REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mouloud Mammeri de Tizi-Ouzou
Faculté Génie Electrique et Informatique
Département d'Informatique

Mémoire de fin d'études

En vue de l'obtention du diplôme de Master2 en Informatique

Thème

Réalisation d'une interface entre deux appliances (bluecoat et stonesoft) pour l'exploitation des logs afin de sécuriser l'accès à internet

Option : Conduite de Projets Informatiques

Dirigé par **:** **M^me^ BELKADI.M**

Réalisé par **:** **M^r^ BOUGUEDOUR Lyes**

Année Universitaire : 2013 - 2014

Remerciements

Je tiens à exprimer ma profonde gratitude à ma promotrice, Madame BELKADI.M, qui m'a fait l'honneur de diriger ce travail et ses précieux conseils furent d'un apport considérable.

Aussi je tiens à lui reconnaître le temps qu'elle m'a consacré.

Je tiens à remercier tous les membres du jury d'avoir accepter de juger notre travail.

Mes sincères sentiments vont à tous ceux qui, de prés ou de loin, ont contribué à la réalisation de ce projet, en particulier ma famille, MonElisa et mes amis (es).

Lyes

Dédicaces

Je dédie ce modeste travail :

A mes parents adorés

A mes sœurs et mes frères

A MonElisa

A toute ma famille

A tous mes amis

.....Lyes

Sommaire

Annexe

Références bibliographiques et webliographiques.

Problématique:

Les récentes études indiquent que «les intrusions les plus nocives pour le système de sécurité d'une entreprise ont souvent lieu grâce à une aide provenant de l'intérieur». Les études affirment que 70% des incidents de sécurité qui causent réellement des pertes pour les entreprises impliquent des personnes internes à l'entreprise. Avoir un pare-feu et un anti-virus peut protéger l'entreprise contre les hackers extérieurs mais ne l'aidera pas contre les attaques provenant de l'intérieur. La seule façon de protéger ses systèmes contre de telles attaques est de surveiller les logs. Notre travail consiste à réaliser un outil pour aider notre organisme d'accueil à minimiser les risques en analysant le fichier log relatif aux sites WEB consultés par les utilisateurs pour mieux sécuriser le réseau contre les attaques internes.

Introduction générale :

A l'heure où l'on prend plus que jamais au sérieux les scénarios d'attaques ciblées ou de fuite d'informations, les entreprises se heurtent souvent à un manque de visibilité sur ce qu'il se passe au sein même de leur système d'information(SI).

Beaucoup ont donc entamé au cours des derniers mois un projet visant à exploiter les logs (ou journaux d'évènements) afin d'anticiper, détecter et diagnostiquer des actes malveillants.

Une grande majorité de machines (équipements réseau, serveurs, postes de travail), bases de données ou applications d'un SI peuvent aujourd'hui générer des logs. Ces fichiers contiennent, pour chaque machine, la liste de tous les évènements qui se sont déroulés : réussite ou échec d'une connexion utilisateur, redémarrage, saturation de la mémoire…

Pour les exploiter, il est possible de se connecter unitairement à chacun des équipements afin d'y observer l'historique. Cette tâche fastidieuse, encore souvent observée sur le terrain, est irréaliste sur des systèmes d'information complexes. Elle est par ailleurs inefficace pour prévenir un incident ou détecter les impacts en temps réel. Pour remédier à cela les entreprises peuvent avoir recours à l'analyseur de fichier journal (log).

Pour voir de prés l'intérêt de cette technologie, nous proposons dans ce mémoire une étude structurée en quatre chapitres :

- ✓ **Chapitre I :** Présentation de l'organisme d'accueil : dans ce chapitre nous allons recueillir les informations qui nous permettent de mettre en œuvre notre travail au sein de l'entreprise.
- ✓ **Chapitre II :** Sécurité : dans ce chapitre nous allons présenter les techniques de sécurité les plus utilisées.

- ✓ **Chapitre III:** Analyse et conception : dans ce chapitre nous allons présenter la modélisation de notre système.
- ✓ **Chapitre IV :** Etudes technique : dans ce dernier chapitre nous présenterons le fonctionnement de notre système.
- ✓ Et enfin nous terminerons par une conclusion générale

I-Présentation de l'organisme d'accueil [2] [18]

I-1.1-Dénomination :

SONATRACH : Société Nationale pour la recherche, la production, le Transport, la Transformation et la Commercialisation des Hydrocarbures.

I-1.2-Forme juridique :

Entreprise publique économique (EPE), qui a connu une transformation (sans création d'une nouvelle personne morale) en une société par actions (SPA) par le décret présidentiel n°98-48 du 11 février 1998.

I-1.3-Siège social :

Le siège social de Sonatrach est situé à Hydra Alger, -Djenane el malik. Il peut être transféré en tout autre lieu du territoire national par délibération de l'assemblée générale.

I-1.4-Capital social :

Il est de l'ordre de: 245.000.000.000 DA (deux cents quarante cinq milliards de dinars) répartis en deux cent quarante cinq mille actions, d'un million de dinars chacune, entièrement et exclusivement souscrit et libéré par l'Etat.

I-1.5- Le logo

Le logo de l'entreprise Sonatrach se présente comme suit :

I-2- Historique de la Sonatrach :

L'entreprise nationale Sonatrach (Société nationale de transport de transformation et de commercialisation des hydrocarbures) a été créée le 31-12- 1963 (décret n°63-491) pour assurer la responsabilité de la production du transport et la commercialisation des hydrocarbures.

Les missions et les prérogatives de l'entreprise nationale Sonatrach ont été élargies en date du 22 septembre 1966 (décret n°66-626) .Ses missions qui se limitaient à l'origine u transport, à la transformation et à la commercialisation des hydrocarbures ont été élargies à tous les domaines de l'industrie pétrolière, à savoir

La prospection, la recherche, la production, le transport, la transformation et la commercialisation des hydrocarbures.

Depuis le 24 février 1971, date de nationalisation des hydrocarbures, l'entreprise a pris en charge l'ensemble du domaine minier et s'est vue confier le développement de toutes les branches de l'industrie pétrolière.

La Sonatrach est passée de 33 agents en 1964 à 103.000 vers la fin des années 1980.

Pour assurer une meilleure gestion et améliorer les performances dans le cadre de la politique nationale pour la réorganisation de l'économie du pays, elle entreprend sa restructuration pour donner naissance à 17 entreprises industrielles.

Actuellement, la Sonatrach compte un effectif de 36.000 agents environ et conserve pour sa part, la charge des opérations de recherche, de production, de transport par canalisation, de traitement, conditionnement et liquéfaction des hydrocarbures liquides et gazeux.

Dans le cadre de la restructuration décidée en 1982, la Sonatrach a fait l'objet d'un découpage qui a donné naissance à treize (13) entreprises parmi lesquelles, NAFTAL, NAFTEC, ENTP, ASMIDAL, ENSP.

I-3-Missions principales de la SONATRACH:

Sous l'autorité d'un Directeur Général, la Sonatrach, a notamment pour missions essentielles:

Le développement, la conservation et la valorisation des réseaux énergétiques sur tout le territoire national.

La reconstitution et l'augmentation des réserves d'hydrocarbures.

L'intensification des efforts d'exploitation et capitalisation des études réalisées dans ce domaine, pour une meilleure connaissance du sous-sol et la mise en évidence des réserves d'hydrocarbures.

La diversification des marchés et des produits destinés à l'exportation.

L'approvisionnement énergétique national à moyen terme, et l'élaboration du compte-rendu des réserves nationales.

L'adaptation de l'outil commercial aux exigences du marché énergétique pour une meilleure maîtrise de ses mécanismes et des performances commerciales accrues.

Le développement, la maîtrise et la maintenance des complexes de production, de transport et de conditionnement des hydrocarbures.

Le développement des techniques modernes de gestion nationale par le biais de la formation continue.

I-3.1-Organigramme de l'organisme d'accueil

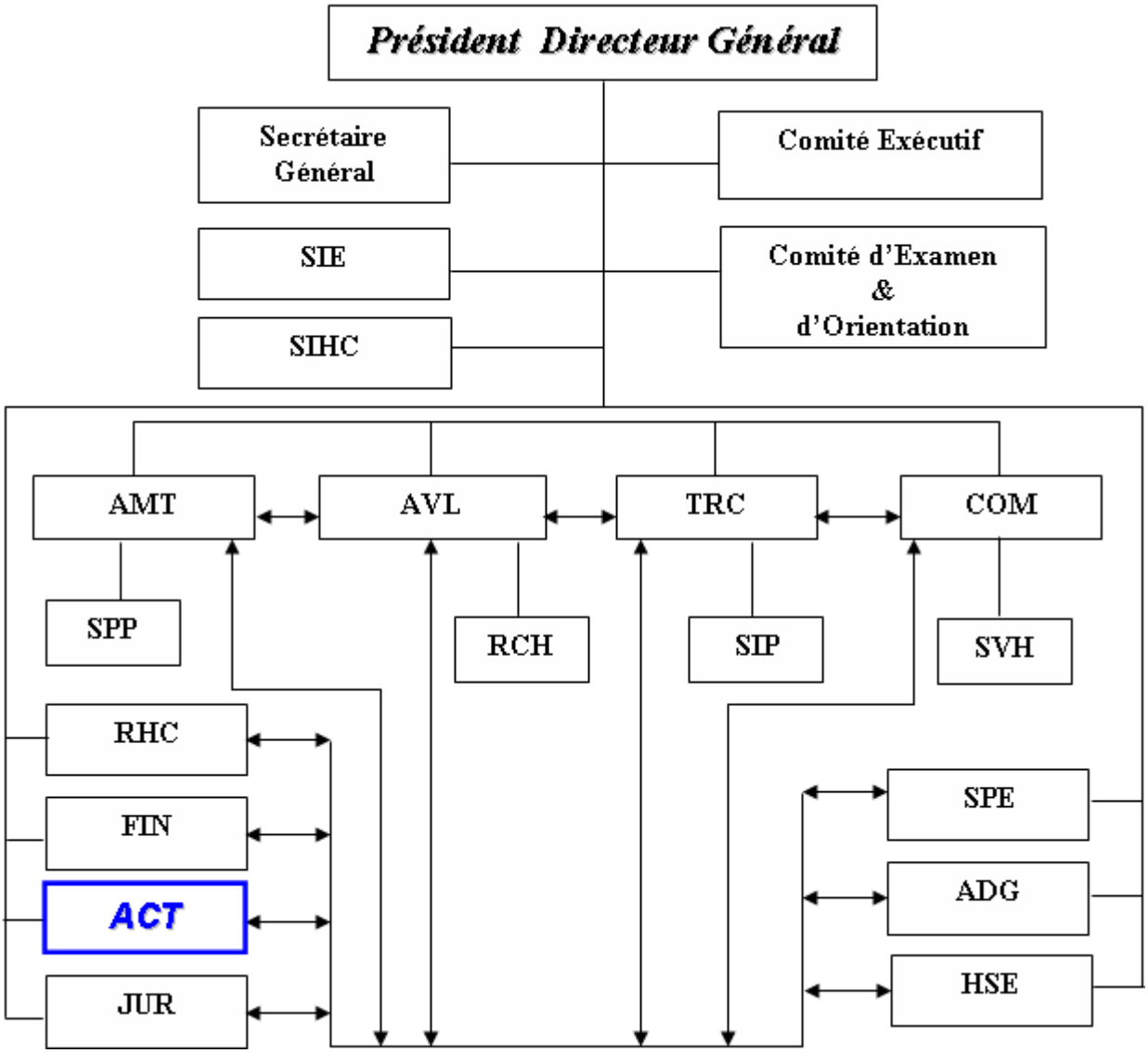


Figure-1-Organigramme de l'organisme d'accueil

ACT ***Notre champ d'études***

I-3.2-Légende :

SPE : Stratégie, Planification et Economie.

AMT : Amont.

AVL : Aval.

TRC : Transport par Canalisation.

COM: Commercialisation.

FIN : Finances.

JUR : Juridique.

ACT : Activités Centrales.

RHC : Ressources Humaines et Communication.

ADG : Audit Groupe.

HSE : Sécurité et Environnement.

I-3.3-PROFIL DU GROUPE :

Le Groupe SONATRACH est présent dans l'ensemble de la chaîne gazière, pétrolière et para pétrolière depuis l'exploration, la production, le transport par canalisations et les transformations (raffinage et pétrochimie), jusqu'à la commercialisation des hydrocarbures et de leurs dérivés.

Le Groupe compte 120.000 employés qui exercent leurs activités à travers l'Entreprise mère Sonatrach et ses filiales.

Sonatrach, avec une effectif de 49.000 employés, se classe 12eme mondialement dans la production d'hydrocarbures et le premier en Afrique.

C'est aussi le deuxième exportateur mondial de GNL et de GPL et le troisième exportateur de gaz naturel.

La production globale de Sonatrach (tous produits confondus) a été de 222,5 millions de tonnes équivalent pétrole (Tep) en 2004, soit une augmentation de 5 % par rapport à l'année 2003.

I-3.4-LES ACTIVITES DU GROUPE :

Les activités du Groupe Sonatrach sont organisées en quatre entités :

- ***L'amont pétrolier :***

  L'activité Amont chargée de la recherche, l'exploitation et la production des hydrocarbures a pour missions le développement des gisements découverts, l'amélioration du taux de récupération et la mise à jour des réserves. L'activité Amont intègre dans sa stratégie opérationnelle les filiales qui lui sont rattachées :

  GCB : Société nationale de génie civil et bâtiment,

  ENSP : Entreprise nationale des services aux puits,

  ENTP : Entreprise nationale des travaux aux puits,

  ENAFOR : Entreprise nationale des forages,

  ENGP : Entreprise nationale des grands travaux aux puits.

- **L'aval pétrolier :**

  Cette activité, chargée de l'élaboration et de la mise en œuvre des politiques de développement et d'exploitation de l'aval pétrolier et gazier, a pour missions essentielles l'exploitation des installations existantes de liquéfaction de gaz naturel et de séparation de GPL, de raffinage, de pétrochimie et de gaz industriels (hélium et azote). L'activité Aval est aujourd'hui constituée de 4 (quatre) complexes de GNL, 2 (deux) complexes pétrochimiques, une unité de polyéthylène à haute densité (PEHD) appartenant à la **filiale Enip**, 5 (cinq) raffineries appartenant à la **filiale Naftec**, une unité d'extraction d'hélium hélios et 2 (deux) filiales de maintenance et de gestion des zones industrielles **Somiz** (Arzew) et **Somik** (Skikda).

- **Le transport des hydrocarbures par canalisations :**

L'activité transport des hydrocarbures liquides et gazeux par canalisations a en charge le développement, la gestion et l'exploitation du réseau de transport, de stockage, de chargement des hydrocarbures. Sonatrach dispose d'un réseau de canalisations d'une longueur globale de 16.000 km dont 2 gazoducs transcontinentaux ; l'un vers l'Espagne via le Maroc (le gazoduc **Pedro Duran Farel**) et l'autre vers l'Italie via la Sicile (le gazoduc **Enrico-Mattei).**

D'autres projets de grande envergure sont en cours de réalisation : le gazoduc **Med gaz** reliant l'Algérie à l'Europe via l'Espagne, le projet **Galsi** reliant l'Algérie à l'Italie via la Sardaigne et, enfin, le gazoduc **Trans-Africa Gasoduc Pipeline** (TSGP), qui reliera le Nigeria à la côte Algérienne**.**

- **La commercialisation des hydrocarbures :**

Cette activité est celle du management des opérations de vente et de shipping dont les actions sont menées par l'activité Commercialisation en coopération avec ses filiales telles que **Naftal** pour la distribution des produits pétroliers à l'échelle nationale, **SNTM Hyproc** pour le transport maritime des hydrocarbures, **SPC** (Londres) pour le trading et **Cogiz** pour la commercialisation des gaz industriels.

La flotte maritime, composée de 6 (six) méthaniers et de 4 (quatre) transporteurs de GPL, a été renforcée par 2 nouveaux navires transporteurs de GPL : l'**Alrar** et le **Rhourde - Nous**, d'une capacité unitaire de 59.000m^3 chacun, réceptionnés en 2004 et de 2 méthaniers : **Berge Arzew**, avec une capacité de 138.000m^3, et **Lalla Fatma N'Soumer**, avec une capacité de 145.000m^3

I-4-Présentation de la structure d'accueil

La direction coordination Groupe Activités centrales(ACT) a pour missions essentielles, l'élaboration de politiques en matière de gestion des moyens de l'entreprise; la gestion de banques de données et des moyens logistiques et approvisionnements des structures ainsi que la comptabilité et finances du siège.

Elle organise également la conférence annuelle des cadres.

Elle comporte six directions chargées respectivement de la gestion du siège, de la comptabilité, de la communication, de la stratégie d'image, des œuvres sociales, des relations publiques et de l'informatique, et ce en plus d'une cellule / administration et d'un coordonnateur chargé du secrétariat du directeur exécutif et des assistants.

a- Missions principales de la structure d'accueil :

La direction informatique est organisée en cinq départements chargés des applications et bases de données, de HELP DESK, de la sécurité informatique, traitements et info/ centre.

- ***Le département sécurité informatique*** est chargé notamment, de l'élaboration de la stratégie et des politiques et procédures en matière de sécurité informatique (matériels, logiciels), leur diffusion et le contrôle de leur mise en œuvre. Comme il est chargé de l'élaboration des études d'analyse de risque et de la réévaluation ainsi que les plans d'urgences, de la consolidation et du reporting de la sécurité informatique.

- *Le département application et base de données* élabore et définit les normes et standards en matière de base de données, et veille à leur diffusion et au contrôle de leur application qui peut-être spécifique (workflow, groupware). Il veille également au développement interne des compétences par des certifications expertise.

- *Le département réseau et maintenance* est chargé notamment, de l'élaboration et l'application des normes et standards du groupe, en matière d'infrastructure réseau du développement et la mise en œuvre d'architectures globales des matériels, de système et de logiciels ainsi que de l'administration du réseau du siège, des serveurs, des équipements actifs et des stations d'administration. Il est chargé également de l'assistance en matière de réseaux informatiques, de la mise en œuvre des service Internet/intranet de la maintenance des équipements informatiques du siège, de l'élaboration des plans de réforme des équipements informatiques en collaboration avec la structure de gestion du siège ainsi que de la gestion des équipements passifs du siège et des systèmes d'exploitation.

- *Le département exploitation traitements* est chargé notamment, de l'élaboration des

manuels opératoires des systèmes de l'adaptation et la mise à jour des systèmes opérationnels, ainsi que de l'exploitation des systèmes (ressources humaines et finances) et la sauvegarde des systèmes d'exploitation et des applicatifs, de l'archivage et la récupération des données.

➢ *Le département info-centre* est chargé notamment, de la gestion de la ferme des serveurs, des équipements actifs et des stations d'administration ainsi que de la logithèque et a les présentations de service pour le compte des structures du siège, en l'occurrence le design et le développement des sites web et la réalisation des activités multimédia.

➢ La documentation traite tous les documents informatiques. Elle est chargée de diffuser l'information à l'ensemble des agents de la direction (siège).

La documentation est constitué de :

- ✓ Ouvrages informatique (encyclopédies, dictionnaires, …….)
- ✓ Revues informatiques
- ✓ Thèses et mémoires de fin d'études.

b-Organigramme de la structure d'accueil

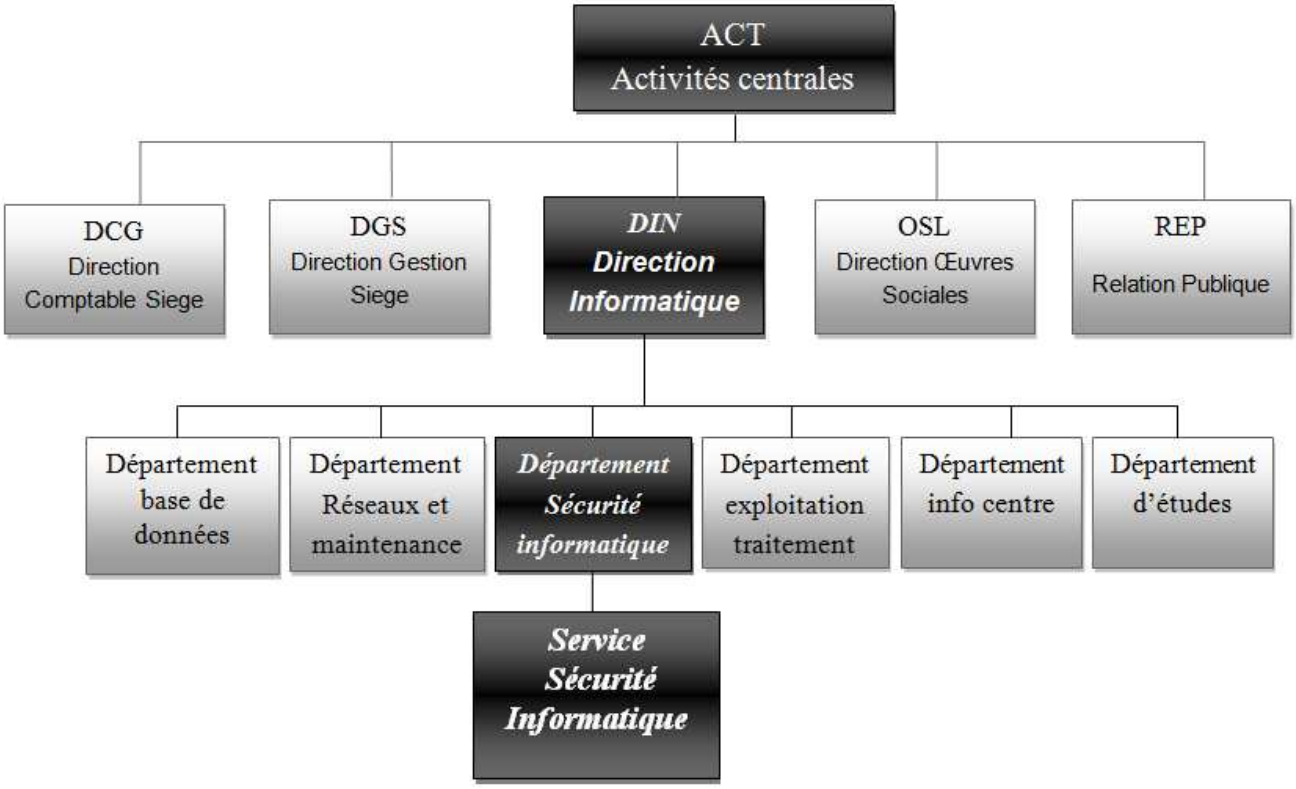


Figure-2- Organigramme de la structure d'accueil

d-Situation humaine et informatique :

d-1-Les moyens humains de DIN :

Un Directeur.

Deux Assistants.

Trois Sous-directeurs.

Huit Chefs de département.

Quinze Chefs de service.

Dix Chefs de projets principaux.

Vingt-neuf Ingénieurs.

Huit Analystes.

Onze Programmeurs.

Soixante-treize Autres se décomposent comme suit :

- Chefs de section.
- Chefs de groupe pupitreurs.
- Agent de saisie.
- Agent de sécurité.
- Le personnel de section administratif.

d-2- Descriptif de l'équipement informatique :

La DIN de l'entreprise possède les machines suivantes selon les domaines :

d-2.1 Internet:

- Deux serveurs Proxy ***BlueCoat***

-Un serveur Alfatron biprocesseur offrant les services suivants :

- ✓ -passerelle antivirus interscan viruswall filtrant les services FTP et http.
- ✓ -un serveur ultra entreprise 450 avec une mémoire de 256 Mo et un disque dur de 4,5 Go hébergeant les sites internet.
- ✓ -Une station SUN sparcstation offrant les services DNS Internet.

d-2.2 Sécurité informatique:

-Deux FireWalls Cisco asa.

-Deux FireWalls juniper.

-Un FireWalls ***Stonesoft.***

-Un serveur Alfatron biprocesseur offrant les services :

-Serveur antivirus officescan

-Serveur de domaines.

-Un serveur Alfatron biprocesseur offrant le service antivirus NAV.

I-5-Conclusion :

Dans ce chapitre nous avons présenté notre organisme d'accueil en spécifiant sa structure informatique cette dernière nous a permis d'avoir une idée du réseau existant au niveau de l'entreprise et le matériel utilisé, et de cerner ses objectifs pour enfin proposer une solution répondant en mieux à ses exigences. Dans le chapitre qui suit nous allons aborder quelques concepts sur la sécurité des réseaux informatiques.

II- Sécurité des réseaux informatiques[1][3][4][6]

II.1-Introduction :

Le réseau Internet est devenu un outil essentiel de communication depuis sa mise en service. Dés qu'un ordinateur d'un réseau est relié à Internet, la question de la sécurité se pose car l'Internet est une voie à double sens, c'est-à-dire elle permet non seulement d'émettre mais aussi de recevoir des informations mais il n'assure pas la sécurité de ces transactions. La garantie de la sécurité de ces informations est devenue un défi majeur pour les concepteurs des réseaux informatiques. Tout au long de ce chapitre nous allons présenter quelques mécanismes qui assurent les différents services de sécurité.

II-2. La sécurité : [3]

Les utilisateurs d'Internet doivent prendre un minimum de précautions, car leurs ordinateurs peuvent être facilement attaqués. La sécurité informatique est mise en œuvre pour éviter ce genre de problèmes, elle désigne un ensemble de techniques et de bonnes pratiques pour protéger les ordinateurs et les données qui y sont stockées, si elles sont élaborées par des spécialistes, les plus simples doivent être connues et mises en œuvre par les utilisateurs. La sécurité informatique est l'ensemble de moyens et de mesures mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles, et aussi pour empêcher l'utilisation non autorisée et le mauvais usage d'un ensemble de connaissances, de faits, de données ou de moyens.

II-2-1.Pourquoi les systèmes sont vulnérables ?

- La sécurité est chère et difficile et il y a un manque de budget pour ça mise en œuvre dans quelques entreprises.

- La sécurité ne peut être sûre à 100%, elle est même souvent inefficace.

- Les organisations acceptent de courir le risque, la sécurité n'est pas une priorité.

- De nouvelles technologies (et donc vulnérabilités) émergent en permanence.

- Les systèmes de sécurité sont faits, gérés et configurés par des hommes.

- Il n'existe pas d'infrastructure pour les clefs et autres éléments de cryptographie.

II-2-2.Les types d'attaques : [10] [15] [1]

1. Les attaques d'accès :

Une attaque d'accès est une tentative d'accès à l'information par un attaquant non autorisé. Cette attaque peut survenir à l'endroit où se trouve l'information et également pendant la transmission de celle-ci.

Catégories d'attaques d'accès :

a) Snooping : C'est le fait d'examiner des fichiers dans l'espoir de découvrir quelque chose d'intéressant.

b) Ecoute : C'est une attaque ou l'attaquant se place dans un endroit où l'information qui l'intéresse va probablement passer.

c) Interception : C'est l'insertion du système d'écoute sur le parcourt de l'information et sa capture avant l'atteinte de la destination.

2- Attaques de modification :

Une attaque de modification consiste à tenter de modifier les informations, elle peut arrivée partout où se trouve l'information et même lors de son transfert dans le réseau.

Catégories d'attaques de modification :

a) La modification : C'est la transformation de l'information.

b) L'insertion : C'est l'ajout des informations qui n'existent pas précédemment.

c) La suppression : C'est l'effacement d'informations existantes.

3- Attaques par déni de service (saturation) :

Une attaque de déni de service est une attaque qui rend impossible l'utilisation des ressources par les utilisateurs légitimes, en général elle est faite sans avoir accès aux informations du système et sans les modifiées.

Catégories d'attaques par déni de service :

a) Déni d'accès à l'information : C'est rendre l'information indisponible en la détruisant ou en la modifiant.

b) Déni d'accès aux applications : C'est une attaque contre un système sur lequel s'exécutent des applications qui traitent des informations.

c) Déni d'accès aux systèmes : Dans ce cas le système, les applications et l'information sont indisponibles.

d) Déni d'accès aux communications : C'est une attaque contre les médias de la communication.

4- Les attaques de répudiation :

Une attaque de répudiation consiste à donner de fausses informations ou de nier qu'un événement ou une transaction s'est réellement produite.

Catégories d'attaques de répudiation :

a) La mascarade : C'est la tentative d'agir à la place de quelqu'un ou d'un autre système.

b) Négation d'un événement : C'est le refus de reconnaître que l'action a été faite malgré son enregistrement.

5- Attaques par maliciels :

Le terme « maliciel » s'applique à une variété de programmes tels que les virus, les vers, et les chevaux de troies . . . etc

Catégorie d'attaques par maliciels :

a) Virus : Le virus est un morceau de code qui s'attache à des fichiers puis se propage d'un ordinateur à un autre par l'échange de ces fichiers ou bien s'attache aux secteurs système du disque dur.

b) Ver : C'est un code qui se propage d'un ordinateur à un autre à l'aide de la messagerie électronique.

c) Cheval de troie : C'est un logiciel d'apparence légitime conçu pour exécuter de façon cachée des actions à l'insu de l'utilisateur, il tente d'utiliser des droits appartenant à son environnement pour détourner , diffuser ou détruire des informations.

d) Keylogger : C'est un dispositif d'espionnage capable de créer une vidéo retraçant toute l'activité de l'ordinateur.

e) Bombe logique : C'est un programme résidant dont la charge finale est activée en fonction d'un ou plusieurs paramètres fournis par le système ou ses entrées/sorties. Effet à retardement plus ou moins grand.

II-3- Quelques techniques de défenses :

- Installer un anti-virus et le tenir à jour.
- Installer un Pare-feu ou Firewall ou bien Garde Barrière : contrôle l'accès à un ordinateur et affiche un message dés qu'un intrus essaye d'y pénétrer.
- Installer un logiciel anti-espion.
- Sauvegarder ses données sur des supports extérieures.
- Authentification : assurance que l'expéditeur d'un message est bien la personne qu'il prétend être, elle peut se faire par mot de passe.

- Contrôle d'accès : ensemble des stratégies et mesures adoptées par une entreprise pour se prémunir contre les différentes formes d'intrusions.
- Cryptographie (chiffrement) : est l'art de rendre des données secrètes.
- Test de vulnérabilité : outil de d
- érection des failles dans les systèmes de protections.
- Test d'intrusion : exploiter une vulnérabilité pour essayer d'accéder à un système.
- Audit : définir les types d'événements à inspecter sur tous les systèmes (exemple : établissement des connexions).

II-4- La planification de la sécurité du réseau : [3] [6]

Elle comporte quatre étapes :

a) Préparation : c'est la définition des limites et de la portée de la sécurité du réseau, inventaire et évaluation des biens informatiques et énoncé de la nature délicate de l'information résidant dans le réseau et circulant sur celui-ci.

b) Évaluation des menaces et exposition à celles-ci : c'est la détermination des menaces qui pèsent sur chaque bien du réseau, incidences pour l'organisation si ces menaces se matérialisaient et probabilité que cela se produise. Les résultats de cette étape permettent d'établir des degrés d'exposition pour chaque scénario sur les biens informatiques.

c) Évaluation des risques : à partir des degrés d'exposition établis pour les biens informatiques menacés, on analyse les points vulnérables du réseau et l'efficacité des mesures de protection en place afin de déterminer les risques associés à chaque scénario.

d) Politique de sécurité du réseau : c'est la préparation d'une politique de sécurité du réseau qui établit les étapes requises afin de réduire les risques à des niveaux acceptables.

III-5- Les services de sécurité : [1][4]

1- Confidentialité :

C'est la propriété qui préserve le secret de l'information, c'est-à-dire qu'une information ne doit être lue que par les personnes à qui elle est transmise. Le secret de confidentialité protège des attaques d'accès par des systèmes de contrôle d'accès pour chaque ressource. Cette propriété doit assurer la confidentialité des informations stockées dans des fichiers et aussi lors de leur transmission sur un réseau, cela est réalisé par le chiffrement de ces informations. Le service de confidentialité doit collaborer avec le service de responsabilité afin de réduire le risque d'intrusions des personnes non autorisées.

2- Intégrité :

Le service d'intégrité assure la conformité de l'information. Il permet aux utilisateurs d'avoir la certitude que l'information est correcte et qu'elle n'a pas été modifiée par un individu non autorisé. Le service d'intégrité protège les systèmes contre les attaques de modifications. Comme pour la confidentialité le service d'intégrité doit collaborer avec le service de responsabilité pour identifier correctement les personnes et ainsi même les modifications de fichiers à l'extérieure de l'entreprise peuvent être détectées.

3- Disponibilité :

Le service de disponibilité veille à ce que l'information puisse être utilisable, elle couvre aussi les systèmes de communications qui transmettent les informations entre sites et entre systèmes. Le service de disponibilité est utilisé pour rétablir les systèmes et les services en cas d'attaque déni de service (DoS) en réduisant les effets et en remettant les systèmes et les services en état de fonctionnement.

4- Responsabilité :

Le service de responsabilité se base sur l'identification, l'authentification et l'audit, mais ce service seul ne protège pas contre les attaques sans sa coordination avec les

autres services, notamment ceux de confidentialité et d'intégrité. Il fournit également un rapport des actions effectuées par l'utilisateur authentifié pour que les événements puissent être reconstitués.

5- Non répudiation :

La non répudiation c'est la propriété qui assure que l'auteur d'un acte ne peut ensuite dénier l'avoir effectué. Deux aspects spécifiques de non répudiation :

a) La preuve d'origine : un message ne peut être dénié par son émetteur.

b) La preuve de réception : un récepteur ne peut ultérieurement dénier avoir reçu un message.

III-6-les firewalls : [9][10][14]

Introduction

La technologie des pare-feux est apparue dans les années 80 pour palier à un nouveau problème de sécurité lié à l'émergence de l'Internet. En 1988, un employé de NASA Armes Research Center en Californie a envoyé un mémo par courrier électronique à son collègue qui a pu lire « Nous sommes actuellement attaqué par un virus Internet appelé *Morris Worm* ». Ce virus était la première attaque à grande échelle sur Internet. La communauté d'Internet a collaboré à la recherche de nouveaux moyens de protection contre ces nouvelles menaces. A la suite de cela nous avons pu voir apparaître de nouveaux produits de protection contre ces attaques comme les anti-virus et les pare-feux.

Un pare-feu est un élément de réseau informatique, logiciel et/ou matériel qui a pour fonction de sécuriser un réseau domestique ou professionnel en définissant les types de communication autorisés ou interdits.

L'origine du terme pare-feu se trouve au théâtre. Le pare-feu ou coupe-feu est un mécanisme qui permet, une fois déclenché, d'éviter au feu de se propager de la salle vers la scène. En informatique un pare-feu est donc une allégorie d'une porte

empêchant feu est appelé Périphérique de protection en bordure (en anglais : Border Protection Device, ou BPD).

Peu importe le domaine dans lequel on parle de pare-feu, la définition nous ramène toujours à quelque chose bloquant ou empêchant autre chose de pénétrer librement quelque part.

2. *Qu'es ce qu'un pare-feu ?*

Un pare-feu est un système ou un groupe de système qui gère les contrôles d'accès entre deux réseaux. Plusieurs méthodes sont utilisées à l'heure actuelle.

Deux mécanismes sont utilisés : le premier consiste à interdire le trafic, et le deuxième à l'autoriser.

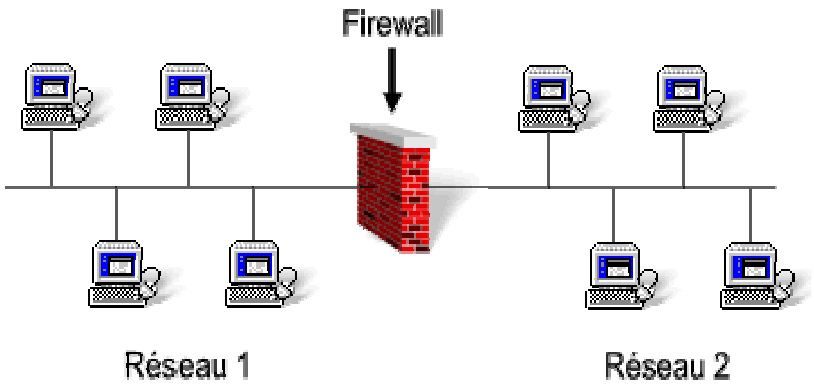


Figure-3- Pare-feu entre deux réseaux.

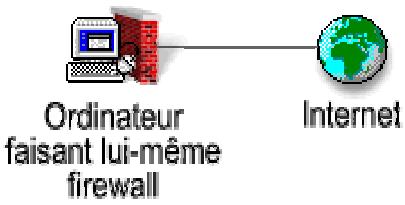


Figure-4- Pare-feu entre l'internet et 1 pc.

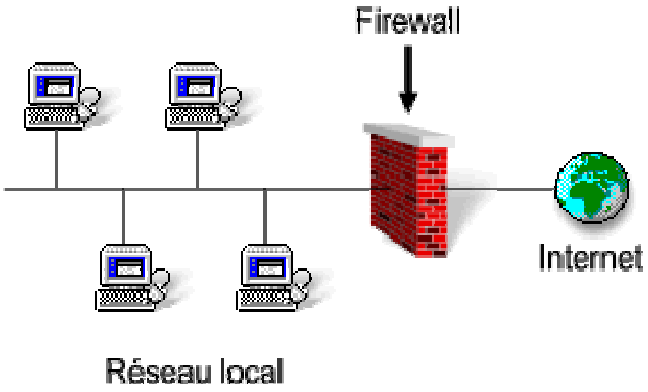


Figure-5- Pare-feu entre l'internet et un réseau de pc.

3. *Les protections que doit offrir tout système informatique :*

Le pare-feu est un système de protection basic, si on va installer un pare-feu, le premier choix est, Qu'est qu'il faut protéger quand on sera connecter a internet, les trois Risques potentiels sont :

Les données : les informations stoker dans un pc

Les ressources : le matériel.

La réputation.

4. *De quoi protège un pare-feu ?*

Certains pare-feux laissent uniquement passer le courrier électronique. De cette manière, ils interdisent toute autre attaque qu'une attaque basée sur le service de courrier. D'autres pare-feux, moins strictes, bloquent uniquement les services reconnus comme étant des services dangereux.

Généralement, les pare-feux sont configurés pour protéger contre les accès non authentifié du réseau externe. Ceci, plus qu'autre chose, empêche les vandales de se loger sur des machines de réseau interne, mais autorise les utilisateurs de communiquer librement avec l'extérieur.

Les pare-feux sont également intéressants dans le sens où ils constituent un point unique où l'audit et la sécurité peuvent être imposés. Tous les échanges passeront par lui. Il pourra donner des résumés de trafic, des statistiques sur ce trafic, ou encore toutes les connexions entre les deux réseaux.

5. *De quoi ne protège pas un pare-feu ?*

Un pare-feu ne protège pas des attaques qui ne passent pas par lui… Certaines entreprises achètent des pare-feux à des prix incroyables alors que certains de leurs employés sont parfois connectés par modem au monde extérieur.

Il est important de noter qu'un pare-feu doit être à la mesure de la politique de sécurité globale du réseau.

Un pare-feu ne peut protéger l'entreprise de menaces venant de l'intérieur de l'entreprise… Si un espion industriel décide de faire sortir des données, il y arrivera, surtout sur disquette… Il vaut mieux vérifier qui a accès aux informations que de mettre un pare-feu dans ce cas.

7. *Quelles sont les points à prendre en compte pour un pare-feu ?*

Le plus important est de refléter la politique de sécurité choisit par l'organisation. Entre tout interdire et tout autoriser, il y a différent degrés de paranoïa. Le choix final doit être le résultat d'une politique globale de sécurité plus que d'une décision d'un ingénieur…

La deuxième est de savoir le degré de contrôle nécessaire. Après avoir analysés les risques, il faut définir ce qui doit être autorisé et interdit.

Le troisième point est financier : c'est de savoir le budget alloué au pare-feu.

8- Les différents types de filtrages :

8.1- Le filtrage simple de paquet (Stateless) :

8.1.1- Le principe :

C'est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre en se basant sur :

- L'adresse IP Source/Destination.
- Le numéro de port Source/Destination.
- Le protocole de niveaux 3 ou 4.

Cela nécessite de configurer le pare-feu ou le routeur par des règles de filtrages, généralement appelées des ACL (Access Control Lists).

8.1.2 Les limite :

Le premier problème vient du fait que l'administrateur réseau est rapidement contraint à autoriser un trop grand nombre d'accès, pour que le pare-feu offre une réelle protection. Par exemple, pour autoriser les connexions à Internet à partir du réseau privé, l'administrateur devra accepter toutes les connexions Tcp provenant de l'Internet avec un port supérieur à 1024. Ce qui laisse beaucoup de choix à un éventuel pirate.

8.2 Le filtrage de paquet avec état (Stateful).

8.2.1 Le Principe.

L'amélioration par rapport au filtrage simple, est la conservation de la trace des sessions et des connexions dans des tables d'états internes au pare-feu.

Le pare-feu prend alors ses décisions en fonction des états de connexions, et peut réagir dans le cas de situations protocolaires anormales. Ce filtrage permet aussi de se

protéger face à certains types d'attaques DoS.

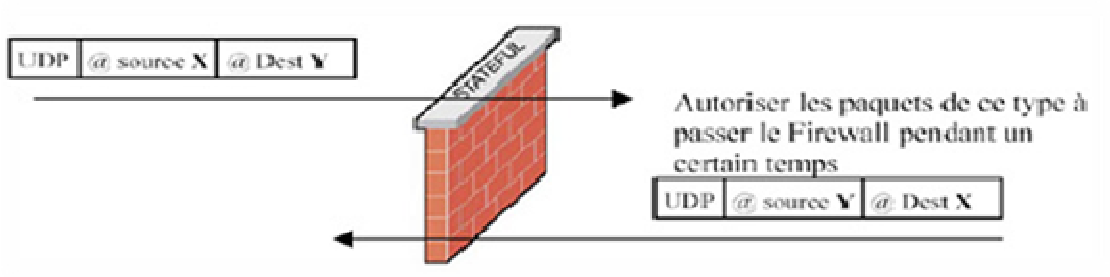


Figure-6- Pare-feu en stateful.

Pour le protocole Ftp, c'est plus délicat puisqu'il va falloir gérer l'état de deux connexions. En effet, le protocole Ftp, gère un canal de contrôle établi par le client, et un canal de données établi par le serveur. Le pare-feu devra donc laisser passer le flux de données établi par le serveur. Ce qui implique que le pare-feu connaisse le protocole Ftp, et tous les protocoles fonctionnant sur le même principe. Cette technique est connue sous le nom de filtrage dynamique (Stateful Inspection).

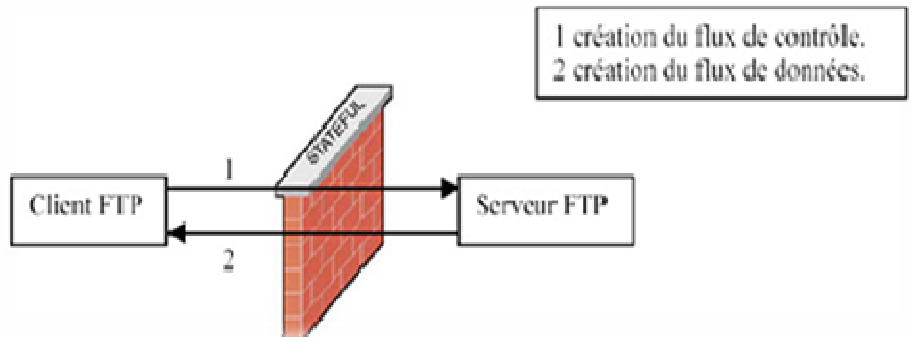


Figure-7-Pare-feu en stateful connections FTP.

8.2.2 Les limite :

Tout d'abord, il convient de s'assurer que les deux techniques sont bien implémentées par les pare-feux, car certains constructeurs ne l'implémentent pas toujours correctement. Ensuite une fois que l'accès à un service a été autorisé, il n'y a

aucun contrôle effectué sur les requêtes et réponses des clients et serveurs. Un serveur Http pourra donc être attaqué impunément. Enfin les protocoles maisons utilisant plusieurs flux de données ne passeront pas, puisque le système de filtrage dynamique n'aura pas connaissance du protocole.

8.3 Le filtrage applicatif (ou pare-feu de type proxy ou proxyin applicatif):

8.3.1- Le principe.

Le filtrage applicatif est réalisé au niveau de la couche Application. Pour cela, il faut extraire les données du protocole de niveau 7 pour les étudier. Les requêtes sont traitées par des processus dédiés, par exemple une requête de type Http sera filtrée par un processus proxy Http. Le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole. Cela implique que le pare-feu proxy connaisse toutes les règles protocolaires des protocoles qu'il doit filtrer.

8.3.2- Les limite :

Il est extrêmement difficile de pouvoir réaliser un filtrage qui ne laisse rien passer, vu le nombre de protocoles de niveau 7. En outre le fait de devoir connaître les règles protocolaires de chaque protocole filtré pose des problèmes d'adaptabilité à de nouveaux protocoles ou des protocoles maisons.

8.4- Que choisir ?

Tout d'abord, il faut nuancer la supériorité du filtrage applicatif par rapport à la technologie Stateful. En effet les proxys doivent être paramétrés suffisamment finement pour limiter le champ d'action des attaquants, ce qui nécessite une connaissance des protocoles autorisés à traverser le pare-feu. Ensuite un proxy est plus susceptible de présenter une faille de sécurité permettant à un pirate d'en prendre le contrôle, et de lui donner un accès sans restriction à tout le système d'information.

Il faut protéger le proxy par un pare-feu de type Stateful Inspection. Ne pas installer les deux types de filtrage sur le même pare-feu, car la compromission de l'un entraîne la

compromission de l'autre. Enfin cette technique permet également de se protéger contre l'ARP spoofing.

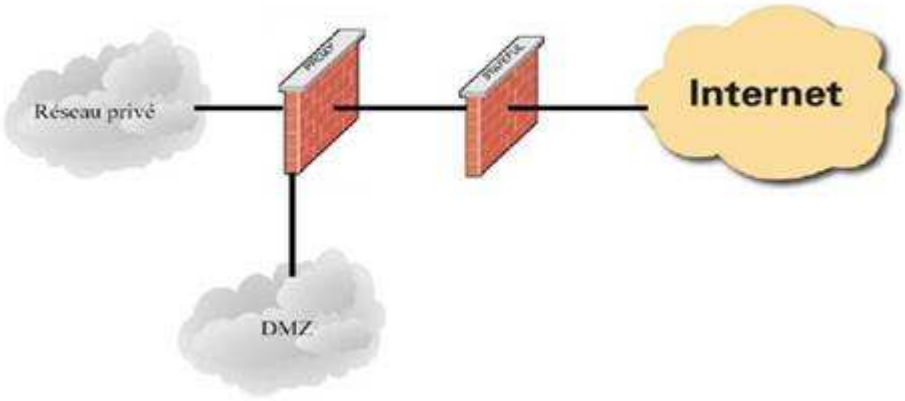


Figure-8- 2pare-feux en stateful entre l'internet, une DMZ et Réseau privé.

9 *Les différents types de pare-feux.[6]*

9.1 *Les pare-feux bridge.*

Ces derniers sont relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de pare-feu. Leurs interfaces ne possèdent pas d'adresse Ip, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le pare-feu est indétectable pour un hacker lambda. En effet, quand une requête ARP est émise sur le câble réseau, le pare-feu ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le pare-feu, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le contourner est de passer outre ses règles de drop. Toute attaque devra donc « faire » avec ses règles, et essayer de les contourner.

Dans la plupart des cas, ces derniers ont une interface de configuration séparée. Un câble vient se brancher sur une troisième interface, série ou même Ethernet, et qui ne doit être utilisée que ponctuellement et dans un environnement sécurisé de préférence.

Ces pare-feux se trouvent typiquement sur les Switch.

9.1.1- Avantages :

- Impossible de l'éviter (les paquets passeront par ses interfaces)

- Peu coûteux

9.1.2- Inconvénients :

- Possibilité de le contourner (il suffit de passer outre ses règles)

- Configuration souvent contraignante

- Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless).

9.2- Les pare-feux matériels :

Ils se trouvent sur les routeurs Cisco ou Nortel. Intégrés directement dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement ardue, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau.

Figure-9- Quelques pare-feu "matériels"

9.2.1- Avantages :

- Intégré au matériel réseau.

- Administration relativement simple.

- Bon niveau de sécurité.

9.2.2- Inconvénients :

- Dépendant du constructeur pour les mises à jour.

- Souvent peu flexibles.

9.3 Les pare-feux logiciels :

Présents à la fois dans les serveurs et les routeurs « faits maison », on peut les classer en plusieurs catégories :

Figure-10-deux pare-feux logiciel: jetico et zone alarm.

9.3.1 - Les pare-feux personnels :

Ils sont assez souvent commerciaux et ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final.

9.3.1.1-Avantages :

- Sécurité en bout de chaîne (le poste client)

- Personnalisable assez facilement

9.3.1.2- Inconvénients :

- Facilement contournable

- Difficiles a départager de par leur nombre énorme.

9.3.2 -Les pare-feux plus « sérieux » :

Tournant généralement sous linux, car cet OS offre une sécurité réseau plus élevée et un contrôle plus adéquat, ils ont généralement pour but d'avoir le même comportement que les pare-feux matériels des routeurs, à ceci prêt qu'ils sont configurables à la main. Le plus courant est iptables (anciennement ipchains), qui utilise directement le noyau linux. Toute fonctionnalité des pare-feux de routeurs est potentiellement réalisable sur une telle plateforme.

9.3.2.1-Avantages :

- Personnalisables

- Niveau de sécurité très bon

9.3.2.2-Inconvénients :

Nécessite une administration système supplémentaire Ces pare-feux logiciels ont néanmoins une grande faille : ils n'utilisent pas la couche bas réseau. Il suffit donc de passer outre le noyau en ce qui concerne la récupération de ces paquets, en utilisant une librairie spéciale, pour récupérer les paquets qui auraient été normalement « droppés » par le pare-feu. Néanmoins, cette faille induit de s'introduire sur l'ordinateur en question pour y faire des modifications... chose qui induit déjà une intrusion dans le réseau, ou une prise de contrôle physique de l'ordinateur, ce qui est déjà Synonyme d'inefficacité de la part du pare-feu.

10-Attaques, outils, défenses [13]

10.1-Scénarios d'attaques (Pénétrations de réseaux) :

Figure-11- Scénarios d'attaques.

Qu'est-ce qu'une backdoor ?

Une backdoor est un accès (« caché ») système qui permet à un pirate d'en prendre le contrôle à distance. Il existe une multitude de sortes de backdoor, et en général dans ce domaine, l'imagination des pirates rivalise avec l'incrédulité des utilisateurs. Voici quelques scénarios d'attaques plus ou moins classique.

10.1.1-Premier cas : Pas de protection :

Considérons un ordinateur victime sur lequel on a installé une backdoor en exploitant une des failles du système. L'attaquant a alors la possibilité d'utiliser tous les services présents sur cet ordinateur. Il lui suffit d'envoyer ses ordres à la backdoor et de récupérer les réponses.

10.1.2-Deuxième cas :

Filtrer les flux entrants illégaux :

La sécurité de notre système ne nous semblant pas infaillible, nous décidons alors d'installer un pare-feu avec états. Le trafic entrant est maintenant stoppé comme il se doit. Malheureusement, le pirate étant rusé et malicieux, il a pris soin de s'arranger pour que sa backdoor initie elle-même les sessions. Du coup le pare-feu laisse passer les requêtes de

l'attaquant qui sont considérées comme des réponses par celui-ci.

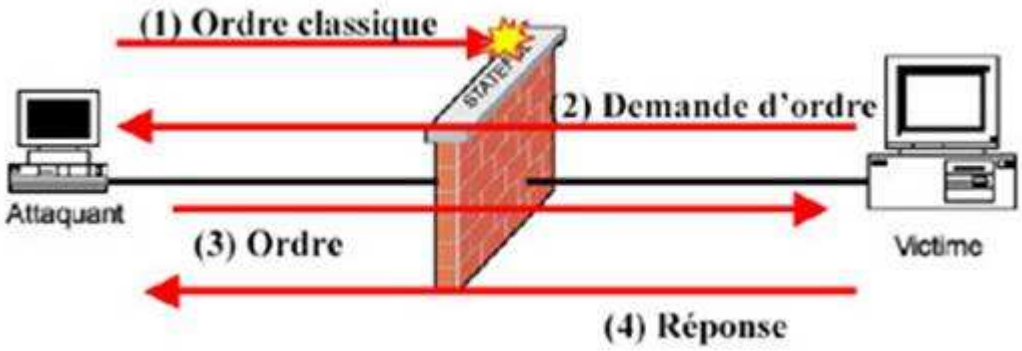


Figure-12- Scénarios d'attaques en présence de pare-feu.

10.1.3 -Troisième cas :

Bloquer les flux entrants et sortants :

Dans le cas précédent, le problème était dû aux flux sortants qui permettaient au cheval de Troie d'initier les sessions avec la machine de l'attaquant. Il s'agit donc de bloquer les flux sortants. Pour cela la défense insère donc un proxy afin de contrôler ce qui sort du réseau. Malheureusement le trojan peut encore sortir, certes avec plus de difficultés puisqu'il devra se renseigner sur les flux autorisés à sortir par le proxy, et les utiliser pour passer le proxy. Par exemple on peut encapsuler des ordres dans du HTTP (Ip over Http),dans du SSL (Ip over Ssl), DNS (Ip over Dns), Smtp (Ip over Smtp).

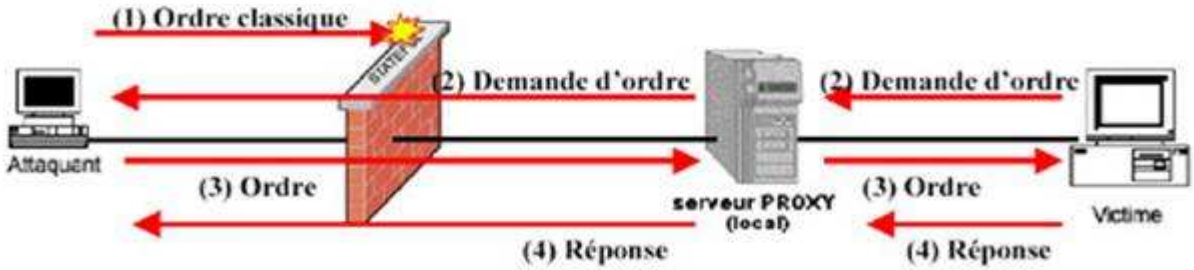


Figure-13- Scénarios d'attaques en présence de pare-feu et un serveur proxy.

Dans le cas d'un proxy avec authentification, le pirate fera preuve de grande imagination en réalisant un trojan capable de profiter des applications (comme IE par exemple) qui une fois qu'elles se sont authentifiées sont utilisées pour passer le proxy.

10.1.4 - Quatrième cas :

Protection locale via un pare-feu personnel :

L'idée du pare-feu personnel est de surveiller le trafic entrant et sortant de la machine infectée. Malheureusement ceux-ci sont fortement attaquables, on peut : Passer au-dessus du pare-feu via une application autorisée. Appel de CreateRemoteThread permettant de l'injection de code à la volée sous Windows.

Passer en dessous du pare-feu via une bibliothèque adaptée (Winpcap sous Windows ou pcap sous Linux).

Attaquer le pare-feu lui-même en tant qu'applicatif (Arrêt du processus).

10.1.5 -Cinquième cas :[6]

Piratage de VPN :

Un pirate mal intentionné installe un trojan sur l'ordinateur d'un commercial. L'ordinateur possédant entre autre un système Windows et un client VPN. Normalement, le client VPN fonctionne de telle sorte que toutes les liaisons réseaux n'étant pas dans le VPN ne fonctionnent pas. Malheureusement, il s'agit du même problème que pour les pare-feu personnels et le trojan permet à l'attaquant d'accéder au réseau de l'entreprise via le VPN.

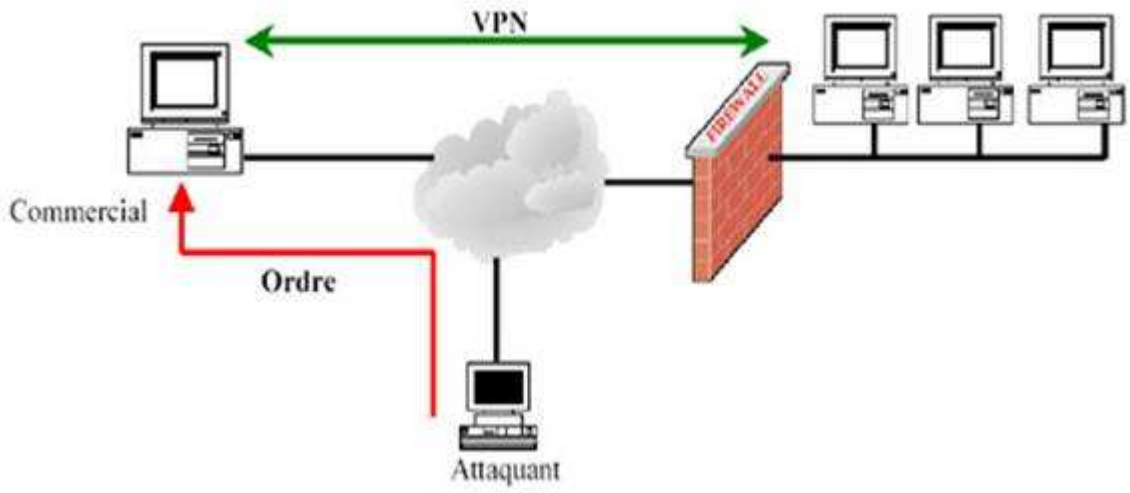


Figure-15-piratage de VPN.

On peut se rendre compte de l'importance de la robustesse du système d'exploitation, sur lequel est installé le VPN. Après une attaque réussie et la prise de contrôle en root de la machine par le pirate, celui-ci va essayer d'installer ce que l'on appelle un rootkit.

Il existe deux types de rootkit, les rootkit simples et les rootkit noyaux. Les rootkit simples se contentent de remplacer toute une collection de programmes système (ps, netstat, ifconfig, ...) lui permettant d'effacer les traces de son passage et ainsi masquer complètement sa backdoor. Un simple outil tel que Tripwire permet de vérifier l'intégrité des commandes, en enregistrant de façon cryptée les signatures (générées par une fonction de hashage) des fichiers de commandes en question.

Les rootkit noyaux sont beaucoup plus difficiles à détecter, puisqu'ils modifient le noyau et donc modifient son comportement. Par exemple rendre invisible un processus à chaque appel (non pas de la commande ps) mais des fonctions systèmes du noyau, qui elles même sont appelées par la commande ps. Evidemment un rootkit noyau modifie en plus les routines de journalisassions du système, masque les connexions réseaux, ... Pour se protéger des rootkit noyaux, le plus simple est de s'en prémunir. Pour cela, l'idéal est de patcher son noyau pour empêcher l'installation d'un rootkit, et de désactiver les LKM (Loadable Kernel Modules qui permettent au root d'introduire un nouveau code dans le système d'exploitation pendant que ce dernier est en cours d'exécution), malheureusement cela ne suffit pas toujours (voir kinsmod.c). Il existe un outil pour Linux capable d'un certain nombre de vérification de modules de backdoor. Cet outil s'appelle rkscan et permet de détecter les versions de rootkits les plus populaires.

10.2-Les techniques et outils de découvertes de pare-feu :

Il existe beaucoup d'outils et beaucoup de techniques permettant d'identifier un pare-feu. L'objectif de ce paragraphe est d'en exposer quelques-uns et quelques-unes. Il est évident que la plupart des outils utilisés par les pirates pour découvrir les pare-feux sont utilisables pour une activité tout aussi louable telle que la vérification du bon fonctionnement du pare-feu et de la robustesse du réseau.

Dans un premier temps il convient de localiser le ou les pare-feux. La localisation du pare-feu ne pose pas de gros problèmes, un simple traceroute (ou tracert.exe) suffira, bien que dans certains cas netcat apporte de meilleurs résultats.

Exemple :

```
C:> nc -v -n 10.10.1.8 25
(UNKNOWN) [10.10.1.8] 25 (?) open
421 10.10.1.8 Sorry, the firewall does not provide mail service to you.
```

Ensuite l'attaquant cherchera à identifier le pare-feu, soit en espérant exploiter une faille même du pare-feu, soit il cherchera à identifier les règles du pare-feu afin d'y détecter une faille dans le filtrage de paquet. Pour identifier les règles d'un pare-feu, il faut utiliser un scanner de port. Il existe de nombreux scanner de ports, les plus connus sont Firewalk, Nmap et Hping2.

10.2.1- Firewalk :

Le Firewalking est une technique qui permet de déterminer les règles de filtrages de niveau 4 (Transport) sur les équipements (routeurs, pare-feu, passerelles) qui acheminent des paquets de niveau 3 (Réseau).

Le principe de cette technique repose sur le champ Ttl (Time To Live) des en-têtes IP des paquets. C'est à dire le nombre d'équipement (routeur) que peut traverser le paquet. Le logiciel traceroute utilise aussi la technique du Ttl. Lorsque l'on envoie un paquet Udp avec un Ttl de 1, le premier routeur recevant le paquet émettra un paquet Icmp Ttl-exceeded. Et l'on répète le procédé en augmentant le Ttl de 1 à chaque fois. En fait ce procédé peut être réalisé avec d'autres protocoles de niveau 4 comme Tcp ou de niveau 3 comme Icmp.

Firewalk fonctionne en construisant des paquets avec un IP Ttl calculé de façon à expirer sur un segment situé après le pare-feu. En fait si le paquet est autorisé par le pare-feu, il pourra le passer et expirera comme prévu en envoyant un message "Icmp Ttl expired in transit". A l'inverse, si le paquet est bloqué par l'ACL du pare-feu, il sera abandonné et aucune réponse ne sera envoyée ou bien un paquet de filtre admin Icmp

de type 13 sera envoyé.

Il est possible de bloquer les paquets Icmp Ttl EXPIRED au niveau de l'interface externe, mais le problème est que ses performances risquent d'en prendre un sérieux coup car des clients se connectant légitimement ne sauront jamais ce qui est arrivé à leur connexion.

10.2.2-Nmap :

Nmap (Network Mapper) est certainement le scanner de port le plus célèbre disponible sous linux, Windows et même MAC. En règle générale, Nmap vérifie que l'hôte à scanner est connecté au réseau. Il réalise pour cela à la fois un Tcp ping sur le port 80 et un ping Icmp normal. Ce comportement peut être détecté par un IDS (Inspection Detection System) et pour cela on peut changer le comportement de Nmap. Nmap permet d'effectuer différents types de scans, en voici les exemples principaux :

- ✓ **Tcp connect:** une connexion Tcp habituelle est tentée sur chaque port. Inconvénient, ce genre de scan est visible dans les logs des pare-feux. Les noms de services sont associés aux ports ouverts par le fichier Nmap-services et non services. Il n'est donc pas exclu que le service désigné soit faux. Avantage, possibilité de déterminer l'utilisateur sous lequel est lancé un démon via Ident.
- ✓ **Syn scan :** Seul un paquet Syn est envoyé. Si le port est ouvert, un Syn|ACK est renvoyé, sinon un RST est renvoyé. En cas de port ouvert Nmap renvoie un paquet RST pour fermer la connexion immédiatement. Avantages, rapide et moins détectable. Fait une différence entre les ports filtrés et ouverts. Inconvénient, impossibilité de déterminer l'utilisateur via Ident.
- ✓ **IDLE scan :** Une machine "zombie" permet de masquer la source du scan. Avantages, quasiment impossible à tracer, permet de déterminer les règles du pare-feu à partir du zombie plutôt que de la machine qui initie le scan. Inconvénients, pas de prise d'empreinte d'OS, ni d'utilisation de Ident.

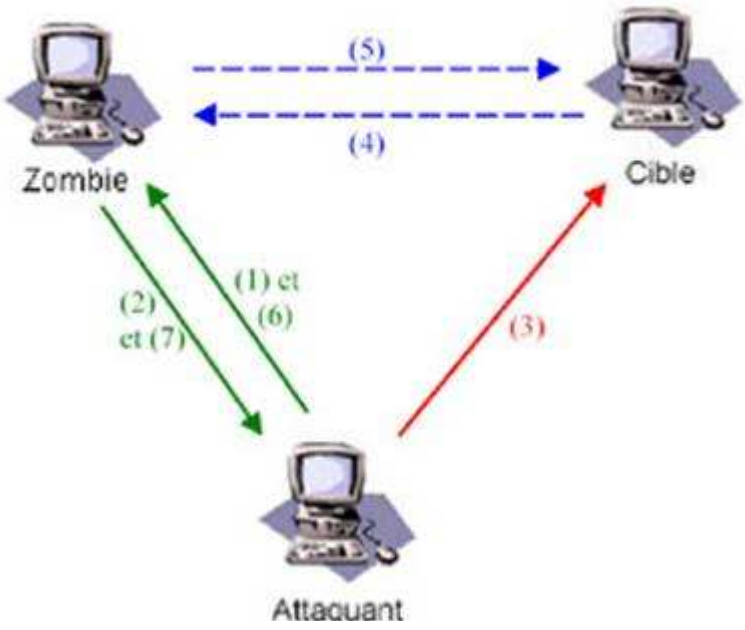


Figure-16- Schéma d'une attaque.

(0) S'assurer que la machine zombie n'est pas trop chargée pour permettre de bien mesurer l'incrémentation (un petit calibrage avant le scan est donc nécessaire en envoyant une dizaine de paquets Syn).

(1) et (6) Envoi d'un paquet Syn|ACK au zombie pour récupérer l'IP ID (le numéro de séquence).

(2) et (7) Réponse à (1) et (6) par un paquet RST contenant l'IP ID du zombie.

(3) Envoi d'un paquet Syn à la cible avec comme adresse source celle du zombie.

(4) Si le port est ouvert, la cible répond en envoyant un paquet Syn | ACK au zombie, sinon par un paquet RST.

(5) Le zombie incrémente son IP ID, et répond à la cible en envoyant un paquet RST à la cible.

(8) Il est aussi conseillé de tester plusieurs fois chaque port pour éviter les faux-positifs.

- ✓ **FIN, XMAS et NULL scans:** envoi respectivement de paquet FIN, de paquet FIN| URG |PSH et de paquet sans aucun flag Tcp activé. Avantages, contournement de certains pare-feux. Inconvénient, ne fonctionne pas contre certains OS qui n'appliquent pas les normes à la lettre (comme Windows, IRIX, ...)

- ✓ **SCAN Udp**: Envoi d'un paquet Udp vide sur chaque port. Les ports fermés retournent un paquet Icmp port unreachable. Avantage, permet d'avoir des informations sur NFS, TFtp et certaines backdoor. Inconvénient, très lent.
- ✓ **Scan RPC (Remote Procedure Call):** envoi de commandes SunRPC. Avantage, détermine s'il s'agit bel et bien de port RPC et si oui, de quel programme et/ou version il s'agit. Inconvénient, assez voyant.
- ✓ **ACK et Window scan:** Envoie respectivement un paquet ACK avec un numéro de séquence aléatoire et un paquet ayant une taille de fenêtre non valide. Les ports qui ne répondent pas par un RST sont filtrés. Avantage, permet de vérifier si un port est filtré et s'il l'est avec une règle stateful. Inconvénient, Le Window scan ne fonctionne pas sur tous les systèmes d'exploitation.

Scans personnalisés : option --scanflags L'utilisateur spécifie les flags Tcp qu'il souhaite activer.

Scan de protocoles : option -sO Permet de déterminer quels sont les protocoles supportés par le système scanné, généralement un routeur.

Il n'est pas difficile de scanner dans l'anonymat :

Changer la vitesse du scan, grâce à l'option -T suivie des arguments Paranoïd, Sneaky, Polite, Normal, Aggressive or Insane. Nmap attend 5 minutes entre chaque paquet envoyé en mode Paranoïd et 15 secondes en mode Sneaky.

Utiliser des leurres (decoys, option -D) en envoyant d'autres paquets IP spoofés et semblant provenir d'une autre adresse. Sur un réseau local on peut spoofer (option -S) l'adresse source, et récupérer les réponses par sniffage en mode promiscuous. Sur la technique de l'IDLE scan.

L'auteur de Nmap, Fyodor, décrit sa technique de prise d'empreinte du système d'exploitation (fingerprinting) dans l'article « Détection d'OS distante par prise d'empreinte de pile Tcp/IP » traduit en français par ArHuman, et l'original en anglais « Remote OS detection via Tcp/IP Stack FingerPrinting ». Le principe repose sur le test de

différentes particularités des piles Tcp/IP des différents systèmes d'exploitation, lesquelles sont :

Le type d'incrémentation du numéro de séquence initiale (ISN).

La présence ou non du flag IP Don't Fragment.

Des tests sur les tailles de fenêtres.

Le type de service (ToS).

Différents tests sur des paquets Tcp.

Différents tests au niveau Icmp, comme la limite de vitesse d'envoi de certains types de paquets Icmp d'erreurs.

Nmap utilise l'option -O pour effectuer une prise d'empreinte du système, et en général on associe l'option -v (Verbose) pour obtenir des informations supplémentaires comme les ports servant à effectuer les tests de la prise d'empreinte.

Il est important de remarquer le fait que de scanner un pare-feu ou un système protégé par un pare-feu prend plus de temps qu'un système non protégé.

10.2.3 -HPING2 :

HPING2 est différent de Nmap d'abord parce qu'il est beaucoup plus configurable. On peut facilement modifier n'importe quel octet de l'entête TcpIP. Cela permet d'être réellement créatif au niveau des techniques de balayage à des fins de reconnaissance. On peut bien sûr insérer des données malveillantes dans les paquets (buffer overflow, trojan, ...) et les utiliser pour pénétrer des réseaux.

HPING2 permet de :

1- Tester les règles de pare-feu.

2- De faire du scan sophistiqué.

3- De tester les performances d'un réseau utilisant différents protocoles, le ToS et la fragmentation.

4- De faire du firewalk.

5- De l'empreinte de système d'exploitation.

Actuellement, la version HPING3 est en train d'être développé par Salvatore SanFilippo, et d'autres volontaires. Selon son site Web, Hping3 sera nettement supérieur à l'actuelle version. Il y aura des améliorations d'installation, des outputs plus lisibles, et sera exploitable par script. Le statut actuel du projet peut être suivi. Il existe aussi des outils d'évaluation de vulnérabilité :

Les payants : Retina (eEye) , NetRecon (Symantec), ISS Internet Scanner (ISS), Cybercop Scanner (Network Associates).

Les freewares : Nessus (Renaud Déraison).

10.2.4 NESSUS :

Nessus a été écrit par Renaud Deraison (depuis début 1998). Nessus est devenu le Linux de l'évaluation de la vulnérabilité. Nessus emploie un modèle de plug-in extensible qui permet à la sécurité d'ajouter à la demande des modules d'exploration. Nessus utilise un langage de script NASL (Nessus Attack Script Language) pour écrire des tests de sécurité rapidement et facilement. Nessus est basé sur une architecture client-Serveur, le serveur réalise les attaques et tourne sur un système UNIX; les clients initialisent les attaques et existent sur différentes plates-formes X11, Win32 et un client Java. Le fait d'être open source et d'utiliser des plug-in permet à Nessus d'être mis à jour régulièrement au niveau de sa base de données d'attaques et d'être à la pointe de la technologie.

10.2.5 -Scanners en ligne :

Un autre moyen de sonder une cible sans passer par notre propre machine, donc sans se faire loguer ou presque, est d'utiliser les outils de balayage "online". En effet, ce n'est plus la machine "pirate" qui envoie la requête vers la machine cible, mais c'est le site web proposant ce service qui va envoyer à notre place la requête de scan et qui nous remonte la la réponse via HTTP.

Exemple:

- Le sanner TCP online de FrameIp qui permet de scanner une rangée de ports TCP.

10.3 Configuration théorique des défenses :

La configuration d'un pare-feu est l'élément clef de son efficacité. C'est la clef de son bon fonctionnement et de son efficacité.

Il existe deux politiques de configurations différentes en ce qui concerne la «base » du pare-feu.

Tout autoriser sauf ce qui est dangereux.

Tout interdire sauf ce dont on a besoin et ce en quoi on a confiance : cette politique est beaucoup plus sécuritaire.

Suivant la politique de l'entreprise, l'accès ou non à certains services peut être bloqué dans les deux sens. Cela peut servir, par exemple, à empêcher le jeu en ligne, ou autres activités que l'entreprise ne désire pas voir se dérouler sur ses propres infrastructures.

10.4 Les réactions des pare-feu aux attaques classiques :

10.4.1 IP spoofing :

L'IP spoofing consiste à modifier les paquets IP afin de faire croire au pare-feu qu'ils proviennent d'une adresse IP considérée comme « de confiance ». Par exemple, une IP présente dans le réseau local de l'entreprise. Cela laissera donc toute latitude au hacker de passer outre les règles du pare-feu afin d'envoyer ses propres paquets dans le réseau de l'entreprise. Les derniers pare-feux peuvent offrir une protection contre ce type d'attaque, notamment en utilisant un protocole VPN, par exemple IPSec.

10.4.2 DOS et DDOS :

Le DOS, ou Denial Of Service attack, consiste à envoyer le plus de paquets possibles vers un serveur, générant beaucoup de trafic inutile, et bloquant ainsi l'accès aux utilisateurs normaux. Le DDOS, pour Distributed DOS, implique venir de différentes machines simultanées, cette action étant le plus souvent déclenchée par un virus : ce dernier va d'abord infecter nombre de machines, puis à une date donnée, va envoyer depuis chaque ordinateur infecté des paquets inutiles vers une cible donnée.

10.4.3-Port scanning :

Ceci constitue en fait une « pré-attaque » (Etape de découverte). Elle consiste à déterminer quels ports sont ouverts afin de déterminer quelles sont les vulnérabilités du système. Le pare-feu va, dans quasiment tous les cas, pouvoir bloquer ces scans en annoncent le port comme « fermé ». Elles sont aussi aisément détectables car elles proviennent de la même source faisant les requêtes sur tous les ports de la machine. Il suffit donc au pare-feu de bloquer temporairement cette adresse afin de ne renvoyer aucun résultat au scanner.

10.4.4 Exploit :

Les exploits se font en exploitant les vulnérabilités des logiciels installés, par exemple un serveur Http, Ftp, etc... ce type d'attaque est très souvent considéré comme des requêtes tout a fait « valides » et que chaque attaque est différente d'une autre, vu que le bug passe souvent par reproduction de requêtes valides non prévues par le programmeur du logiciel. Autrement dit, il est quasiment impossible au pare-feu d'intercepter ces attaques, qui sont considérées comme des requêtes normales au système, mais exploitant un bug du serveur le plus souvent. La seule solution est la mise à jour périodique des logiciels utilisés afin de barrer cette voie d'accès au fur et à mesure qu'elles sont découvertes.

11. Conclusion :

Nous avons vu, les différents types de pare-feux, les différentes attaques et parades. Il ne faut pas perdre de vue qu'aucun pare-feu n'est infaillible et que tout pare-feu n'est efficace que si bien configuré. De plus, un pare-feu n'apporte pas une sécurité maximale et n'est pas une fin en soi. Il n'est qu'un outil pour sécuriser et ne peut en aucun cas être le seul instrument de sécurisation d'un réseau. Un système comportant énormément de failles ne deviendra jamais ultra-sécurisé juste par l'installation d'un pare-feu.

II-7- Mécanismes de la sécurité : [1][3][11][12]

Pour qu'un système puisse fournir des services de sécurité, plusieurs mécanismes peuvent être mis en place, tel que le chiffrement, les signatures numériques, les certificats…etc. Nous allons présenter dans ce qui suit quelques mécanismes qui assurent les services de sécurité les plus importants.

1- Cryptographie :

L'homme a toujours ressenti le besoin de dissimuler des informations, bien avant même l'apparition des premiers ordinateurs et de machines à calculer. Depuis sa création, le réseau Internet a tellement évolué qu'il est devenu un outil essentiel de communication.

Cependant, cette communication met de plus en plus en jeu des problèmes stratégique liés à l'activité des entreprises sur le Web. Les transactions faites à travers le réseau peuvent être interceptées, d'autant plus que les lois ont du mal à se mettre en place sur Internet, il faut donc garantir la sécurité de ces informations, c'est la cryptographie qui s'en charge.

1-1- Définition :

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le verbe « chiffrer » est beaucoup plus utilisé que le verbe « crypter ».

La cryptologie est essentiellement basée sur l'arithmétique : Il s'agit dans le cas d'un texte de transformer les lettres qui composent le message en une succession de chiffres puis faire des calculs sur ces chiffres pour :

- d'une part les modifier de telle façon à les rendre incompréhensibles. Le résultat de cette modification (le message chiffré) est appelé cryptogramme (en anglais *ciphertext*) par opposition au message initial, appelé *message en clair* (en anglais *plaintext*).
- faire en sorte que le destinataire saura les déchiffrer.

1-2- Les fonctions de la cryptographie :

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via Internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

1-3- Les méthodes de cryptographie :

1-3-1- Quelques méthodes anciennes de cryptographie : [4] [14]

Le chiffrement n'a pas attendu l'invention des premiers ordinateurs pour se développer, mais il existait déjà plusieurs techniques de chiffrement pour sécuriser les échanges d'informations.

a) Substitution par décalage :

Le principe de ce chiffrement était très simple. Chaque lettre de l'alphabet est remplacée par une autre figurant quelques lettres plus loin dans l'alphabet. La clé était en fait le nombre de lettre de décalage.

Exemple :

Pour une clé de 3 on aura pour le texte suivant :

« Rendez vous 18h00 au quartier général » le texte chiffré :

« Uhqghc yrxv 41k33 dx txduwlgu jhqhudo ».

b) Substitution par tableau :

Ce procédé est basé sur un tableau de lettres accessible en connaissant leurs coordonnées : ligne et colonne. Les messages étaient donc écrits entièrement en chiffres. La clé à transmettre pour le déchiffrement du message est le tableau.

Exemple : Voici le tableau de lettres :

	1	2	3	4	5	6
1	A	B	C	D	E	F
2	G	H	I	J	K	L
3	M	N	O	P	Q	R
4	S	T	U	V	W	X
5	Y	Z	1	2	3	4
6	5	6	7	8	9	0
7		.	,	:	?	!

En utilisant ce tableau comme outil de chiffrement le texte :

« Rendez vous 18h00 au quartier général » devient

«3615321415527144334341715364226666711143713543113642231536712115321
5361126 »

1.3.2- Le chiffrement moderne :

Les méthodes anciennes étaient simples car elles étaient manipulées par l'homme. Le développement des outils informatiques et leur capacité à effectuer des opérations mathématiques très rapidement a permis la mise au point de méthodes de chiffrement de plus en plus complexes et efficaces. Aujourd'hui on distingue deux catégories de chiffrement : symétrique et asymétrique.

1.3.2.1- Chiffrement symétrique :

Il est aussi appelé chiffrement à clé privée ou chiffrement à clé secrète, il consiste à utiliser la même clé pour le chiffrement et pour le déchiffrement, en appliquant un algorithme sur les données à chiffrer. Ce chiffrement assure la confidentialité car seuls ceux qui connaissent la clé peuvent déchiffrer le message, mais il n'assure pas l'authentification car quiconque possède cette clé peut créer, chiffrer et envoyer un message. Aujourd'hui, il existe deux familles d'algorithmes de chiffrement symétrique : chiffrement par bloc et chiffrement par flux.

a- Chiffrement symétrique par bloc (Block Ciphers) :

Ces algorithmes chiffrent les données bloc par bloc. Le message original est découpé en plusieurs segments, dont la taille dépend de l algorithme de chiffrement (généralement 64 ou 128 bits, soit 8 ou 16 octets). Les opérations de chiffrement sont ensuite réalisées sur chacun de ces blocs, en prenant comme paramètre la clé symétrique pour produire un bloc chiffré de taille identique. Dans ce qui suit nous allons présenter deux exemples de chiffrement par blocs DES et AES.

Principe de DES:

DES est un algorithme de chiffrement symétrique qui transforme un bloc de 64 bits en un autre bloc de 64 bits, il manipule des clés individuelles de 56 bits représentées par 64 bits avec un bit de chaque octet servant pour le contrôle de parité.

D'une manière générale, on peut dire que DES fonctionne en trois étapes :

- Permutation initiale et fixe d'un bloc.
- Le résultat est soumis à 16 itérations d'une transformation.
- Le dernier résultat est transformé par la fonction inverse de la permutation initiale.

a-2-2- Principe de AES :

C'est un algorithme de chiffrement itératif par bloc, qui admet des clés de 128, 192 ou 256 bits ; le nombre Nb de tours est respectivement de 10, 12 ou 14 pour chacune des tailles de clé. Chaque bloc contient 16 *8 = 128 bits (16 octets), rangés dans un tableau 4*4. Chaque bloc subit les opérations suivantes :

1. Addition de la clé secrète (par un ou exclusif).

2. Transformation non linéaire d'octets : les 128 bits sont répartis en 16 blocs de 8 bits (8 bits=un octet), eux-mêmes dispatchés dans un tableau 4×4. Chaque octet est transformé par une fonction non linéaire S.

3. Décalage cyclique de lignes vers la gauche.

4. Brouillage des colonnes : Chaque colonne est transformée par combinaisons linéaires des différents éléments de la colonne (ce qui revient à multiplier la matrice 4×4 par une autre matrice 4×4). Les calculs sur les octets de 8 bits sont réalisés dans le corps à 28 éléments.

5. Addition de la clé de tour au dernier bloc obtenu.

b-Principe de l'algorithme RSA :

Le principe de cet algorithme est la génération d'une paire de clés : clé publique et clé privée à partir de deux grands nombres premiers. La force de cet algorithme réside dans le fait qu'il est mathématiquement difficile de trouver ces nombres premiers à partir de la valeur publique. Cet algorithme est utilisé pour le chiffrement et pour la signature électronique, et est aujourd'hui le plus utilisé.

2-3- Le hachage:

Le hachage est un cas particulier de chiffrement. Le principe de la fonction de hachage est que pour une donnée fourni en entrée (message) de taille quelconque, l'algorithme est cabale de générer un condensat (empreinte) de taille fixe à partir duquel il est impossible de trouver le message original

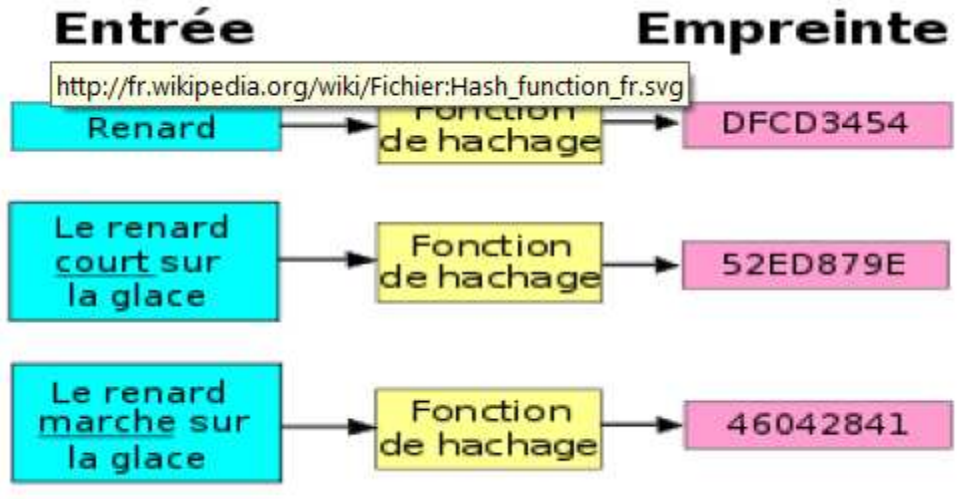


Figure-17- Rôle de hachage

3 -Certificats électroniques :

Les mécanismes à clé publique ne garantissent pas la sécurité des échanges, car cette clé peut appartenir à un imposteur au lieu à une personne de confiance, les infrastructures à clé publique sont conçues pour répondre au besoin de sécuriser la clé publique.

3-1- Définition d'infrastructure à clé publique :

Une infrastructure à clé publique (ou PKI - Public Key Infrastructure) est un ensemble de composants, moyens techniques, humains, documentaires et contractuels mis à la disposition d'utilisateurs pour assurer la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique.

3-2- Définition d'un certificat :

Un certificat électronique est une carte d'identité numérique dont l'objectif est d'identifier une entité physique ou non physique. Le certificat numérique ou électronique est un document permettant de valider le lien entre une signature électronique et son signataire. Le standard le plus utilisé pour la création des certificats est le X.509, et elles sont signées par une autorité pour garantir l'intégrité et la véracité des informations. Les champs les plus significatifs des certificats numériques sont les suivants :

- numéro de série.
- identifiant de l'algorithme de signature.
- nom de l'Autorité de Certification émettrice.
- nom distinctif du titulaire.
- dates de début et de fin de validité du certificat.
- la clé publique du titulaire.
- la liste des usages autorisés (signature, confidentialité…).
- le champ de certification par l'Autorité émettrice (signature de l'Autorité de Certification).

3.3- Classes de certificats :

Il existe trois classes de certificat électronique :

Classe I : ne garantit pas l'identité du titulaire du certificat mais seulement l'existence de son adresse e-mail.

Classe II : Garantit les informations du titulaire et de son entreprise (contrôlées par l'autorité de certification sur pièces justificatives transmises par voie postale).

Classe III : Idem à la Classe II, assure un contrôle supplémentaire de l'identité du titulaire.

3.4- Définition d'une autorité d'enregistrement (AE) :

Une autorité d'enregistrement vérifie la correspondance entre une clé publique et son propriétaire et aussi l'identité des demandeurs de certificats c'est le lien entre l'Autorité de Certification et les demandeurs de certificat. Les tâches qui sont confiées à une Autorité d'Enregistrement sont de : - réceptionner et traiter les demandes de certificats - établir que les demandeurs de certificat ont bien l'identité et les droits qui seront indiqués dans les propriétés du certificat. - réceptionner et traiter les demandes de révocation de certificats - établir que les demandeurs de révocation d'un certificat sont bien les titulaires du certificat. - archiver les dossiers de demande ou de révocation de certificats.

3.5- Définition de l'autorité de certification (AC) :

C'est elle qui valide la correspondance entre une personne/serveur/organisation et sa clé publique, après réception de la demande par l'AE, c'est elle qui génère ces certificats, les signes avant de les émettre et les gère durant tout leur cycle de vie. L'Autorité de Certification rédige la politique de certification et valide les déclarations de pratique de certification qui doivent être respectées par les différentes composantes de l'Infrastructure à Clé Publique (ICP). Elle est également responsable de la révocation des certificats et de la publication des listes de certificats révoqués.

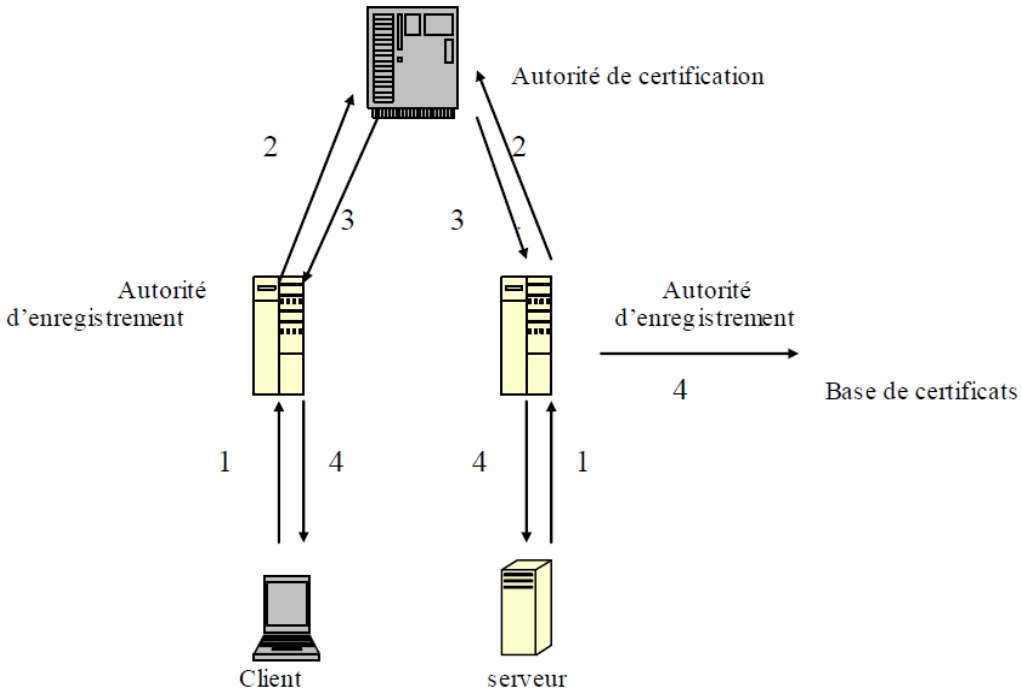


Figure-18- : création d'un certificat.

Les flux représentés sont les suivants :

-1- L'utilisateur final (client ou serveur) génère une paire de clés. Il émet une demande de certificat à son autorité d'enregistrement. Il transmet sa clé publique et les éléments prouvant son identité.

-2- L'autorité d'enregistrement vérifie que le demandeur du certificat est bien celui qu'il prétend être et après validation transmet la clé publique et les attributs de l'utilisateur à l'autorité de certification pour signature et création du certificat.

-3- L'autorité de certification concatène la clé publique avec les attributs propres au porteur qu'elle signe pour créer le certificat. Ce dernier est ensuite transmis à l'autorité d'enregistrement.

-4- L'autorité d'enregistrement transmet le certificat à son porteur elle peut éventuellement publier le certificat dans un annuaire pour qu'il soit facilement accessible aux interlocuteurs potentiel du porteur.

3-6- Fonctionnement :

Le principe de fonctionnement est le suivant:

- l'utilisateur A télécharge un certificat donné par l'utilisateur B.
- l'ordinateur de A va contrôler la validité et les paramètres de codage en se référant à une autorité de certification;
- la clé publique est envoyée à l'utilisateur B.
- à son tour, l'ordinateur de B, va contrôler la cohérence entre le certificat et les données reçues en se référant à l'autorité de certification;
- les données reçues peuvent être déchiffrées.

3-7- Utilité du certificat : Les certificats garantissent :

- la non-répudiation et l'intégrité des données avec la signature numérique ou signature électronique (avancée).
- la confidentialité des données grâce au chiffrement des données.
- l'authentification ou l'authentification forte d'un individu ou d'une identité non-physique.

II.8-Conclusion

Tout au long de ce chapitre on a abordé le rôle des pare-feux dans la sécurité et les différents mécanismes de sécurité tels que le chiffrement, les signatures numériques et les certificats électroniques. Ces mécanismes garantissent les différents services de sécurité : confidentialité, intégrité, disponibilité, responsabilité et non répudiation.

III-Analyse et conception :[5] [9][10]

Dans ce chapitre, nous abordons la phase d'analyse et spécification des besoins. Ainsi, nous présentons les besoins fonctionnels et non fonctionnels de notre application. Nous utilisons le langage UML comme un moyen simple et compréhensible afin de décrire les principaux cas d'utilisation.

1-Besoins fonctionnels

Cette partie décrit les exigences que le système doit satisfaire d'une façon informelle. Les fonctionnalités qu'on se propose de fournir dans notre logiciel sont les suivantes :

- Générer des statistiques relatives aux connexions Internet. Ces statistiques concernent particulièrement :
  - les sites web les plus visités avec des informations relatives aux nombres de visites, l'utilisation de la mémoire cache et de la bande passante,
  - les utilisateurs et les postes les plus actifs sur le réseau avec une description des activités.
  - les pics d'utilisation du réseau (évolution du trafic au cours du temps),
  - le taux d'exploitation de la mémoire cache.
- Filtrer les statistiques à générer selon les critères définis par l'utilisateur : les critères de filtrage sont :
  - par utilisateur.
  - par poste.
  - par protocole.
  - par date.
- Assurer une navigation entre les statistiques suivant certaines relations qui peuvent exister entre elles.
- Générer à la demande un rapport détaillé contenant toutes les statistiques.

2-Besoins non fonctionnels :

- L'application doit présenter des interfaces conviviales et ergonomiques afin de faciliter l'utilisation de l'application par un utilisateur qu'il soit spécialiste ou non.
- Seuls les journaux de Bluecoat seront pris en considération. Afin de mieux comprendre les fonctionnalités de notre outil nous présentons les diagrammes de cas d'utilisations qui nous jugeons les plus représentatifs.

3-les cas d'utilisation du système :

Dans ce qui suit, nous présentons un formalisme semi formel de spécification des besoins de notre système, à l'aide des diagrammes de cas d'utilisation [figure19] accompagnés par une explication textuelle de ses principaux cas d'utilisation.

Le cas d'utilisation «**Configurer**» :L'administrateur peut communiquer à l'outil un fichier « log ». Ce dernier l'intercepte, l'analyse, le convertit dans un format générique et le stocke sous ce format dans une base de données, ensuite l'administrateur introduit le nombre d'enregistrements à prendre en considération lors de l'affichage des graphes ainsi qu'il peut configurer les paramètres de filtrage.

- Le cas d'utilisation «**Editer rapport**» : L'administrateur peut introduire directement ou au fur et à mesure de la navigation les différentes statistiques à inclure dans le rapport et il a la possibilité d'enregistrer le rapport final sous format PDF qui pourrait être imprimé par la suite

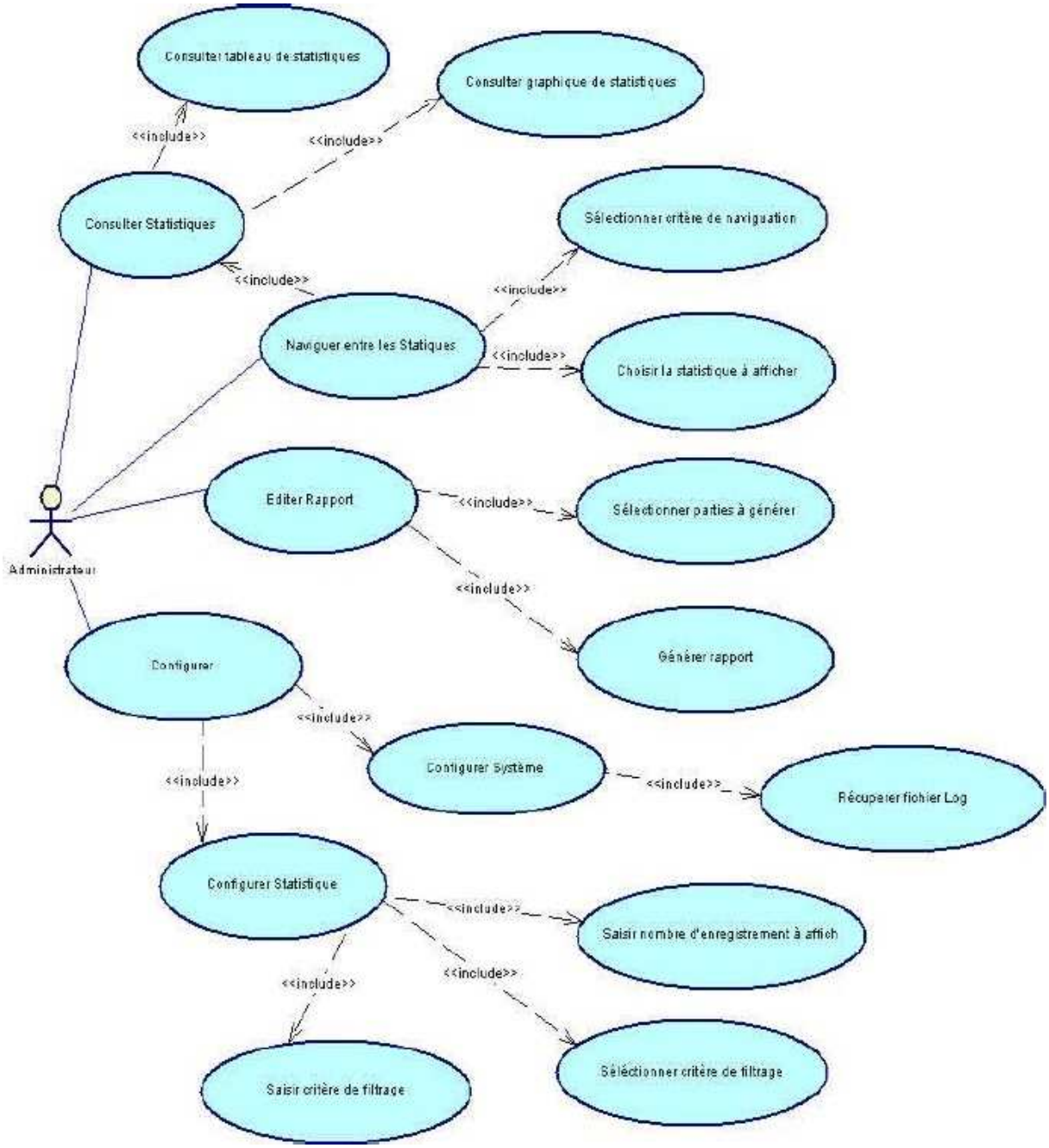


Figure 19 : Le diagramme de cas d'utilisation

- ✓ Le cas d'utilisation «**Naviguer entre les statistiques**» :L'administrateur peut naviguer aisément entre les différentes statistiques ; un scénario possible consiste à explorer les statistiques relatives aux sites les plus visités, et ensuite dégager les informations en relation avec ces derniers comme ceux relatives aux utilisateurs, aux postes qui les ont consultés, aux protocoles,… etc

- ✓ Le cas d'utilisation «**Consulter statistiques**» : L'administrateur, après avoir choisi un critère de filtrage (par date, par poste, par url,…etc.), peut visualiser les statistiques correspondantes sous formes tabulaire et graphiques.

4- Conception du logiciel :

Comporte une première section relative à la conception générale de cette application. Cette section décrit deux solutions envisagées et justifie le choix de la solution retenue, et par suite, décrit la décomposition de l'application en paquetages et les dépendances entre eux. La deuxième section décrit la conception détaillée de la solution retenue suivant une approche orientée objet. La dernière section décrit la base de données utilisée pour le stockage des informations obtenues à partir des fichiers « log ».

I-Conception générale :

1. Solutions envisagées et choix d'une solution :

Notre conception doit prévoir deux transformations de données. La première transformation permet le passage des données du fichier « log » sous leur format brut vers une forme adaptée aux calculs ultérieurs. La deuxième transformation reprend les résultats de la première transformation et permet de déduire les résultats à afficher sous une forme facile, intelligible et conviviale. La difficulté de ce travail réside dans la navigation entre les différentes statistiques. La navigation consiste en la transition d'une statistique à une autre en se basant sur un critère déjà fixé dans une phase de navigation préalable.

Par exemple, après la consultation des statistiques concernant les utilisateurs les plus actifs, un des utilisateurs est sélectionné et il est alorspossibled'obtenir d'autres statistiques comme les sites les plus visités ou le débit généré relatifs à l'utilisateur sélectionné. Ainsi nous obtenons la liste des sites les plus visités par l'utilisateur sélectionné. Nous avons envisagé deux solutions possibles qui diffèrent essentiellement au niveau de l'organisation des flots de données entre les modules et la manière d'assurer la navigation

Une première solution consiste à lire le fichier Access.log, stocker les résultats dans des variables en mémoire centrale et ensuite passer à la génération des statistiques qui seront affichées par la suite en effectuant des calculs sur ces variables. Cette solution présente plusieurs inconvénients. Parmi les problèmes qui se posent, la lecture du fichier « log » de nouveau à chaque fois qu'on veut générer une nouvelle statistique ou tracer une nouvelle courbe. D'autre part, le nombre de variables intermédiaires en

mémoire centrale risque d'être important étant donné que l'application permet de consulter les statistiques de manière restreinte à différents critères ainsi qu'elle offre des possibilités de navigation variées. Notons enfin que la sélection des données à utiliser pour obtenir les résultats à afficher, selon un ou plusieurs critères, ne peut pas se réaliser facilement en travaillant directement sur ces variables. Une deuxième solution consiste en l'utilisation d'une base de données pour y stocker les résultats du « parsing » du fichier. Dans ce schéma, tous les calculs et la génération des statistiques seront faits à partir de la base. Cette solution permet de remédier aux problèmes rencontrés dans la solution précédente en exploitant le fichier « log » une seule fois et en utilisant des variables intermédiaires permettant d'accélérer certains calculs pour la navigation sans revenir systématiquement à la base de données. En comparant ces deux solutions, nous avons opté pour la deuxième vu les avantages qu'elle offre, et nous avons choisi une conception orientée objet pour la développer.

2. Décomposition de l'application

Pour pouvoir trouver une bonne décomposition pour notre application, nous devons commencer par tracer les grandes lignes de notre travail. Nous allons commencer par lire le fichier Access.log, en extraire les informations nécessaires et les stocker convenablement dans une base de données, ensuite, nous allons exploiter ces informations pour la génération des statistiques lors de la navigation

Ainsi nous distinguons trois grands paquetages dans notre travail : le premier est celui responsable de l'analyse et de l'extraction des données utiles du fichier « log » qu'on appellera «**parserlog**», la deuxième, «**basededonnees**», est le paquetage responsable de la gestion de la basede données et de l'exécution des requêtes. Le dernier paquetage appelé «**calculaffichstat**» a pour rôle la génération et l'affichage des statistiques ainsi que la navigation. Maintenant que nous avons distingué ces trois paquetages, nous allons nous concentrer sur la communication et les données échangées entre elles.

Nous avons essentiellement deux communications comme le décrit la figure 20

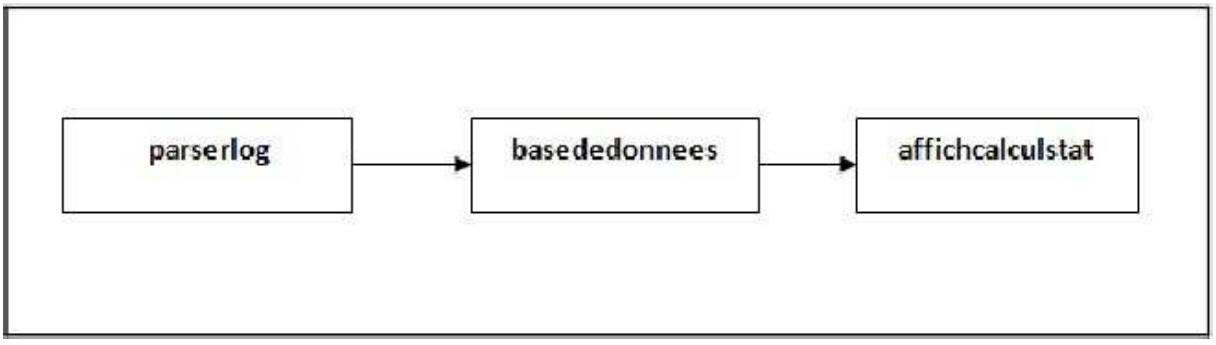


Figure 20 : La communication entre les différentes parties

La première est celle entre le paquetage «**parserlog**» et lepaquetage «**basededonnees**» . Cette communication traduit le stockage des informations extraites du fichier « log » dans la base de données. Pour s'y faire, le paquetage «**parserlog**» fera appelle à une méthode **connecter()** pour se connecter à la base de données, une méthode **insererEnreg()** du paquetage «**basededonnees**» permettant l'insertion dans la base d'un enregistrement lu à partir du fichier « log » et la méthode **deconnecter()** pour se déconnecter en fin des insertions.La deuxième communication est celle reliant les deux paquetages «**basededonnees**» et «**calculaffichstat**». Pour la génération des statistiques, le paquetage «**calculaffichstat**» appelle laméthode **connecter()**de «**basededonnees**», ensuite la méthode **executer()** pour l'exécution desrequêtes appropriées à chaque statistique, cette méthode renvoie des enregistrements de la base etenfin la méthode **deconnecter()** pour la déconnexion

II-Conception détaillée :

Dans cette partie, nous allons détailler les paquetages décrits dans la conception générale un par un, à savoir les classes présentes dans chaque paquetage ainsi que les méthodes de chaque classe. Pour le paquetage «**parserlog**», nous avons une seule classe **Parser**. Cette classe permet la lecture du fichier Access.log ligne par ligne, les décompose en champs séparés et ensuite nous les insérons dans la base en utilisant la méthode **insererEnreg()** du paquetage «**basededonnees**» pour avoir ainsi une nouvelle représentation du fichier « log » dans la base et plus précisément dans une table générale appelée **tableLog**. Lors de l'analyse lexicale du fichier « log », deux solutions se présentent. Dans la première solution, chaque ligne lue à partir du fichier est stockée dans une variable intermédiaire comme chaîne de caractères, ensuite elle est découpée champ par champ en tenant compte des délimiteurs qui sont les espaces et dont le nombre diffère d'un champ à un autre. Ces champs seront stockés par suite dans des variables intermédiaires avant qu'ils ne soient passer en paramètre à la méthode **insererEnreg()** responsable de l'insertion de la ligne dans la base de données. L'inconvénient de cette solution est que le traitement sur les chaînes de caractères prend beaucoup de temps et face à un fichier « log » volumineux, l'analyse lexicale risque de prendre plusieurs dizaines de minutes. La deuxième solution consiste à récupérer une ligne du fichier « log », éliminer tous les espaces superflus et stocker ensuite la ligne obtenue dans un tableau de chaînes de caractères en s'appuyant sur l'existence d'un délimiteur unique entre tous les champs. Enfin, on passe le contenu du tableau à la méthode **insererEnreg()** pour l'insertion dans la base. Cette solution nous épargne de longs traitements sur les chaînes de caractères et par suite nous offre un énorme gain en temps lors de l'analyse lexicale par rapport à la première solution

En ce qui concerne le stockage dans la base, nous avons opté pour l'insertion des données au fur et à mesure qu'on lit le fichier, au lieu de lire le fichier tout entier et ensuite insérer les données dans la base, parce que ceci nous évitera d'utiliser des variables intermédiaires et par suite optimiser le temps de remplissage de la base. Pour le paquetage «**basededonnees**», nous avons besoin d'une classe qui gère la connexion et la déconnexion à la base de données, c'est la classe **GestionBD**. Deux autres classes héritent de celle-ci : la classe **AdminBD** et la classe **Requêtes**. Ces deux classes utilisent les méthodes **connecter()** et **déconnecter()** de la classe **GestionBD** d'où l'existence de l'héritage. La classe **AdminBD** permet d'apporter des modifications sur le contenu de la base de données c'est à dire qu'elle est responsable de l'insertion dans la base de nouveaux enregistrements via la méthode **insererEnreg()** ainsi que de la suppression de la base par le billet de la méthode **vider()** . La classe **Requêtes** est celle responsable de l'interrogation de la base. Elle contient laméthode **executer()** qui assure l'exécution des requêtes qui lui ont été passées en paramètres etrenvoie le résultat des requêtes aux classes qui ont invoqué cette méthode.Une autre classe figure dans le paq uetage «**basededonnees**», c'est la classe **GenererTableStat**. Cette classe permet le remplissage des tables auxiliaires dans notre base de données à partir de la table principale **TableLog**. Ces tables auxiliaires sont du nombre de six : la table **Utilisateurs**, la table **Sites**, la table **Postes**, la table **Protocoles**, la table **Cache** et la table **UtilisationReseau**. Ces tables ont le rôle de générer les statistiques les plus utilisées ce qui se traduira par la suite par un gain de temps lors de la navigation. Elles seront décrites plus en détail dans la partie conception de la base de données. Chaque méthode de cette classe sera responsable du remplissage d'une table p récise :

GenererStatUtilisateurs() remplit la table **Utilisateurs**, **GenererStatSites()** remplit la table **Sites**, **GenererStatPostes()** remplit la table **Postes** , **GenererStatProtocoles()** remplit la table **Protocoles**, **GenererStatCache()** remplit la table **Cache** et enfin **GenererStatUtilisationReseau()** remplit la table **UtilisationReseau**

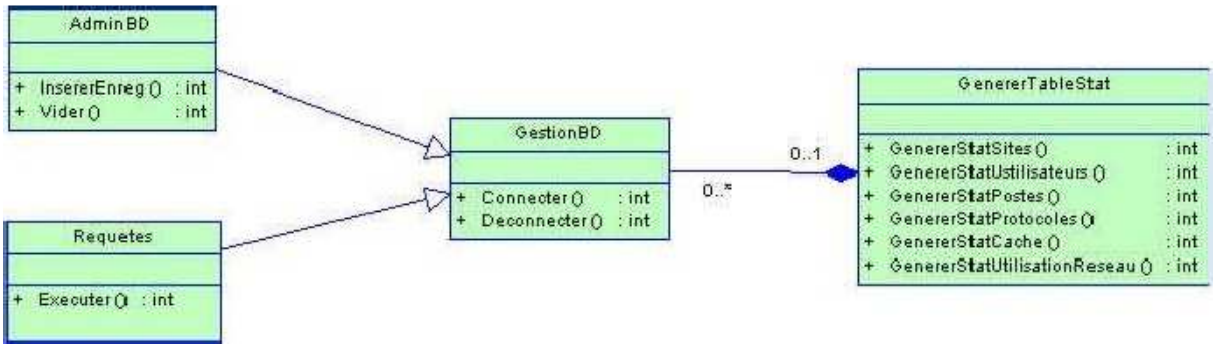


Figure21: La description du paquetage « basededonnees »

Enfin, le troisième et dernier paquetage de notre application, c'est le paquetage«**calculaf fichstat**». Il est responsable du calcul des statistiques via la classe **CalculStat** qui utilise la méthode **genererStatsPrincipaux()** qui permet de récupérer les statistiques déjà générées dans les tables auxiliaires de notre base et la méthode **genererStat()** pour le calcul des statistiques nécessaires lors la navigation et la méthode **genererGraphe()** qui permet la génération des graphes des différentes statistiques. Cette méthode fait appelle à la classe **Graphe** pour générer différents graphiques correspondant aux statistiques affichées en utilisant le graphe le mieux adapté pour chaque statistique. La classe **Graphe** contient trois méthodes qui génère chacune un type de graphe : la méthode **GrapheBarChart3D()** génère un histogramme comme c'est le cas pour les statistiques concernant les postes, les utilisateurs, les protocoles ou encore les sites, la méthode **GraphePieChart3D()** génère un « pie » utilisé pour les statistiques concernant l'utilisation de la cache et Enfin, la méthode **GrapheTimeXYChart()** qui génère des courbes pour les statistiques portant sur l'utilisation du réseau. La classe **CalculStat** joue un grand rôle dans le fonctionnement de la navigation. Pour s'y faire, il faut à chaque fois récupérer la trace du passage entre les différentes statistiques. Ce passage se fait en échangeant des informations entre les différentes classes de calcul de statistiques pour permettre leurs communications avec la base de données afin de pouvoir récupérer les résultats souhaités.

Une première solution consiste à définir des chemins de navigation statiques c'est à dire que pour aboutir à une statistique bien précise, il faut suivre à chaque fois le même chemin de navigation ce qui a pour effet de limiter l'utilisateur à quelques chemins prédéfinis et de réduire les possibilités de naviguer librement entre les statistiques. La deuxième solution consiste à prévoir un mécanisme qui permet de garder la trace de la navigation. Ce mécanisme doit nous permettre de passer d'une statistique déjà calculée à n'importequelle statistique souhaitée en prenant différents chemins de navigation et pouvant boucler infiniment sur toutes les statistiques tout en sauvegardant la trace du chemin parcouru. Cemécanisme doit aussi nous permettre de revenir à n'importe quelle statistique déjà calculée, récupérer la trace qui a abouti au calcul de cette dernière et de calculer à partir d'elle d'autres statistiques. Par exemple, si on avait des statistiques sur les utilisateurs les plus actifs calculées antérieurement et qu'on veut savoir, pour un utilisateur, quels sont les sites qu'il a le plus visité et puis pour ce même utilisateur on veut savoir sur quels postes il a demandé l'un des sites obtenus de la statistique précédente, et après, on veut revenir aux utilisateurs les plus actifs et choisir un autre utilisateur et calculer d'autres statistiques le concernant, ce scénario doit être réalisable avec notre mécanisme. Cet exemple est détaillé davantage dans la « figure 22 »

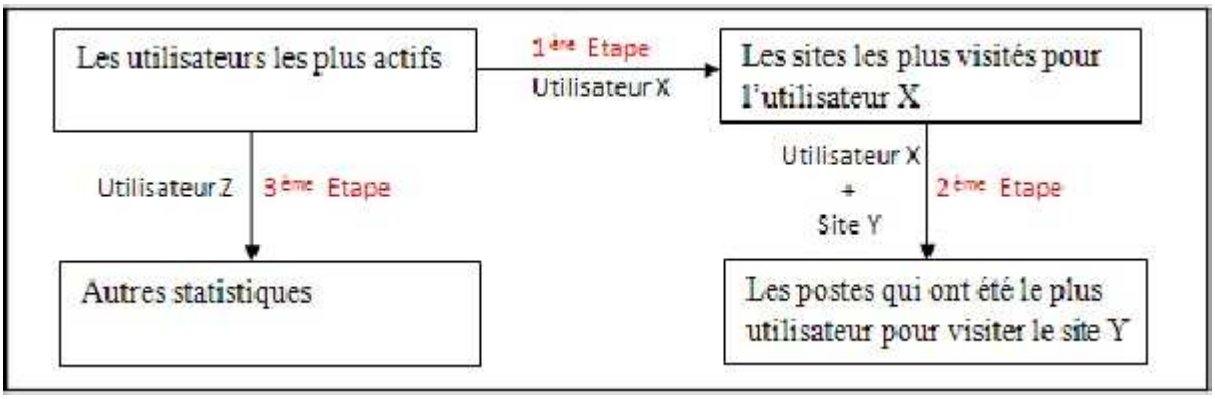


Figure22 : Un exemple de navigation

Pour mettre en œuvre cette solution, nous allons concevoir une classe mère **CalculStat** et sixautres classes **Sites**, **Utilisateurs**, **Postes**, **Protocoles**, **Cache**, **UtilisationRéseau** qui héritent decelle-ci. Cette dernière classe contient deux méthodes abstraites **genererStat()** et **genererGraphe()** qui prennent comme paramètres des chaînes de caractères servant à tracer le chemin de navigation entre les différentes statistiques. Ces deux méthodes abstraites sont implémentées dans les six classes qui héritent de **CalculStat.**

Pour naviguer entre les statistiques, il suffit d'invoquer l'une des méthodes de cette dernière classe en lui passant la condition de navigation pour qu'elle soit exécutée dans l'une des six classes filles et ainsi le passage d'une classe à une autre sera assuré. Le paquetage «**calculaffichstat**» contient aussi une classe **Rapport** responsable de la génération de rapports contenant les différentes statistiques. Cette classe contient une méthode **AjouterParagraphe()** qui permet d'ajouter des titres de paragraphes et des commentaires dans lerapport, une méthode **AjouterTableau()** qui ajoute une statistique au rapport, une méthode **AjouterGraphe()** qui ajoute un graphe au rapport et enfin la méthode **GenererRapport()** qui permet de générer le rapport final sous le format PDF.

Enfin, la dernière classe présente dans le paquetage «**calculaffichstat**» est la classe **StonecoatLogAnalyserFrame** qui va générer l'interface graphique de notre application et qui va faire appel aux différentes classes assurant le fonctionnement de notre application

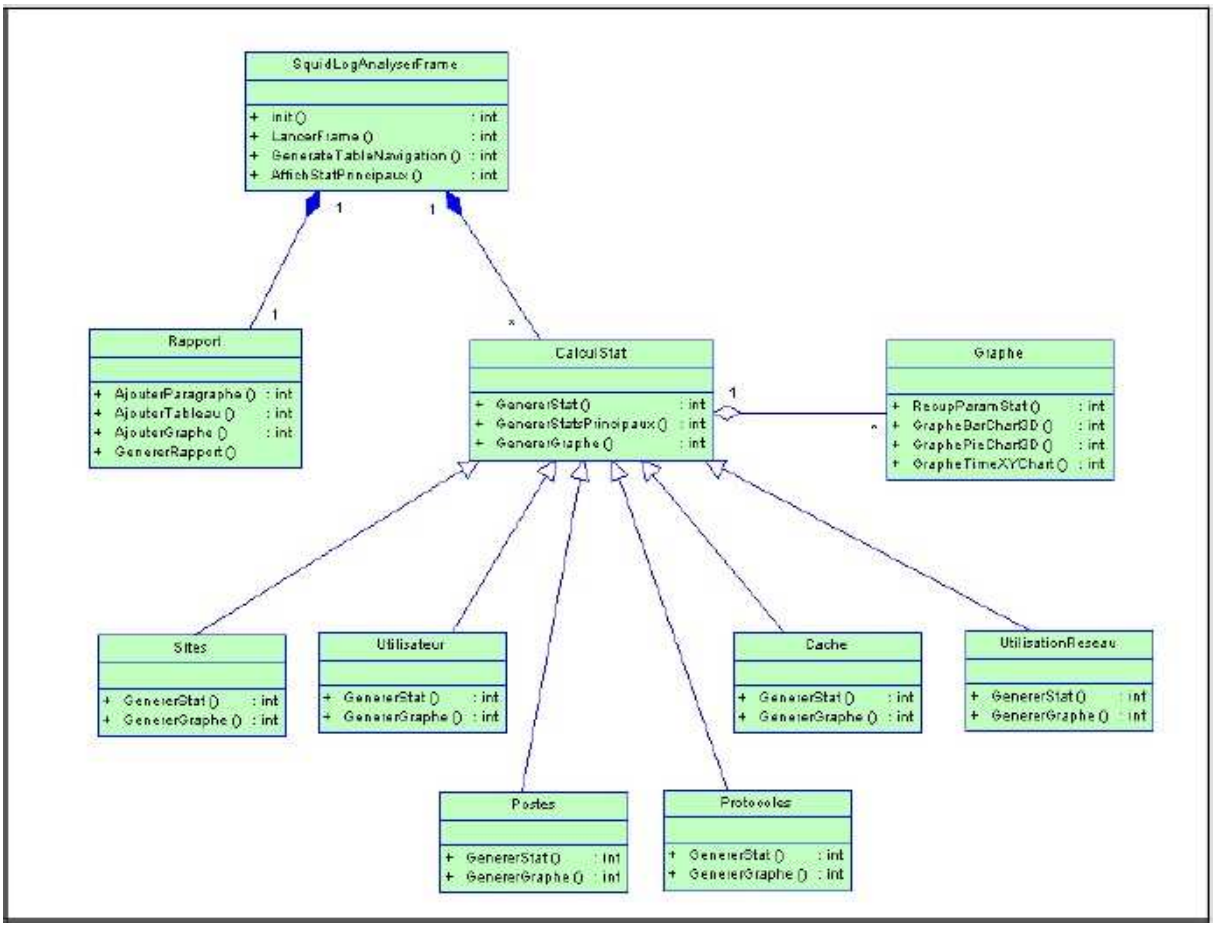


Figure 23 : La description du paquetage « Calculaffichstat »

Suite à cette description détaillée des différents paquetages, il nous est maintenant possible d'en déduire le diagramme de classe de notre application décrit dans la

[figure 23]

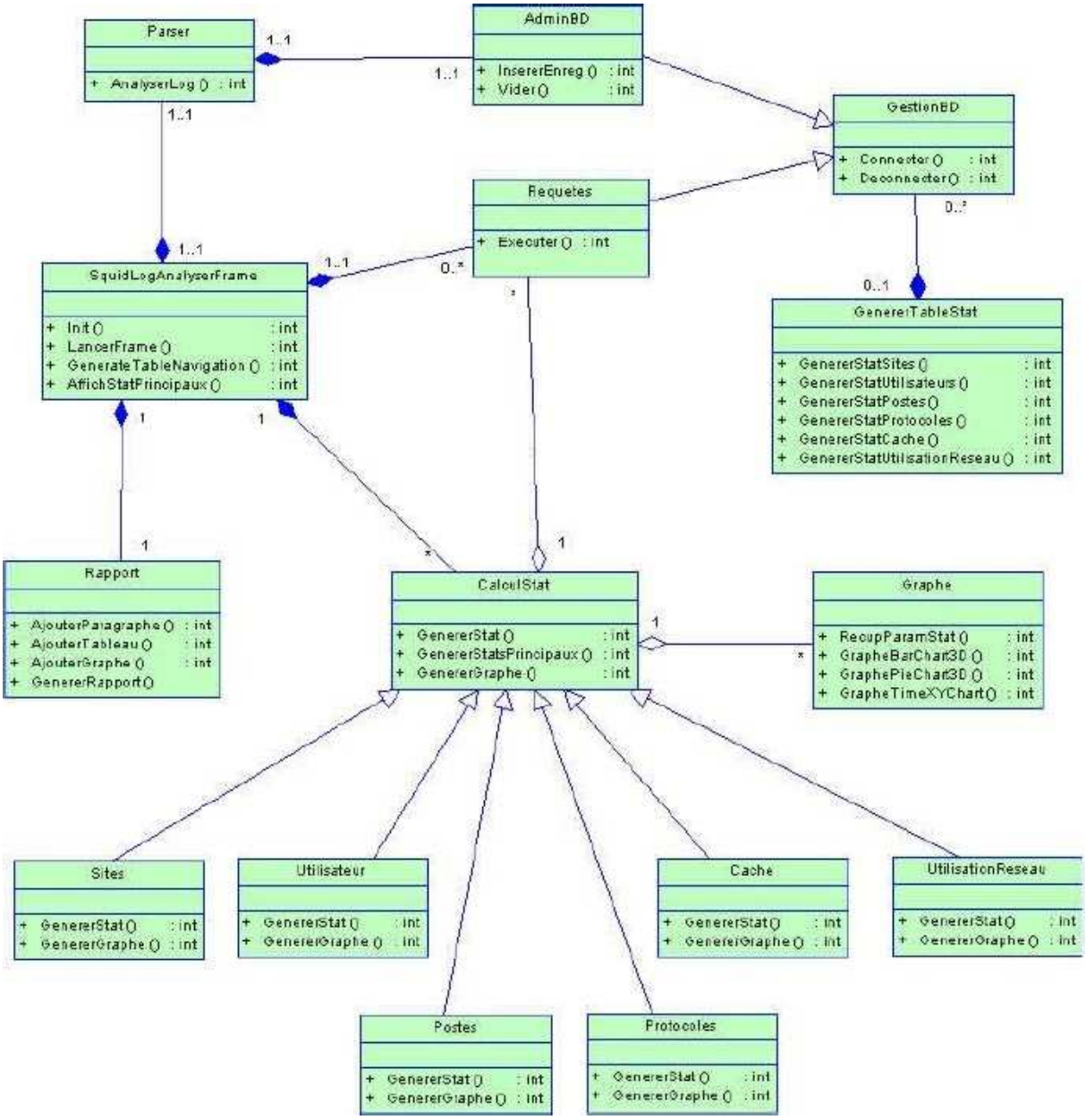


Figure24 : Le diagramme de classe

III-Conception de la base de données :

Nous allons commencer par stocker toutes les informations extraites du fichier Access.log dans une seule table principale appelée **TableLog** de sorte qu'on ait une représentation fidèle dufichier « log » et en même temps des enregistrements mieux adaptés et nos calculs. Cette table comporte les champs num, dates, duree, nom Poste, traitement Cache, bytes, reqmeth, nomProtocole, url, nomUtilisateur, hiercode, type. Ensuite nous allons avoir d'autres tables en relation avec la première. Ces tables

contiennent les statistiques les plus utilisées par notre application. La première statistique concerne les sites les plus visités. Elle est stockée dans la table **Sites** qui contient comme champs l'url visité, le volume total téléchargé pour ce site, le volume chargé à partir de la cache et celui non chargé de la cache .La deuxième statistique concerne les utilisateurs les plus actifs. Elle est stockée dans la table **Utilisateurs** qui contient comme champs le nom de l'utilisateur, le nombre de sites qu'il a consulté et le volume total téléchargé. La troisième statistique concerne les postes les plus actifs. Elle est stockée dans la table **Postes** qui contient comme champs le nom du poste, le nombre de sites consulté à partir de ce poste et le volume total téléchargé. La quatrième statistique concerne les protocoles les plus utilisés. Elle est stockée dans la table **Protocoles** dont les champs sont le nom du protocole utilisé et le volume total téléchargé en utilisant ce protocole. La cinquième statistique concerne l'utilisation de la cache. Elle est stockée dans la table **Cache** qui a comme premier champ le code résultat du Proxy Bluecoat et comme deuxième champ le volume téléchargé suite à une requête générant ce code.

La dernière statistique est celle de l'utilisation du réseau. Elle est stockée dans la table **UtilisationReseau** qui contient comme premier champ la date et l'heure d'une requête et comme deuxième champ le débit relatif à cette requête.

Conclusion :

Ce chapitre a décrit l'étape la plus importante du cycle de vie du logiciel et nous a permis de couvrir tous les cas d'utilisation concernant l'utilisation de notre présent analyseur de fichiers « log » et de définir les besoins non fonctionnels à prendre en considération afin de satisfaire les utilisateurs.

IV-Etude technique

Introduction :

Dans ce chapitre, nous proposons plusieurs choix techniques pour la réalisation de notre travail, ensuite nous présentons les différentes étapes nécessaires à l'implémentation de notre conception comme (le prétraitement, le nettoyage, l'exploration et l'analyse du fichier log) et enfin nous décrivons l'environnement de développement en illustrant quelques interfaces de notre logiciel.

1-Les étapes de l'implémentation :

- ✓ Fichier Log.
- ✓ Table d'une BDD.
- ✓ Connexion BD.
- ✓ Nettoyage des graphiques, image.
- ✓ Statistiques.
- ✓ Transformation.
- ✓ Exécuter des requêtes.
- ✓ Exploration.
- ✓ Prétraitement.
- ✓ Nettoyage.
- ✓ Utiliser LOG ANALYZER.
- ✓ Analyse.

2-Le prétraitement des données :

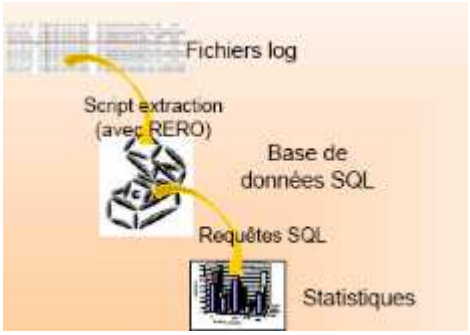
2.1-Chargement de fichier log et transformation en une table d'une base de données :

La première étape d'un processus (bluecoat reporter ou stonesoft) se compose principalement de deux types de tâches :

- Tâches classiques de prétraitement : fusion des fichiers logs web, nettoyage et structuration de données.

- Tâches avancées de prétraitement : stockage des données structurées dans une base de données (notée BD par la suite), généralisation et agrégation des données.

Le fichier LOG est un fichier Texte appelé aussi journal des connexions, qui conserve les traces des requêtes et des opérations traitées par le serveur. Généralement il est de la forme suivante:



```
66.82.9.16 - - [30/Aug/2004:01:12:27 +0000] "GET /images/main_nor2.gif HTTP/1.1" 200 73797 "http://www.utilities.h12.ru/Fre
66.82.9.16 - - [30/Aug/2004:01:13:56 +0000] "GET /images/main_nor2.gif HTTP/1.1" 200 73797 "http://www.utilities.h12.ru/Fre
66.82.9.16 - - [30/Aug/2004:01:14:39 +0000] "GET /images/main_nor2.gif HTTP/1.1" 200 73797 "http://www.utilities.h12.ru/Fre
80.170.104.145 - - [30/Aug/2004:01:18:13 +0000] "GET /download.htm HTTP/1.1" 200 7901 "http://telecharger.01net.com/windows/
80.170.104.145 - - [30/Aug/2004:01:18:15 +0000] "GET /favicon.ico HTTP/1.1" 200 1406 "-" "Mozilla/5.0 (Windows; U; Windows
80.170.104.145 - - [30/Aug/2004:01:18:15 +0000] "GET /images/search_no.GIF HTTP/1.1" 200 215 "http://www.coolfilesearch.com/
80.170.104.145 - - [30/Aug/2004:01:18:15 +0000] "GET /images/search_hi.GIF HTTP/1.1" 200 215 "http://www.coolfilesearch.com/
80.170.104.145 - - [30/Aug/2004:01:18:16 +0000] "GET /images/search_tri.gif HTTP/1.1" 200 874 "http://www.coolfilesearch.com/
80.170.104.145 - - [30/Aug/2004:01:18:36 +0000] "GET /index.html HTTP/1.1" 200 11393 "http://www.coolfilesearch.com/downloa
80.170.104.145 - - [30/Aug/2004:01:18:38 +0000] "GET /images/main3.jpg HTTP/1.1" 200 8721 "http://www.coolfilesearch.com/in
63.238.163.75 - - [30/Aug/2004:01:22:06 +0000] "HEAD / HTTP/1.1" 200 0 "-" "InternetSeer.com" coolfilesearch.com text/html
12.20.121.52 - - [30/Aug/2004:01:33:25 +0000] "GET /images/minibtn6-3.gif HTTP/1.0" 200 3378 "http://www.geocities.com/nasc
81.241.83.239 - - [30/Aug/2004:01:39:06 +0000] "GET /download.htm HTTP/1.1" 200 7901 "http://telecharger.01net.com/windows/
81.241.83.239 - - [30/Aug/2004:01:39:06 +0000] "GET /images/search_hi.GIF HTTP/1.1" 200 215 "http://www.coolfilesearch.com/
81.241.83.239 - - [30/Aug/2004:01:39:06 +0000] "GET /images/search_no.GIF HTTP/1.1" 200 215 "http://www.coolfilesearch.com/
81.241.83.239 - - [30/Aug/2004:01:39:06 +0000] "GET /images/search_tri.gif HTTP/1.1" 200 874 "http://www.coolfilesearch.com/
81.241.83.239 - - [30/Aug/2004:01:39:10 +0000] "GET /screen_shots.htm HTTP/1.1" 200 7428 "http://www.coolfilesearch.com/dow
81.241.83.239 - - [30/Aug/2004:01:39:14 +0000] "GET /images/main_nor.gif HTTP/1.1" 200 31365 "http://www.coolfilesearch.com/
81.241.83.239 - - [30/Aug/2004:01:39:21 +0000] "GET /images/main_nor2.gif HTTP/1.1" 200 73797 "http://www.coolfilesearch.com/
```

Figure-21- Un fichier LOG avant le prétraitement.

Dans cette étape, les données structurées sont enregistrées sous une forme persistante, généralement, dans une base de données.

- Les différent champs de ce fichier vont être, importé dans une base données déterminée comme suit :

hote_client	login_client	utilisateur_clien	date_et_heure	methode	url_des_pages	protocole	code_de_retour	taille_chargé
66.82.9.16	-	-	30/Aug/2004:01:12:27	GET	/images/main_nor2.gif	HTTP/1.1"	200	73797
66.82.9.16	-	-	30/Aug/2004:01:13:56	GET	/images/main_nor2.gif	HTTP/1.1"	200	73797
66.82.9.16	-	-	30/Aug/2004:01:14:39	GET	/images/main_nor2.gif	HTTP/1.1"	200	73797
80.170.104.145	-	-	30/Aug/2004:01:18:13	GET	/download.htm	HTTP/1.1"	200	7901
80.170.104.145	-	-	30/Aug/2004:01:18:15	GET	/favicon.ico	HTTP/1.1"	200	1406
80.170.104.145	-	-	30/Aug/2004:01:18:15	GET	/images/search_no.GIF	HTTP/1.1"	200	215
80.170.104.145	-	-	30/Aug/2004:01:18:15	GET	/images/search_hi.GIF	HTTP/1.1"	200	215
80.170.104.145	-	-	30/Aug/2004:01:18:16	GET	/images/search_tri.gif	HTTP/1.1"	200	874
80.170.104.145	-	-	30/Aug/2004:01:18:36	GET	/index.html	HTTP/1.1"	200	11393
80.170.104.145	-	-	30/Aug/2004:01:18:38	GET	/images/main3.jpg	HTTP/1.1"	200	8721
63.238.163.75	-	-	30/Aug/2004:01:22:06	HEAD	/	HTTP/1.1"	200	0
12.20.121.52	-	-	30/Aug/2004:01:33:25	GET	/images/minibtn6-3.gif	HTTP/1.0"	200	3378
81.241.83.239	-	-	30/Aug/2004:01:39:06	GET	/download.htm	HTTP/1.1"	200	7901
81.241.83.239	-	-	30/Aug/2004:01:39:06	GET	/images/search_hi.GIF	HTTP/1.1"	200	215
81.241.83.239	-	-	30/Aug/2004:01:39:06	GET	/images/search_no.GIF	HTTP/1.1"	200	215
81.241.83.239	-	-	30/Aug/2004:01:39:06	GET	/images/search_tri.gif	HTTP/1.1"	200	874
81.241.83.239	-	-	30/Aug/2004:01:39:10	GET	/screen_shots.htm	HTTP/1.1"	200	7428
81.241.83.239	-	-	30/Aug/2004:01:39:14	GET	/images/main_nor.gif	HTTP/1.1"	200	31365
81.241.83.239	-	-	30/Aug/2004:01:39:21	GET	/images/main_nor2.gif	HTTP/1.1"	200	73797
12.20.121.52	-	-	30/Aug/2004:01:45:18	GET	/images/minibtn6-3.gif	HTTP/1.0"	304	-
201.4.61.250	-	-	30/Aug/2004:01:52:41	GET	/favicon.ico	HTTP/1.1"	200	1406

Figure-22-Un fichier LOG dans une base de données.

Le fichier log se transforme en une table composée de plusieurs colonnes, chaque colonne correspond à un champ spécifié du fichier LOG :

- ✓ La colonne « hote_client » correspond aux adresses IP des visiteurs
- ✓ La colonne « login_client » correspond au Nom du serveur utilisé par le visiteur
- ✓ La colonne « utilisateur_client » correspond au Nom de l'utilisateur (en cas d'accès par mot de passe).
- ✓ La colonne « date_et_heure » correspond à la date d'accès
- ✓ La colonne « méthode » correspond à la méthode utilisée (GET/POST)
- ✓ La colonne « url_des_pages » correspond au URL demandé
- ✓ La colonne « protocole » correspond au protocole utilisé
- ✓ La colonne « code_de_retour »
- ✓ La colonne « taille_chargé » correspond à la taille chargée.

3-Nettoyage des données :

Le nettoyage des données est une étape cruciale dans le processus du (bluecoat reporter ou stonesoft) en raison du volume important des données enregistrées dans les fichiers Log Web. En effet, la dimension de ces fichiers dans les sites Web et les portails Web très populaires peut atteindre des centaines de giga-octets par heure. L'étape du nettoyage consiste à filtrer les données inutiles à travers la suppression des requêtes ne faisant pas l'objet de l'analyse et celle provenant des robots Web. La suppression du premier type de requêtes dépend de l'intention de l'analyste. En effet, si son objectif est de trouver les failles de la structure du site Web ou d'offrir des liens dynamiques personnalisés aux visiteurs du site Web, la suppression des requêtes auxiliaires comme celles pour les images ou les fichiers multimédia est possible. Quand il ne faut pas supprimer ces requêtes puisque dans certains cas les images ne sont pas incluses dans les fichiers HTML mais accessibles à travers des liens, ainsi l'affichage de ces images indique une action de l'utilisateur.

La suppression du second type de requêtes i.e. les entrées dans le fichier Log produites par les robots Web (WR) permet également de supprimer les sessions non

intéressantes. En effet, les Web Robots suivent automatiquement tous les liens d'une page Web. Il en résulte que le nombre de demandes d'un WR dépasse en général le nombre de demandes d'un utilisateur normal. Pour identifier les requêtes et les visites issues des WRs on utilise trois heuristiques:

1. Identifier les adresses IPs qui ont formulé une requête à la page « robots.txt».

2. Utiliser des listes des «User agents» connus comme étant des WRs.

3. Utiliser un seuil pour « la vitesse de navigation» BS (Browsing Speed), qui représente le rapport entre le nombre de pages consultées pendant une visite de l'utilisateur et la durée de la visite. Si BS est supérieure à deux pages par seconde et la visite dépasse 15 pages, alors la visite a été initiée par un WR.

3.1-Nettoyage des graphiques, image :

Les données concernant les pages possédant des graphiques, Images, n'apporteront rien à l'analyse. Elles seront donc filtrées :

Pour cela on est amené à supprimer de notre base de données les URLs suivants :

- ✓ Les urls correspondant aux images d'extension « .gif » par la requête
- ✓ ("delete * from tab where url_des_pages like '*.*gif'")
- ✓ Les urls correspondant aux images d'extension « .jpg » par la requête
- ✓ ("delete * from tab where url_des_pages like '*.*jpg'")
- ✓ Les urls correspondant aux images d'extension « .png » par la requête
- ✓ ("delete * from tab where url_des_pages like '*.*png'")

Figure-23-exemple sur les urls (.GIF, .JPG,....).

Les urls correspondant aux robots par la requête :

- Il est presque impossible aujourd'hui d'identifier tous les robots Web puisque chaque jour apparaissent des nouveaux. Pour les robots dont l'adresse IP et le User-Agent sont inconnus, nous procédons à un examen de leurs comportements sachant que les robots Web procèdent à une visite relativement exhaustive (nombre de pages visitées par un robot est supérieur au nombre de pages visitées par un utilisateur normal) et rapide et qu'ils cherchent généralement un fichier nommé »robot.txt».

("delete * from tab where url_des_pages like '\robots.txt'").

4- Réalisation

Processus d'analyse de fichier log du proxy bluecoat :

La plus grande partie de l'application est celle de la navigation entre les différentes statistiques qu'on arrive à dégager à partir du fichier Access.log. Dans la partie ci-dessous on présente les enchaînements à suivre ainsi que quelques imprimes écrans pour donner un aperçu sur l'utilisation de notre analyseur.

1. **Interface d'accueil**

L'interface d'accueil est la page de garde de notre outil qui contient son menu principal et qui va donner l'accès soit à la configuration soit aux statistiques.

2. Configuration2.1-Configuration Système

Pour définir les paramètres de configuration :

➢ Cliquer sur le bouton de recherche dans le panneau «chemin du fichier log ».

➢Sélectionner le fichier « log » à analyser. La figure 25 illustre la configuration des paramètres système de notre application.

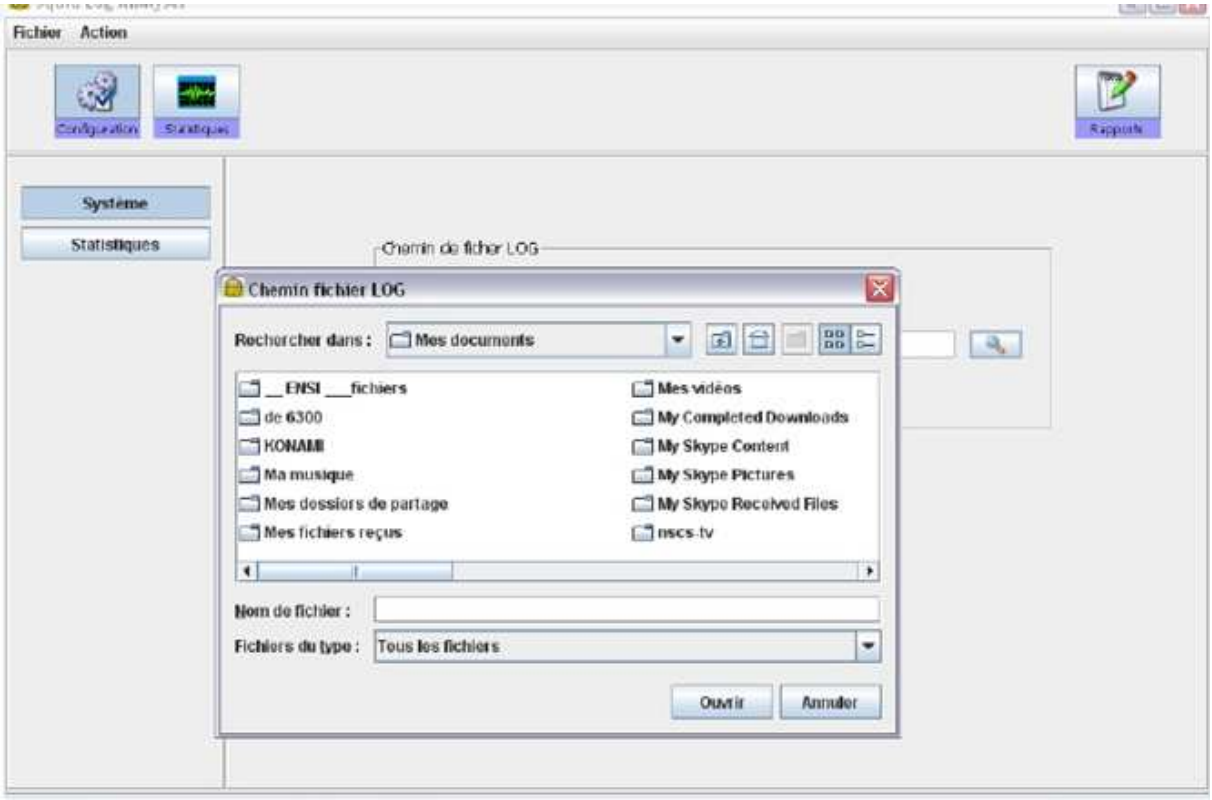


Figure 25 : La communication du fichier « log »

2.2-Configuration des statistiques

Pour définir les paramètres de l'affichage des statistiques :

- ✓ Saisir un nombre qui correspond à la taille maximale des tables statistiques à générer.
- ✓ Saisir un nombre qui correspond à la taille maximale des graphiques à afficher.

Pour définir les paramètres de filtrage :

- ✓ Choisir le critère de filtrage en cochant l'une des cases « Par utilisateur », « Par poste » ou « Par date ».
- ✓ Saisir un nom d'utilisateur si la case « Par utilisateur » est cochée.
- ✓ Saisir un nom de poste si la case « Par poste » est cochée.
- ✓ La figure 26 illustre la configuration des paramètres d'affichage des statistiques et le filtrage

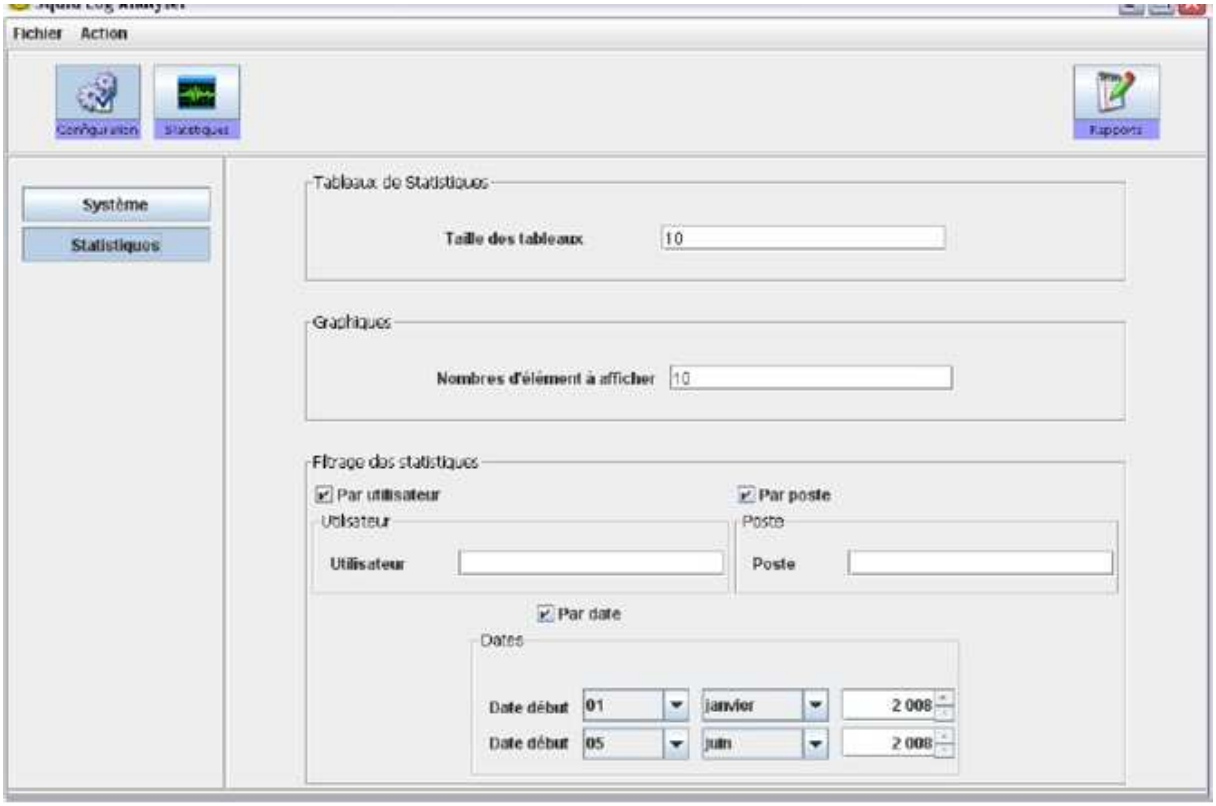


Figure26 : La configuration des statistiques de l'analyseur

3. Statistiques :

Après la définition des paramètres d'analyse du fichier « log »il reste à :

- ✓ Cliquer sur le bouton « statistiques » pour passer à l'interface relative aux statistiques.
- ✓ Cliquer sur le bouton « action » puis « générer statistiques » pour procéder à la génération des statistiques déduites du fichier « log » et qui concernent les url, les utilisateurs, les postes, les protocoles, l'utilisation de la cache et l'utilisation du réseau.
- ✓ Cliquer sur l'un des boutons de gauche, à savoir « url », « utilisateurs », « postes », «protocoles », « utilisation du cache » ou « utilisation du réseau », pour passer à l'interface des statistiques relative à ce choix.

La figure 27 et la figure 28 illustrent le cas du choix des statistiques propres aux URL

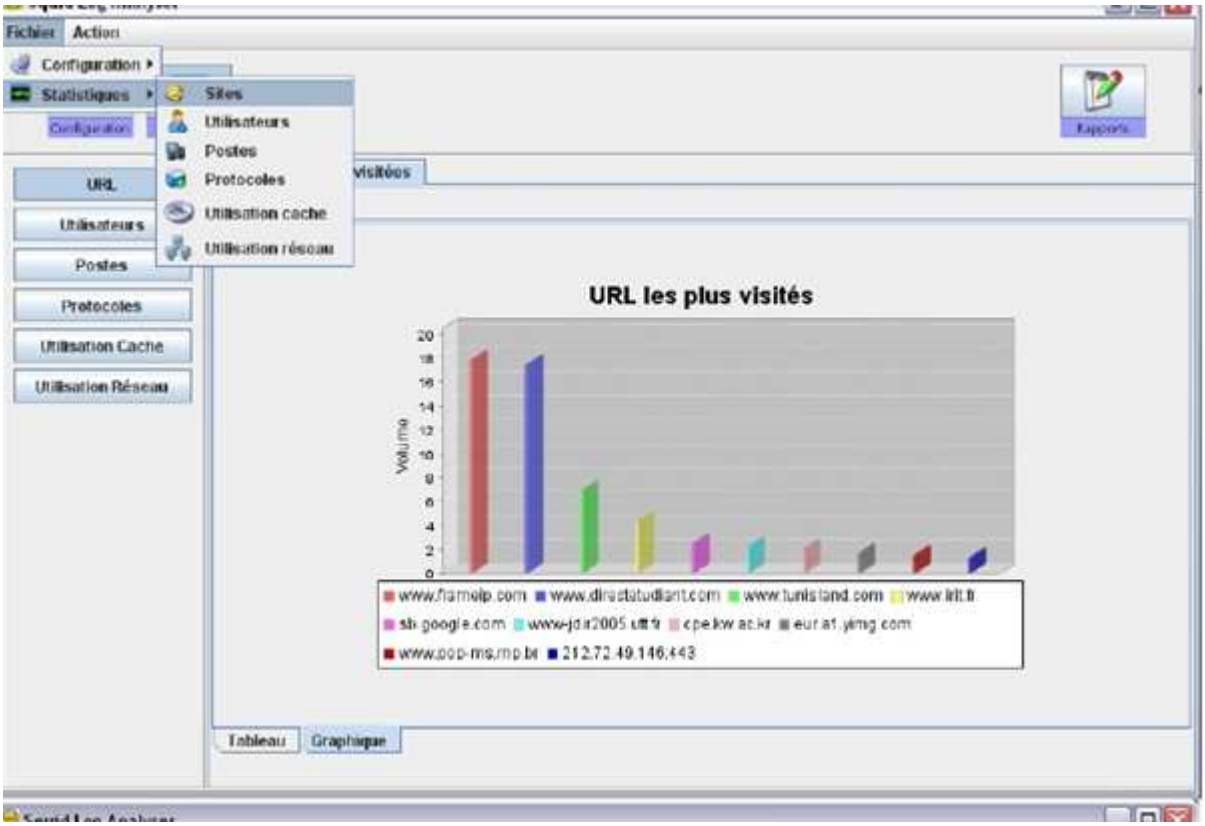


Figure 27 : La table de statistiques sur les sites les plus visités

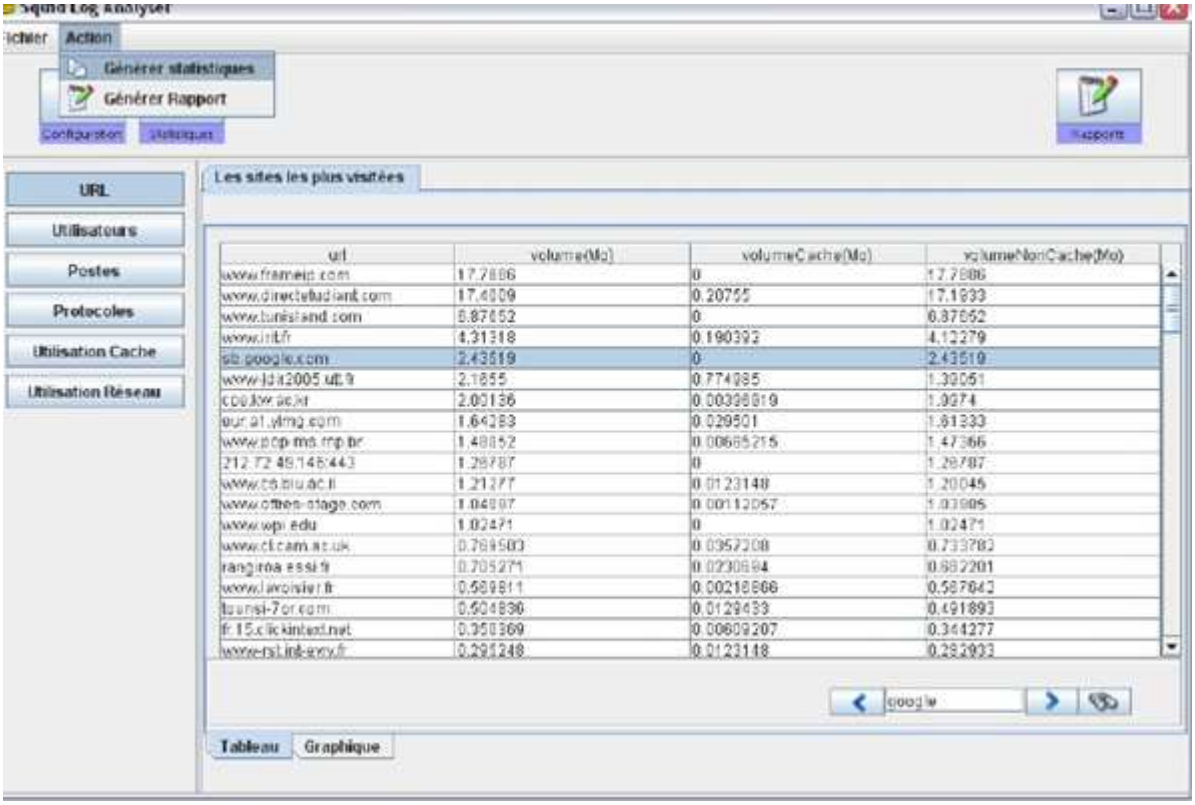


Figure28 : Le graphe des sites les plus visités

La figure 29 montre un cas d'utilisation de l'analyseur ou l'utilisateur aura choisi de visualiser le taux d'utilisation du cache. On distingue bien la légende qui explique la signification de chaque couleur avec le volume exacte. Elle représente une possibilité parmi plusieurs autres qui seront mis à la disposition del'utilisateur pour voir au mieux la répartition du trafic

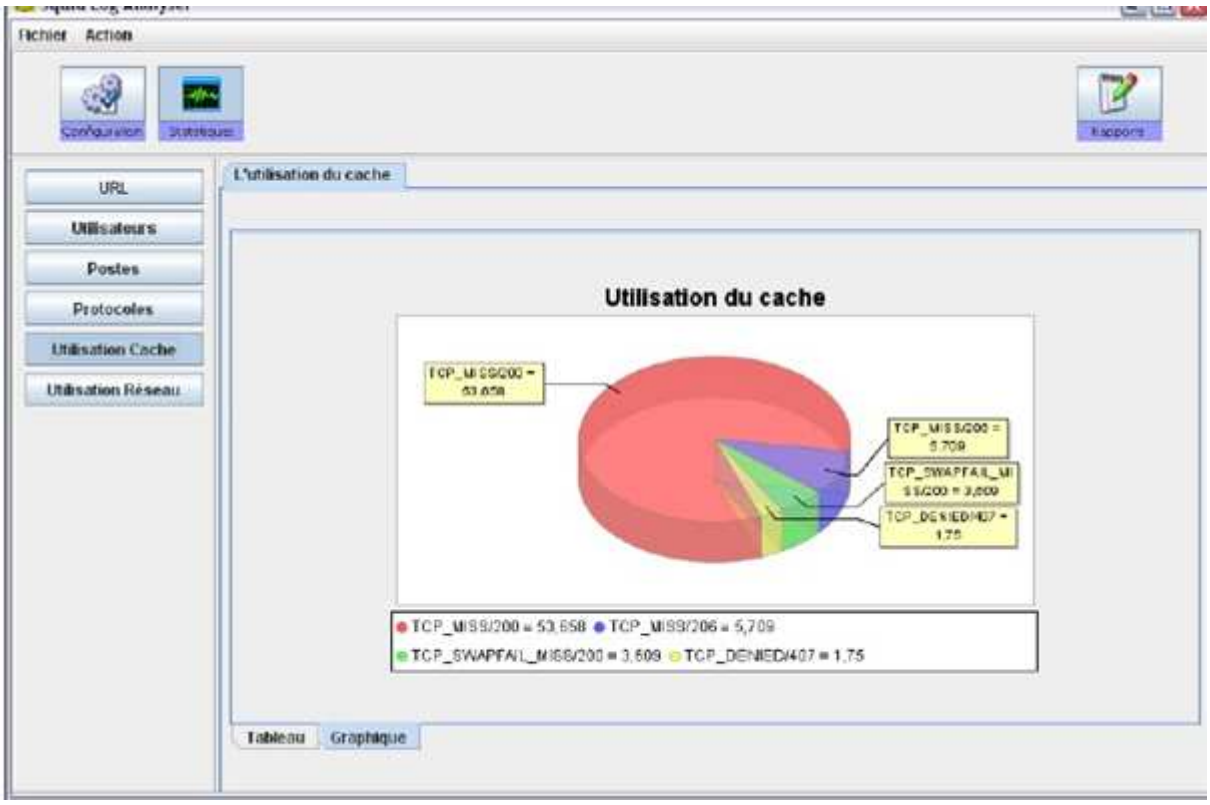


Figure 29 : Le graphe de l'utilisation du cache

L'utilisation du réseau peut être représentée par une table et un graphe traçant le débit en fonction du temps (par heure, par jour et par mois). La figure 30 illustre l'utilisation générale du réseau par heure.

Figure 30 : Le graphe d'utilisation du réseau par heure

Les deux figures 31 et 32 reflètent un scénario possible de navigation entre les différentes statistiques : en partant des sites les plus visités, on sélectionne un site web dont le suivi nous parait important, par exemple le site www.frameip.com à partir duquel on affiche les utilisateurs les plus actifs, et on suit la navigation pour déterminer le taux d'utilisation du cache pour ce site et pour un utilisateur particulier (par exemple l'utilisateur le plus actif).

Par ce mécanisme de navigation on arrive à affiner notre analyse pour aboutir à des statistiques claires, pertinentes et utiles pour l'administrateur du réseau

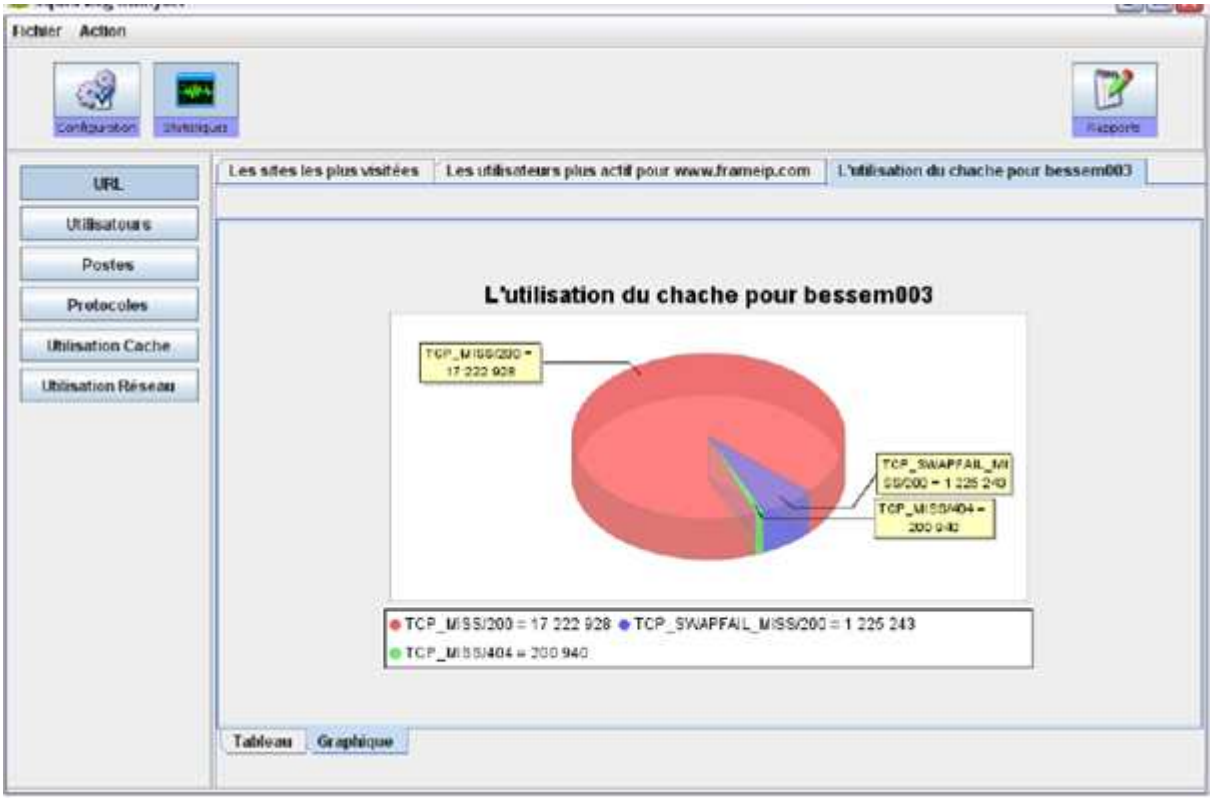


Figure 31: Le mécanisme de navigation

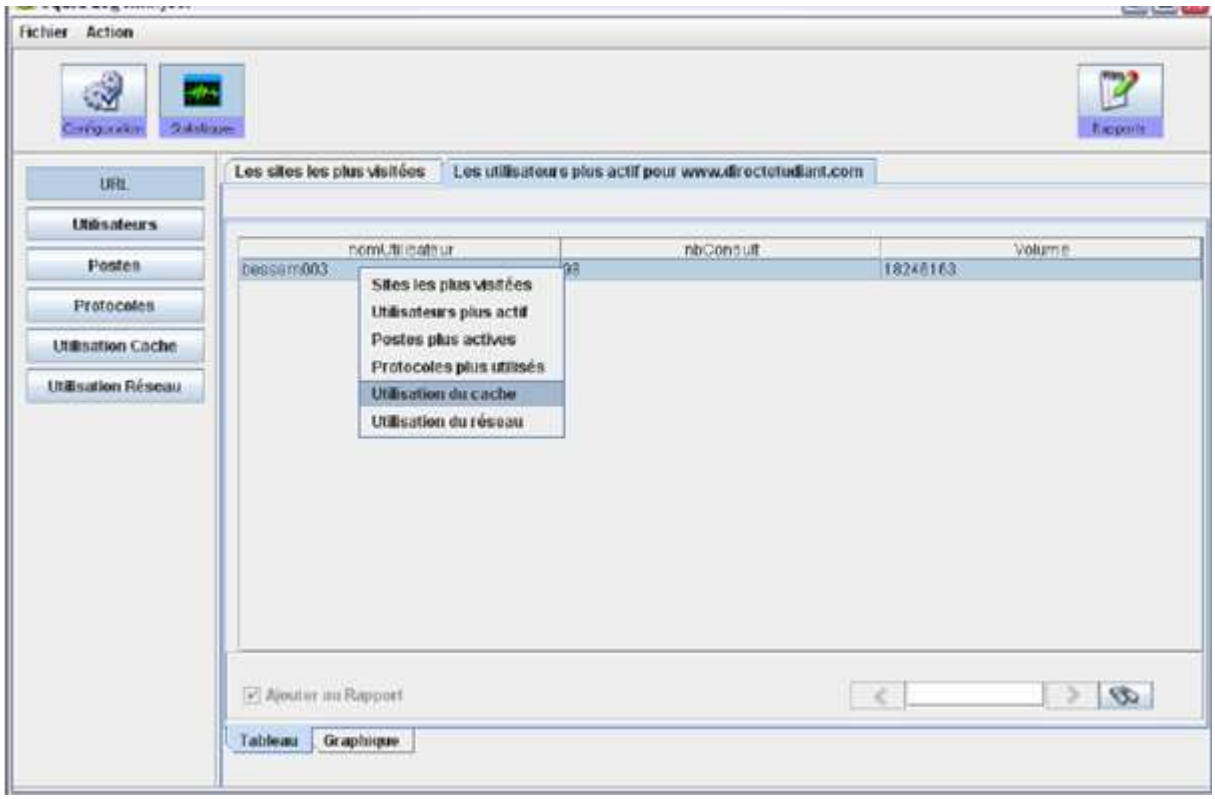


Figure32 le graphe de l'utilisation de cache pour bessem003 pour le site frameip.com

Conclusion

On rappel brièvement que pour mettre en œuvre notre prototype, on a utilisé la méthodologie UML (Unified Modeling Language) dans les phases de spécification et con ception, le système de gestion de bases de données MySQL pour la réalisation de la base de données et le langage JAVA sous Sun Java Studio Enterprise 8 pour le développement de notre prototype.

Conclusion générale :

Pour conclure, nous rappelons que le but de notre projet est de développer une application permettant d'analyser les fichiers logs de « BLUECOAT et STONESOFT » (dans notre cas c'est le fichier « access.log ») et de permettre à l'administrateur d'avoir une idée sur l'état du trafic et de pouvoir évaluer le fonctionnement du serveur par la mise en place d'un mécanisme de navigation permettant d'affiner l'analyse. Nous sommes parvenus en fin de compte à achever notre application dans les délais malgré quelques problèmes que nous avons rencontrés et que nous avons pu résoudre grâce aux personnes qui ont contribués à la réalisation de ce modeste projet. Ce projet a eu plusieurs apport bénéfiques et a présenté une compétente occasion pour mettre en évaluation ce que nous avons appris lors de nos deux derniers années, nous citons ci-dessous quelques apports :

- ✓ Appliquer ce que nous avons appris en matière de sécurité informatique.
- ✓ Appliquer ce que nous avons appris en matière de génie logiciel.
- ✓ Apprendre et appliquer le langage de spécification et de conception UML et d'améliorer nos connaissance quant aux cycles de développement du logiciel.
- ✓ Se familiarisé davantage à la manipulation des bases de données.
- ✓ S'adapter au langage de programmation Java, et maîtriser le puissant outil Sun Java Studio Enterprise 8.Enfin, l'outil qu'on a réalisé reste une plateforme de départ qui laisse des grandes possibilités d'extension et d'amélioration surtout pour intégrer la fonction corrélation entre les mesures statistiques.

A. BLUECOAT [7][19]

1. Introduction

BlueCoat Systems Inc., fondée en 1996, est une société anonyme basée à Sunnyvale, en Californie. BlueCoat s'est donné pour mission de sécuriser les communications Web et d'accélérer les applications métier dans toute les entreprises distribuées.

Les appliances et solutions de la gamme BlueCoat, déployés au niveau des sites distants, des passerelles Internet, des points terminaux et des centres de données, constituent des dispositifs de contrôle intelligents basés sur règles. Ils permettent aux directions informatiques d'optimiser la sécurité et d'accélérer les performances de tous les utilisateurs et applications.

2. La solution ProxySG BlueCoat :

Le ProxySG BlueCoat prend en charge tous les protocoles Web les plus courants, notamment les protocoles de messagerie instantanée (AOL, MSN, Yahoo), les protocoles HTTP, HTTPS, FTP, SOCKS, DNS, Real Streaming et Microsoft Streaming. En outre, le ProxySG prend en charge la mise en tunnel TCP, une méthode permettant de contrôler tous les protocoles applicatifs fonctionnant sous TCP et ne possédant pas de prise en charge proxy native.

Des règles d'accès complexes peuvent facilement être déployées. A l'aide du Visual Policy Manage intégré, les administrateurs peuvent rapidement créer et mettre en œuvre des politiques de filtrage Web efficaces, sur l'ensemble de la société. Cette solution est basée sur le moteur PPE (Policy Processing Engine) de BlueCoat, qui offre un contrôle granulaire évolutif pour les environnements les plus rigoureux.

3. Le Proxy Web de BlueCoat permet entre autre :

- ✓ D'obtenir une visibilité complète des communications Web sur l'ensemble de la société et de créer des rapports d'activité
- ✓ De mettre en place des règles granulaires d'accès au Web, basée sur les utilisateurs, les groupes, les plages horaires, le lieu, l'adresse réseau, le type de navigateur et autres attributs
- ✓ D'intégrer les principales listes de filtrage sur abonnement, qui sont mises à jour automatiquement au fil de l'évolution du Web
- ✓ D'intégrer le contrôle des messageries instantanées afin de prendre en charge les formats de messageries instantanées les plus courants, notamment AOL, MSN et Yahoo!.
- ✓ D'analyser le contenu Web contre les virus et codes malicieux.
- ✓ D'encadrer les utilisateurs par le biais de page de gardes personnalisées, qui représentent la politique de sécurité de la société en matière d'accès à Internet
- ✓ De simplifier l'administration et la mise en œuvre des politiques de la société relatives à l'utilisation du Web
- ✓ D'obtenir des performances, grâce à la mise en cache intégrée
- ✓ De remplacer les serveurs Proxy logiciels par un équipement évolutif et facile à gérer

4. Modes de fonctionnement :

Le ProxySG s'installe dans le réseau selon trois modes de fonctionnement différents :

4-1. Le mode Explicite :

Les browsers des utilisateurs doivent être configurés pour utiliser le Proxy.

4-2. Le mode transparent :

Soit on installe le Proxy dans le réseau et tout le flux Web est redirigé par le Firewall vers le Proxy, soit on intègre le Proxy dans le flux c-à-d entre le firewall et le

réseau et rien n'est à faire au niveau des browsers, les utilisateurs ne savent même pas qu'un Proxy est installé. Une carte de Pass-Through optionnelle permet de bypasser le Proxy en cas de défaillance de celui-ci.

4-3. Le mode reverse Proxy :

Pour l'accélération et la connexion SSL sécurisée sur un serveur Web.

5. La fonction de « Coaching » du BlueCoat :

BlueCoat a le pouvoir de « coacher » les utilisateurs en les obligeant à, aller lire les conditions et politiques d'entreprise que la direction de l'établissement a définies. Ceci peut être fait en les redirigeant vers une page de garde les prévenant que l'usage d'internet est contrôlé, surveillé et monitoré. L'utilisateur peut soit accepter les règles et politiques définies, et dans ce cas il aura le droit de surfer sur le web, ou il pourra alors accepter cette contrainte pour une durée déterminée d'un jour, et là un cookie d'une durée d'un jour sera créé et stocké sur sa station.

Figure-A1- page de garde politique entreprise

6. Filtrage d'URL :

Les solutions de filtrage actuellement disponibles dans le BlueCoat sont : BlueCoat Web Filter; InterSafe; Optenet; Proventia; SmartFilter; SurfControl; WebSense; WebWasher.

Ici un exemple de catégories de SmartFilter

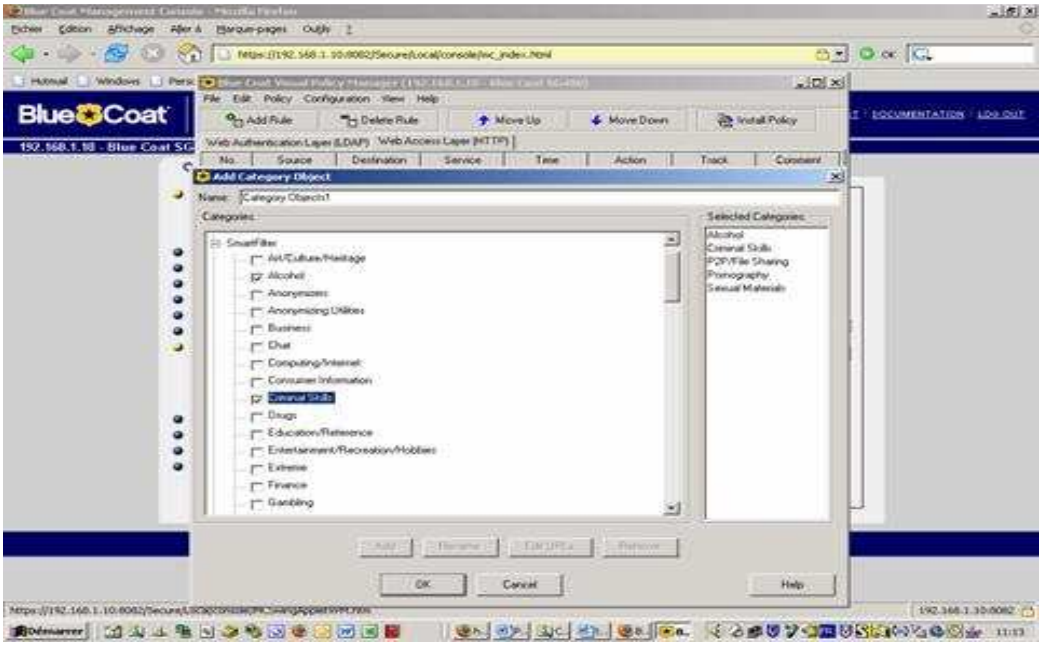


Figure-A2-SmartFilter

7. Authentification

L'authentification des utilisateurs se fait grâce à la reconnaissance de différentes sources d'authentification telles que :

NTLM, LDAP, Radius ou Netegrity et des séquences complexes mélangeant plusieurs authentifications peuvent être combinées, cela est utile lorsque l'on a plusieurs entités qui ont des procédés d'authentification différents. Le paramétrage se fait de manière simple et l'on va pouvoir créer des polices selon les utilisateurs, groupes ou objets du domaine.

Exemple LDAP :

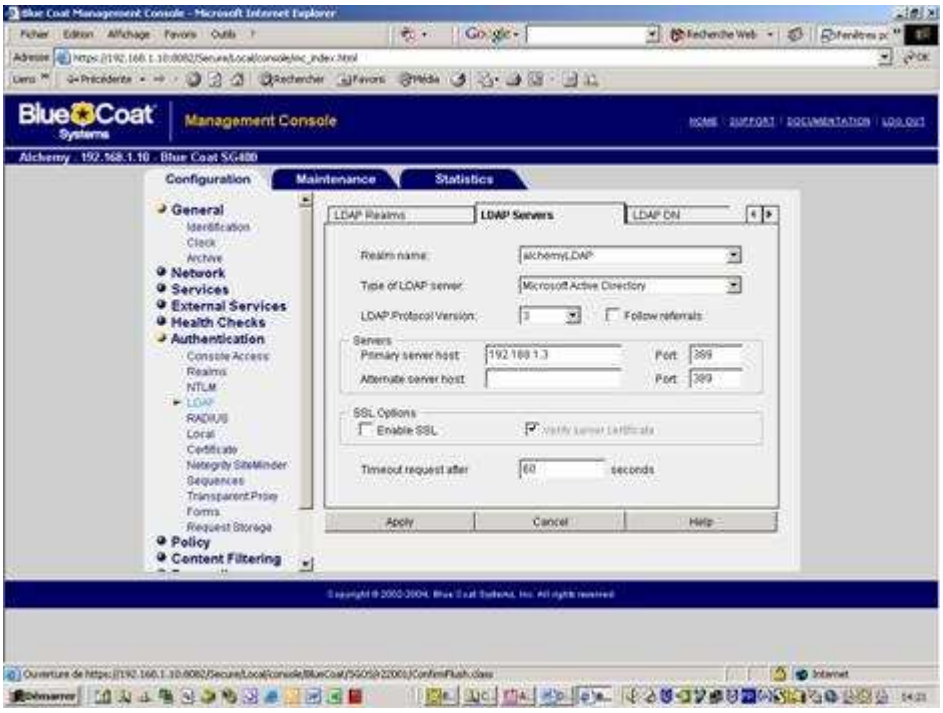


Figure-A3-source d'authentification LDAP

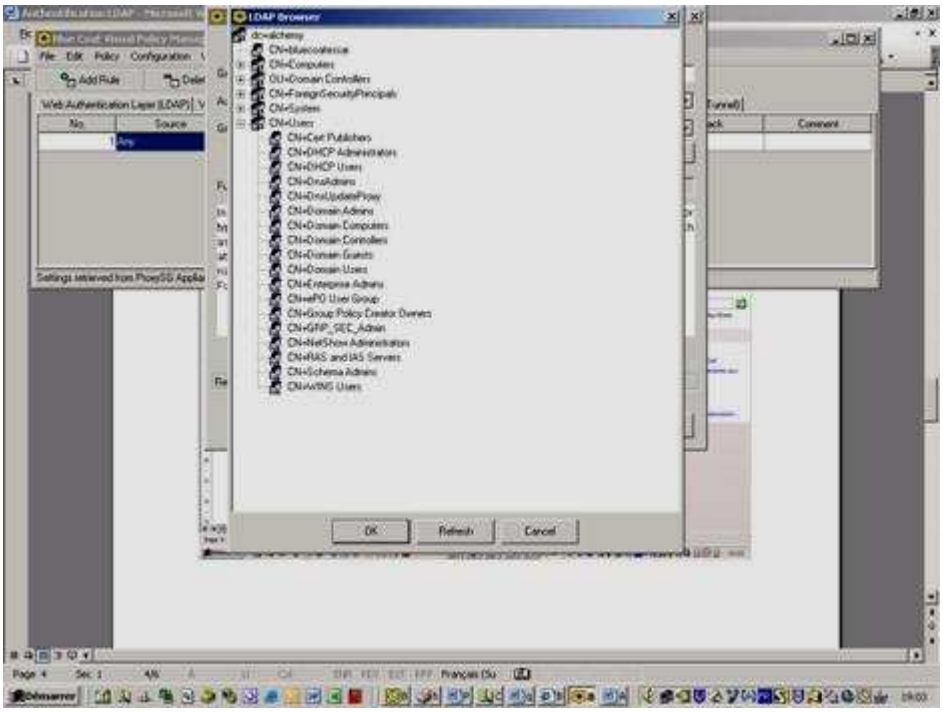


Figure-A4-LDAP Browser

Les fonctionnalités de logging permettent de surveiller et tracer l'activité. Ceci peut être directement lu sur le boîtier dans les « event logs » ou « access logs »

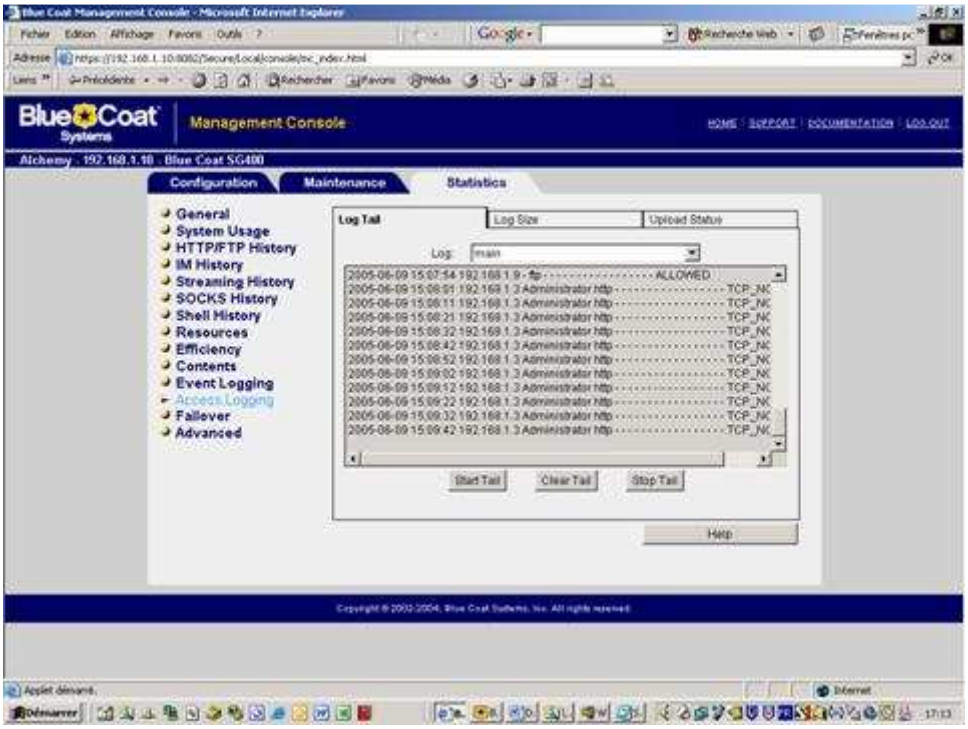


Figure-A5-bluecoat management console

Ou alors on envoie toutes ces informations par ftp (par exemple) sur un serveur distant

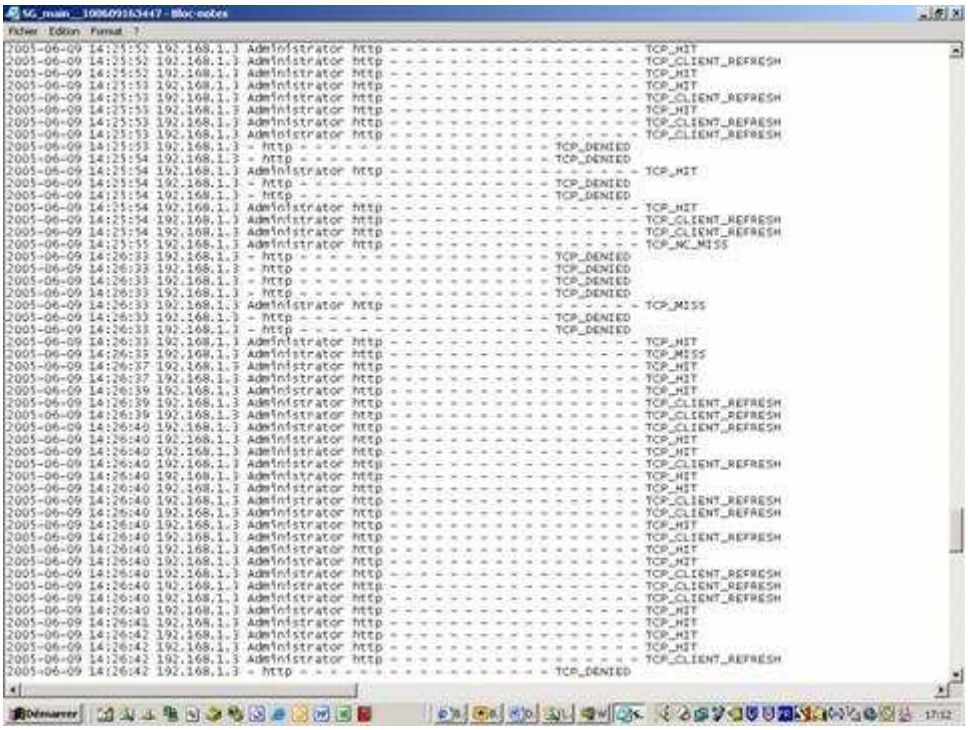


Figure-A6-fichier logs

8. BlueCoat Reporter

Permet aux entreprises de comprendre et d'analyser l'utilisation des contenus vidéos web auxquels les utilisateurs accédent via le réseau d'entreprise.

La technologie Blue Coat assure un monitoring de l'utilisation et de la consommation de ressources inhérente à la consultation, la visualisation et au téléchargement du vidéo web. Blue Coat Reporter permet de visualiser l'utilisation de la vidéo par utilisateur, groupes d'utilisateurs mais aussi le type de protocoles et de méthodes d'accès à la vidéo.

Blue Coat Reporter fournit une visibilité sur toute l'activité WEB des utilisateurs. Au-delà du filtrage d'URL, Blue Coat Reporter permet de manière intuitive de personnaliser les tableaux de bord et rapports pour être un élément inestimable en termes de sécurité, réglementation, gestion et contrôle de la bande passante et tout élément

critique en environnement concurrentiel. Blue Coat Reporter traite rapidement les données provenant des Blue Coat ProxySG, Blue Coat WebFilter, Blue Coat ProxyClient et Blue Coat ProxyAV, et génère des rapports intuitifs pour les responsables sécurité, Responsables RH, Administrateurs.

Figure-A7-bluecoat reporter

B. STONESOFT [8][20]

1. Description générale du produit StoneGate de Stonesoft :

Le produit StoneGate IPS-1205 est une solution matérielle intégrée (de type appliance) de système de détection et de prévention d'intrusion réseau (NIDPS = Network Intrusion Détection and Prevention System) développée par la société StoneSoft.

Il s'agit d'un produit commercial proposant une analyse de flux réseau, des remontées d'alertes et un blocage des tentatives d'intrusion détectées.

L'IPS dispose d'un système d'exploitation intégré correspondant à un Linux durci dont les packages non nécessaires ont été retirés. L'ensemble des logiciels de l'IPS est mis à jour lors de la montée en version de l'IPS.

L'IPS StoneGate propose les fonctionnalités suivantes :

- *Des méthodes de détection d'intrusion* :
  - ✓ Détection basée sur l'utilisation de signatures.
  - ✓ Détection d'anomalies basées sur des analyses statistiques des flux.
  - ✓ Détection des contournements de protocole.
  - ✓ Corrélation d'évènements.
- *Des mécanismes de réponse faisant suite à la détection d'un trafic anormal tels que :*
  - ✓ La remonté d'alertes.
  - ✓ L'enregistrement du trafic.
  - ✓ La terminaison de connexions TCP.
  - ✓ L'utilisation d'une liste noire pour bloquer des flux de certains réseaux. Cette liste noire correspond à une liste d'adresses IP bloquées temporairement et définie soit manuellement par l'administrateur, soit automatiquement par l'IPS.
  - ✓ Le blocage des flux par l'IPS positionné en coupure.

*Un système StoneGate IPS se compose de (***Figure-B1-***) :*

- *Une ou plusieurs appliance IPS.*
- *Un système d'administration SMC (StoneGate Management Center) pour la configuration de l'IPS comprenant les composants suivants :*

- ✓ Un serveur de gestion (Management Server) pour la configuration de l'IPS.
- ✓ Un ou plusieurs serveurs de journalisation (Log Server) pour le stockage et la *gestion des journaux.*
- ✓ Un ou plusieurs clients du serveur de gestion (Management Client) qui fournissent une interface graphique de configuration et de suivi de l'IPS.

Les connexions entre l'IPS et le serveur de gestion ou le serveur de journalisation sont protégées par un canal SSL/TLS avec authentification mutuelle et chiffrement.

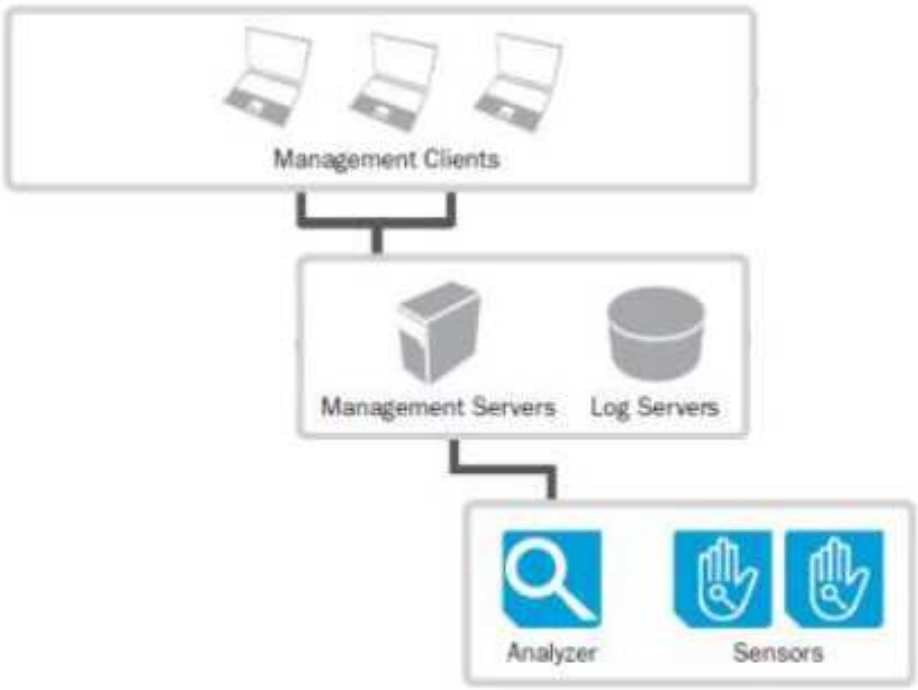


Figure-B1- Composants d'un système StoneGate IPS

Une appliance IPS peut être installée des deux façons suivantes :

• En mode IDS (Intrusion Dectection System) : Installation en mode capture pour une capture et analyse des flux sans coupure.

• En mode IPS (Intrusion Prevention System) : Installé en mode coupure pour une analyse et une coupure des flux.

2-1. Mode d'utilisation et environnement du produit :

Le produit StoneGate IPS est connecté au réseau en mode coupure ou en mode capture en fonction de son mode d'installation.

Un IPS installé en mode IPS (configuration évaluée) se connecte au réseau en mode coupure à l'intérieur du réseau à protéger (**Figure-B2-**)

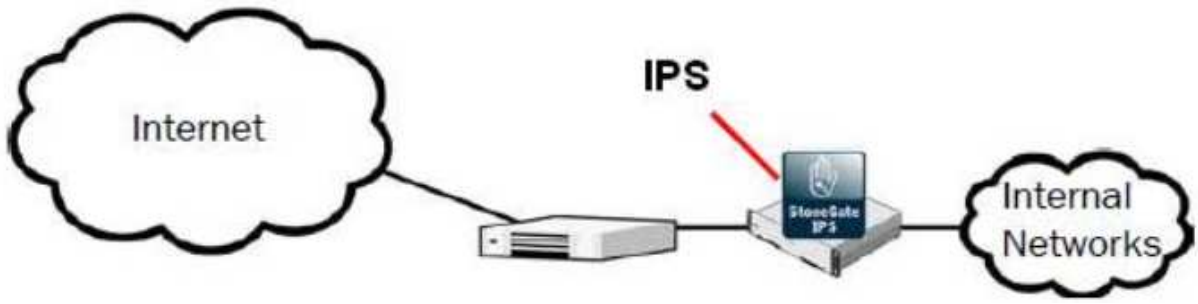


Figure-B2-Exemple de positionnement d'un IPS installé en mode IPS.

Un IPS positionné en mode capture doit être relié au réseau par un dispositif TAP ou un SWITCH SPAN possédant des propriétés de mirroring permettant la capture du réseau de manière transparente et robuste.

La configuration de l'IPS est réalisée au travers un système d'administration SMC (StoneGate Management Center) qui inclut un système client/serveur de gestion et un serveur de log. Le SMC s'installe sur une plate-forme de type Linux ou Windows sur une ou plusieurs machines.

2-2. Utilisateurs typiques du produit :

Les utilisateurs du système d'IPS sont les suivants:

Un administrateur qui a en charge :

- L'installation du SMC.
- L'installation de l'IPS.
- La configuration et maintenance du SMC et de l'IPS

. Ces administrateurs disposent de droits d'accès privilégiés au système d'exploitation SMC (droit root pour Linux et droits administrateur sous Windows).

Un exploitant qui a en charge de :

• La mise à jour de la base de signatures.

• Le traitement des alertes.

- ✓ L'audit des journaux.

Le SMC propose une gestion des rôles afin de restreindre les droits de certains administrateurs. Un compte administrateur avec pleins pouvoirs est automatiquement créé lors de l'installation du SMC. Ce compte permet la création d'autres comptes d'exploitants ayant moins de droits que l'administrateur principal.

2-3. Hypothèses sur l'environnement

Plate-forme sécurisée :

Le SMC est installé sur un système d'exploitation correctement administré et configuré (mises à jour périodiques, désactivation des services et partages non utilisés, contrôle d'accès restreint aux seuls utilisateurs autorisés).

Locaux :

L'appliance IPS et les équipements contenant le SMC doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

Administrateurs :

Les administrateurs de l'IPS et du SMC sont des personnes considérées comme non hostiles. Ils sont formés pour administrer et configurer les produits.

Ils suivent les manuels et procédures d'administration.

Audit :

L'administrateur consulte régulièrement les données de journalisation et traite les alarmes de sécurité générées par l'IPS StoneGate.

3. Biens sensibles que le produit doit protéger

Le produit contribue à protéger les biens sensibles énumérés ci-dessous.

Biens des utilisateurs du réseau protégé

Les données et services des utilisateurs du réseau protégé.

Données de configuration de l'IPS

Les fichiers de configuration de l'IPS incluant la liste noire.

La base de signatures

Une méthode de détection d'intrusion de l'IPS est basée sur l'utilisation d'une base de signatures qui est mise à jour périodiquement.

Les journaux d'audit et d'alertes

Des journaux d'alertes sont remontés par l'IPS afin d'être traités par un administrateur. En outre, une journalisation des opérations réalisées sur le produit telles que la modification de la configuration, l'authentification des utilisateurs est mise en place.

Les informations sur l'état d'une appliance IPS

Le serveur de gestion récupère automatiquement les traces des composants IPS. Un système de monitoring est proposé par le SMC.

4 Menaces supposées de l'environnement :

Les attaquants potentiels sont des attaquants externes (des personnes extérieures au réseau protégé).

Pour rappel, les hypothèses considèrent que les administrateurs ne sont pas des attaquants potentiels.

Les attaques peuvent être menées à partir de l'externe ou de l'interne (si une machine interne a été compromise par un attaquant externe).

Les menaces portant sur l'IPS sont les suivantes :

Attaque par contournement du système de reconnaissance des signatures

Un attaquant peut exploiter une faille dans le processus de mise à jour de la base de signatures lorsque cette opération n'est pas régulière (données de signature obsolètes)

ou réalisée à partir de données de signature de mauvaise qualité (ne répertoriant pas toutes les signatures publiques).

Attaque protocolaire :

Un attaquant peut tenter de contourner l'IPS par une attaque protocolaire. Ce type d'attaque peut exploiter des biais ou des absences d'implémentation du système de contrôle protocolaire de l'IPS.

Attaque par déni de service :

Un attaquant peut inonder l'IPS en émettant une quantité de données suffisamment importante (*ex: multiples demandes de connexion*) pour le rendre inactif le temps de mener une intrusion perspicace. Il est également envisageable d'exploiter une faille dans l'implémentation de l'IPS afin de générer un débordement de tampon. Un autre type d'attaque consiste à générer de nombreuses simulations d'intrusion afin de provoquer une émission de nombreux faux-positifs (ex : multiples scans réseau).

5. Fonctions de sécurité du produit

Mise à jour de la base de signatures :

Le SMC propose une fonctionnalité de mise à jour de la base de signatures. Pour ce faire, le serveur de gestion se connecte périodiquement au site Web de Stonesoft afin de vérifier si une nouvelle base de signature est disponible. La mise à jour peut être automatisée ou manuelle suite à une remonté d'alerte. Cette fonction de sécurité est renforcée par une fonctionnalité de restauration automatique du système dans sa configuration précédente qui peut être activée lors d'une opération de mise à jour du système. Ce processus permet d'éviter qu'un IPS dispose d'une base de signature incomplète ou non fonctionnelle en cas d'échec de la mise à jour.

La société StoneSoft met régulièrement à jour la base de signature sur leur site internet.

Détection des intrusions :

La détection des intrusions consiste en la capture des flux réseau, le décodage des protocoles et la comparaison du trafic basée sur les signatures.

Corrélation d'évènements

Une fonction de corrélation propose les fonctionnalités suivantes :

-« Compress » : Rassemble des évènements du même type dans un log (ex : accès à des fichiers serveur).

-« Count » : Comptabilise le nombre de connexions récurrentes sur une période donnée.

-« Group » : Regroupe des suites d'évènements similaires. Ceci permet par exemple de détecter l'attaque d'un logiciel par la mise en œuvre des vulnérabilités publiques.

-« Match » : Offre la possibilité d'utiliser des filtres sur des situations spécifiques.

-« Sequence » : Vérifie l'utilisation de suites de messages reconnus comme valides (Une demande d'ouverture de fichier suivie d'un accès au fichier).

Liste noire :

Une liste noire permet de bloquer, pour une durée définie, les flux provenant d'adresses IP suspectées d'intrusion.

Blocage des intrusions :

Une fonctionnalité de blocage des intrusions est implémentée par l'IPS.

Gestion des alertes et des journaux :

Lorsque certains évènements ne peuvent pas être bloqués faute de garantie sur la véracité de l'attaque, des alertes pertinentes et de qualité sont remontées par l'IPS. En outre, une journalisation permet de conserver les évènements remontés par l'IDS.

6. Périmètre de l'évaluation

Le périmètre d'évaluation comprend l'IPS StoneGate Intrusion Prevention System installé en mode IPS.

. L'IPS peut être installé sur les plates-formes suivantes :

-Appliance StoneGate,

-Serveur Intel,

-Serveur VMware ESX.

L'appliance IPS StoneGate est retenue pour cette évaluation

. La liste noire n'est pas activée par défaut.

L'utilisation de la liste noire est incluse dans le périmètre de l'évaluation.

L'IPS peut être positionné en mode coupure ou écoute selon son utilité (IDS ou IPS).

Un positionnement de l'IPS en mode coupure est retenu pour cette évaluation.

Références Bibliographiques

[1]:Doug Lowe,''Les réseaux '',édition first interactive ,2002

[2] : Revue sonatrach.

[3]: Pujolle.G,''Les réseaux'',Groupes Eyrolles 2002,2003

[4]:Guillaume Desgeorge,''La sécurité des réseaux''.

[5]:Grady Booch, James Rumbaugh et Ivar Jacobson. ''Le guide de l'utilisateur UML''.

[6] : Administration réseaux.

[7]: Administrator guide BLUECOAT

[8]: Administrator guide STONESOFT

II-Références Webliographiques :

[9]:http://www.Wikipédia.org.

[10] :http//www.commentcamarche.com.

[11]:http://www.math.u-bordeaux1.fr.

[12]:http://www.cryptez.ifrance.com.

[13]:http://www.frameip.com.

[14]:http://www.guill.net.

[15]:http://www.securiteinfo.com.

[16]:http://www.wapiti.telecom_lille1.eu.

[17]:http://www.lacl.univ-paris12.fr.

[18] : http//sonatrach.dz.

[19] : http//www.bluecoat.com.

[20] :http//www.stonesoft.com.