(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 876 855**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **04 52361**

(51) Int Cl[8] : **H 04 M 3/22** (2006.01), H 04 M 3/38, 3/42, H 04 L 12/22, 12/24, 29/06

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 19.10.04.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 21.04.06 Bulletin 06/16.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *CHECKPHONE Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** KAAS GERARD.

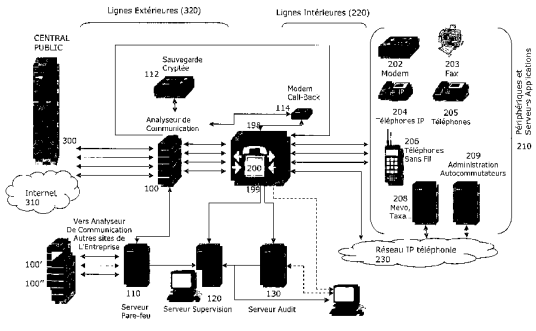
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** BREESE DERAMBURE MAJEROWICZ.

(54) DISPOSITIF DE SECURISATION D'UN AUTOCOMMUTATEUR.

(57) La présente invention se rapporte au domaine des télécommunications et de la sécurité des réseaux.

La présente invention se rapporte à un système pare-feu de sécurisation d'un autocommutateur (200) d'entreprise connecté, d'une part, à au moins un réseau de communication en mode commuté, de type PSTN, et, d'autre part, à un ensemble de périphériques de communications et/ou de serveurs d'application (210), ledit système comprenant un analyseur de communication (100) des couches basses (1 à 3) du modèle OSI de communications numériques en mode circuit et analogiques, un serveur pare-feu (110) connecté audit analyseur (100), caractérisé en ce que ledit système comprend, en outre, un serveur de supervision (120) connecté à la sortie « fil de l'eau » (199) de l'autocommutateur (200) pour l'analyse des tickets de communication et l'application de règles sécuritaires portant sur les couches hautes applicatives (4 à 7) du modèle OSI.



FR 2 876 855 - A1

DISPOSITIF DE SÉCURISATION D'UN AUTOCOMMUTATEUR

La présente invention se rapporte au domaine des télécommunications et de la sécurité des réseaux.

La présente invention concerne plus particulièrement un système et un procédé pour sécuriser un autocommutateur d'entreprise par le contrôle des appels.

L'autocommutateur d'entreprise constitue la porte d'entrée dans un réseau d'une entreprise. De ce fait, la sécurité doit y être fortement présente notamment depuis la convergence de la gestion des réseaux en mode circuit et celle des réseaux en mode paquets.

De trop nombreux abus ont lieu actuellement sur les autocommutateurs d'entreprise dans lesquels les communications sont détournées par des personnes extérieures pour téléphoner à moindre coût.

L'art antérieur connaît déjà, par le brevet américain US 6 687 353 (Securelogix), un système et un procédé pour un système de sécurisation téléphonique. Illustré par la figure 1, l'invention consiste à contrôler et à réaliser l'accès entre des terminaux d'une entreprise à une pluralité de sites et leurs circuits respectifs dans le réseau public commuté. Le système et le procédé peuvent comprendre : un capteur de ligne discret à l'intérieur des sites pour déterminer la nature des appels, le capteur de ligne n'interférant pas avec les communications existantes. Le capteur de ligne peut comprendre : une paire de relais pour router les données à travers le capteur de ligne sans altérer les données, une paire d'émetteurs-récepteurs et une unité de traitement pour router les données à travers le capteur de ligne en stockant et copiant les données et

en transmettant les nouvelles données à travers le capteur de ligne. Le système peut également comprendre : un autocommutateur PBX dans les sites et connectés au capteur de ligne ; un commutateur central connecté au capteur de ligne et au PBX ; et un serveur de gestion de pare-feu.

L'intégralité des systèmes connus pour la sécurisation des réseaux de télécommunications d'entreprise et plus particulièrement des autocommutateurs privés, reproduit une architecture similaire à celle décrite dans la figure 1. A savoir, un analyseur (capteur 13) est placé sur la ligne réseau (11) entre le réseau commuté (10) et l'autocommutateur privé (14). Ce capteur analyse la nature des appels émis depuis/vers les périphériques (16) du réseau privé (15), puis confronte les informations obtenues à des règles sécuritaires contenues dans un serveur (17).

Cela est notamment le cas dans le brevet américain US 6 226 372 (Securelogix) qui décrit un système et un procédé pour la mise en oeuvre d'un coupe-feu/scanneur de télécommunications coopérants, totalement intégrés, permettant la mise en oeuvre de fonctions de sécurité améliorées du coupe-feu et du scanneur de télécommunications, et la mise en place d'une structure de sécurité spécialisée demandée par l'entreprise, d'une visibilité événementielle et de la consolidation des rapports, dans une entreprise à répartition globale. Dans la configuration la plus basique, le coupe-feu/scanneur intégré présente des fonctions de contrôle d'accès protégé continu et de commande, des fonctions de contrôle et de commande de mots-clés et de contenu, et assure l'authentification d'accès éloigné, des évaluations de vulnérabilité coordonnées ainsi que des ajustements synchrones automatiques par rapport à la Politique de Sécurité, en réponse aux résultats de l'évaluation de

vulnérabilité. De plus, les opérations, les résultats d'évaluation et les réponses du coupe-feu et du scanneur peuvent être consolidés dans des rapports détaillés ou synthétiques à utiliser par les administrateurs de la sécurité, pour l'analyse des tendances et la prise de décision en matière de sécurité.

Cette solution propose une analyse des vulnérabilités des équipements afin d'adapter la politique de sécurisation en fonction de celles-ci.

On connaît également, par le brevet américain US 6 760 421 (Securelogix), un système et un procédé de gestion de ressources et de sécurité téléphoniques qui permettent de surveiller et/ou de commander et d'enregistrer l'accès à un réseau téléphonique public commuté entre des stations d'utilisateurs finaux d'une entreprise et leurs circuits respectifs. Une politique de sécurité, constituée par exemple par un ensemble de règles de sécurité, est définie pour chacun des postes, ces règles spécifiant des actions à entreprendre sur la base d'au moins un attribut de l'appel sur le poste. Les appels sont détectés sur les postes pour déterminer les attributs associés à chaque appel. Les actions sont ensuite exécutées sur l'appel sélectionné sur la base de leurs attributs en fonction des règles de sécurité définies pour ces postes.

L'art antérieur connaît également, par la demande de brevet américain US 2004 / 0 161 086 (Securelogix), un système et un procédé de gestion et de sécurisation des ressources téléphoniques pour visualiser et contrôler les appels entrants et sortants entre les terminaux d'une entreprise et un réseau public commuté en mode circuit et/ou un réseau public commuté en mode paquet. Une politique sécuritaire est constituée d'une ou plusieurs

règles désignant au moins une action à réaliser sur la base d'au moins un attribut de l'appel entrant ou sortant. Les appels sont détectés, captés sur la ligne et analysés pour déterminer les attributs associés à chacun de ces appels. Des actions sont menées sur la base de ces attributs déterminés en accord avec les règles de politique de sécurisation.

Les solutions apportées par ces documents réalisent une analyse des « couches basses » des protocoles de communication (couches 1/2/3 du modèle OSI) sur un réseau commuté de télécommunications en déterminant la nature des appels (type fax, type voix, numéro appelé, ...). Elles ne permettent pas de protéger le réseau contre d'éventuelles attaques utilisant les fonctionnalités (« couches hautes » applicatives, par exemple le renvoi d'appel, la conférence) offertes par l'autocommutateur et leurs failles.

En effet, les analyseurs de communication délivrent les informations suivantes :

- la nature de l'appel : Fax modem ou voix ;
- l'heure de début et de fin de la communication ;
- le numéro de l'appelant et de l'appelé ;
- la voie et le lien utilisés pour la communication.

L'analyseur de communication ne délivre pas l'ensemble des fonctionnalités qui ont été mises en œuvre ni leur chaînage. Les deux exemples suivants dénotent les limitations d'un tel système quant à la détection d'actions « frauduleuses ».

Exemple 1 :

Une communication d'un appel extérieur A vers un poste B de l'entreprise renvoyé immédiatement sans sonnerie vers un poste C extérieur à l'entreprise.

L'analyseur va observer l'appel de A vers B puis de B vers C sans observer qu'il s'agit de la même communication. Ce n'est qu'avec l'analyse des fonctionnalités mises en œuvre pour cet appel que l'observation pourra être établie

Exemple 2 :

Une communication d'un appel extérieur A vers un poste de l'entreprise B peut écouter la conversation avec un interlocuteur C par l'activation de la fonctionnalité « entrée en tiers discrète ». Là encore l'analyseur de communication ne détectera que deux communications séparées et autorisées.

De plus, la convergence des réseaux commutés (RNIS par exemple) et en mode paquets (réseau IP) voit l'apparition des autocommutateurs mixte « commuté-IP ». Aucune solution n'a encore été apportée pour l'analyse des communications, du type voix sur IP (VoIP), en entrée d'un autocommutateur mixte.

La présente invention entend remédier aux inconvénients de l'art antérieur en proposant un système et un procédé de sécurisation d'un autocommutateur, soit en mode commuté, soit mixte « commuté-IP », sur la base d'une analyse des couches « basses » (nature de l'appel) et « hautes » (fonctionnalités de l'autocommutateur utilisées) mises en œuvre lors des appels.

Le procédé effectue, d'une part, une analyse des appels entrants ou sortants afin de déterminer leur nature, et d'autre part, reçoit des informations émises par l'autocommutateur, informations indiquant, entre autres, les fonctionnalités mises en œuvre pendant l'appel. Une comparaison est effectuée avec un ensemble de règles de sécurité du réseau (ou scénarii), le procédé permettant alors de donner suite à l'appel ou de le terminer.

Dans ce dessein, le système de l'invention dispose d'un analyseur de communication quelque peu semblable en termes fonctionnels à ceux décrits dans les brevets susmentionnés, et associé à un serveur ainsi qu'un second serveur analysant les informations émises par l'autocommutateur sur les appels en cours.

Le système propose également un serveur dit « d'audit » permettant d'établir des règles de sécurité en fonction des spécificités du réseau et de l'autocommutateur.

Le procédé et le système selon la présente invention répondent particulièrement bien aux attentes des entreprises dont les réseaux privées sont de trop nombreuses fois piratés par l'utilisation d'une des 400 fonctionnalités ou plus de l'autocommutateur (par exemple, l'appel en conférence ou *conference call*).

A cet effet, l'invention concerne dans son acception la plus générale un système pare-feu de sécurisation d'un autocommutateur d'entreprise connecté, d'une part, à au moins un réseau de communication en mode commuté, de type PSTN, et, d'autre part, à un ensemble de périphériques de communications et/ou de serveurs d'application, ledit système comprenant un analyseur de communication des couches basses (1 à 3) du modèle OSI de communications numériques en mode circuit et analogiques, un serveur pare-feu connecté au dit analyseur,

caractérisé en ce que :

- ledit système comprend, en outre, un serveur de supervision connecté à la sortie « fil de l'eau » de l'autocommutateur pour l'analyse des tickets de communication et l'application de règles sécuritaire portant sur les couches hautes (4 à 7) du modèle OSI.

De préférence,

- ledit autocommutateur est, en outre, relié à un réseau de communication en mode paquet, de type l'Internet ;
- ledit analyseur de communication est placé en parallèle des lignes entre l'autocommutateur et les réseaux commutés et en mode paquets ;
- ledit analyseur de communication analyse, en outre, les informations des couches basses des communications en mode paquet (entrantes et sortantes) de l'autocommutateur.

Avantageusement, ledit analyseur est un DSP permettant la détection des communications numériques circuits, numériques paquets et analogiques.

Selon un mode de réalisation, ledit serveur de supervision comprend un système expert pour l'apprentissage de règles sécuritaires dans le cas d'un scénario inconnu.

Selon une mode de mise en œuvre particulier, ledit serveur de supervision comprend une base de données pour stocker les informations remontées par ledit analyseur de communication et les informations relatives à l'analyse desdits tickets.

De préférence, ledit système comprend, en outre, un serveur d'audit connecté au serveur de supervision apte à analyser les fonctionnalités de l'autocommutateur, l'architecture système et à établir un ensemble de scénarii d'appels.

Avantageusement, ledit serveur d'audit comprend un système expert pour l'établissement desdits scénarii.

Selon un mode de réalisation, ledit serveur pare-feu est connecté à une pluralité d'analyseurs de communications situés sur divers sites d'entreprise.

Selon un mode de réalisation particulier, ledit système comprend, en outre, un serveur de sauvegarde cryptée des configurations de l'autocommutateur.

Selon une variante, ledit système comprend, en outre, un modem *call-back* connecté au port de télémaintenance dudit autocommutateur.

L'invention concerne également un procédé de sécurisation d'un autocommutateur d'entreprise connecté, d'une part, à au moins un réseau de communication en mode commuté, de type PSTN, et, d'autre part, à un ensemble de périphériques de communications et/ou de serveurs d'application, le procédé comprenant une étape d'analyse des couches basses (couches OSI 1 à 3) des communications par un analyseur de communication et d'application de règles de sécurité pour mettre fin aux appels illicites,

caractérisé en ce qu'il comprend, en outre, :

- une étape de récupération par un serveur de supervision des tickets de communication émis par l'autocommutateur,
- une étape de confrontation des informations contenues dans lesdits tickets aux règles de sécurité contenant dans le serveur de supervision,
- une étape d'application des règles de sécurité en fonction de ces informations contenues dans lesdits tickets.

De préférence, ledit procédé comprend, en outre, une étape de remontée des informations d'appels et de décisions

prises depuis ledit analyseur de communication vers ledit serveur de supervision.

Avantageusement, ledit procédé comprend, en outre, une étape d'auto-apprentissage par un système expert dans le serveur de supervision des scénarii non gérés par les règles sécuritaires.

De préférence, ledit procédé comprend, au préalable, une étape de détermination des scénarii possibles par un serveur d'audit et une étape d'établissement des règles sécuritaires par sélection desdits scénarii.

Selon un mode de réalisation, ladite étape de détermination des scénarii comprend :

- une étape de récupération des fichiers de l'architecture circuit par ledit serveur d'audit auprès de l'autocommutateur et des fichiers de l'architecture système ;
- une étape de détermination des risques et contre-mesures associées à partir desdits fichiers récupérés.

L'invention concerne également un élément de programme d'ordinateur comprenant des moyens de code de programme d'ordinateur organisés pour accomplir les étapes du procédé.

On comprendra mieux l'invention à l'aide de la description, faite ci-après à titre purement explicatif, d'un mode de réalisation de l'invention, en référence aux figures annexées :

- la figure 1 représente l'architecture standard des systèmes de sécurisation d'autocommutateur sur réseau téléphonique commuté (*art antérieur*) ;

- la figure 2 illustre l'architecture de la présente invention ;
- la figure 3 illustre la structure fonctionnelle de l'analyseur de communication ;
- la figure 4 est un diagramme logique représentant le fonctionnement de l'analyseur de communication ;
- la figure 5 est un diagramme logique illustrant l'établissement des règles sécuritaires selon la présente invention ;
- la figure 6 illustre les différentes tables de données initiales récupérées par le système expert d'analyse ;
- la figure 7 illustre un exemple de matrice de correspondances entre les menaces et les vulnérabilités d'un système de type autocommutateur ;
- la figure 8 illustre un exemple de matrice de correspondances entre les menaces et les fonctionnalités fournies par un autocommutateur ;
- la figure 9 illustre de façon logique le module d'audit et de contre-mesures selon la présente invention ;
- la figure 10 représente schématiquement le moteur d'inférence pour l'audit du système ;
- la figure 11 représente schématiquement le module d'établissement des contre-mesures ;
- la figure 12 représente un diagramme logique du fonctionnement de la sécurité selon l'invention ; et
- la figure 13 illustre un exemple de communication en mode paquets.

L'invention va être décrite à l'aide d'exemples de modes de réalisation. Il est entendu que ces exemples ne sont pas limitatifs de l'invention et qu'un homme du métier

serait à même de réaliser cette invention sous différentes variantes.

ARCHITECTURE ET DESCRIPTION DES DIFFÉRENTS MODULES

La figure 2 représente un exemple de réalisation du système selon la présente invention, comprenant un autocommutateur (200), un analyseur de communication (100) et un ensemble de serveurs (110, 120 et 130) pour la gestion de la politique sécuritaire.

L'autocommutateur (200) d'entreprise est un autocommutateur permettant le traitement et la commutation en temps réel d'appels entre les périphériques (210) privés de l'entreprise et le réseau téléphonique commuté (300) et/ou un réseau en mode paquets, par exemple l'Internet (310). L'autocommutateur (200) fournit, en outre, des fonctionnalités (parfois plus de quatre cents) pouvant être mises en œuvre lors des appels : par exemple, le double appel, le renvoi d'appel, la conférence, … Il présente également deux ports dédiés, d'une part, à la télémaintenance (198) et, d'autre part, à l'envoi (199) de « tickets » utilisés, entre autres, à la facturation des appels. Ce dernier port (199), aussi appelé port « au fil de l'eau » est un port série d'émission de données, les tickets. Ceux-ci contiennent de nombreuses informations sur les appels commutés par (200). Une description plus détaillée est fournie ci-après.

Les fonctions essentielles d'un autocommutateur sont : la commutation, les interfaces avec les terminaux, l'application téléphonique. L'autocommutateur (200) peut être de type PBX (*Private Branch eXchange*) ou PABX (*Private Automatic Branch eXchange*) dédié uniquement à un réseau commuté, auquel cas l'analyse des communications en mode paquets n'est pas réalisée, ou « mixte », par exemple un

PABX-IP centralisé dans lequel sont mises en œuvre toutes les fonctions exceptée la commutation réalisée par un *switch* (commutateur) réseau. Dans la suite de la description, nous utiliserons de façon non restrictive le terme de PABX pour l'autocommutateur (200) qu'il soit dédié au réseau commuté ou « mixte ».

Le réseau d'entreprise peut être du type LAN (*Local Network Area*) et est composé du PABX (200), des périphériques (210) et des lignes intérieures (220) reliant les périphériques au PABX.

Les périphériques sont de type fax (203), modem (202), téléphone (204), téléphone IP (205), téléphone sans-fil (206), par exemple DECT, serveurs d'applications (208) par exemple serveur boîte vocale, serveur de facturation, …, ou serveurs d'administration (209) des autocommutateurs.

Les serveurs « de téléphonie » (208) et (209) sont reliés, en outre, au PABX par un réseau IP (230) isolé dédié uniquement à l'échange de données entre ces diverses entités : pilotage du PABX depuis le serveur d'administration, par exemple.

Toujours en référence à la figure 2, un analyseur de communication (100) est placé en parallèle des lignes réseaux (320) entre le réseau public commuté/en mode paquets (300, 310) et le PABX (200).

Un serveur pare-feu (110) est relié à l'analyseur de communication (100) et éventuellement à d'autres analyseurs (100', 100''). Le serveur pare-feu (110) contient l'ensemble des règles ou scénarii à appliquer sur le réseau et les transmets aux analyseurs de communication. Une description plus détaillée d'un tel serveur peut être fournie par l'un des documents US 6 687 353, US 6 226 372, US 6 760 421 et US 204 / 0 161 086 mentionnées précédemment. Le serveur 110 consolide en temps réel

l'ensemble des informations de l'ensemble des analyseurs de communication des différents sites et gère les alertes liées aux dysfonctionnements éventuels de ces analyseurs.

Un serveur de supervision (120) est relié au port « au fil de l'eau » (199) du PABX, au serveur pare-feu (110) et à un troisième serveur d'audit (130). Ce serveur (120) assure le management des analyseurs de communication (100) et la gestion des règles de sécurité. Les serveurs 110 et 120 doivent être physiquement différents pour des raisons de traitement temps réel et de sécurité de fonctionnement.

Le serveur d'audit (130) héberge un système expert permettant l'établissement des règles sécuritaires ou scénarii, règles qu'il transmet au serveur de supervision (120) pour application de celles-ci.

Ces différents serveurs sont par exemple des ordinateurs dédiés, comprenant un processeur, une mémoire vive de type RAM, un système d'exploitation, un logiciel pour la mise en œuvre du procédé de l'invention, logiciel exécuté sur ce système d'exploitation, et des moyens de connexion réseau.

Le système comprend également un dispositif de sauvegarde (112) et un modem de type *call-back* (114). Le dispositif (112) permet d'effectuer une sauvegarde, de préférence cryptée par clé dynamique, des configurations de l'autocommutateur. Le modem (114) fournit, quant à lui, une protection au niveau de l'accès au port de télémaintenance (198) en mettant en œuvre des mécanismes de détection d'appel, d'identification et de rappel en fonction de l'identification obtenue.

L'ANALYSEUR DE COMMUNICATION

Les fonctionnalités de l'analyseur de communication (100) sont illustrées par la figure 3.

Pour des questions de coûts, l'analyseur de communication (100) est réalisé sous forme de DSP (*Digital Signal Processing*) avec un logiciel adapté. Ceci permet, entre autres, de faire cohabiter aisément un analyseur de réseau en mode circuit (RNIS) et un analyseur de réseau en mode paquets (IP). L'art antérieur connaît ces analyseurs dédiés aux réseaux commutés. Dans un mode de réalisation de l'invention, l'analyse du réseau IP est faite par un filtre récupérant l'en-tête des paquets transmis.

Le procédé d'analyse des communications est fourni par la figure 4.

(1) : l'analyseur (100) reçoit des appels numériques en mode circuit (a), en mode paquets (b) et des appels analogiques (c).

(3) : un premier module (106) identifie le type d'appel (voix, données, …). Ce module se base sur la récupération des en-têtes des paquets transmis, sur la signalisation du canal D des communications numériques commutées (RNIS T0 et T2) ou sur la valeur des porteuses pour les liens analogiques.

(4) : dans un second module (105), les caractéristiques de l'appel sont comparées avec les règles de communications transmises par le serveur pare-feu (110) par l'intermédiaire de l'unité centrale (108) de l'analyseur.

En dehors des règles génériques liées à la sécurité du système (décision d'autoriser ou d'interdire tous les appels en cas de défaillance de l'analyseur de communication 100), les règles dites acquittées sont les règles en provenance uniquement du serveur d'audit (130)

qui a en charge le contrôle de cohérence de l'ensemble des règles. Le comportement par défaut autorise les appels qui ne sont pas explicitement interdits et lorsqu'une des règles coïncide avec la communication en cours, la règle s'applique.

L'ensemble des règles qui ne font intervenir que les informations recueillies par l'analyseur de communications (100) est résident dans celui-ci pour le site concerné ; ceci afin d'assurer un traitement en temps réel (suffisamment rapide au regard du temps de connexion des communications). Ces règles y sont stockées soit en mémoire *Flash*, soit sur disque dur, suivant le nombre de liens à observer. Les règles de sécurité sont envoyées par le serveur de supervision (120) via le serveur (110). Un exemple d'analyseur de communication (100) est un des produits de la gamme « Wavetel ». Le serveur pare-feu (110) est le garant des règles relatives aux couches 1-2-3 et contrôle périodiquement l'intégrité des données des analyseurs de communication pour prévenir d'éventuelles modifications malicieuses au niveau de ces derniers.

S'en suit le traitement (104) de l'appel en fonction de ces règles. Soit l'appel est autorisé, soit il est autorisé avec des restrictions de plage horaire, de numéros, de destinations soit il est terminé par une procédure de raccrochage (5). Cette procédure s'effectue, pour les différentes natures de liens de la manière suivante :

- pour les liens numériques « circuits », s'il existe un lien API au niveau du PABX alors est générée une commande de coupure de la communication en cours. Sinon, on réalise un brouillage de la communication par l'entrée en tiers avec annonce du modem de l'analyseur de communication

(100) connecté sur un joncteur de poste analogique jusqu'au raccroché par l'utilisateur,

- pour les liens numériques « paquets », un comportement « *Firewall data* » est appliqué par blocage de l'appel après extraction et analyse de l'en-tête IP au niveau RTP ou RTCP dans le cas de figure d'une communication utilisant un protocole de communication H323, au niveau SDP dans le cas d'une communication utilisant le protocole de communication SIP et/ou MGCP, ces couches permettant l'identification des codecs (G711 à G729), du protocole fax (T30, T38) ou du protocole modem (G723.1). L'appel sera bloqué soit par la commande « *Cancel* » au niveau de la signalisation pour SIP, soit par la commande « *Reject* » du protocole H245 pour H323, soit par la commande « *DeleteConnection* » pour MGCP.

- pour les liens analogiques, on réalise une coupure par micro-relais.

L'analyse est réalisée en boucle tant que l'appel n'a pas pris fin. Une fois cet appel terminé, les informations de l'appel sont remontées (6) vers le serveur pare-feu (110), puis envoyées à travers un « pipe de communications » vers le serveur de supervision (120) en temps réel.

L'exemple suivant concerne l'analyse des paquets émis sur le réseau dans le protocole H.323.

Exemple 1 : Analyse du protocole H.323

La figure 13 illustre d'une part, les couches sur lesquelles repose le protocole H.323 et d'autre part, le format de l'en-tête RTP (*Real-time Transfert Protocol*) utilisé pour la voix sur IP sur le protocole H.323. L'analyseur de communication analyse l'en-tête RTP contenu dans la trame UDP ou TCP afin de déterminer la nature de la communication en prenant en compte dans cet en-tête, la

valeur « *Payload Type* ». Dans l'exemple fourni, il s'agit d'une communication G711 encore appelé PCMA.

LE SERVEUR D'AUDIT

Illustré par la figure 5, le serveur d'audit (130) permet la mise en place des scénarii de sécurisation du réseau, scénarii qui seront choisis par un opérateur humain pour l'établissement des règles de sécurité.

ANALYSE FONCTIONNELLE

Une première étape est réalisée avant l'exploitation du système. Elle vise à déterminer les caractéristiques fonctionnelles du PABX (200) qui changent d'un fabricant à l'autre (1010) et les spécificités de l'architecture réseau en place (1020). Les opérations décrites ci-après sont reproduites après une mise à jour du PABX ou après une modification de l'architecture du réseau (ajout de périphériques par exemple), c'est pourquoi il est préférable que le serveur d'audit (130) ne partage pas les mêmes ressources que le serveur de supervision (120).

Lors d'une phase préliminaire avant la mise en exploitation du système, le serveur (130) est connecté au port de maintenance V24 (198) du PABX pour obtenir les fichiers d'architecture circuit (1020) contenus dans le PABX ainsi qu'au réseau IP (230) pour obtenir les informations d'architecture système (1010). Une application du type NESSUS permet d'obtenir par le réseau IP (230) l'ensemble des informations IP du réseau : VLAN, adresses IP, nombre de serveurs d'application, …

Les fichiers architecture circuit mentionnent les configurations des liens internes (annuaire des numéros de téléphone) et des liens externes (T0, T2, voix IP pour la voix).

La figure 6 représente un exemple des bases de données de configurations (1000) obtenues par le serveur

d'audit (130) après analyse du système (1010) et des circuits (1020).

La base de données des liens extérieurs renseigne :

- la nature des liens (RNIS TO ou T2, analogique IP) ;
- s'il s'agit d'un Intranet ;
- le type de flux (entrant, sortant, mixte) ;
- le nombre de voies ;
- le débit effectif.

La base de données des liens internes renseigne :

- le numéro de téléphone ;
- s'il possède une SDA (sélection directe à l'arrivée) ou non ;
- la nature du liens (analogique, numérique, IP) ;
- le type de périphérique (téléphone, modem, fax).

La base de données système renseigne :

- les éléments présents (PABX, messagerie vocale, serveur de facturation) ;
- la version du système d'exploitation ;
- les mises à jour ;
- les mots de passe ;
- les ports de communication ;
- l'adresse logique ;
- l'adresse physique.

La base de données des fonctionnalités du PABX renseigne :

- les numéros de téléphone ;
- les profils ou classes associés ;
- les fonctionnalités ouvertes sur chacun des numéros de téléphone (renvoi, conférence, groupement) ;
- les restrictions associées.

Préalablement, est effectuée une étape de définition des attributs et des valeurs correspondantes mis en œuvre par le PABX (200) (en fonction du constructeur), par exemple :

Valeurs_services_associées : mevo (messagerie vocale), Svi, Acd, taxation… ;

Valeurs_états_logiciels : mise à jour, mot de passe, ports communication ouverts ;

Valeurs_architecture : Vlan, indépendant, QoS ;

Valeurs_télémaintenance : sda, mot de passe, ip, v24, call back ;

Valeurs_sauvegardes : crypté, périodique ;

Valeurs_mobilité : borne ouverte, Dect, Wifi ;

Valeurs_fonctionnalités : opérateur, interphonie, multi Cco, multisociété, Disa, conférence, enregistrement, entrée en tiers, transfert, renvois, écoute, groupement, Sda… ;

Valeurs_restrictions : horaires, géographique, plage numéros, accès prioritaire, verrouillage logique…

Toujours en référence à la figure 5, une analyse des différentes vulnérabilités (1100) du PABX par rapport à ces valeurs permet de distinguer trois principaux types de vulnérabilités : les vulnérabilités d'accès (possibilité d'accès au système et aux données contenues à l'intérieur), celles de création/modification/suppression (cms) (possibilité d'interagir avec le système et les données associées) et celles de récupération (possibilité de récupérer l'action qui se passe).

La base de données des règles (1110) contient, quant à elle, l'ensemble des règles de sécurité appliquées par le système. Cette base est généralement vide à l'installation

du système et s'enrichit à l'issue de cette phase d'audit du système. Les règles sont sous la forme :

Si *(nom unité opérateur valeur) et ... et (nom_de_plusieurs_mots opérateur valeur)*

Alors *(nom = valeur) et .. et (nom = formule)*

Voici deux exemples de règles :

Exemple 2

Si *Valeurs_services_associés = (messagerie vocale, mot de passe standard, sda)* ***et*** *Valeurs_fonctionnalités = (rappel automatique après dépôt de message, numéro extérieur)* ***et*** *Valeur_architecture = (liens extérieurs,pas de restriction)*

Alors *risque = (écoute)*

Cet exemple illustre le risque de subir une écoute téléphonique mise en œuvre en utilisant les faiblesses du système en matière de rappel automatique d'un numéro extérieur après le dépôt de message dans une messagerie vocale.

Exemple 3

Si *valeur_télémaintenance = (mot de passe constructeur, numéro sda, pas de restriction)* ***et*** *valeur_fonctionnalités = (renvoi extérieur)* ***et*** *valeur_architecture = (liens extérieurs, pas de restriction)*

Alors *risque = (détournement de trafic)*

Cet exemple illustre le détournement de trafic de communication en utilisant le renvoi extérieur d'une communication rendu possible par l'obtention du mot de passe constructeur…

Egalement, la méthode EBIOS permet d'établir, indépendamment de l'architecture du réseau d'entreprise, une matrice caractérisant les dépendances entre menaces et vulnérabilités du PABX (200), et une matrice caractérisant

les dépendances entre les menaces et les fonctionnalités offertes par le PABX.

La figure 7 représente un exemple de matrice « menaces / vulnérabilités » où les menaces sont du type *espionnage industriel* ou *détournement de trafic*, et les vulnérabilités peuvent être la *possibilité d'accéder directement à un poste* ou la *possibilité d'effacer ou modifier des programmes*.

La figure 8 représente un exemple de matrice « menaces / fonctionnalités » où les fonctionnalités fournies par le PABX (200) peuvent être la *numérotation abrégée commune*, le *renvoi* ou encore le *groupement*.

Ces matrices peuvent être remplies manuellement, c'est-à-dire que les dépendances sont établies en fonction de la connaissance du matériel et de la sécurité du réseau.

MOTEUR EXPERT - INFERENCE ET CONTRE-MESURES

Chacune des configurations système/circuit (1000) définies précédemment est confrontée aux informations de menaces, vulnérabilités et règles établies pour évaluer les risques de cette configuration et les contre-mesures adéquates contre cette situation. Une représentation schématique de ce système expert est fournie en figure 9 dont les modules SCN1 (1120) et SCN2 sont illustrés par les figures 10 et 11.

Ce système expert est contenu dans le serveur (130).

Un chaînage avant et arrière est réalisé entre les menaces et les vulnérabilités du système (selon la matrice définie précédemment) par le module SCN1 (1120). On entend par « chaînage avant et arrière » l'analyse consistant à partir d'une part de chacune des menaces (rôle symétrique des vulnérabilités) pour lui associer les vulnérabilités dépendantes et de boucler cette analyse par la vérification à partir des vulnérabilités déterminées de la menace

originelle. Une analyse successive des vulnérabilités **d'accès**, des vulnérabilités de **création/modification/suppression** et des vulnérabilités de **récupération**, permet d'établir les risques éventuels encourus par le système face à cette menace. Ces risques sont stockés dans une base de données.

Ces risques ont la forme suivante : « *vulnérabilités(accès) et vulnérabilités(Mcs) et vulnérabilités (Récup)* ***alors*** *Menace (xx)* », et permettent d'établir des contre-mesures. Ces nouvelles contre-mesures ou scénarii tiennent compte de ceux déjà existants (base de données des contre-mesures 1210) et sont réalisés par le module SCN2 illustré par la figure 11.

Un classement des risques permet de déterminer les cas à autoriser, ceux à interdire et enfin ceux à autoriser avec restriction (plage horaire, géographique, ...) : ce sont les scénarii. Les risques sont classés suivant deux critères.

Un classement selon les quatre grandes familles de risques :

- les risques liés au détournement de trafic,
- ceux liés à l'écoute,
- ceux liés à l'usurpation (la fonction *sqatt*, par exemple, permet de récupérer l'ensemble des caractéristiques d'un autre poste y compris son numéro de téléphone),
- ceux liés au déni de service (scénario permettant l'introduction d'un élément malin dans le logiciel du système).

Puis, à l'intérieur de ces familles, est effectué un classement par ordre de facilité suivant la règle : *moins un scénario comporte d'item plus il est facile à mettre en œuvre*.

En conséquence et suivant la politique de sécurité de l'entreprise, il s'agira d'interdire au maximum ce qui parait le plus dangereux.

Une intervention humaine permet de choisir les contre-mesures définissant la politique de sécurité du PABX (200) :

- exemples concernant les vulnérabilités d'architecture : supprimer les liens inactifs, modifier les numéros de télémaintenance s'il répondent aux standards constructeurs, réorganiser l'annuaire... compte tenu des proposition faites par le système expert ;

- exemples concernant les fonctionnalités fournies par le PABX : les contre-mesures relatives aux scénarii de risques se présentent sous la forme de choix, car il ne peut être question de supprimer l'ensemble des fonctionnalités ouvertes, par définition du rôle du PABX. Il s'agira de limiter les scénarii et de surveiller ceux qui n'ont pas pu être éradiqués, par exemple, *supprimer le scénario en interdisant le ou les fonctionnalités mises en cause, autoriser les fonctionnalités et surveiller leur usage* ou encore, *restreindre les fonctionnalités par plage horaire, par plage de numéros, par destination, ... ;*

- exemples concernant les périphériques : autoriser ou restreindre un périphérique, un groupe de périphérique, un numéro de téléphone, ... un type de périphérique. Une itération du système expert se déroulera pour, en temps réel, vérifier que le couple fonctionnalités/périphérique ne crée pas de nouveau scénario de risque ;

- gestion d'accès logiques et de mis à jour suivant les recommandations du module « Audit » ou aménagement avec itération du système expert. Ceci s'explique, par exemple, par le fait qu'il existe dans chaque composant du système de communication d'entreprise un certain nombre de ports

logiques de communications ouverts. Certains ne servent pas et il est alors recommandé de les fermer quitte à les rouvrir en cas de nécessité. Par exemple, pour un PABX de type Alcatel, vingt ports sont ouverts en configuration standard et la moitié d'entre eux servent uniquement à l'installation du système.

De plus, les bases de données des règles (1110), des vulnérabilités (1100) et des contre-mesures (1210) sont mises à jour lors la création des nouveaux scénarii.

Voici l'établissement de contre-mesures en référence aux deux exemples 2 et 3 susmentionnés.

Exemple 3 : détournement de trafic

Un détournement peut provenir de la combinaison des vulnérabilités suivantes :

Vulnérabilité d'accès concerne la *valeur_télémaintenance* (mot de passe constructeur, numéro SDA, pas de restriction)

Vulnérabilité de « cms » concerne la *valeur_fonctionnalités* (renvoi extérieur, pas de restrictions)

Vulnérabilité de récupération concerne la *valeur_architecture* (liens extérieurs, pas de restriction)

La règle de risque alors établie devient :

Si *valeur_télémaintenance*(mot de passe constructeur, numéro sda, pas de restriction) **et** *valeur_fonctionnalités*(renvoi extérieur) **et** *valeur_architecture*(liens extérieurs, pas de restriction)

alors risque(détournement de trafic)

Les contre-mesures proposées sont alors :

Valeur_télémaintenance (mot de passe constructeur)	Interdire	Changement mot de passe
		Gestion mot de passe
		Modem call back
	Autoriser	Surveiller

		Débrancher modem
		Numéro hors SDA
	Restreindre	Surveiller
		Modem call back
		Numéro hors SDA
Valeur_fonctionnalités (renvoi extérieur)	Autoriser	Surveiller
	Interdire	Supprimer la faculté
	Restreindre	N° téléphone, Classe
		Géographique
		Plage horaire
		Surveiller
Valeur_architecture (liens extérieurs, pas de restriction)	Autoriser	Surveiller
	Restreindre	Possible selon modèle

Ce scénario peut se produire fréquemment car le hacker externe peut, à travers un « *war-dialer* » (programme qui permet à partir d'une série de numéros de téléphone de lancer massivement des appels pour identifier une porteuses modem ou fax et d'autoriser l'entrée dans un système informatique ou télécom), identifier le modem de télémaintenance, par Internet trouver les mots de passe constructeur, accéder et activer la fonctionnalité renvoi ou détourner le trafic à son compte.

Pour déterminer ces scénarii, le moteur de règles utilise les matrices de correspondance évoquées précédemment afin :

- d'identifier toutes les vulnérabilités d'accès (Ports maintenance et télémaintenance mal protégés, postes non protégés, fonctionnalités d'accès ouvertes (DISA), etc.),
- d'identifier toutes les vulnérabilités autorisant la création-suppression-modification des facilités

répondant aux menaces (renvoi, transfert, DISA, conférence, etc.),

- d'identifier toutes les vulnérabilités permettant de récupérer l'action précédemment mise en œuvre répondant à la menace (liens extérieurs, serveurs associés, etc.).

Exemple 2 : écoute

Les vulnérabilités du système quant à l'écoute concernent :

Accès : *valeurs_services_associés* (messagerie vocale, mot de passe standard, sda),

Cms : *valeurs_fonctionnalités* (rappel automatique après dépôt de message, numéro extérieur),

Récupération : *valeur_architecture* (liens extérieurs, pas de restriction).

La règle de risque alors établie devient :

Si *Valeurs_services_associés* (messagerie vocale, mot de passe standard, sda) **et** *Valeurs_fonctionnalités* (rappel automatique après dépôt de message, numéro extérieur) **et** *Valeur_architecture* (liens extérieurs, pas de restriction) **alors** risque(écoute)

Les contre-mesures proposées sont alors :

Valeurs_services_associés (messagerie vocale, mot de passe standard, Sda)	Autoriser	Surveiller
		Gestion mot de passe
	Interdire	Supprimer Mevo
	Restreindre	Plage horaire
		Rendre inaccessible depuis l'extérieur
		Gestion mot de passe
		Restreindre les N° appelant si possible

Valeurs_fonctionnalités (rappel automatique après dépôt de message, numéro extérieur)	Autoriser	Surveiller
	Interdire	Supprimer la fonctionnalité
	Restreindre	Restreindre les N° appelé si possible
Valeur_architecture (liens extérieurs, pas de restriction)	Néant	

ANALYSE ET APPLICATION POLITIQUE SECURITAIRE

L'étape d'audit a permis d'établir les configurations et instructions (règles) nécessaires à l'application de la sécurité des transactions, communications passant par le PABX.

Comme illustrées par la figure 12, les règles établies sont triées selon leur domaine d'application : celles concernant les « couches basses » de communication (couche OSI 1-3) sont transmises à la base de données du serveur pare-feu (110) via le serveur de supervision (120), celles concernant les « couches hautes » (applicatives OSI 4-7) et les fonctionnalités du PABX sont transmises à la base de données du serveur de supervision (120).

Certaines règles affectent de façon permanent le PABX : elles sont donc directement paramétrées dans la base de données du PABX, automatiquement et/ou manuellement. Les autres règles sont comparées sur le serveur de supervision (120) avec les tickets de communications émis sur le port « au fil de l'eau » (199) du PABX.

TICKETS

A chaque appel, est généré un ticket de communication comportant 128 octets. Ces tickets sont généralement utilisés pour la facturation des appels.

Dans le cadre de la présente invention, le ticket fournit, entre autres, les informations suivantes :

- Numéro appelant
- Numéro appelé

- Date
- Heure de début d'appel
- Heure de fin d'appel
- Numéro intermédiaire
- Numéro T2/T0
- Voie
- IP
- Opératrice
- Interface (numérique, analogique, IP)
- Site
- Fonctionnalités mises en œuvre
- Nom de l'annuaire

Un contrôle de cohérence entre les informations contenues dans le ticket et la base de données du PABX est effectué: une alerte est levée en cas d'incohérence, et l'appel peut être terminé. C'est, par exemple, le cas lorsque pendant une reconfiguration manuelle du PABX, tous les nouveaux paramètres édités par le module audit n'ont pas été introduits dans le PABX (pas de mise à jour de l'annuaire, oubli d'interdire une fonctionnalité pour un poste, etc…). Ce contrôle permet de limiter les appels aux possibilités fournies et autorisées (les paramètres) par le PABX.

Les données issues de cette analyse sont remontées avec les informations des tickets de communications au serveur de supervision (120). Les informations concernant l'appel en cours sont combinées avec les alertes remontées du serveur pare-feu (110) d'analyse couches OSI 1-3 (*BDD alertes firewall*) et comparées aux règles de sécurité du serveur de supervision (120). Une analyse complémentaire peut être effectuée ; elle confronte les données de l'appel en cours à un historique des derniers appels (*Fichier Tempo*

Attaques) pour établir s'il y a une attaque ou un non-respect de la politique de sécurité (selon des modèles d'attaques types).

Cet historique peut être sous la forme d'un fichier renseignant les cent derniers appels traités par le PABX et leurs caractéristiques (poste appelé, sonnerie inférieure à 4 coups, absence de réponse, poste appelant extérieur, ...). L'objectif de cette historisation est d'être capable de déterminer les attaques répétées.

La supervision en temps réel du système de communication de l'entreprise repose sur une analyse des tickets du trafic, la surveillance et la supervision des fonctionnalités mises en œuvre par un appel et qui présentent des vulnérabilités, la surveillance et l'alerte dans le cas où un scénario de risque est en train de se produire, l'auto-apprentissage des scénarii non envisagés et qui se produisent et enfin la veille en détection d'attaques par le rapprochement d'informations, par exemple :

- Nombre d'appels inférieurs à 4 et raccrochés comparé à la moyenne. Analyse de l'écart type avec seuil de déclenchement,
- Nombre d'appels tels que ci-dessus et analyse si le phénomène se déroule de manière séquentielle ou aléatoire, avec indication des temps entre chaque appel de cette nature et seuil de déclenchement,
- Nombre d'appels répondus au travers de la messagerie vocale et détectés comme étant des appels de type modem.

Un algorithme de pondération, aux vues de ces informations, établira la présence ou non d'une attaque et mettra en œuvre la procédure d'alerte et d'action établie auparavant.

Lorsqu'une attaque, un non-respect de la politique sécuritaire, un nouveau scénario de risques est détecté, un traitement des contre-mesures adéquates est effectué.

Exemple 4

Si une attaque se présente, la décision peut être prise de couper tous les liens extérieurs si l'évènement se passe lors d'une période pendant laquelle l'entreprise est fermée (la nuit).

Exemple 5

En cas de non-respect de la politique sécuritaire, le numéro de téléphone intérieur concerné peut être inactivé.

Exemple 6

En cas de mise à jour d'un nouveau scénario de risque, le PABX est reconfiguré en prenant en compte ce risque.

Dans le cas où la configuration de l'appel en cours n'est prise en charge par aucun scénario, un système expert, similaire à celui décrit ci-dessus, permet l'auto-apprentissage du système. Un nouveau risque est déterminé, des scénarii éventuellement proposés et un opérateur humain détermine les scénarii correspondants à la politique de sécurité. Cet apprentissage se fait par chaînage flou : on analyse les scénarii les plus proches. Par exemple, un scénario ayant quatre critères sur cinq identiques à l'appel en cours est considéré comme proche.

- soit les scénarii proches sont cohérents entre eux, et un nouveau scénario est établi pour l'appel en cours,

- soit les scénarii ne sont pas cohérents entre eux, auquel cas une alarme est remontée, par exemple par email ou SMS, pour demander l'établissement d'une règle adaptée.

Le système permet également des remontées statistiques permettant entre autres de connaître le nombre

d'appels terminés, le nombre de tentatives d'accès frauduleux, …

Selon un mode de réalisation, l'invention consiste en un logiciel exécuté sur un système d'exploitation de type « Windows Serveur » (nom commercial) et les bases de données mises en œuvre sont de type SQL et plus tard sur des plateformes plus élaborés tel que « Oracle » (Nom commercial).

EXEMPLE D'UN SCÉNARIO

Voici un exemple de traitement de scénario d'appel frauduleux, depuis son origine jusqu'aux contre-mesures appliquées par le système.

La situation est la suivante :

1. Un pirate s'est introduit au travers du réseau IP data en profitant du fait que :

- le port de communication logique de l'autocommutateur est ouvert et pas de configuration VLAN pour le réseau Ethernet dédié aux serveurs téléphone,
- le *Firewall* Data autorise le port ftp 80 ce qui a permis de rentrer dans le PABX dont ce port est aussi rester ouvert,
- le pirate a ensuite introduit un exécutable qui lui donne la main sur le port télémaintenance,
- le mot de passe a été corrompu par un outil de « Crackage » car le mot de passe a été changé et n'est plus celui du constructeur.

2. Le pirate a ensuite créer un poste virtuel dans le PABX avec la fonction numérotation ouverte (il s'agit d'un poste où l'interface a été activé sans connecter un poste physiquement et qui lorsqu'il est sollicité compose l'indicatif de sortie vers le réseau et attend le numéro à composer).

3. Le pirate s'est attribué la fonction DISA (fonction qui permet à un poste extérieur à l'entreprise d'être perçu comme un poste de l'entreprise).

4. Le pirate a ensuite repéré des postes dit en groupement cyclique (un groupement cyclique est un groupe de poste qui possède un numéro interne générique commun, ce qui n'empêche pas ces postes d'avoir un numéro individuel, et qui pour chaque nouvel appel à ce groupement l'oriente vers le poste suivant libre appartenant au groupement).

5. La communauté des pirates a été prévenue des numéros à composer. Cette communauté est constituée de 50 membres dont un dispose d'un serveur vocal situé aux Bahamas avec une surfacturation du service (1 € la minute reversé par l'opérateur sur un compte en suisse).

6. Le pirate a activé un renvoi du groupement vers le serveur vocal situé aux Bahamas pendant les heures non ouvrées.

Le pirate a ainsi à sa disposition :

- un poste DISA qui lui permet d'être appelé et de transférer toutes les communications vers les destinations souhaitées par les appelants,
- de joindre le serveur vocal avec des mobiles anonymes (cartes prépayées) et de partager le gain lié au service surfacturé pendant les heures non ouvrées grâce au groupement de poste,
- de pouvoir appeler avec le poste fictif à n'importe quelle heure n'importe quelle destination sans être repéré car ce poste ne figure pas dans l'annuaire.

La facture peut être très salée pour l'entreprise et l'hémorragie ne pourra pas être stoppée aussi facilement car plusieurs actions ont été menées sans un lien manifeste.

Après installation du système pare-feu de sécurisation du PABX de l'entreprise, selon la présente invention :

- l'application « audit », grâce au module SCN1, par l'application des règles de vulnérabilité / menaces / risques, va mettre à jour les scénario suivants :

Vulnérabilités accès :

Valeurs_états_logiciels = (ports communication ouverts)

Valeurs_architecture = (Vlan)

Valeurs_télémaintenance = (IP)

Vulnérabilités (cms) :

Valeurs_fonctionnalités = (Disa)

Valeurs_fonctionnalités = (renvoi, groupement)

Valeurs_fonctionnalités = (poste fictif, appel au décroché extérieur temporisé)

Vulnérabilités (Récup) :

Valeur_architecture = (liens extérieurs, pas de restriction)

- Règles

A. **Si** Valeurs_états_logiciels = (ports communication ouverts) **et** Valeurs_architecture = (vlan) **et** Valeurs_télémaintenance = (ip) **et** Valeurs_fonctionnalités = (disa) **et** Valeur_architecture = (liens extérieurs, pas de restriction)

Alors risque = (Détournement de trafic)

B. **Si** Valeurs_états_logiciels = (ports communication ouverts) **et** Valeurs_architecture = (vlan) **et** Valeurs_télémaintenance = (ip) **et** Valeurs_fonctionnalités = (poste fictif, appel au décroché extérieur temporisé)

Alors risque = (détournement de trafic)

C. **Si** Valeurs_états_logiciels = (ports communication ouverts) **et** Valeurs_architecture = (vlan) **et** Valeurs_télémaintenance = (ip) **et** Valeurs_fonctionnalités = (renvoi, groupement)

Alors risque = (détournement de trafic)

- Dans le module SCN2, le logiciel classe ces risques :

Famille : Détournement de trafic

Difficulté croissante : A, C, B

- Contre-mesures retenues :

Ports communication ouverts : Autorisé le port 80 car utile pour les mises à jour et Patchs,

Vlan : Interdire l'absence de Vlan,

Poste fictif : restreindre le nombre de postes pouvant être créés et surveiller les numéros autorisés par le logiciel de supervision au travers des tickets et les afficher dans l'annuaire,

Appel au décroché temporisé : interdire,

Renvoi : interdire le renvoi extérieur pour tous les postes faisant partie d'un groupement sur le numéro du groupement,

Groupement : autoriser.

L'ensemble de ces données est ainsi enregistré dans la base de données « nouvelle configuration »

L'application « supervision » va trier les règles et les paramétrages soit vers le serveur pare-feu (110) soit vers le PABX.

Le paramétrage du PABX se fera manuellement car le PABX ne dispose pas d'interface API ou IAE dans notre exemple : l'opération mise en place d'un Vlan s'exécutera

par acquittement de la direction informatique et sa réalisation sera contrôlée et constatée lors du prochain audit automatique.

Pour le serveur pare-feu : aucune action prévue car les couches 1 à 3 du modèle OSI gérées par l'analyseur de communication ne sont pas sollicitées dans cet exemple.

Le contrôle de cohérence de la configuration se fera au fur et à mesure des appels et si une des facilités ci-dessus est retrouvée pour les postes incriminés et ne répond pas aux contre-mesures adoptées alors une alerte est levée pour correction.

Dans le traitement du « module expert », le scénario d'appel en cours sera comparé avec l'ensemble des scénarios de la base pour trouver un éventuel nouveau scénario proche ou original.

Le programme d'alerte « attaque » ne se déclenchera pas dans cet exemple.

L'appel sera stocké avec ses caractéristiques dans la base de données fil de l'eau.

L'invention est décrite dans ce qui précède à titre d'exemple. Il est entendu que l'homme du métier est à même de réaliser différentes variantes de l'invention sans pour autant sortir du cadre du brevet.

REVENDICATIONS

1. Système pare-feu de sécurisation d'un autocommutateur (200) d'entreprise connecté, d'une part, à au moins un réseau de communication en mode commuté, de type PSTN, et, d'autre part, à un ensemble de périphériques de communications et/ou de serveurs d'application (210), ledit système comprenant un analyseur de communication (100) des couches basses (1 à 3) du modèle OSI de communications numériques en mode circuit et analogiques, un serveur pare-feu (110) connecté au dit analyseur (100),

caractérisé en ce que :

- ledit système comprend, en outre, un serveur de supervision (120) connecté à la sortie « fil de l'eau » (199) de l'autocommutateur (200) pour l'analyse des tickets de communication et l'application de règles sécuritaire portant sur les couches hautes (4 à 7) du modèle OSI.

2. Système pare-feu selon la revendication précédente, caractérisé en ce que :

- ledit autocommutateur (200) est, en outre, relié à un réseau de communication en mode paquet, de type l'Internet,

- ledit analyseur de communication (100) est placé en parallèle des lignes entre l'autocommutateur (200) et les réseaux commutés et en mode paquets ;

- ledit analyseur de communication (100) analyse, en outre, les informations des couches basses des communications en mode paquet (entrantes et sortantes) de l'autocommutateur (200) ;

3. Système pare-feu selon la revendication 1 ou 2, caractérisé en ce que ledit analyseur (100) est un DSP

permettant la détection des communications numériques circuits, numériques paquets et analogiques.

4. Système pare-feu selon l'une des revendications 1 à 3, caractérisé en ce que ledit serveur de supervision (120) comprend un système expert pour l'apprentissage de règles sécuritaires dans le cas d'un scénario inconnu.

5. Système pare-feu selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit serveur de supervision (120) comprend une base de données pour stocker les informations remontées par ledit analyseur de communication (100) et les informations relatives à l'analyse desdits tickets.

6. Système pare-feu selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend, en outre, un serveur d'audit (130) connecté au serveur de supervision (120) apte à analyser les fonctionnalités de l'autocommutateur, l'architecture système et à établir un ensemble de scénarii d'appels.

7. Système pare-feu selon la revendication 6, caractérisé en ce que ledit serveur d'audit (130) comprend un système expert pour l'établissement desdits scénarii.

8. Système pare-feu selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit serveur pare-feu (110) est connecté à une pluralité d'analyseurs de communications (100, 100', 100'') situés sur divers sites d'entreprise.

9. Système pare-feu selon l'une quelconque des revendications 1 à 8, caractérisé en ce qu'il comprend, en

outre, un serveur de sauvegarde cryptée (112) des configurations de l'autocommutateur.

10. Système pare-feu selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend, en outre, un modem *call-back* (114) connecté au port de télémaintenance (198) dudit autocommutateur (200).

11. Procédé de sécurisation d'un autocommutateur (200) d'entreprise connecté, d'une part, à au moins un réseau de communication en mode commuté, de type PSTN, et, d'autre part, à un ensemble de périphériques de communications et/ou de serveurs d'application (210), le procédé comprenant une étape d'analyse des couches basses (couches OSI 1 à 3) des communications par un analyseur de communication (100) et d'application de règles de sécurité pour mettre fin aux appels illicites,

caractérisé en ce qu'il comprend, en outre, :

- une étape de récupération par un serveur de supervision (120) des tickets de communication émis par l'autocommutateur (200),
- une étape de confrontation des informations contenues dans lesdits tickets aux règles de sécurité contenant dans le serveur de supervision (120),
- une étape d'application des règles de sécurité en fonction de ces informations contenues dans lesdits tickets.

12. Procédé de sécurisation selon la revendication 11, caractérisé en ce qu'il comprend, en outre, une étape de remontée des informations d'appels et de décisions prises depuis ledit analyseur de communication (100) vers ledit serveur de supervision (120).

13. Procédé de sécurisation selon la revendication 11 ou 12, caractérisé en ce qu'il comprend, en outre, une étape d'auto-apprentissage par un système expert dans le serveur de supervision (120) des scénarii non gérés par les règles sécuritaires.

14. Procédé de sécurisation selon l'une des revendications précédentes, caractérisé en ce qu'il comprend, au préalable, une étape de détermination des scénarii possibles par un serveur d'audit (130) et une étape d'établissement des règles sécuritaires par sélection desdits scénarii.

15. Procédé de sécurisation selon la revendication précédente, caractérisé en ce que ladite étape de détermination des scénarii comprend :

- une étape de récupération des fichiers de l'architecture circuit par ledit serveur d'audit (130) auprès de l'autocommutateur (200) et des fichiers de l'architecture système ;
- une étape de détermination des risques et contre-mesures associées à partir desdits fichiers récupérés.

16. Elément de programme d'ordinateur comprenant des moyens de code de programme d'ordinateur organisés pour accomplir les étapes du procédé selon l'une quelconque des revendications 11 à 15.

Figure 1
Art antérieur

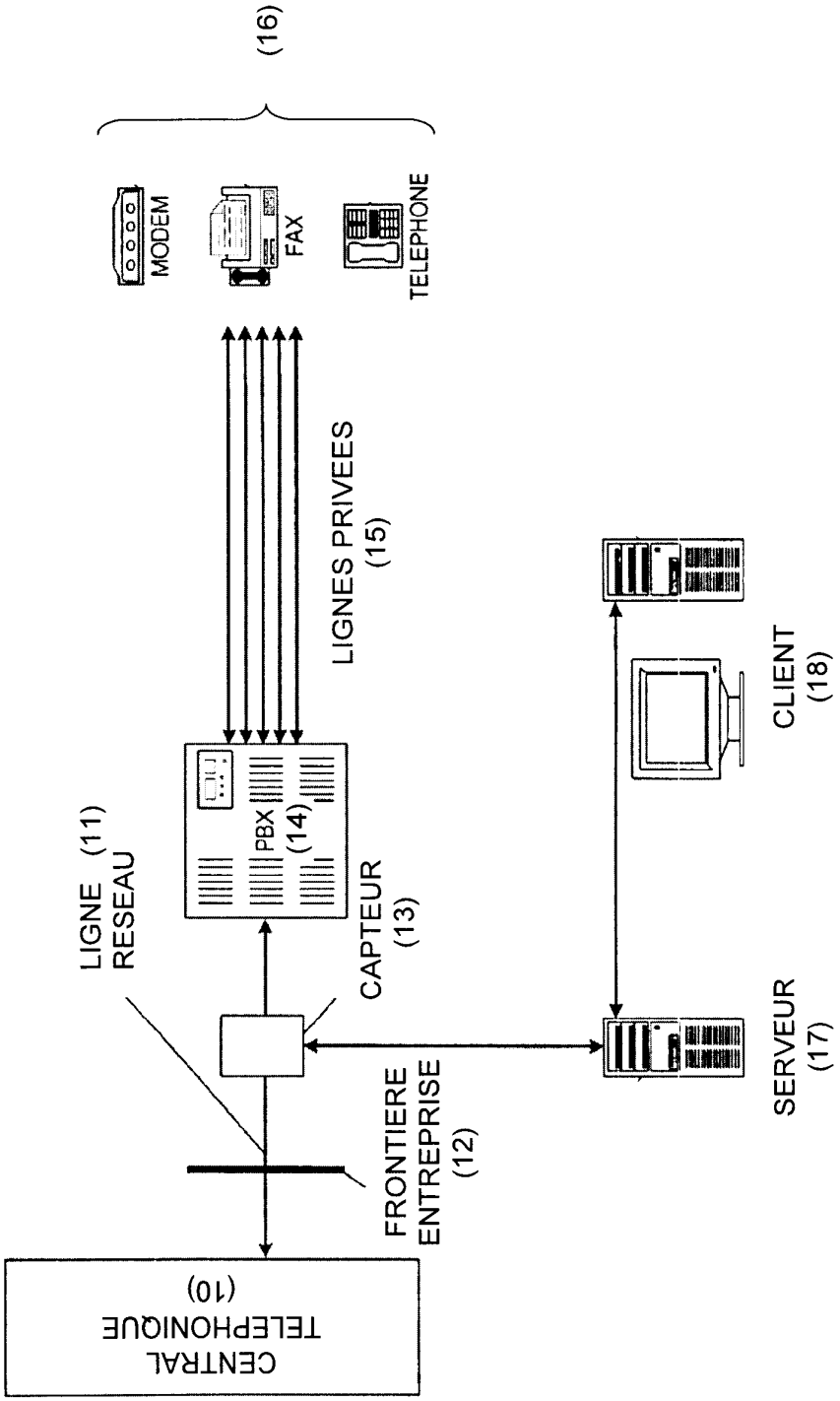


Figure 2

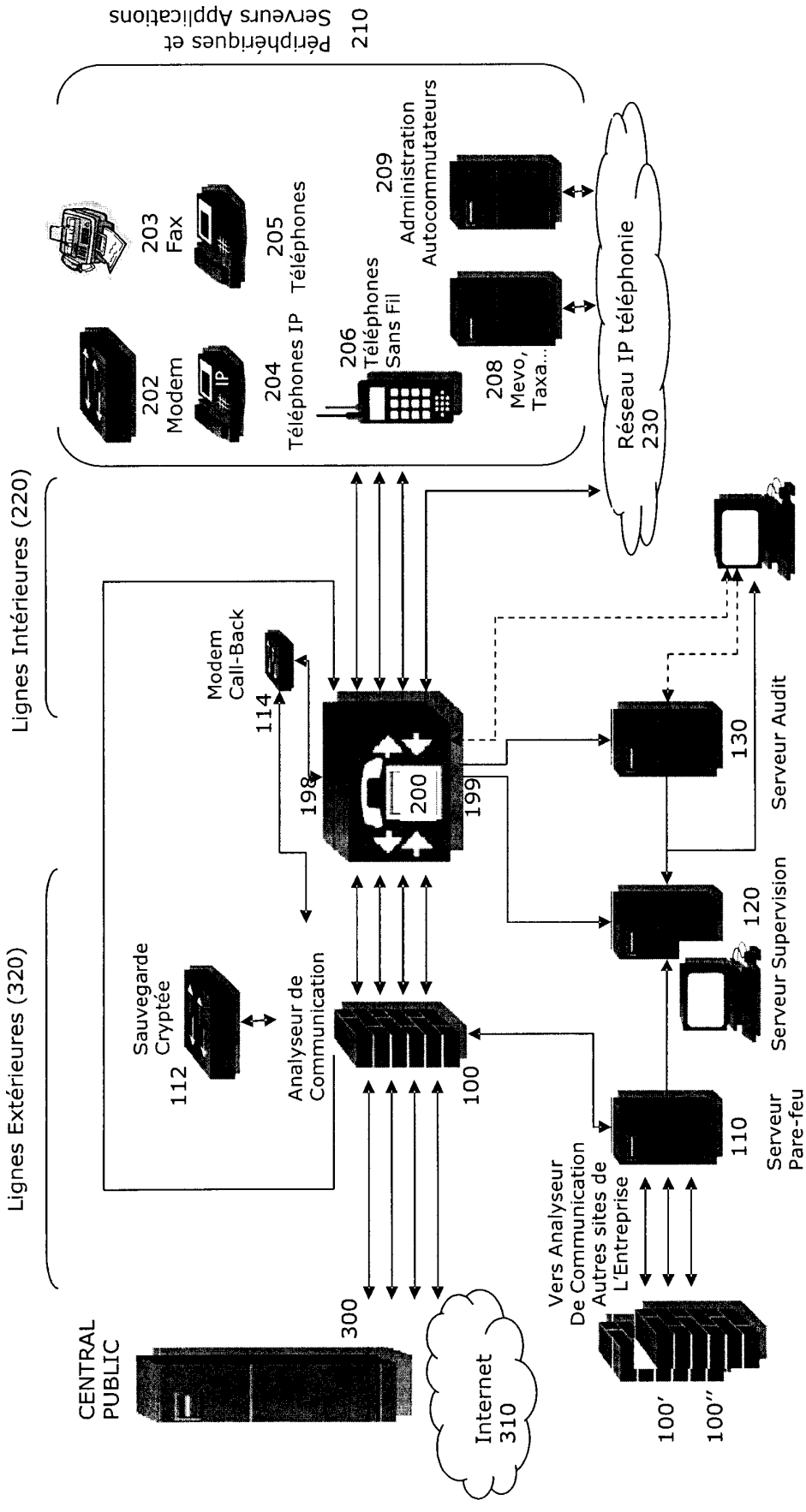

Périphériques et
Serveurs Applications
210
203
Fax
205
Téléphones
209
Administration
Autocommutateurs
202
Modem
204
Téléphones IP
206
Téléphones
Sans Fil
208
Mevo,
Taxa...
Réseau IP téléphonie
230
Lignes Intérieures (220)
Modem
Call-Back
114
198
200
199
130
Serveur Audit
120
Serveur Supervision
Sauvegarde
Cryptée
112
Analyseur de
Communication
100
110
Serveur
Pare-feu
Vers Analyseur
De Communication
Autres sites de
L'Entreprise
Lignes Extérieures (320)
CENTRAL
PUBLIC
300
Internet
310
100'
100''

Figure 3

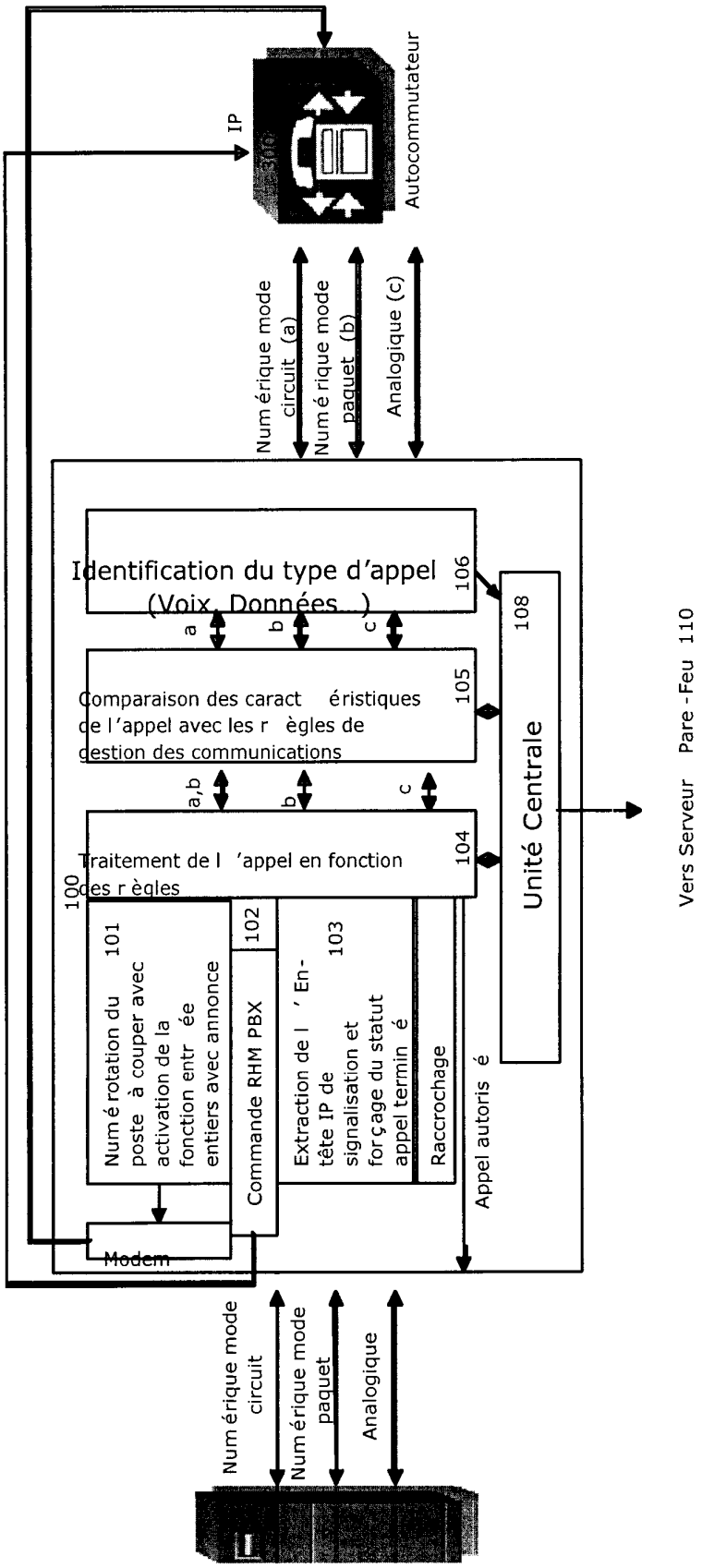

IP
Autocommutateur
Numérique mode circuit (a)
Numérique mode paquet (b)
Analogique (c)
Identification du type d'appel (Voix, Données...)
106
a
b
c
Comparaison des caractéristiques de l'appel avec les règles de gestion des communications
105
a,b
b
c
Traitement de l'appel en fonction des règles
104
100
Numérotation du poste à couper avec activation de la fonction entrée entiers avec annonce
101
Commande RHM PBX
102
Extraction de l'En-tête IP de signalisation et forçage du statut appel terminé
103
Raccrochage
Appel autorisé
Modem
Unité Centrale
108
Vers Serveur Pare-Feu 110
Numérique mode circuit
Numérique mode paquet
Analogique

Figure 4

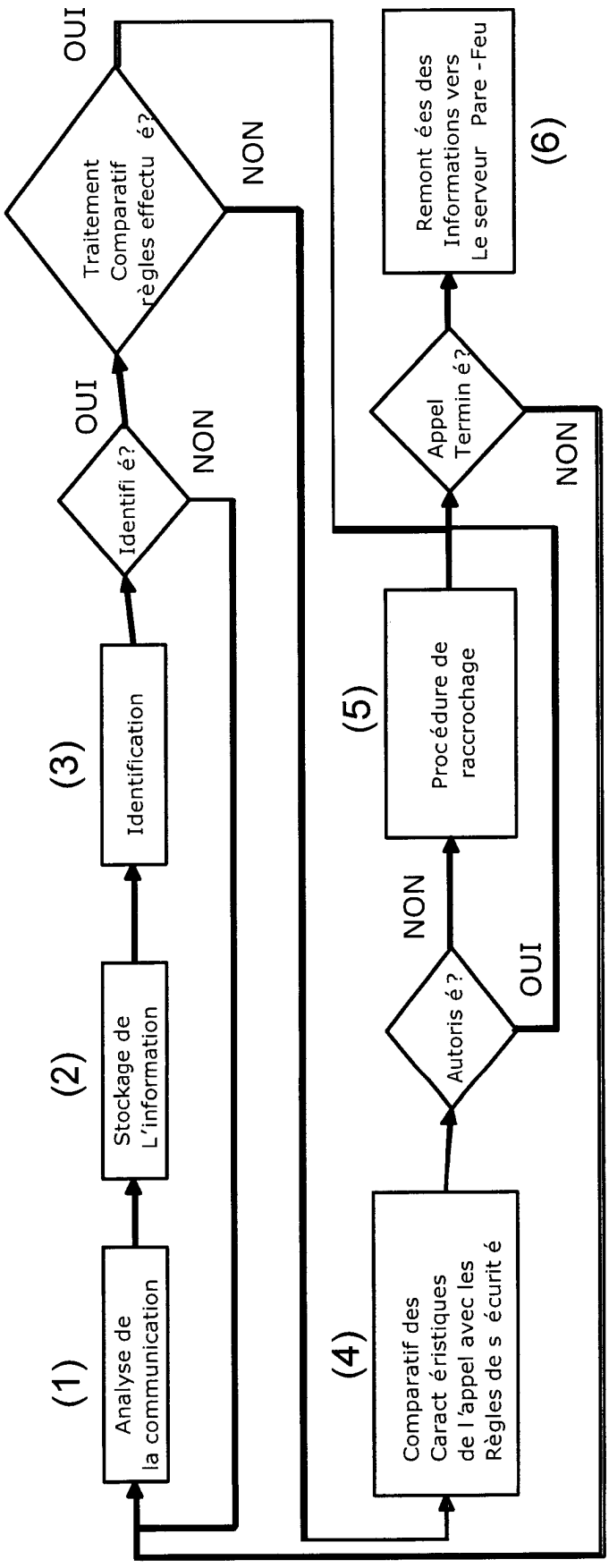

(1)
Analyse de la communication
(2)
Stockage de L'information
(3)
Identification
Identifi é?
OUI
NON
Traitement Comparatif règles effectu é?
OUI
NON
(4)
Comparatif des Caract éristiques de l'appel avec les Règles de s écurit é
(5)
Proc édure de raccrochage
Autoris é?
NON
OUI
Appel Termin é?
NON
(6)
Remont ées des Informations vers Le serveur Pare -Feu

Figure 5

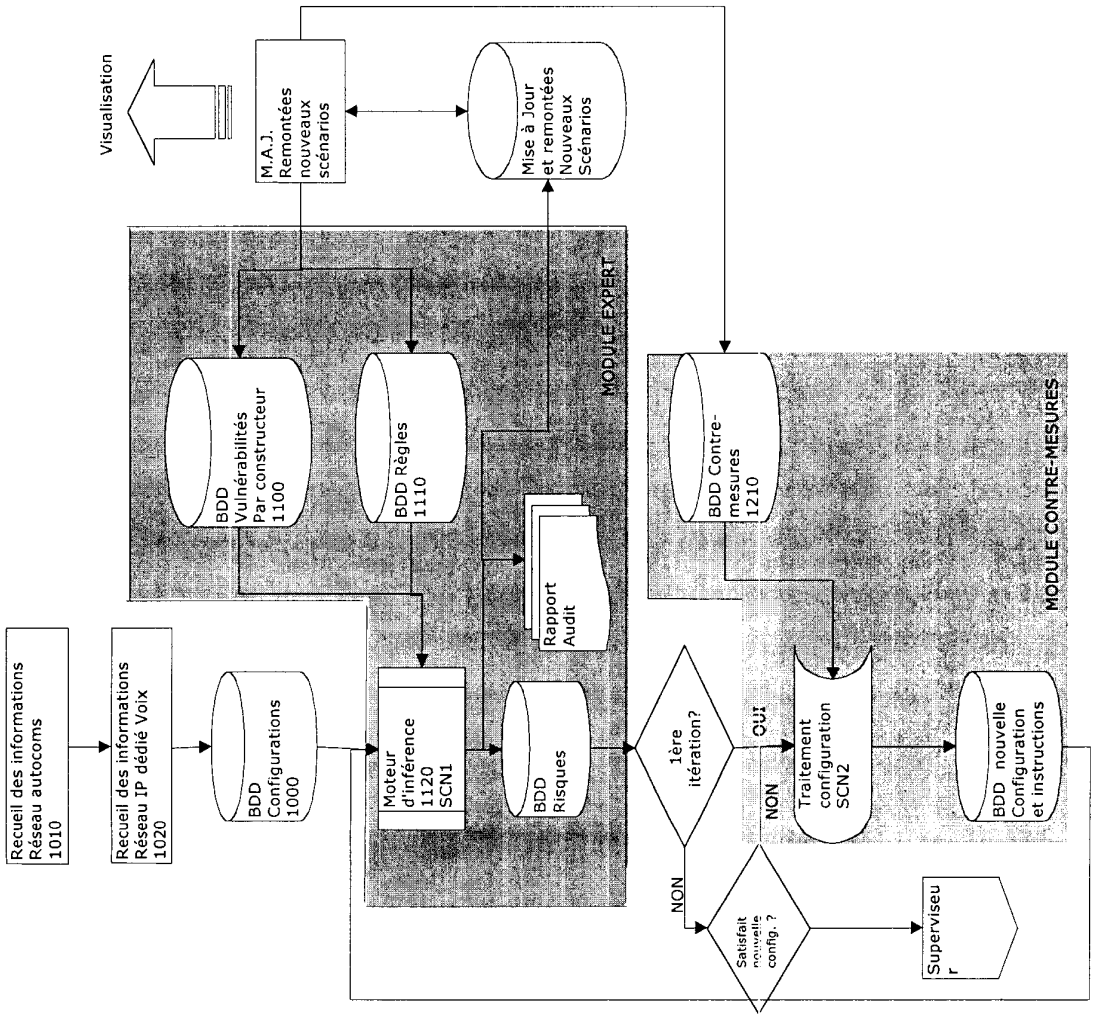

Recueil des informations Réseau autocoms 1010
Recueil des informations Réseau IP dédié Voix 1020
BDD Configurations 1000
Moteur d'inférence 1120 SCN1
BDD Vulnérabilités Par constructeur 1100
BDD Règles 1110
Rapport Audit
BDD Risques
MODULE EXPERT
Visualisation
M.A.J. Remontées nouveaux scénarios
Mise à Jour et remontées Nouveaux Scénarios
1ère itération?
OUI
NON
NON
Traitement configuration SCN2
BDD Contre-mesures 1210
BDD nouvelle Configuration et instructions
MODULE CONTRE-MESURES
Satisfait nouvelle config. ?
Superviseur

Figure 6

BDD liens extérieurs

Site	nature liens	Intranet	Flux	Nombre de voies	débit
	rnis (TO,T2) analogique IP	Oui/Non	Entrant Sortant Mixte		

BDD liens Internes

Site	N° tel	SDA	Nature	Type Périphérique
		Oui/Non	Num. Ana IP	

BDD Systèmes

Site	Element	Version OS	M.A.J.	Mots de Passe	Ports comm.	Logique	Physique
	PBX Taxa...						

BDD fonctionnalités

Sites	N° tel	Classe	Fonctionnalités ouvertes	Restriction

2876855

Figure 7

Vulnérabilités / Menaces	Possibilité d'accéder directement au poste	Possibilité de sortir vers l'extérieur	Possibilité de créer de modifier le paramétrage depuis l'extérieur de l'entreprise	Possibilité de créer de modifier le paramétrage depuis l'intérieur de l'entreprise	Possibilité d'effacer ou modifier des fichiers	Possibilité d'implanter des programmes pirates	Le système facilite par nature la divulgation à l'intérieur à l'extérieur de l'entreprise	Le système a des caractéristiques techniques qui permettent l'écoute	Possibilité d'utiliser les PS sans contrôle	Possibilité d'utiliser les BY sans contrôle	Absence de consignes en matière de code confidentiel	Possibilitéde pose d'éléments matériels additionnels pour stocker, transmettre ou altérer	Le système permet d'utiliser les services depuis l'extérieur sans identification/authentification	Obtention d'un avantage
Espionnage industriel	X	X	X	X			X	X	X	X	X	X	X	X
Ecoute passive	X			X			X	X	X	X	X	X		X
Divulgation externe		X	X	X			X	X		X	X	X		X
divulgation interne		X	X	X			X	X		X	X	X		X
Piégeage du matériel	X		X	X			X		X	X	X		X	X
Utilisation illicite du matériel	X	X	X	X	X				X	X	X	X	X	X
Piégeage du logiciel			X	X	X	X					X	X	X	X
Abus de droit		X	X	X	X	X	X	X	X	X	X	X	X	X
Usurpation de droit	X		X	X	X				X	X	X		X	X
Détournement de trafic	X	X	X	X	X	X			X				X	X
Altération des données	X		X	X	X	X			X	X	X		X	X

Figure 8

APPEL DEPART											
Sur-num r otation Q23	x	x	x	x						x	
Num rotation abr g e commune								x	x	x	
Num rotation abr g e de s services sp ciaux (urgences)								x	x	x	
Appel avec code affaire								x		x	
Groupement ˆ t te fixe					x	x	x			x	x
Groupement ˆ t te mobile					x	x	x			x	x
Groupement g n ral					x	x	x			x	x
Groupement au Çplus long tempsÈ de repos					x	x	x			x	x
Distribution multi-groupement					x	x	x			x	x
S lection directe ˆ lÕA rriv e (SDA)	x	x	x	x	x	x	x	x	x	x	x
Renvois pr d termin s È imm d iat										x	
Renvois pr d termin sur occupation										x	
Renvois pr d termin sur non r ponse										x	
Renvoi variable syst matique										x	
Renvoi variable sur non r ponse										x	
Renvoi variable sur poste occup										x	

Figure 9

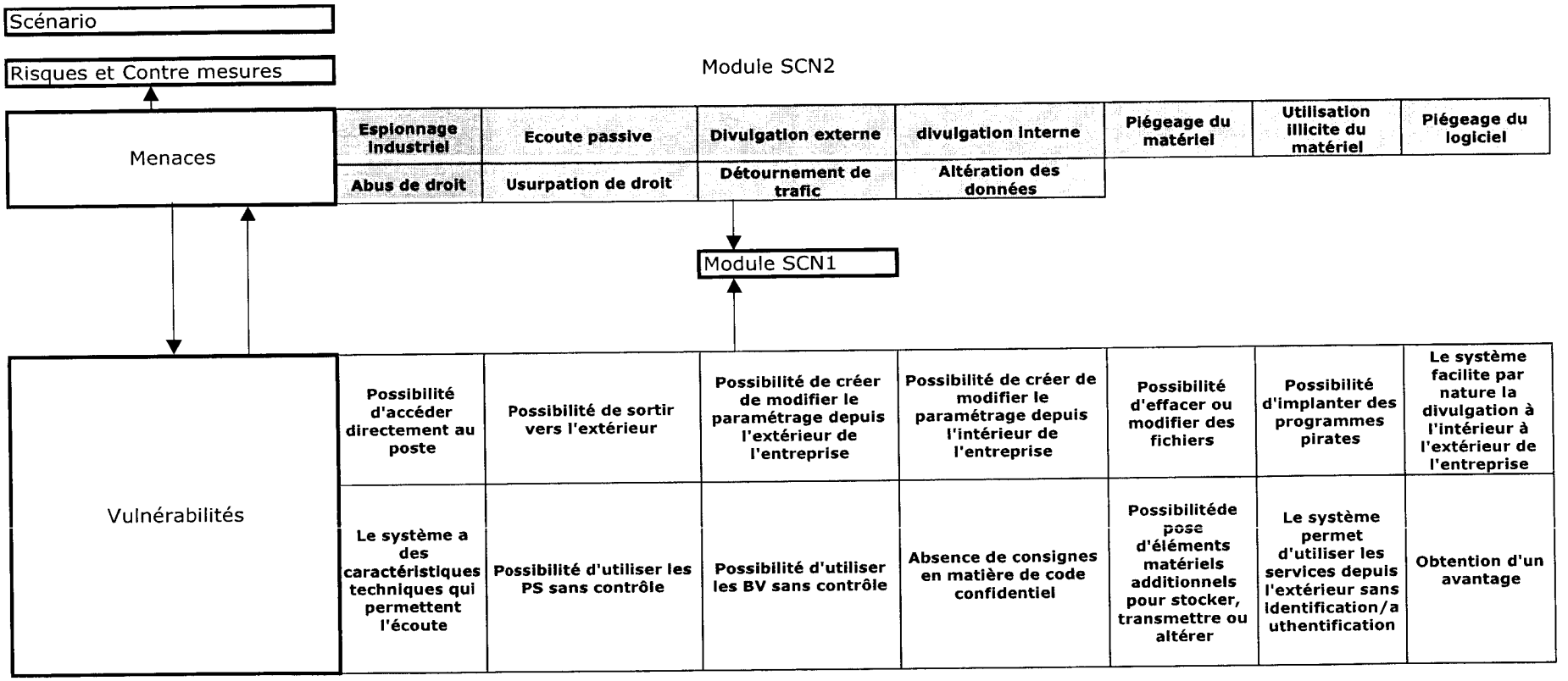

Scénario
Risques et Contre mesures
Module SCN2
Menaces
Espionnage industriel
Ecoute passive
Divulgation externe
divulgation interne
Piégeage du matériel
Utilisation illicite du matériel
Piégeage du logiciel
Abus de droit
Usurpation de droit
Détournement de trafic
Altération des données
Module SCN1
Vulnérabilités
Possibilité d'accéder directement au poste
Possibilité de sortir vers l'extérieur
Possibilité de créer de modifier le paramétrage depuis l'extérieur de l'entreprise
Possibilité de créer de modifier le paramétrage depuis l'intérieur de l'entreprise
Possibilité d'effacer ou modifier des fichiers
Possibilité d'implanter des programmes pirates
Le système facilite par nature la divulgation à l'intérieur à l'extérieur de l'entreprise
Le système a des caractéristiques techniques qui permettent l'écoute
Possibilité d'utiliser les PS sans contrôle
Possibilité d'utiliser les BV sans contrôle
Absence de consignes en matière de code confidentiel
Possibilitéde pose d'éléments matériels additionnels pour stocker, transmettre ou altérer
Le système permet d'utiliser les services depuis l'extérieur sans identification/authentification
Obtention d'un avantage

Figure 10

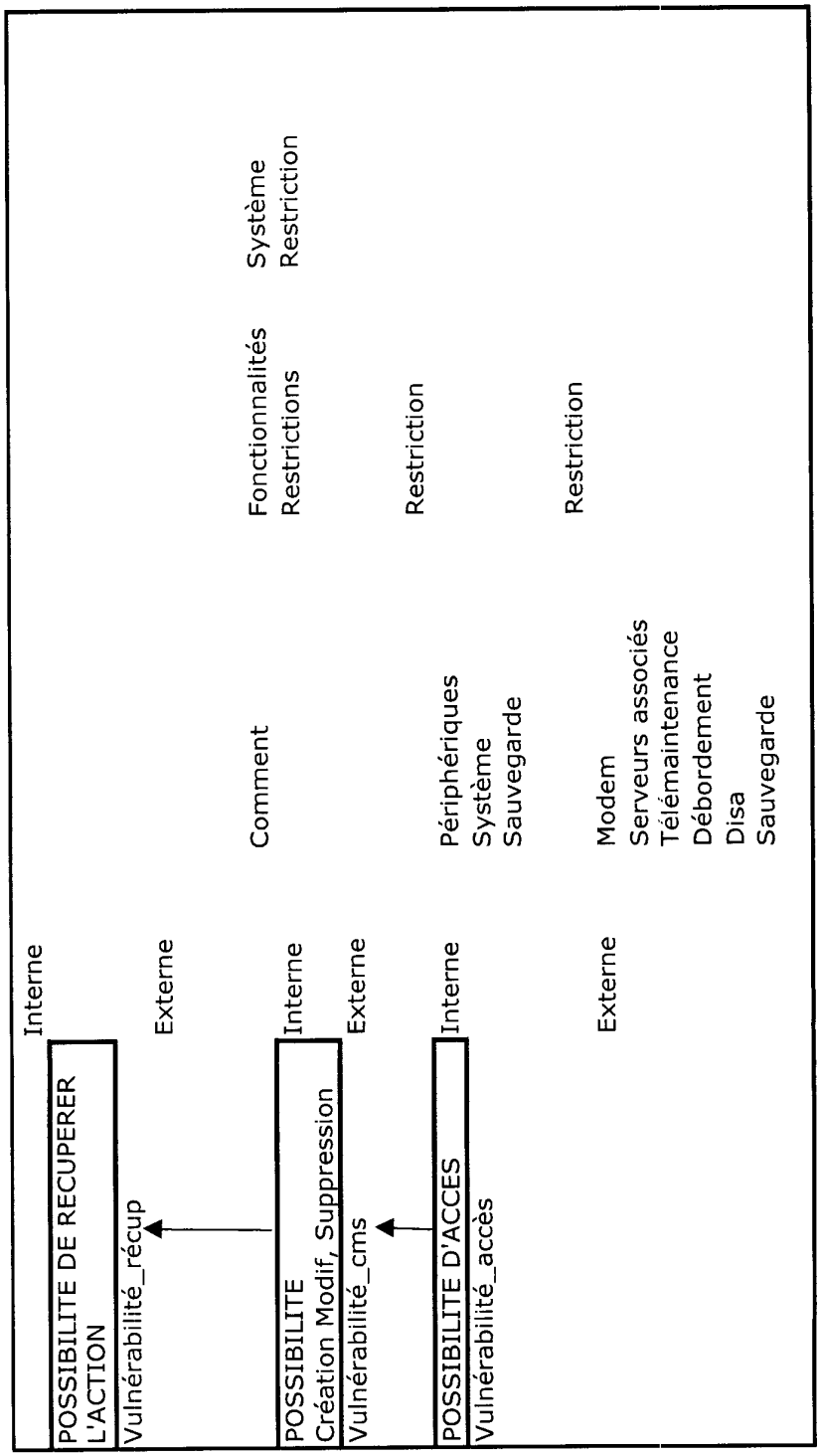

Interne
POSSIBILITE DE RECUPERER L'ACTION
Vulnérabilité_récup
Externe
Comment
Fonctionnalités
Restrictions
Système
Restriction
POSSIBILITE Création Modif, Suppression
Interne
Vulnérabilité_cms
Externe
Restriction
POSSIBILITE D'ACCES
Interne
Vulnérabilité_accès
Périphériques
Système
Sauvegarde
Externe
Restriction
Modem
Serveurs associés
Télémaintenance
Débordement
Disa
Sauvegarde

Figure 11

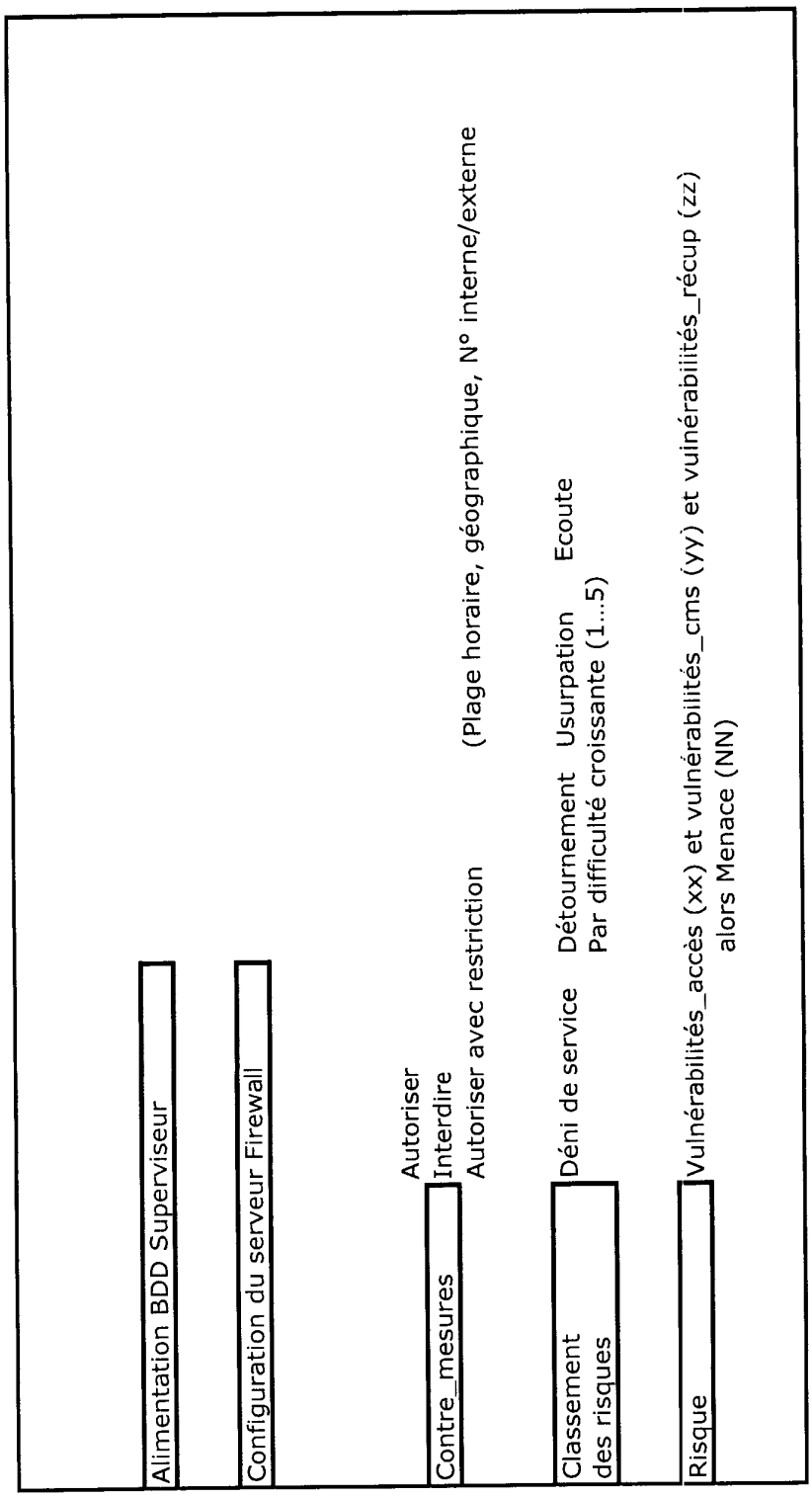

Alimentation BDD Superviseur
Configuration du serveur Firewall
Contre_mesures
Autoriser
Interdire
Autoriser avec restriction
(Plage horaire, géographique, N° interne/externe
Classement des risques
Déni de service
Détournement
Usurpation
Ecoute
Par difficulté croissante (1...5)
Risque
Vulnérabilités_accès (xx) et vulnérabilités_cms (yy) et vulnérabilités_récup (zz)
alors Menace (NN)

Figure 12

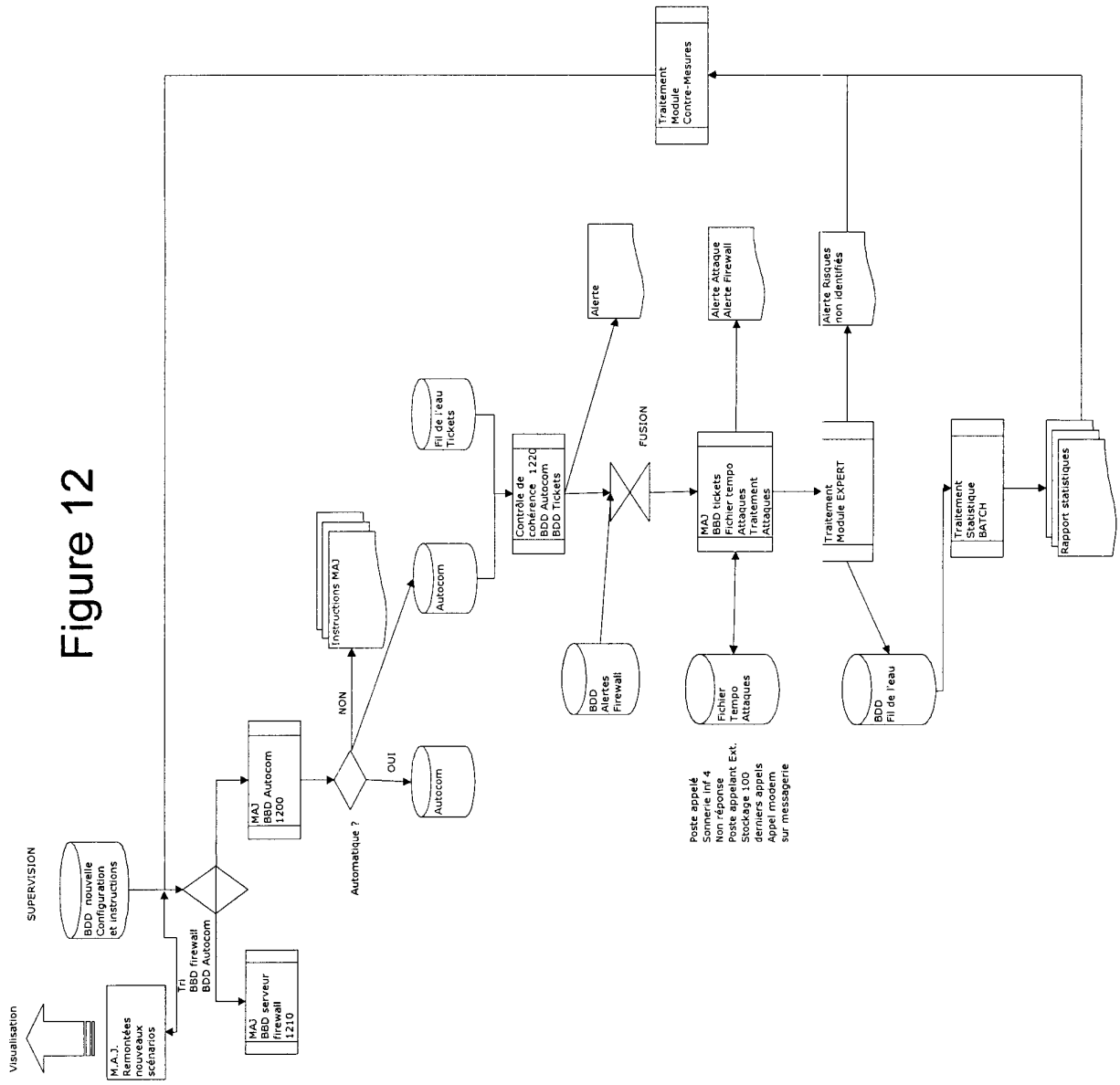
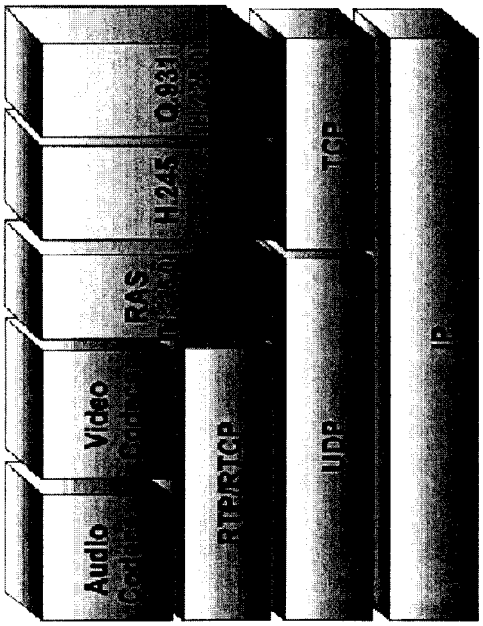

Visualisation
M.A.J. Remontées nouveaux scénarios
SUPERVISION
BDD nouvelle Configuration et instructions
Tri BBD firewall BBD Autocom
MAJ BBD serveur firewall 1210
MAJ BBD Autocom 1200
Automatique ?
NON
OUI
Instructions MAJ
Autocom
Autocom
Fil de l'eau Tickets
Contrôle de cohérence 1220 BDD Autocom BDD Tickets
Alerte
FUSION
BDD Alertes Firewall
MAJ BBD tickets Fichier tempo Attaques Traitement Attaques
Fichier Tempo Attaques
Poste appelé
Sonnerie inf 4
Non réponse
Poste appelant Ex.
Stockage 100 derniers appels
Appel modem
sur messagerie
Alerte Attaque Alerte Firewall
Alerte Risques non identifiés
Traitement Module EXPERT
BDD Fil de l'eau
Traitement Module Contre-Mesures
Traitement Statistique BATCH
Rapport statistiques

Figure 13



QuickTime™ et un
décompresseur TIFF (LZW)
sont requis pour visionner cette image.

RÉPUBLIQUE FRANÇAISE

2876855

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 660961
FR 0452361

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
D,Y	US 2004/161086 A1 (BUNTIN DAVID L ET AL) 19 août 2004 (2004-08-19) * alinéas [0005] - [0008] * * alinéas [0040] - [0045] * * alinéas [0053], [0054] * * alinéas [0070] - [0121] * * alinéa [0154] * * alinéa [0165] * * alinéas [0172], [0173] * * alinéa [0187] * -----	1-4, 8-11,13, 16	H04M3/22 H04M3/38 H04M3/42 H04L12/22 H04L12/24 H04L29/06
Y	US 2004/111305 A1 (GAVAN JOHN ET AL) 10 juin 2004 (2004-06-10) * abrégé * -----	1-4, 8-11,13, 16	
Y	US 6 801 607 B1 (MARCHAND DEAN C ET AL) 5 octobre 2004 (2004-10-05) * abrégé * * colonne 1, ligne 47 - colonne 3, ligne 59 * * colonne 5, ligne 3-65 * -----	1-3, 8-11,16	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) H04M H04L
A	WO 03/009573 A (SECURELOGIX CORPORATION) 30 janvier 2003 (2003-01-30) * alinéas [0058] - [0063] * * alinéa [0200] * * alinéas [0204] - [0207] * -----	1,3,5,6, 8,11,12, 15,16	
A	US 2001/014150 A1 (BEEBE TODD ET AL) 16 août 2001 (2001-08-16) * alinéas [0014] - [0024] * * alinéas [0059] - [0079] * -----	1,3,5,6, 8,11, 14-16	

Date d'achèvement de la recherche	Examinateur
28 juin 2005	Ruiz Sanchez, J

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

.....

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0452361 FA 660961

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 28-06-2005
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2004161086 A1	19-08-2004	US 2002021791 A1	21-02-2002
		US 6735291 B1	11-05-2004
		US 2003016803 A1	23-01-2003
		US 2005025302 A1	03-02-2005
		US 2005047570 A1	03-03-2005
		EP 1415459 A1	06-05-2004
		WO 03009573 A1	30-01-2003
		US 2004234056 A1	25-11-2004
		CA 2428472 A1	19-09-2002
		EP 1332606 A1	06-08-2003
		JP 2004519929 T	02-07-2004
		WO 02073945 A1	19-09-2002
		US 2004218742 A1	04-11-2004
		CA 2438976 A1	28-02-2005
US 2004111305 A1	10-06-2004	US 6601048 B1	29-07-2003
		US 5854834 A	29-12-1998
		US 6621833 B1	16-09-2003
		AU 9386598 A	29-03-1999
		CA 2303107 A1	18-03-1999
		EP 1016024 A2	05-07-2000
		JP 2001516107 T	25-09-2001
		WO 9913427 A2	18-03-1999
		US 6732082 B1	04-05-2004
		US 2005075992 A1	07-04-2005
		US 2004213227 A1	28-10-2004
US 6801607 B1	05-10-2004	CA 2446732 A1	14-11-2002
		EP 1388256 A2	11-02-2004
		JP 2004527185 T	02-09-2004
		WO 02091713 A2	14-11-2002
WO 03009573 A	30-01-2003	US 2002021791 A1	21-02-2002
		EP 1415459 A1	06-05-2004
		WO 03009573 A1	30-01-2003
		US 2004161086 A1	19-08-2004
		US 2004234056 A1	25-11-2004
US 2001014150 A1	16-08-2001	US 6226372 B1	01-05-2001
		US 6249575 B1	19-06-2001
		AU 1950301 A	18-06-2001
		WO 0143343 A1	14-06-2001
		AU 6161699 A	26-06-2000
		CA 2354149 A1	15-06-2000
		EP 1138144 A1	04-10-2001
		JP 2002532967 T	02-10-2002

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0452361 FA 660961

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 28-06-2005
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2001014150 A1		US 2002090073 A1	11-07-2002
		WO 0035172 A1	15-06-2000
		US 2003112940 A1	19-06-2003
		US 6718024 B1	06-04-2004
		US 6320948 B1	20-11-2001
		US 6687353 B1	03-02-2004
		US 6735291 B1	11-05-2004

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82