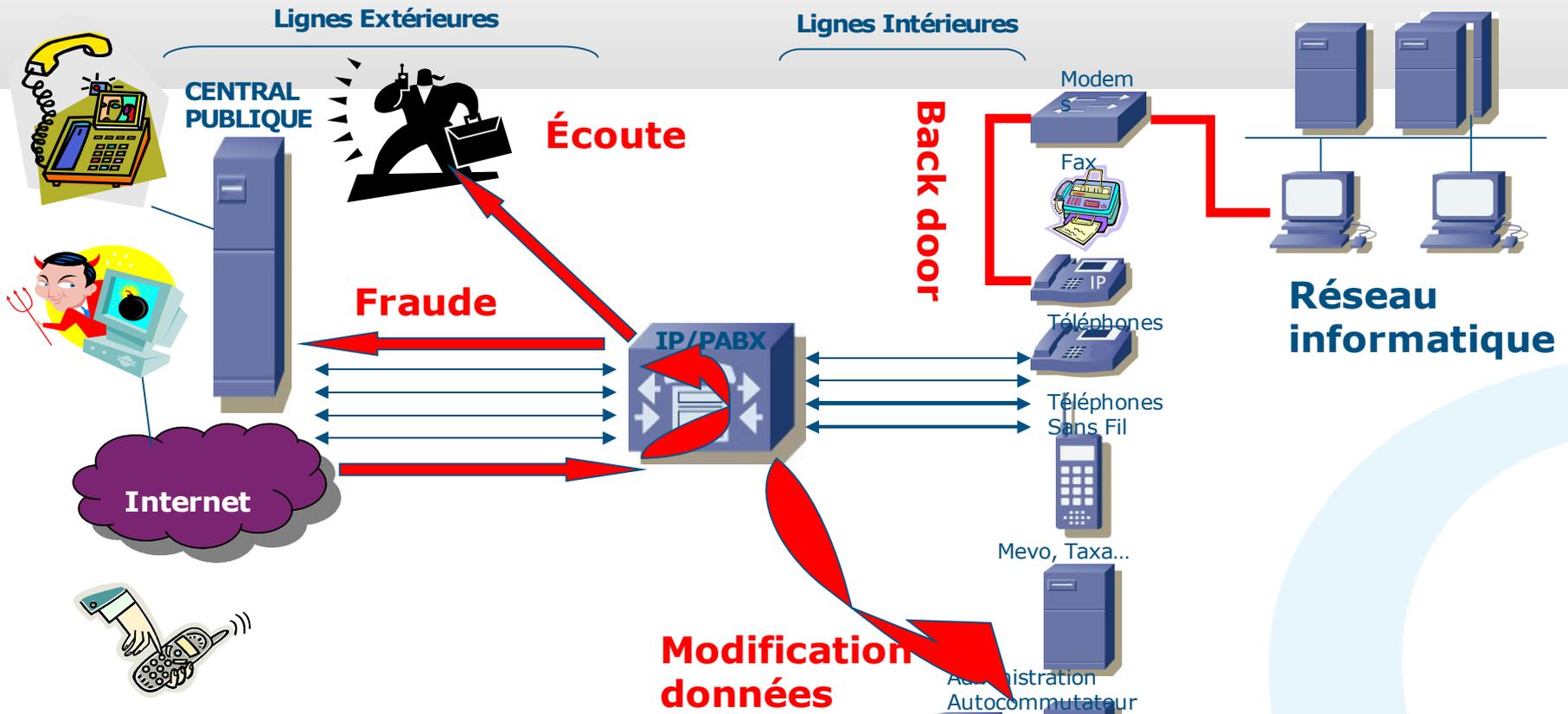
-Le Monde- 31.03.2005 -

- « **3 Phreakers condamnés à 41500 euros** » : Versement à France Télécom à titre de dommages et intérêts. Victimes : Dell, Michelin, Good Year, LVMH, Esso .Impact financier total de **300 000 euros**. - DAS du 16/12/2002

## « **La Loi LEN - article 226-17** »

- *Pour la divulgation d'informations, le code pénal impute également la responsabilité à l'espionné.*
  - *L'entreprise (l'espionné) est responsable des conséquences engendrées pour les tiers*
  - *Les personnes « responsables » (de la sécurité ou le DSI, voire le DG) peuvent être personnellement impliquées (obligation de résultat), sans préjuger des poursuites individuelles (non respect de la PSI de l'entreprise...)*

# Les grandes familles d'attaques



**Détournement de Trafic & de Moyens/ Escroquerie à la facturation**

**Écoute téléphoniques, de boîtes vocales ...**

**Back Door, Vols ou Modifications de données ...**

**Dénis de Service & Sabotages en tout genres ...**

## 🔒 Sécuriser les applications téléphoniques (Sécurité)

- ▶ Adresser les problématiques non résolues de sécurité sur les infrastructures TDM et VoIP

## 🔍 Superviser les organes de sécurité voix (Technologie)

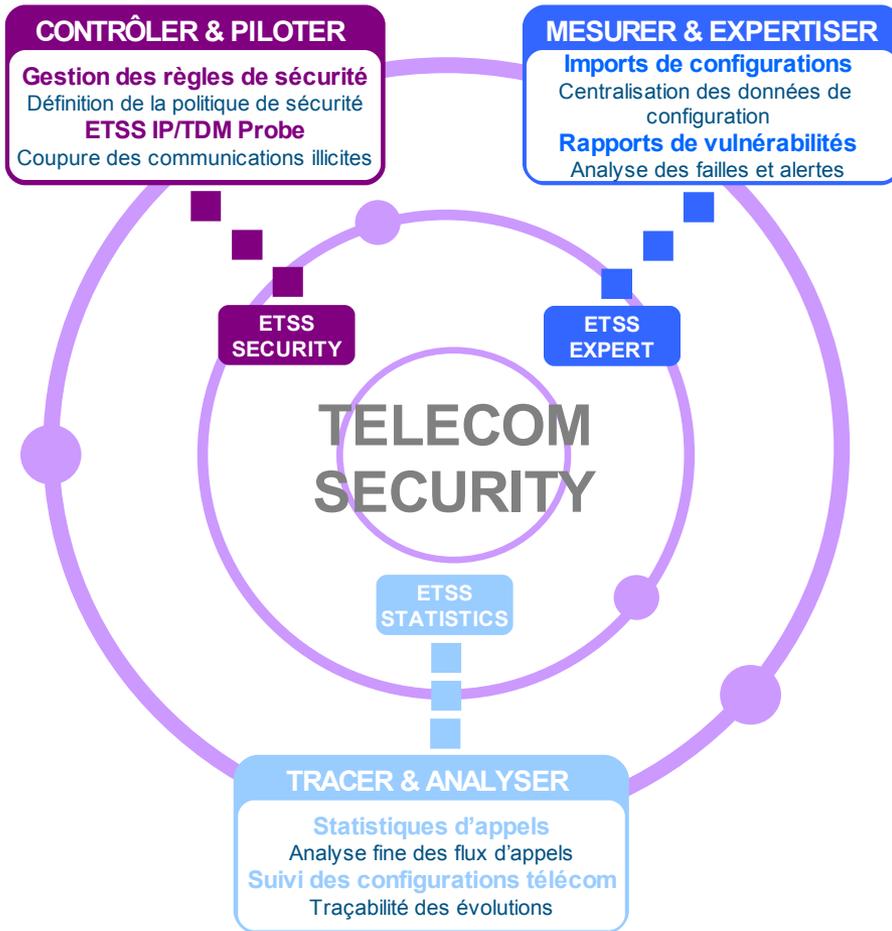
- ▶ Centraliser et consolider l'information en provenance de ces sous organes (PABX, Firewall, SBC, IPBX, Proxy, ...)

## 👤 Proposer des interfaces adaptées et synthétiques (Organisation)

- ▶ Rendre la téléphonie compréhensible aux RSSI et DSI (contrôle)

- ◉ **ELEMENTS DE CONTEXTE**
- ◉ **L'OFFRE TECHNIQUE ETSS**
  - ▶ Security
  - ▶ Expert
  - ▶ Statistics
- ◉ **MENACES ET CONTRE-MESURES**
- ◉ **CONCLUSION ET PERSPECTIVES**

# L'offre ETSS



## 🕒 **Piloter & contrôler :**

- Définir une politique de sécurité téléphonique centralisée

## 🕒 **Mesurer & Expertiser :**

- Application temps réel de la politique de sécurité (coupure des communications illicites)
- Audits périodiques du système téléphonique et alertes sur détection de failles

## 🕒 **Tracer & Analyser :**

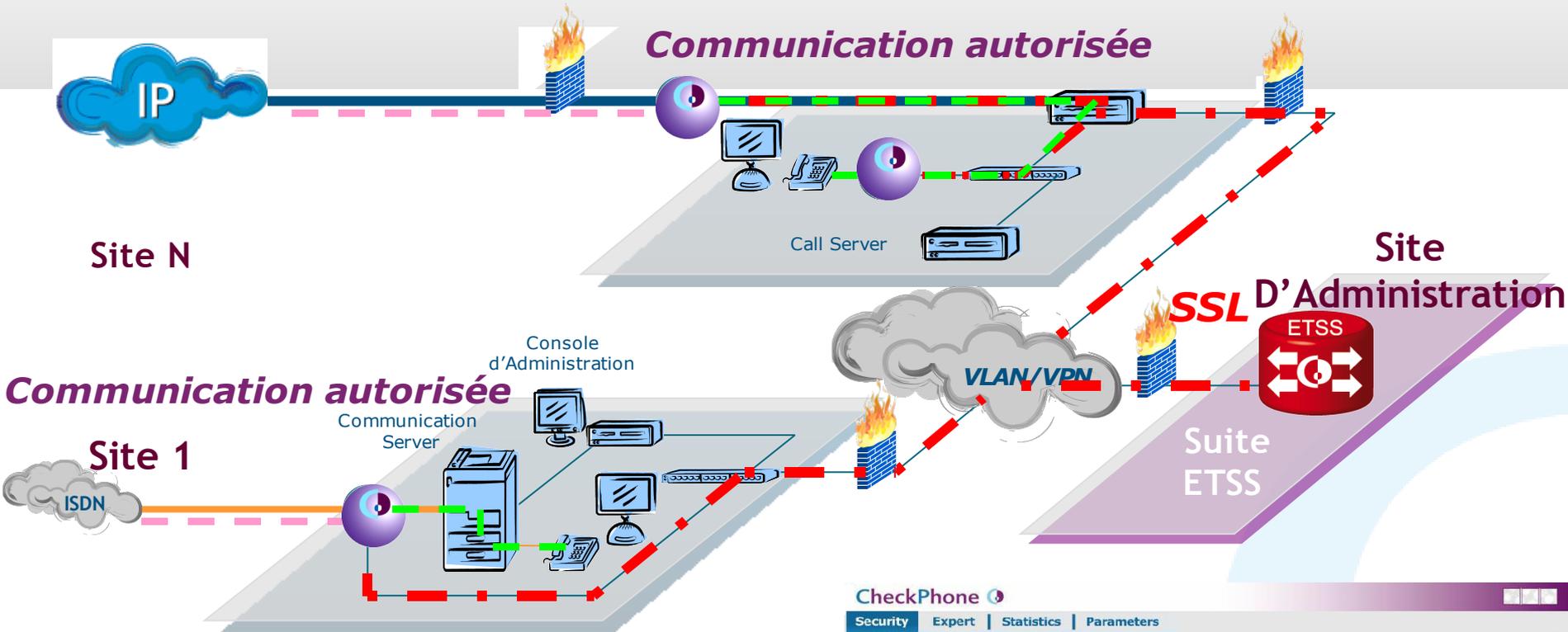
Suivi de configuration et analyse de trafic

## 🕒 **ARCHITECTURE :**

- Distribuée (sondes autonomes et redondantes)
- Multi technologies (TDM, Hybride, Full IP)
- Multi protocoles (SIP, protocoles propriétaires)
- Multi plateformes (principaux équipementiers)

🕒 **Protection :** Voice Access Management, Phreaking, DoS, War Dialing, Directory Harvesting, Spam

# Architecture Distribuée



## ETSS Security :

Construction des Règles

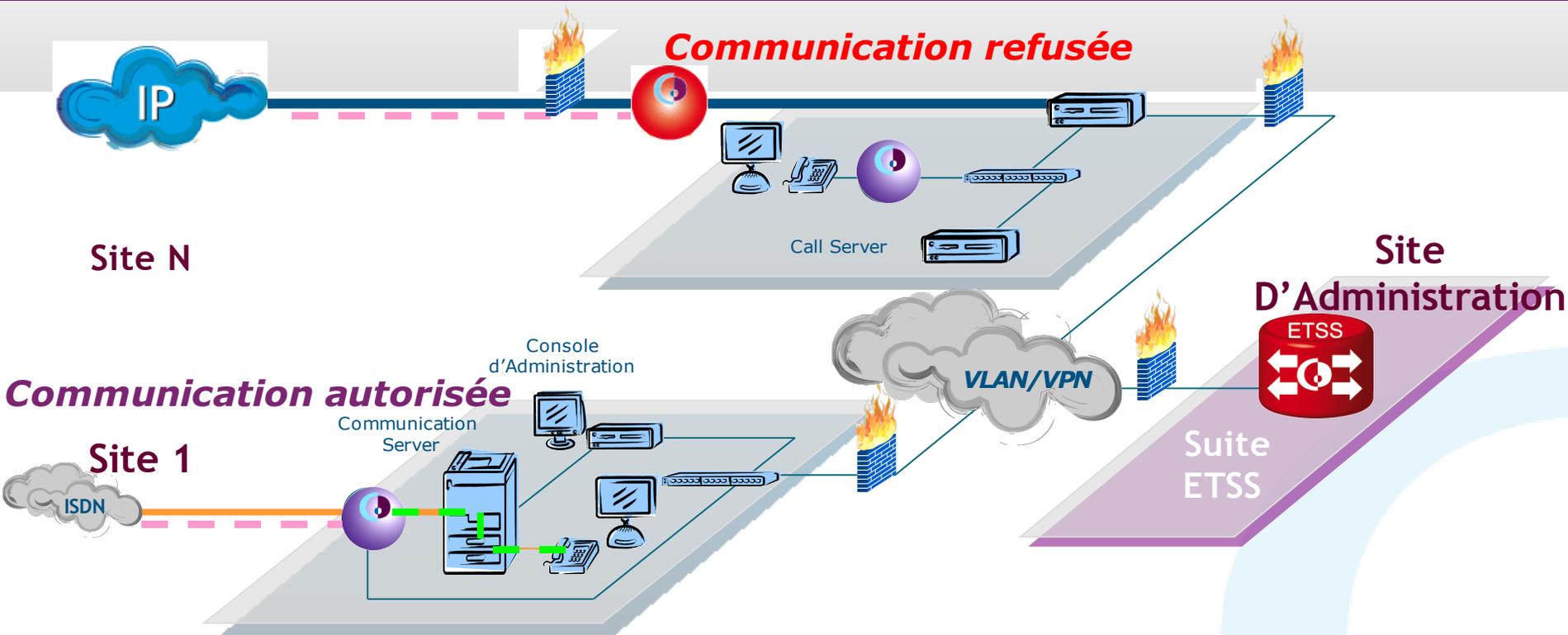
Chargement de la configuration  
des règles vers les Probes

## ETSS Probes :

Consolidation des Règles

Observation du trafic &  
Application des règles

# Architecture Distribuée



## ETSS Security :

Construction des Règles

Chargement de la configuration  
des règles vers les Probes

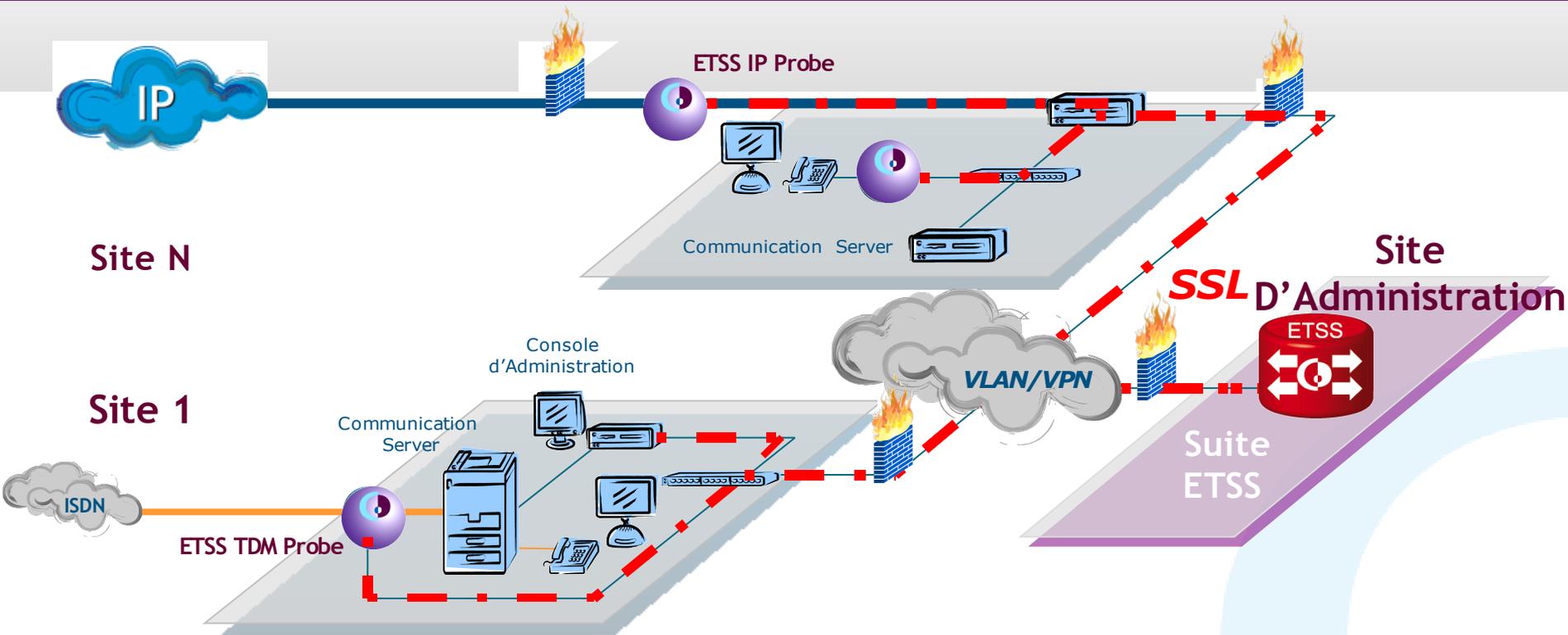
## ETSS Probes :

Consolidation des Règles

Observation du trafic &  
Application des règles



# Architecture Distribuée



## ETSS Expert :

Import des configurations  
Communications Servers Via la Console  
d'Administration

Expertise des vulnérabilités

## ETSS Statistics :

Consolidation des remontées de tickets  
d'appels des ETSS Probes

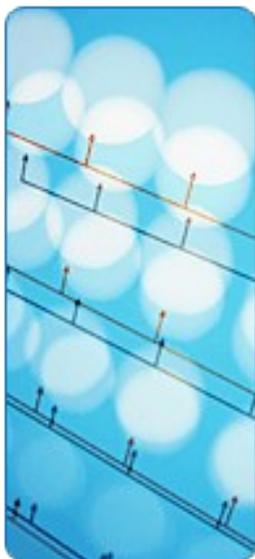
Historisation des configurations  
importées et gestion des différentiels  
de paramétrages

# Les différentiateurs

- Un positionnement unique orienté à 100% sur la sécurité voix
- Une solution de sécurité indépendante des équipementiers télécoms
- Une couverture multi environnements : TDM, Hybride, Full SIP
- Une couverture des failles spécifiques à l'application téléphonique et pas uniquement protocolaire IP
- Innover et perpétuer une politique de dépôt de brevets (1,2 M€ d'investissement R&D en 2005)
- Préserver et intégrer l'existant en multipliant des accords d'interconnexion avec les principaux PBX, IPBX, Firewall, SBC ... du marché
- Démarche de qualification de sécurité auprès de la DCSSI (Cible EAL3+)

# ETSS Security

## Gestion des règles



Analyser, contrôler  
et sécuriser vos  
applications  
téléphoniques



## Protéger la périphérie de votre réseau téléphonique

- ◉ **Instaurer une politique de sécurité téléphonique efficace:**
  - ▶ Centralisée
  - ▶ Indépendante des plates formes utilisées
  - ▶ Indépendante des technologies utilisées (TDM, ToIP, hybride)
- ◉ **Bénéficier à tout moment d'une vue synthétique :**
  - ▶ des droits utilisateurs
  - ▶ des traces du système et de son utilisation
- ◉ **Contrôler en temps réel l'application de la politique de sécurité:**
  - ▶ Alarmes
  - ▶ Fichiers log
  - ▶ Règles appliquées
  - ▶ Détection et traces des attaques et comportements à risques

# L'interface d'exploitation

The screenshot displays the CheckPhone web interface, specifically the 'Rules' section. The interface has a purple header with the 'CheckPhone' logo and navigation tabs for 'Security', 'Expert', 'Statistics', and 'Parameters'. Below these are sub-tabs for 'Rules', 'Profiles', and 'Warnings'. There are buttons for 'Add rule', 'Delete rule', and 'Submit'.

The main content is a table of rules with the following columns: Id, Description, Peer 1, Way, Peer 2, Type, Schedules, Dur., and Action. The rules are as follows:

Id	Description	Peer 1	Way	Peer 2	Type	Schedules	Dur.	Action
1.	drop incomming call great than 1 hour and alert by mail	Internal Mo	→	All	[Call] [Log] [Deny] [Allow] [Priority] [Queue] [?]	All	3600	DROP
2.	Allow incomming call from shanghai to paris (available time range)	RnD Dpt	←	All	[Call] [Log] [Deny] [Allow] [Priority] [Queue] [?]	shanghai-p	0	PASS
3.	Allow outgoing call from paris to shanghai (available time range)	RnD Dpt	→	: recipient	[Call] [Log] [Deny] [Allow] [Priority] [Queue] [?]	shanghai-p	0	PASS
4.		All	←	All	[Call] [Log] [Deny] [Allow] [Priority] [Queue] [?]	All	0	'wardialing
5.	SIP - Denial of Service	All	→	All	[Call] [Log] [Deny] [Allow] [Priority] [Queue] [?]	All	0	PASS
6.	SIP - Directory Harvesting							
	Default policy							DROP

# Les Sites & Correspondants

## 1 Gestion des sites et des sondes associées

- ▶ Création, modification et suppression d'un site, d'une sonde

## 2 Gestion des correspondants internes et externes

- ▶ Création, modification et suppression d'un correspondant interne ou externe
- ▶ Gestion des correspondants internes par listes:
  - ▶ Option listes séquentielles (tranches SDA)
- ▶ Gestion des correspondants externes par listes
- ▶ Listes par défaut :
  - ▶ tous les correspondants internes et externes,
  - ▶ correspondant inconnu (N° caché)
  - ▶ listes de correspondants externes spécifiques fournies par défaut (Ex: N° ISPs)

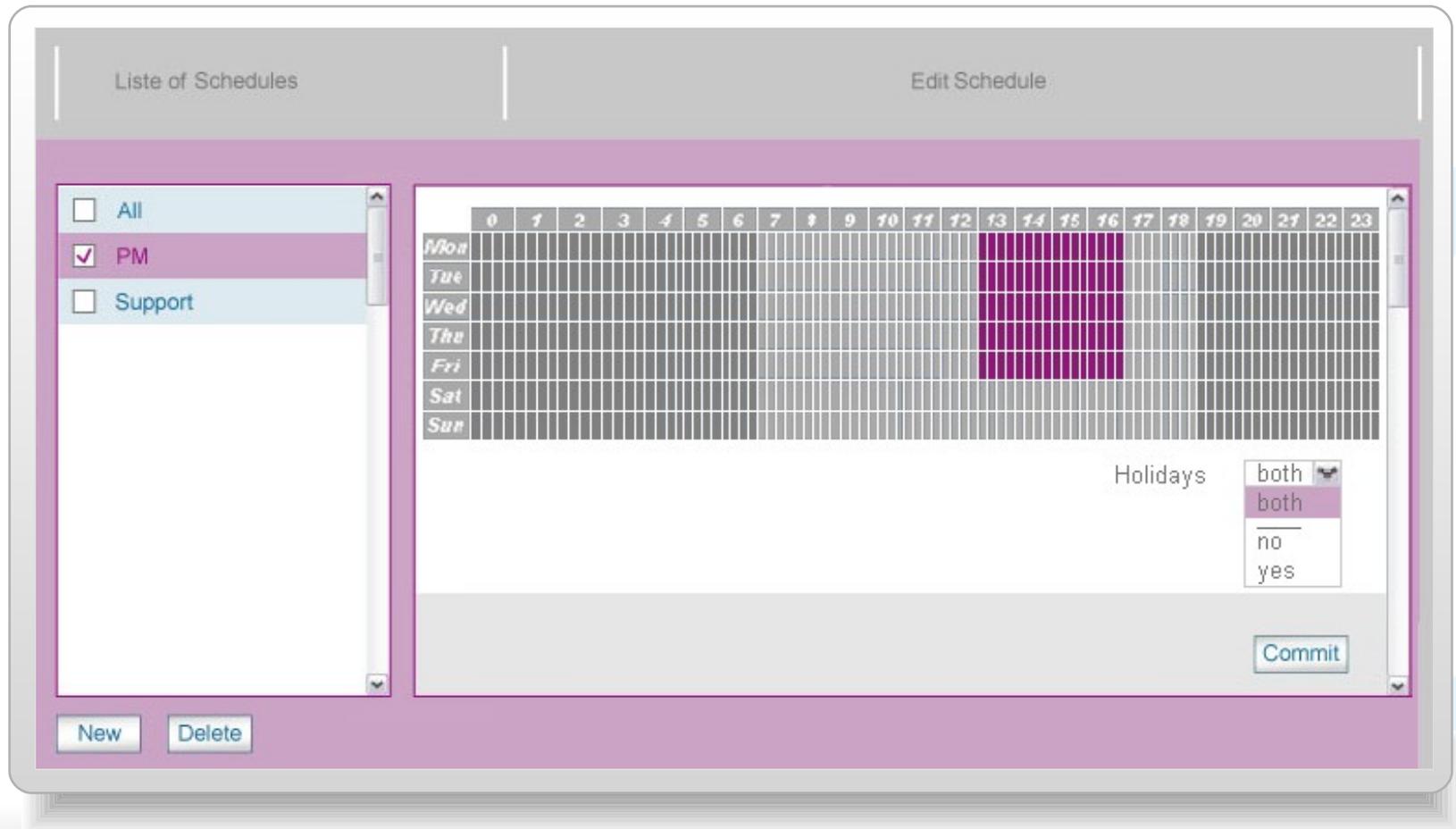
The screenshot shows a web interface for managing correspondants. It features a sidebar with a list of categories: 'Black List', 'Modem' (checked), and 'Green List'. The main area displays a table with the following data:

Description	Prefix	First	Last
<input type="checkbox"/> Modem_paye	01 64 66	60 73	
<input type="checkbox"/> Maintenance_PABX	01 64 66	67 20	
<input type="checkbox"/> Maintenance_SVR	01 41 33	85 70	85 78

Buttons for 'Add.', 'Delete', 'New', and 'Delete' are visible at the bottom of the interface.

# Le Temps

- **Gestion des plages horaires**
  - ▶ Création, modification et suppression de plages horaires spécifiques



# Les Règles de Gestion & Warning

## ◉ Mode interdiction / autorisation par défaut

- ▶ Tout ce qui n'est pas interdit est autorisé
- ▶ Tout ce qui n'est pas autorisé est interdit

## ◉ Critères de règles

- ▶ Site
- ▶ Mode inclusif ou exclusif d'un critère
- ▶ Direction, appels entrants et/ou sortants
- ▶ Correspondants, ou liste de correspondants internes
- ▶ Correspondants, ou liste de correspondants externes
- ▶ Type de communication (voix, fax, modem)
- ▶ Un, plusieurs ou tous les modèles horaire (heures ouvrables, etc...).
- ▶ durée de communication

## ◉ Warnings

- ▶ Règles types fournies par défaut
- ▶ activation / désactivation des warnings

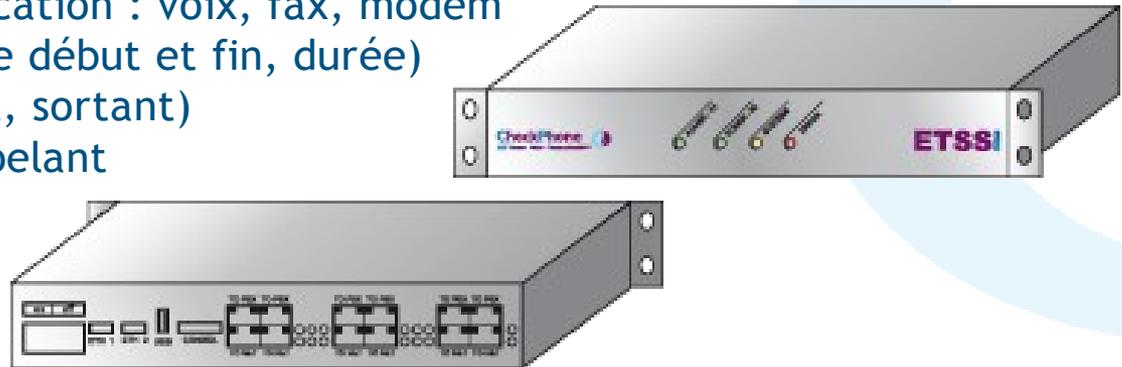
## 🔍 Règles stateful

- ▶ Gestion de compteurs pour définir le nombre d'appels en cours avec le même N° interne (renvois et conférences)
  - ▶ Définition d'un premier seuil avec action
  - ▶ Définition d'un deuxième seuil avec action
- ▶ Gestion de compteurs pour définir le nombre d'appels en cours avec le même N° externe.
  - ▶ Définition d'un premier seuil avec action
  - ▶ Définition d'un deuxième seuil avec action
- ▶ Gestion d'un compteur pour définir le nombre d'appels reçus dans un temps imparti. (ex : war dialing, ...)
  - ▶ Définition d'un premier seuil avec action
  - ▶ Définition d'un deuxième seuil avec action
- ▶ Mise à jour automatique d'une liste de N° externes sur critères (Ex: Cas de SPAM)
  - ▶ le nombre d'appels reçus depuis la source
  - ▶ périodicité des appels reçus depuis la source
  - ▶ L'administrateur peut vider cette liste vers une green list ou une black list

## • ACTIONS

- ▶ chaque règle conduit à une action directe ou après un timeout paramétrable
- ▶ envoi d'un email
- ▶ interdiction : coupure de la communication ou bannissement temporaire
- ▶ autorisation
- ▶ marquage spécial permettant d'identifier ces appels dans les logs pour une analyse externe
- ▶ Analyse : tracking d'appels pour les qualifier sur occurrence dans le temps

- ❶ TDM PROBE: Sonde PRI(E1/T1) & BRI fonctionnant sur le principe IDS / IPS
  - ▶ 2 Modes de fonctionnement :
    - ▶ Haute Impédance : mode parallèle sans coupure dans lequel les flux sont identifiés sans interaction avec le réseau télécom
    - ▶ Drop & Insert : mode Coupure qui permet la coupure des communications illicites sur commande de l'ETSS Security Manager
  - ▶ Interception sur le réseau publique de l'intégralité des communications entrantes et sortantes
  - ▶ Stacks d'analyse RNIS : Identification temps réel des critères de communication
    - ▶ Type de communication : voix, fax, modem
    - ▶ Horodatage (heure début et fin, durée)
    - ▶ Direction (entrant, sortant)
    - ▶ N° appelé, N° appelant

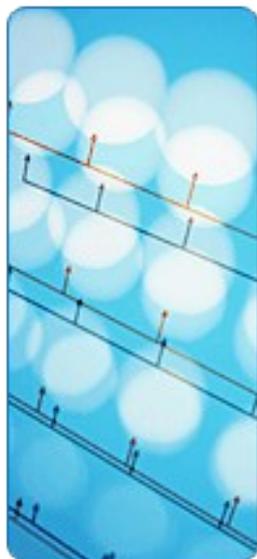


### Sonde IP fonctionnant sur le principe IDS / IPS

- ◉ Interception sur le réseau informatique de l'intégralité des communications téléphoniques SIP
- ◉ Identification temps réel des critères suivants:
  - ▶ Type de flux : voix, fax, visio, data, applicatif
  - ▶ Horodatage (heure début et fin, durée)
  - ▶ Appel Interne/Externe
  - ▶ Adresse IP et N° de port Source ou Destination
  - ▶ URI Source ou Destination
- ◉ Coupure des communications illicites

# ETSS EXPERT

## Connecteurs IPBX - PABX



Analyser, contrôler  
et sécuriser vos  
applications  
téléphoniques



# La Mise à Disposition des Données

The screenshot displays the CheckPhone web interface. At the top, there is a navigation menu with tabs for Security, Expert, Statistics, and Parameters. Below this, there are sub-tabs for Imports, Reports, and System. The main content area is divided into several sections:

- List of configurations:** A list of configuration files with columns for name, date, and size. The selected configuration is 'conf1 07/01/2005 12:00 am (3523 b)'. Below the list are 'Delete' and 'Import' buttons.
- Configuration details:** A panel titled 'Configuration : conf1 07/01/2005 12:00 am (3523 bytes)'. It contains the following information:
  - Company : checkphone
  - Address : 19-21 rue colonel avia
  - Phone : 33 (0)1 41 33 96 96
  - File opened : conf1\_07012005\_1200.xml
  - Edited : October 4th 2005 (2:34 pm)
- Configuration Tree:** A tree view on the left showing the hierarchy of configurations. The selected path is 'Site\_Lyon | pabx\_Astra1 | list of companies | France Telecom id 4 | list of classes of department | Director phone 8 | list of subscribers'.
- Subscriber List:** A table displaying subscriber information. The table has columns for subscriber, first name, name, department, and phone. The data is as follows:

subscriber	first name	name	department	phone
	Serge	Darne	Expenses	01 44 09 10 33
	Francis	Roudez	R&D	01 44 09 10 34
	Aurélien	Monvoisin	R&D	01 44 09 10 35
- Functionality Table:** A table below the subscriber list showing various functions and their attributes. The table has columns for fonction, attribute, and value. The data is as follows:

fonction	attribute	value
entry in third	activated	off
protection of entry in third	activated	off
squatt	activated	both
forward	activated	both
forward to the initial	activated	both
three-party call	activated	both
conference call with several	activated	both

# Alerte & Contre Mesures

- Traitement des données après rapatriement (manuel ou automatique)
  - ▶ Choix d'une configuration de référence
  - ▶ Analyse différentielle par rapport à cette configuration ou par rapport à la précédente configuration rapatriée
  - ▶ **Lancement du système Expert pour l'évaluation des risques ...**

- Pondération des gravités dans l'analyse des risques :
  - ▶ Note de Gravité d'exposition aux risques et de Probabilité d'exposition

- Impact sur les personnes & process de l'entreprise
  - ▶ Enumération des classes de service & abonnés affectées

- Propositions de Contre Mesure

CheckPhone

Security | Expert | Statistics | Parameters

Imports | Reports | System

List of reports

- report1 07/01/2005 12:00 am (352)
- report1 05/22/2005 12:00 am (241)
- report1 05/21/2005 6:25 pm (1239)
- report1 01/14/2005 8:00 am (1624)

Delete Generate

Report Tree

- site\_Lyon
  - pabx\_Astra1
  - pabx\_Astra2
    - 1. Espionage
    - 2. Warning
    - 3. Diversion of traffic
    - 4. Trapping of station
    - 5. Listening
    - 6. Listening
    - 7. Refusal of service
    - 8. Warning
    - 9. Espionage
    - 10. Listening
    - 11. Refusal of service

Report : report1 07/01/2005 12:00 am (3523 bytes)

View see by default not see by default Company: checkphone Address: 19-21 rue colonel avia Phone: 33 (0)1 41 33 96 96 File opened: report1\_07012005\_1200.xml Edited: October 4th 2005 (2:34 pm)

5. Listening

6. Listening

7. Refusal of service

Possibility to refuse a user a service thanks to the function forwarding

Probability: 6/10 Seriousness: 9/10 Day / Night: day

Counter measures

To prohibit the function immediate forwarding

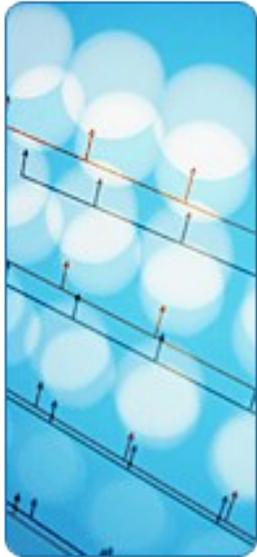
Companies

Hoche Partners

- Directors department
  - Marie Dumont 01 45 09 14 38
  - Sales department
    - Joel Francois 01 45 82 64 59
    - Florent Dirart 01 45 32 18 64
- Checkphone
  - Directors department
    - Franck Ford 01 43 21 54 87

- ④ **Bénéficier à tout moment d'une vue synthétique des équipements téléphoniques (Connecteurs) :**
  - ▶ Rapatriement des configurations système
  - ▶ Consolidation et présentation synthétique des informations
  - ▶ Historisation et suivi des configurations
  
- ④ **Analyse automatique des configurations**
  - ▶ Analyse de configuration
  - ▶ Analyses différentielles
  - ▶ Détection des paramétrages à risque
  
- ④ **Mécanismes d'alerte et Contre Mesure**
  - ▶ Alarmes et traces sur modifications
  - ▶ Proposition de rapports et contre mesures
  - ▶ Etude de vulnérabilité des périphériques PABX

***Contrôler et maîtriser le réseau téléphonique***



Analyser, contrôler  
et sécuriser vos  
applications  
téléphoniques

# STATISTICS



# Les Données d'appels

## Affichage & Requêtes :

- ▶ Tri des appels à l'affichage selon leur type, leur direction, leurs numéros d'appel, si elles ont été acceptées ou non
- ▶ Gestion d'un profil « CNIL » pour masquer en partie les numéros selon la confidentialité d'accès à l'application
- ▶ Affichage complémentaire des heures d'appels, durée de communication, ....

calls.log size : 3317 bytes time : 31/01/2006 11:01:33

ACTION	STATE	RULE	TYPE	WAY	SOURCE		DESTINATION		TIME	DURATION
					# / @IP	URI	# / @IP	URI		
WARN	opened	Rule # 5	fax	in	0123456****		0123456****		13/01/2006 14:04:21	1
MAIL	ended	Rule # 4	visio	in	0123456****		0123456****		13/01/2006 14:04:21	2
PASS	unknown	Rule # 1	voice	in	0123456****		0123456****		13/01/2006 14:04:21	3
DROP	ringing	Rule # 2	modem	out	0123456****		0123456****		13/01/2006 14:04:21	5
ANALYZE	opened	Rule # 3	fax	both	0123456****		0123456****		13/01/2006 14:04:21	6
BAN	opened	Rule #17	fax	out	*****	sip.*****@192.168.1.***:5060	158.1.230.***	sip.*****@192.168.1.***:5060	13/01/2006 14:04:21	7
BAN	opened	Rule #17	fax	out	*****@chk.com	sip.*****@192.168.1.***:5060	158.1.230.***	sip.*****@192.168.1.***:5060	13/01/2006 14:04:21	8
BAN	opened	Rule #17	fax	in	192.168.1.***	sip.*****@192.168.1.***:5060	158.1.230.***	sip.*****@192.168.1.***:5060	13/01/2006 14:04:21	9
MAIL	ended	Rule #14	visio	out	192.168.1.***	sip.*****@192.168.1.***:5060	*****@checkphone.fr	sip.*****@192.168.1.***:5060	13/01/2006 14:04:21	11
TAG	opened	Rule #16	fax	both	192.168.1.***	sip.*****@192.168.1.***:5060	*****	sip.*****@192.168.1.***:5060	13/01/2006 14:04:21	12
PASS	unknown	Rule #11	voice	unknown	192.168.1.***	sip.*****@192.168.1.***:5060	10.1.1.***	sip.*****@192.168.1.***:5060	13/01/2006 14:04:21	13
DROP	ringing	Rule #12	modem	in	*****@checkphone.fr	sip.*****@192.168.1.***:5060	10.1.5.***	sip.*****@192.168.1.***:5060	13/01/2006 14:04:21	14

ACTION: PASS  DROP  BAN  ANALYZE  MAIL  TAG  WARN

TYPE: VOICE  MODEM  DATA  APPLI.  FAX  VIDEO

WHO: SRC (#/@IP,URI) [ ] [ ] DST (#/@IP,URI) [ ] [ ]

WAY: IN  OUT  UNK.

# Les Données de Configuration SIT

## Exécution manuelle ou automatique des différentiels de configuration :

- ▶ Génération d'un Différentiel
- ▶ Identification et Consultation de chacun des rapports
- ▶ Possibilité de Suppression manuelle
- ▶ Vue Liste ou Vue par catégorie de paramètres

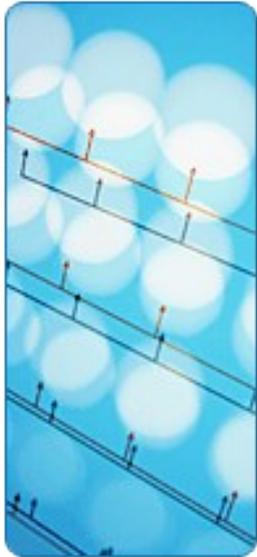
The screenshot displays the CheckPhone web interface, which is used for managing configuration differences. The interface is divided into several sections:

- Navigation:** Includes tabs for Security, Expert, Statistics, and Parameters. Sub-tabs for Calls, Imports, Viewer, and System are also visible.
- List of differences:** A list of configuration differences with columns for ID, date, time, and size. The selected difference is 'diff1 07/01/2005 12:00 am (3523 bytes)'. Buttons for 'Delete' and 'Generate' are provided.
- Difference Detail:** A detailed view of the selected difference, showing a 'View' section with checkboxes for 'modified', 'added', and 'removed'. It also displays company information: 'Company: checkphone', 'Address: 19-21 rue colonel avia', 'Phone: 33 (0)1 41 33 96 96', 'File opened: diff\_07012005\_1200.xml', 'Edited: October 4th 2005 (2:34 pm)', 'Configuration of reference: 12/12/2004 (12:00 am)', and 'Compared configuration: 12/24/2004 (7:00 pm)'. Buttons for 'Trash' and 'See Trash' are also present.
- Table Elements:** A table showing a list of elements with columns for 'status', 'attribute', 'old', and 'new'. The table is organized into sections: 'Links', 'Groupings', and 'Subscribers'.

Section	Attribute	old	new
Links	Card	1	2
	Id	1	5
Groupings	Id	1	2
	Id	1	3
Subscribers	First name	Paul	Robert
	Name	Dupond	Durant
	Ph		
Subscribers	First name	Vincent	Pierre
	Name	Frolent	Raubin
	Ph		
Subscribers	First name	Sophie	Emilie
	Name	Raufouin	Pantel
Subscribers	Ph		

- ◉ **ELEMENTS DE CONTEXTE**
- ◉ **L'OFFRE TECHNIQUE ETSS**
- ◉ **MENACES ET CONTRE-MESURES**
  - ▶ Périimètre de sécurité
  - ▶ Exemples de failles SIP
  - ▶ Risques analysés
- ◉ **CONCLUSION ET PERSPECTIVES**

# MENACES ET CONTRE- MESURES



Analyser, contrôler  
et sécuriser vos  
applications  
téléphoniques



# Périmètre de sécurité CheckPhone

<b>Menaces</b> <i>et exemples</i>	  <b>Protection</b> <small>Secure Voice Communications</small>
<b>Atteinte à l'intégrité:</b> •Voice SPAM; Theft of Services	 <b>contrôle d'identité et d'accès sur les appels</b>
<b>Ecoutes passives illicites :</b> •Number Harvesting	 <b>contrôle des règles d'attribution des droits</b>
<b>Interception et Modification :</b> •Call Rerouting; Conversation Impersonation and Hijacking	 <b>contrôle d'identité, d'autorisation et d'intégrité de la configuration</b>
<b>Abus de service :</b> •Call Conference abuse; Bypass or adjustment to billing	 <b>contrôle d'identité, d'autorisation et d'intégrité de la configuration</b>
<b>Interruption de Service (DoS)</b>	 <b>contrôle de la source et du comportement (analyse des débits d'appels)</b>

## La solution CheckPhone

**ETTS Security**

**ETSS Expert**

**ETTS Security & Expert**

**ETTS Security & Expert**

**ETTS Security & Expert**

# Exemples de failles SIP gérées

## ④ Interception and Modification / Call Back Holing

- ▶ Ce type d'attaque se fait en injectant des CANCEL dans le flux des communications légitimes depuis une autre machine. La contre mesure ETSS est d'utiliser les protections state-machine qui excluent les messages qui ne proviennent pas des @ IP des deux interlocuteurs. Historisation et suivi des configurations

## ④ Interception and Modification / Impersonation and Hijacking

- ▶ Pour le protocole SIP, cela se concrétise par une tentative de message REDIRECT que l'on peut bloquer spécifiquement avec une règle (Option SIP, type de message)

## ④ Malformed requests and messages / Disabling endpoints with invalid requests

- ▶ Les messages invalides peuvent être bloqués par ETSS avant qu'ils n'atteignent l'agent utilisateur(UA), soit parce qu'ils s'éloignent trop de la norme SIP, soit parce qu'ils contiennent une charge dangereuse connue

## ④ Network service DOS

- ▶ En construisant des règles qui limitent le nombre de message SIP sur une période de temps, on bloque les éventuels flooding qui peuvent aboutir à un DoS SIP

④ ...

# Les Risques analysés

Paramètres/Évènements sous Observation ETSS Manager	Risque à prévenir	Security	Expert	Statistics
<b>Intrusion via le téléphone</b>				
Contrôle des Modems RTC	Modem en écoute constituant une porte dérobée ou un rebond vers le SI	X		
Contrôle des Fax	Modem en écoute constituant une porte dérobée ou un rebond vers le SI	X		
<b>Analyse de trafic</b>				
Contrôle des flux en mode IDPS	Détection et Coupures des "Attaques" en cours, comportement anormaux ...	X		
Analyse et traçabilité des flux d'appels	Analyse des flux non taxés	X		X
Traçabilités des Aboutements sans décrochés	Identification des rebond sur l'architecture			X
Contrôle des flux vers des postes interne mais de source unique	Risque de qualification des modems, Fax, Boîtes vocales ... par des hackers	X		X
Contrôle des flux convergeants vers un ou plusieurs postes	Risque de tentative d'intrusion, de crackage de mot de passe ou rebond en appels sortants surtaxés	X		X
Contrôle des volumétries d'appels massives	Tentative de dénis de service global, de qualification des modems, Fax, Boîtes vocales, de tentative d'intrusion, de crackage de mot de passe, de rebond en appels sortants surtaxés	X		X
<b>Espionnage</b>				
Contrôle de la possibilité de s'infiltrer dans une conversation à l'aide d'une fonction 'd'entrée en tiers' ...	Risque d'écoute discrète de conversation sans y être invité		X	
Identification de messagerie vocale accessible et pas ou faiblement protégée contre les écoute abusives	Risque de détournement/vol d'informations contenu dans les boîtes vocales	X		
Contrôle des possibilités d'"Écoute de Conférence", d'"Écoute Bébé" ...	Possibilité pour un tiers de s'introduire dans une conversation, une conférence, une réunion un bureau de direction ...		X	

# Les Risques (suite)

Enregistrement des Conversations				
Contrôle des fonction de "transfert ou renvoie de boîte vocale"	Risque de transfert des communications vers une boîte vocale pour enregistrement ou réécoute ultérieure par un tiers		X	
Contrôle des mise en "Conférence" systématique	Risque de détournement des conférences vers des boîtes vocales, postes distants, systèmes d'enregistrement ...		X	
Détournement de trafic				
Contrôle des "Renvois Immediat" (sans sonnerie) abusifs	Risque d'usurpation d'identité, détournement d'appels, blocage de poste. La fonction sans sonnerie garanti la discrétion du détournement		X	
Contrôle des "Renvois Conditionnel" (filtrage : accepter les appels x et renvoyer les appels Y)	Risque d'usurpation d'identité, détournement d'appels, blocage de poste. La fonction conditionnelle permet le ciblage du détournement sur des appels sensibles		X	X
Contrôle des "Renvois sans Conditions"	Vers un poste interne = risque d'usurpation d'identité, détournement d'appels		X	
Contrôle des "Renvois" et "International"	Vers un poste externe = risque de surfacturation( vers mobile, vers N° surtaxés ...)	X	X	X
Contrôle des "Out-Dial" et "DISA"	Risque d'aboutement sur PABX vers N° surtaxés ..	X	X	X
Contrôler les usages abusif de poste "Virtuels"	Risque de masquage d'appels surtaxés		X	X
Piégeages de postes				
Contrôle des usages du "Squat de fonctionnalité"	Risque de détournement des privilèges d'un poste		X	
Déni de service				
Contrôle des paramètres conduisant à l'isolement d'un poste	Risque de neutralisation d'un poste	X	X	X
Contrôle des paramètres conduisant à l'isolement d'un groupe de postes	Risque de neutralisation d'un groupe par des renvois bouclés par exemple	X	X	X
Contrôle des paramètres conduisant à l'isolement de tous les utilisateurs	Interruption complète du PBX	X	X	X
Contrôle des Fax	Spam et/ou Saturation complète des fax par envois massifs ou occupation permanente	X		

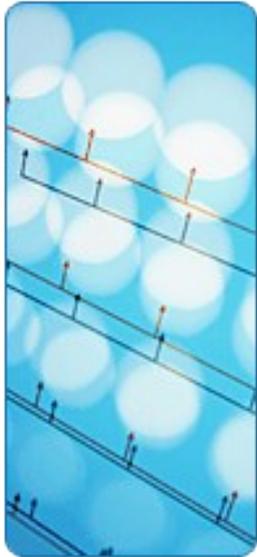
- ◉ **ELEMENTS DE CONTEXTE**
- ◉ **L'OFFRE TECHNIQUE ETSS**
- ◉ **MENACES ET CONTRE-MESURES**
- ◉ **CONCLUSION ET PERSPECTIVES**
  - ▶ Perspectives
  - ▶ Conclusions

# Conclusion & perspectives

- Continuation de l'effort R&D
- Adaptation des produits aux demandes clients, opérateurs, intégrateurs, équipementiers
  - ▶ Création d'un club utilisateur (forum, FAQ...)
- Mise en place d'un maintien en condition de sécurité (MCS)
  - ▶ Démarche de qualification (en cours)
  - ▶ Veille dédiée aux attaques VoIP (projet)
  - ▶ Habilitation de la société (projet)

**CHECKPHONE PARTENAIRE  
INCONTOURNABLE DE LA SECURITE DE LA VOIX**

# Questions ?



Analyser, contrôler  
et sécuriser vos  
applications  
téléphoniques

