# Projet Sécurité Réseaux

| | |
|---|---|
| **Nom de l'université :** | Université de Nice Sophia-Antipolis |
| **Intitulé du cours :** | Sécurité Réseaux |
| **Binôme :** | Ferro Luca & Salman Nader |
| **Date :** | 31/01/2006 |

## CONTENU DU SOMMAIRE

INTRODUCTION :

Les attaques informatiques constituent aujourd'hui l'un des fléaux de notre civilisation moderne. Il ne se passe plus une semaine sans que l'on apprenne que telle entreprise ou tel institut a essuyé de lourdes pertes financières en raison d'une déficience de la sécurité de son système d'information. Par conséquent les entreprises ne peuvent plus ignorer ces risques et se croire à l'abri de telles épreuves.

C'est donc pour cela que nous nous sommes penchés sur la sécurité de l 'activité électronique d'une entreprise de loterie comme la Française des Jeux. Nous allons donc, pour lever toute ambiguïté, présenter le système tel que nous l'avons compris. Nous avons donc une entreprise qui propose à de nombreux commerçants une franchise qui leur permet d'enregistrer des paris. Chaque transaction est effectuée a l'aide d'un terminal spécifique fournit par l'entreprise. Chaque semaine, un tirage au sort à lieu sous le contrôle d'un représentant légal dans les studios de télévision. Les paris sont centralisés au siège de l'entreprise, ainsi que les résultats du tirage. Les rapports et les statistiques sur les gagnants sont fournis aux différents organes de presse ainsi qu'au contrôleur légal – lequel peut exiger un rapport détaillé – par Email. Les gagnants se présentent sur n'importe quel point de vente pour encaisser leur gain ceci implique donc que le commerçant devra en tenir informer le siège. Le logiciel des terminaux est quant a lui développé par une équipe de programmeurs opérants en province, on suppose donc que ces derniers sont a distance par rapport au siège. Une autre équipe d'administrateurs développe la base de donnée du siège sur leur lieu de travail.

Nous commencerons par étudier les principaux cas d'utilisation engendrés par notre système et en tirer les risques potentiels encourus ainsi que les solutions à mettre en oeuvre pour limiter les risques majeurs. Puis nous déterminerons la structure des réseaux de l'entreprise ainsi que l'emplacement des principaux serveurs et composants du système. Finalement nous localiserons les composants physiques ou logiques du système de sécurité que l'on aura mis en ouvre.

# RISQUES ET PARADES

Aujourd'hui les différentes transactions commerciales s'appuient de plus en plus sur les réseaux informatiques. Avec la libre circulation des informations et la haute disponibilité de nombreuses ressources, les responsables de réseaux d'entreprise, telle que la FDJeux, doivent connaître toutes les menaces susceptibles de compromettre la sécurité. Celles-ci prennent de nombreuses formes, mais résultent toutes en une compromission de la confidentialité à un certain degré et en une destruction possible de données ou de ressources pouvant conduire a des pertes financières considérables.

Il est important de connaître les points de vulnérabilité d'un réseau pouvant servir de porte d'entrée à d'éventuels intrus et de distinguer les différentes catégories d'attaquants. Le niveau de confiance doit quant à lui être défini selon les besoins. Il sera donc nécessaire de restreindre l'utilisation des équipements et des ressources de l'infrastructure de réseau. Limiter l'accès uniquement aux personnes qui en ont besoin représente un bon moyen de se protéger des nombreuses menaces de sécurité.

Nous allons donc voir dans ce qui suit les principaux acteurs et activités de notre système ainsi que les différents risques pouvant êtres encourus pour lesquels nous donnerons une solution a mettre en ouvre.

## DEFINITION DES CAS D'UTILISATION PRINCIPAUX

SUJETS ET OBJETS DU SYSTEME MIS EN CAUSE

Notre interprétation du système comporte les acteurs suivants :

a) Commerçant

b) Studios de télévision

c) Siège

d) Représentant légal

e) Organes de presse

f) Equipe des programmeurs

g) Equipe des administrateurs

On peut alors constater que le joueur/gagnant n'est pas présente. Cela est du au fait qu'il n'interagit pas directement avec le "système". Certains acteurs identifient un groupe de sujets ayant exactement le même rôle dans un cas donné (par exemple "Organes de presse").

Les cas d'utilisations remarquables sont :

A) Enregistrer un pari (transaction)

B) Signaler un encaissement du gain (transaction), comportant l'identification stricte du gagnant

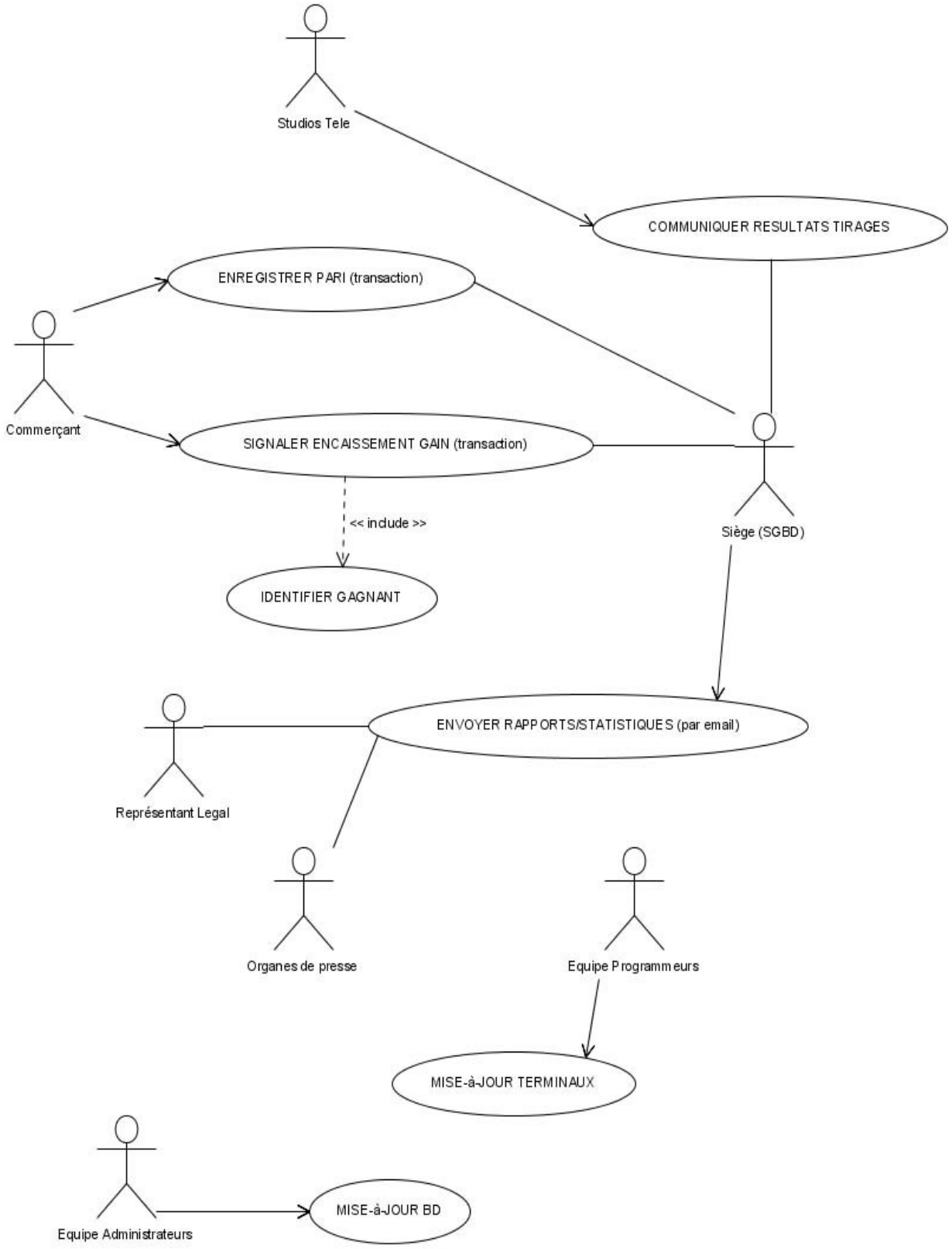
C) Communiquer les résultats des tirages

D) Envoyer les rapports et les statistiques par email

E) Mise-à-jour du logiciel des terminaux

F) Mise-à-jour de la BD

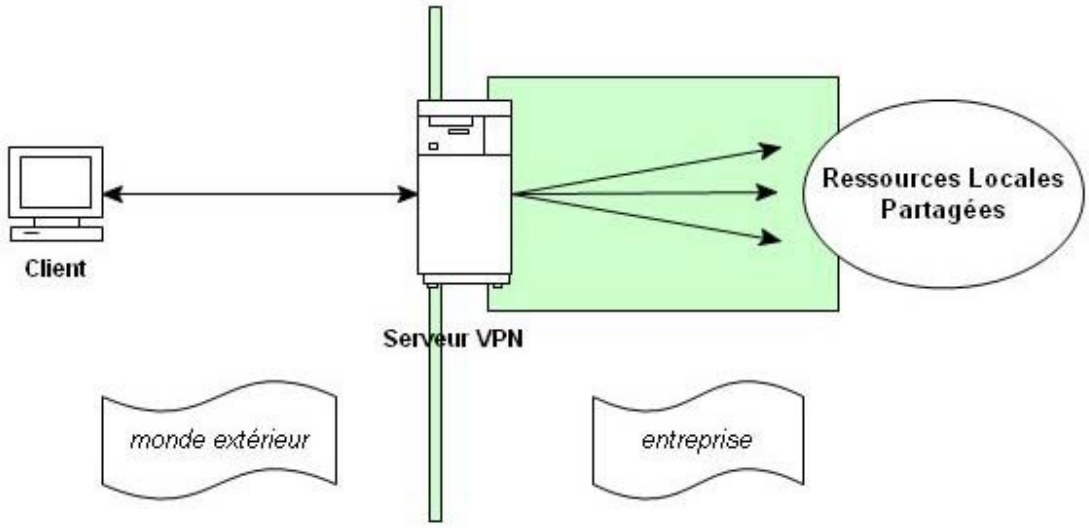
Le schéma à la page suivante montre les "relations" entre les différentes acteurs et cas d'utilisations.


Studios Tele
COMMUNIQUER RESULTATS TIRAGES
ENREGISTRER PARI (transaction)
Commerçant
SIGNALER ENCAISSEMENT GAIN (transaction)
Siège (SGBD)
<< include >>
IDENTIFIER GAGNANT
ENVOYER RAPPORTS/STATISTIQUES (par email)
Représentant Legal
Organes de presse
Equipe Programmeurs
MISE-à-JOUR TERMINAUX
Equipe Administrateurs
MISE-à-JOUR BD

RISQUES POTENTIELS ENCOURUS ET RISQUES MAJEURS

A tout moment le siège (et le SGBD) peut subir des intrusions illégales et des dénis de service (DoS). Si on exclut temporairement les DoS, on peut alors généraliser les risques existants sous trois catégories : accès, stockage des données, transit des données. Si l'ensemble des données est éparpillé sur différentes machines et il n'est pas centralisé nous devons alors multiplier inutilement les efforts pour protéger les informations (par exemple, il serait absurde de garder localement dans un terminal les paris effectués chez un certain commerçant). Cependant, centraliser ne signifie pas "concentrer" toutes les programmes et les données sur une seule machine! Il faut évidemment prévoir des backups pour les données ainsi qu'une subdivision des services en différentes couches.

La sécurisation du transport des données est principalement réalisable au travers de couches logicielles visant à chiffrer les échanges. Le déploiement d'un accès chiffré global de type "Virtual Private Network" (VPN) peut constituer une solution intéressante mais elle requiert des moyens considérables.




Les risques potentiels encourus au sein de cette activité électronique sont plus nombreuses et bien plus complexes par rapport aux problématiques qui peuvent concerner un utilisateur isolé. Par exemple, le risque d'intrusion et d'espionnage des données privées peut ne pas être consistant pour une seule personne, mais il s'avère crucial pour notre activité.

Le tableau suivant présente les types de menaces possibles, en associant à chaque menace ses conséquences, ses parades et les cas qui peuvent en être concernés. Le tableau ressemble différentes catégories de risques, ces derniers pouvant se ramener à deux origines : environnementale et humaine. De plus, les risques peuvent être classifiés

comme "hardware" (physiques) où "software". Les lignes du tableau en jaune indiquent les risques majeurs nécessitant une solution importante.

| ***Type de Menace*** | ***Conséquences*** | ***Parades*** | ***Cas et objets concernés*** |
|---|---|---|---|
| Incendie | Indisponibilité / Destruction des équipements.<br>Indisponibilité totale ou partielle du réseau. | Système de détection et/où protection contre l'incendie avec retour d'alarme vers un poste permanent.<br>Vérifications périodiques.<br>Informations spécifiques pour chaque locale. | Siège. |
| Dégâts des eaux | Indisponibilité / Destruction des équipements.<br>Indisponibilité totale ou partielle du réseau. | Etude approfondie préalable du risque eau.<br>Système de prévention / sonde avec retour d'alarme vers un poste permanent.<br>Système de coupure automatique de l'électricité.<br>Schéma des canalisations. | Siège. |
| Panne électrique / surtension | Indisponibilité / Destruction des équipements.<br>Indisponibilité totale ou partielle du réseau. | Alimentation secourue (groupe électrogène) et stabilisée (onduleur).<br>Schéma de câblage.<br>Régulateur de tension, parafoudre, terres normalisées.<br>Double pénétration électrique (éventuellement). | Siège. |
| Coupure de courant | Perte de données. Dysfonctionnements.<br>Indisponibilité totale ou partielle du réseau. | Alimentation réglée et secourue.<br>Pour le siège :<br>remontées d'alarmes | Siège, mais aussi terminaux (transactions depuis les terminaux, envoi / réception des |

| *Type de Menace* | *Conséquences* | *Parades* | *Cas et objets concernés* |
|---|---|---|---|
| | | vers un poste permanent.<br>Pour les transactions :<br>contrôles d'exceptions bien soignés, codages et détections de la consistance des transactions, "commits" et "rollbacks", ... | données) |
| Erreurs de manipulation | Indisponibilité des équipements et du réseau. | Schéma de câblage. Information et formation du personnel.<br>Cahier d'intervention.<br>Matériel de secours. | Siège. |
| Intrusion | Détérioration / Dégâts des équipements.<br>Vol de matériel.<br>Pose de sonde d'écoute. | Accès sécurisé avec au besoin un enregistrement des accès.<br>Alarmes et systèmes de détection d'ouverture.<br>Identification des équipements (différents moyens). | Siège. |
| Piratage : écoute | Perte de confidentialité.<br>Lecture illicite des informations. | Pour le siège et les terminaux :<br>orienter les matériels de façon à empercher l'observation.<br>Pour le siège : sensibiliser le personnel (économiseurs d'écrans avec mot de passe, ...). | Siège, terminaux chez les commerçants. |
| Piratage : vol d'information | Perte de confidentialité.<br>Lecture et utilisation illicites des informations. | Chiffrement, Encryptage.<br>Minimiser la durée des transactions. | Transactions.<br>Communication des résultats.<br>Envoi des rapports et |

| *Type de Menace* | *Conséquences* | *Parades* | *Cas et objets concernés* |
|---|---|---|---|
| | Triche. | | statistiques.<br>Mise-à-jour en ligne. |
| Piratage : détournement / falsification emails | Perte de confidentialité.<br>Engendrer le désordre.<br>Lecture illicite des informations. | Messagerie sécurisée, PGP, S/MIME.<br>Chiffrements couplés avec des certificats. | Envoi des rapports et statistiques. |
| Piratage : déni de service (DoS) | Privation des services!<br>Indisponibilité totale ou partielle du réseau et du système. | Test de la taille des paquets, test des adresses source et destination (ainsi que loop-back, unicast, multicast...), test de la fragmentation, utilisation d'adresses IP virtuelles pour validation de sessions et ACK (contre attaques TCP), test du nombre de SYN (contre attaques TCP), NAT d'adresses locales vers IP virtuelles basées sur IP globales, contrôles de flux, contrôles de contenus (port, tag, url, extensions de fichiers), autres fonctions de firewall, le tout basé sur du load-balancing et de la redondance, ...<br>Les contre-mesures sont généralement compliqués et très ciblées vis-à-vis du type de deni.<br>"Full scalability". | Siège.<br>Transactions.<br>Communication des résultats. |
| Piratage : intrusion sur le réseau | Récupération, modification d'informations.<br>Dégâts et dénis de | Firewall.<br>IPS.<br>Cloisonnement, | Siège. |

| *Type de Menace* | *Conséquences* | *Parades* | *Cas et objets concernés* |
|---|---|---|---|
| | service.<br>Triche. | filtrage.<br>Authentification forte. | |
| Piratage : utilisation d'un terminal / introduction virus | Dégâts et dénis de service sur le réseau.<br>Engendrer le désordre. | Anti-virus. Filtrage.<br>Empêcher l'accès distant à un terminal.<br>Mot de passe et authentification forte. | Terminaux, transactions et mise-à-jour en ligne. |
| Branchement "pirate" | Ecoute, récupération, modification d'informations.<br>Triche. | Protection des chemins des câbles.<br>Vérifications visuelle et physique des chemins de câble pour la partie privée du réseau.<br>Surveillance des flux.<br>Chiffrement des informations. | Transactions.<br>Communication des résultats.<br>Envoi des rapports et statistiques.<br>Mise-à-jour en ligne. |
| Perturbation des liaisons | Brouillage du signal.<br>Modification / Perte d'informations. | Matériel répondant aux normes précisées dans la directive Européenne 89/336/CEE.<br>Passage du câble sous gaines dans les endroits "à risques". | Siège (réseau interne).<br>Transactions. |

# SOLUTION DE SECURITE

Nous allons aborder dans cette partie l'infrastructure physique du réseau, ceci inclus donc une multitude de composants physiques ou logiques nécessaires au bon fonctionnement de notre entreprise. L'infrastructure physique du réseau englobe le choix d'un type de média approprie et un chemin de câblage (la topographie du réseau). On doit s'assurer qu'aucun intrus ne puisse capturer les données traversant le réseau au moyen d'une écoute clandestine et que tous les systèmes vitaux offrent un haut degré de disponibilité.

D'un point de vue purement physique, le type de câble choisi pour les différentes parties du réseau peut dépendre de la sensibilité des informations qui doivent circuler sur le réseau. Sachant que l'entreprise pour laquelle nous assurons la sécurité a un chiffre d'affaire assez « colossal » (millions d'euros), il serait « intéressant » (mais coûteux ☺ ) d'utiliser la fibre optique en tant que support. Comparée aux câbles coaxiaux et aux paires torsadées, la fibre optique est plus utilisée lorsque l'on a une large bande passante ou que l'on ai a travailler sur des espaces étendus (distance s'élevant a plusieurs Km entre le Siège et les terminaux dans cette architecture). Contrairement aux deux autres types de câbles, la fibre optique ne produit pas de rayonnement électromagnétique parasite et bénéficie par conséquent d'un haut degré de protection contre la capture (elle est aussi insensible aux interférences). D'un autre coter, il est difficile pour un cyber-criminel d'y greffer un dispositif d'interception clandestine. On pourrai introduire dans le réseau de notre entreprise un outil permettant de mesurer la qualité du signal. On utilise en général un réflectomètre a balayage temporel (câble coaxial) ou réflectomètre optique (fibre optique). Nous nous attarderons pas plus sur ce genre d'outils bien trop compliques a expliquer.

Il est également indispensable de prendre en considération la topographie du réseau étalée par l'entreprise (FDJeux) car elle a une influence sur la disponibilité du réseau et des équipements connectés ainsi que sur la fiabilité et sécurité de l'infrastructure. Un point de départ serait d'avoir une structure de câblage qui minimiserait les risques d'immobilisation massive (voir schéma 1 et 2). On remarquera que dans le schéma1 une rupture de segment provoquerait une panne touchant plusieurs filiales et donc plusieurs terminaux, alors que dans le schéma2 la rupture de n'importe quel câble ne touche qu'un terminal.

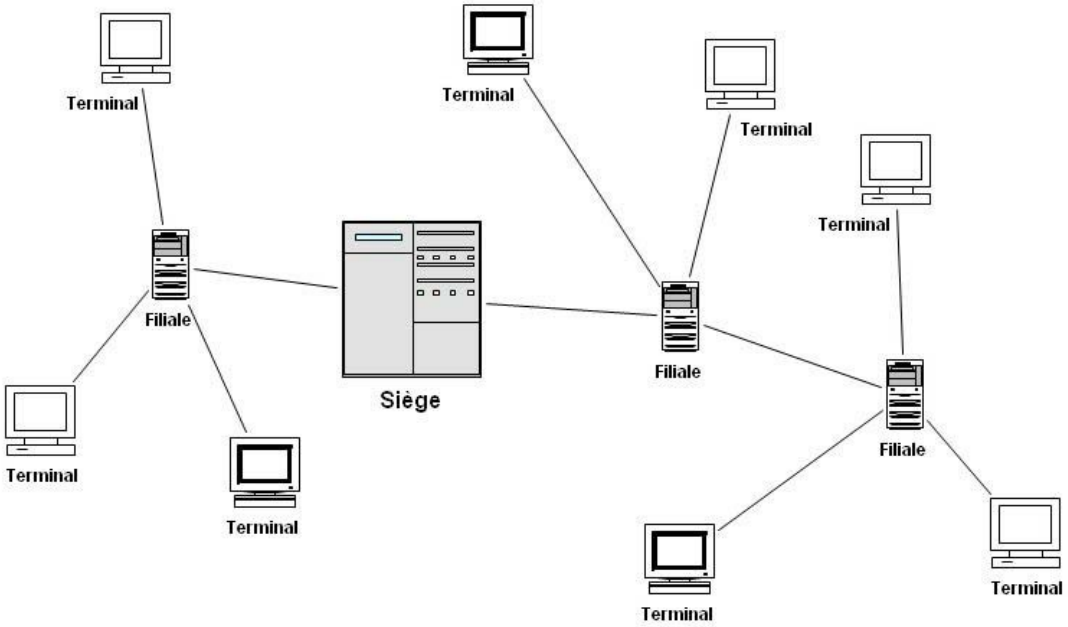



*Schéma 1 : réseau n'étant pas en étoile*

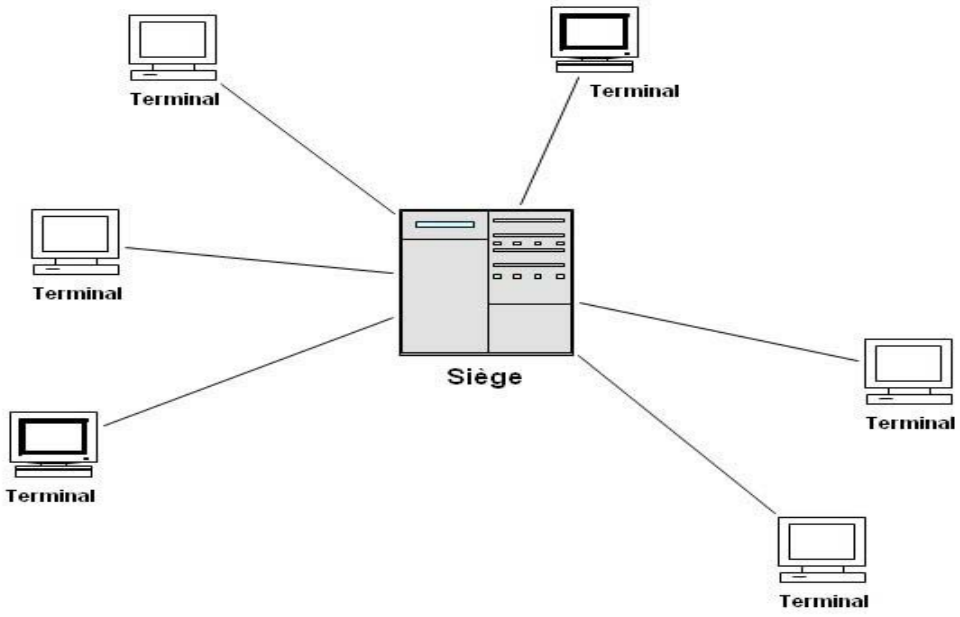



*Schéma 2 : topographie en étoile*

## STRUCTURE DES RESEAUX DE L'ENTREPRISE (RACCORDEMENTS AU RESEAU PUBLIC)

Il faut imaginer un circuit de connexion entre le monde extérieur et le réseau de l'entreprise, incluant des moyens de sécurisation pour accéder à chaque couche réseau. La rapidité des échanges sera un élément important garantissant la réactivité d'éventuelles interventions distantes. Dans le cas d'un programmeur (où encore plus important, d'un administrateur), on peut imaginer comme complément de sécurité un système de "call back" qui permet de rappeler automatiquement le numéro de téléphone de la personne concernée (enregistré au préalable) : l'authentification de la ligne sera ainsi assurée et l'accès limité.

Une séparation physique du réseau d'administration informatique du réseau d'entreprise est conseillée, au travers d'interfaces spécifiques et dédiées. Une solution idéale peut etre d'avoir trois séries d'interfaces pour chacun des serveurs, afin de séparer les trois flux suivants :

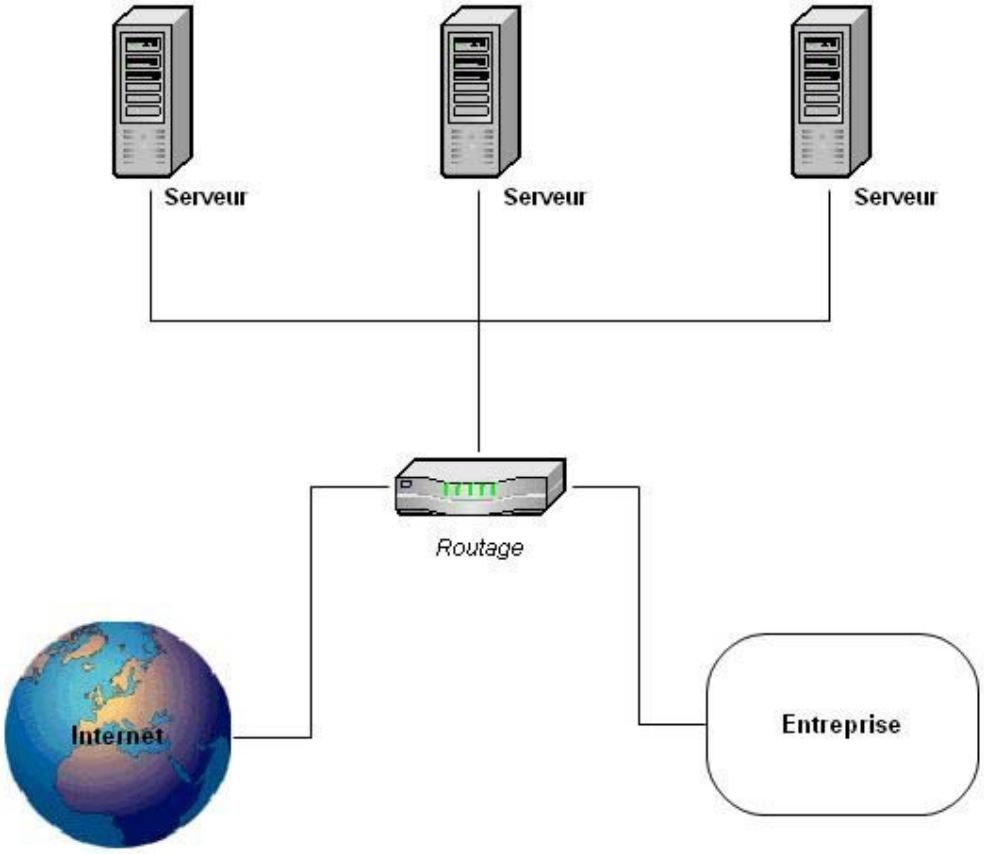
i. interface publique : flux à destination des terminaux et des organes qui attendent les rapports

ii. interface privé : flux d'administration et de prise de contrôle à distance

iii. interface de sauvegarde : flux de sauvegarde (BD) des données

Pour réduire le coût global, il est possible de coupler les deux dernières pour n'obtenir au final que deux interfaces : publique et privé.

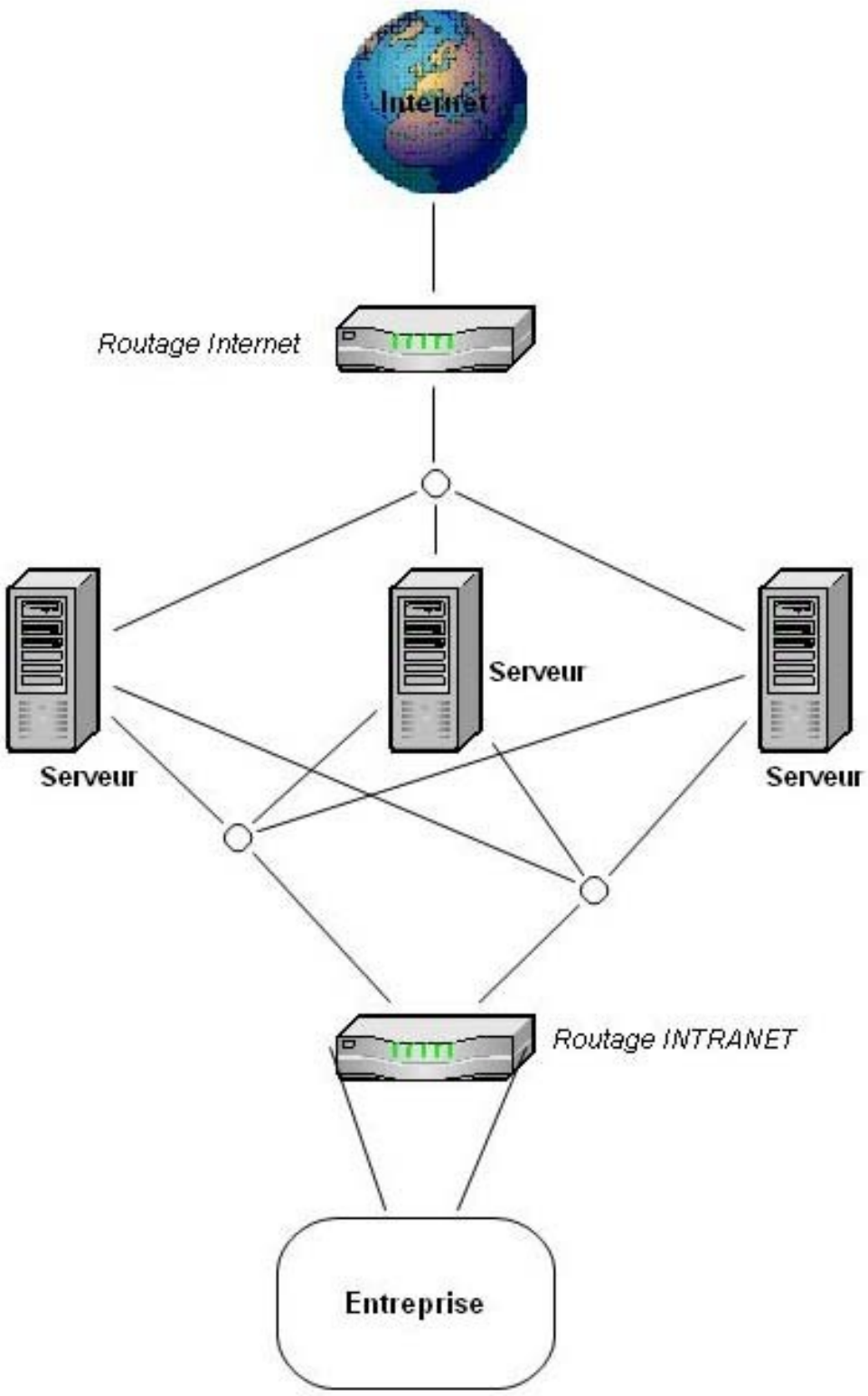
L'image à la page suivante identifie un réseau d'interconnexion simplifié entre les serveurs et les administrateurs (où programmeurs, dans le cas du(des) serveur(s) pour le logiciel des terminaux).




Réseau d'interconnexion simplifié

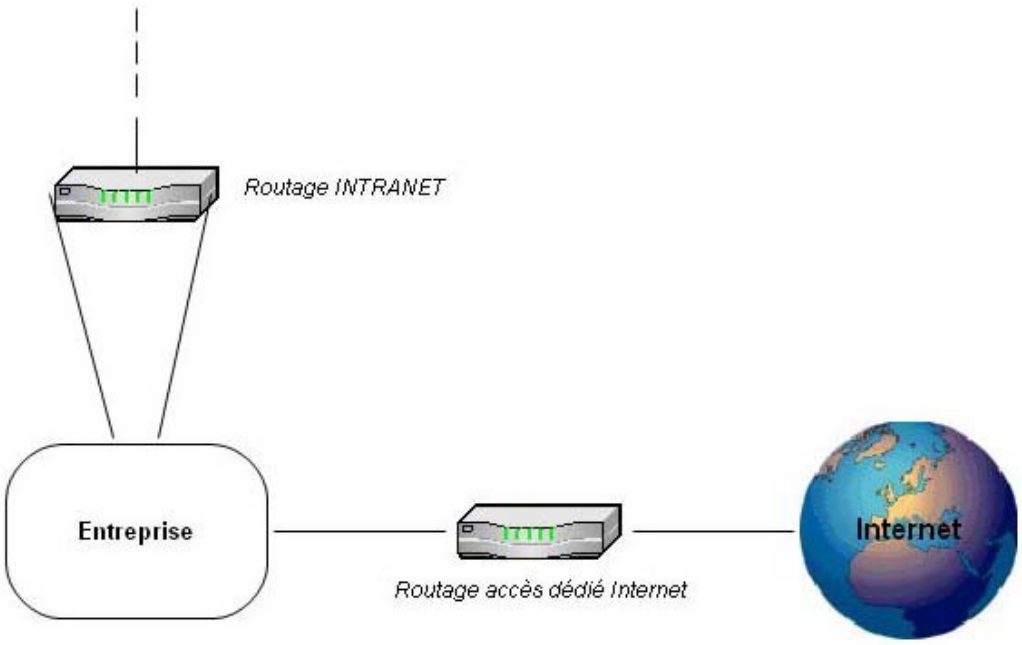
Ici le trafic est concentré autour d'un point de routage unique. En cas de prise de contrôle d'un serveur (par un "cyber-criminel" quelconque), le risque est maximal, à la fois pour les autre serveurs dont le trafic d'administration n'est pas isolé et pour les données extranet de l'entreprise qui circulent sur ce même réseau.

Il serait préférable de concevoir une structure comme celle qui suit :



Dans ce cas les serveurs ont d'interfaces réseau (logiques ou physiques) différenciées pour le trafic destiné à Internet et  pour celui destiné à l'entreprise. On voit aussi que le contact avec le point de "routage INTRANET" est double : l'un est dédié à l'administration distante des serveurs (de la part des administrateurs ou des programmeurs pour certains serveurs uniquement), l'autre est dédié au réseau de sauvegardes.

L'accès Internet du personnel (s'il a lieu) ou celui pour l'envoi des rapports (si ces derniers sont gérés par le personnel) sera différencié de celui permettant l'accès aux serveurs hébergés :




Accès Internet

Probablement la meilleure solution pour effectuer cet accès dédié serait d'utiliser un fournisseur d'accès Internet différent du fournisseur d'hébergement afin de mieux tester l'accès aux infrastructures "publiques". Si cela n'est pas possible, il faudra impérativement obtenir cette isolation des types de trafic par le moyen des règles de routage.

EMPLACEMENT DES PRINCIPAUX SERVEURS, COMPOSANTS PHYSIQUES ET LOGIQUES

La première étape essentielle consiste à déterminer à quel "public" s'adresse un service donné, en subdivisant les ressources selon plusieurs catégories (interne à l'entreprise, externe à l'entreprise et anonyme, externe à l'entreprise et authentifié). L'isolation des trafics est un moyen de protection adapté pour la sécurisation de l'administration, une fois que la nature du trafic (émetteur, récepteur) a été identifie.

Dans notre cas spécifique l'entreprise ne devrait accepter aucun trafic (en entrée) provenant d'une "source" différente des terminaux ou des administrateurs (ou programmeurs). La gestion des droits d'accès sera facilitée par le regroupement des différents serveurs en zones "démilitarisées" (DMZ) : au sein d'une même zone se trouveront des serveurs accessibles par le même type de "public". Des règles spécifieront que l'ensemble du trafic en provenance d'Internet pourra accéder à la zone Internet / extranet alors que seules les IP non routables en provenance de l'intranet pourront atteindre la DMZ intranet ou les interfaces d'administration de l'extranet.

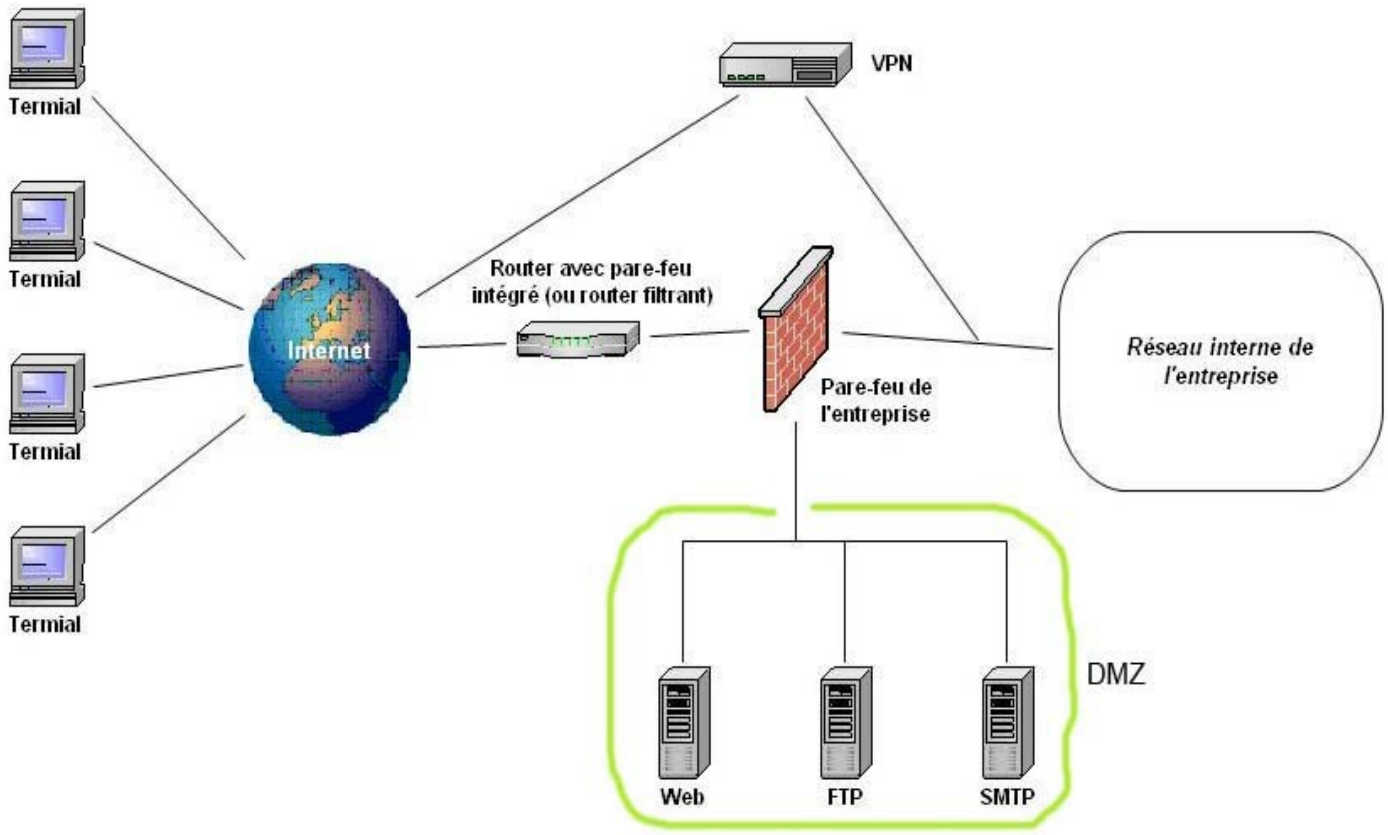



*Schéma général de la structure du réseau*

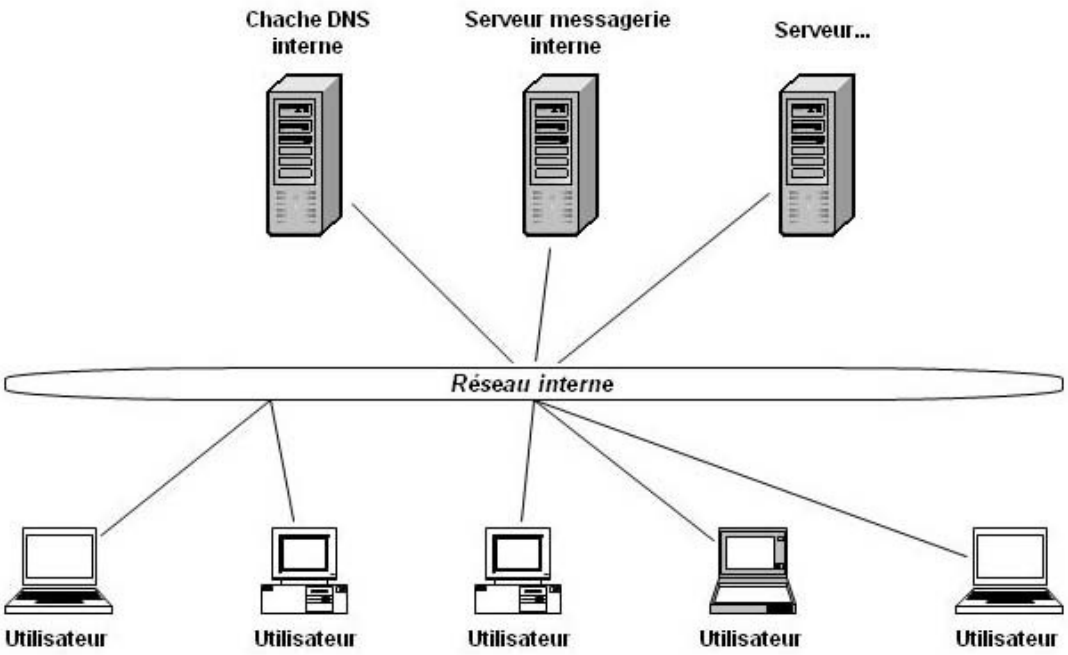



*Schéma du réseau interne de l'entreprise*

Le router

Puisque le réseau de notre entreprise est relié à Internet (liaison spécialisée permanente), la société se voit attribuer une plage d'adresses IP publique uniques. La mise en place d'un routeur en frontal de ce point d'accès Internet permet de canaliser les flux (TCP-IP) sur les machines et d'ouvrir ou fermer les accès.

Pour mettre en oeuvre ce cloisonnement, il faut :

1. Découper notre réseau privé en domaines de sécurité
2. Déterminer les flux entre nos différents domaines
3. Définir une politique de sécurité sur ces flux (qui a le droit ou pas de passer)
4. Appliquer ces règles de flux sur les équipements de cloisonnement (router, pare-feu, ...)

## Le pare-feu

Ce filtrage n'est, pour autant, pas suffisant pour protéger le réseau car les trames transmises ne sont pas analysées en profondeur. Par exemple, des attaques de type "IP spoofing" (usurpation d'adresse IP) ou "Land Attack" (trame IP avec même source et destinataire), simulant un trafic interne, peuvent déjouer la sécurité des routeurs autorisant uniquement le trafic interne vers une ressource de l'entreprise (élaboration des résultats et statistiques, etc.). Il est donc préférable de faire appel à une (ou plusieurs) infrastructure filtrante plus puissante : le "firewall" (pare-feu). Malheureusement, quelle que soit la solution de filtrage mise en oeuvre, si celle-ci est prise en défaut, un pirate aura accès aux machines internes de notre activité électronique!

## DMZ

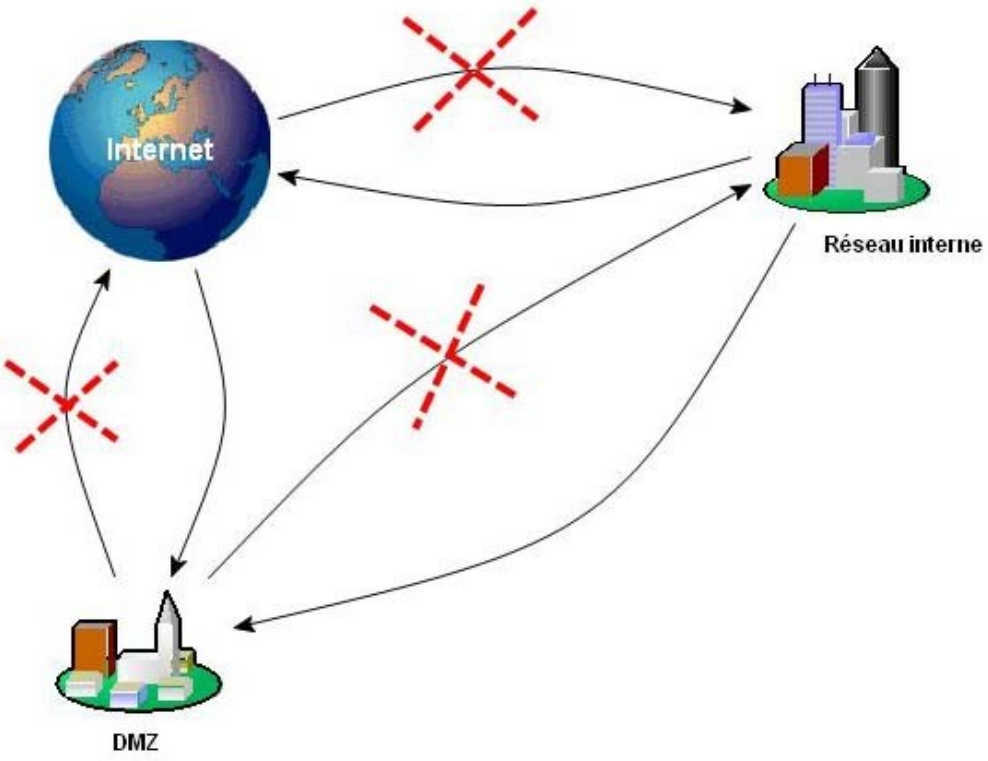
Il est nécessaire de choisir une topologie de réseau qui se prête à la sécurité et d'appliquer des principes d'isolation. En séparant le réseau en sous-réseaux, on pourra mieux gérer chacune des plates-formes indépendamment. Il est donc nécessaire de créer un nouvel espace distinct du réseau public et du réseau interne, afin de ne pas mettre en péril la sécurité et de garantir la confidentialité des données.

Le schéma générale qui précède montre une découpage pour une configuration de base : un premier réseau comporte l'ensemble des machines de la FDJeux qui n'ont aucun service à fournir à l'extérieur, un deuxième réseau (la zone "démilitarisée", ou DMZ) regroupe les machines qui fournissent un service vis-à-vis de l'extérieur (Serveur Web, Applications et Interfaces spécialisées pour les terminaux, ...).

Les serveurs situés dans la DMZ seront renforcés en termes de sécurité : des authentifications et une gestions des droits plus forte, des mécanismes de surveillance comme les sondes d'intrusion, des fausses failles ("pots de miel") pour faire perdre leur temps aux pirates / hackers, etc.

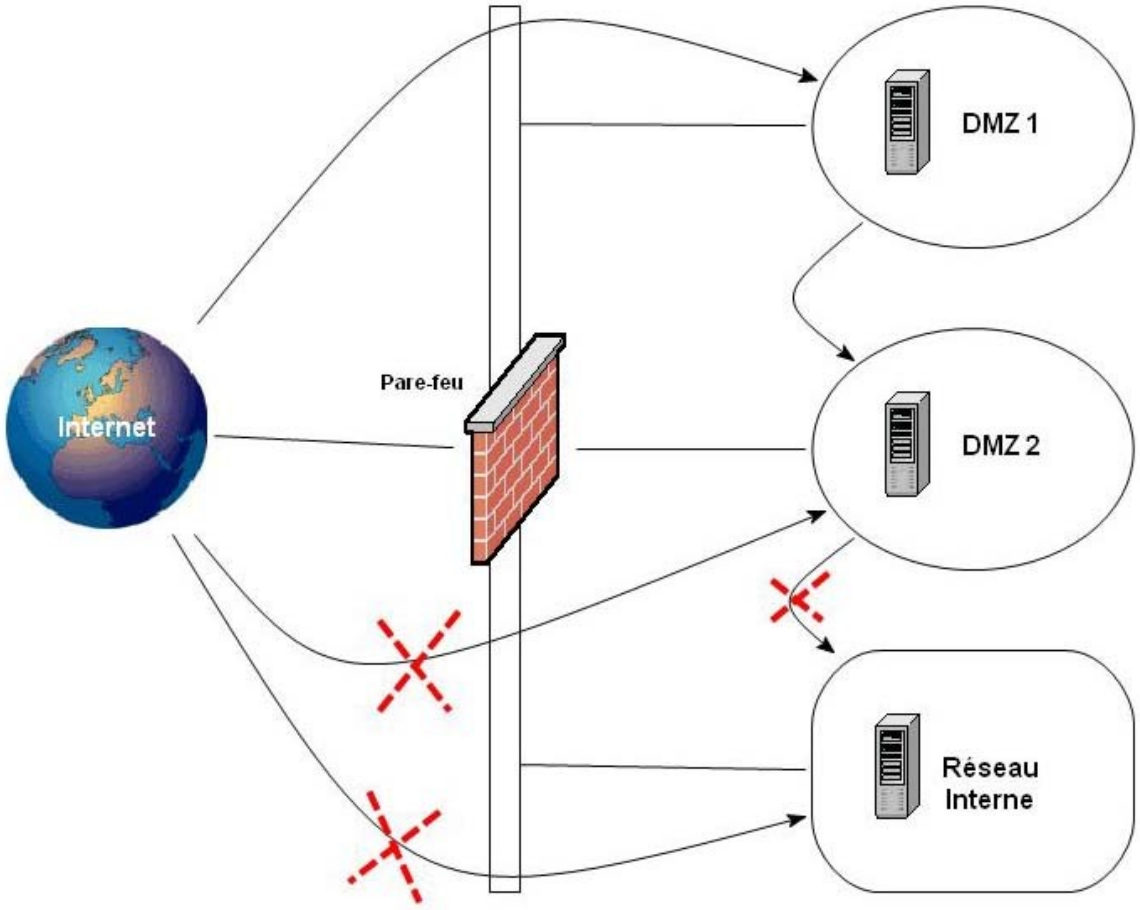
Si un serveur de la DMZ (appelé aussi "bastion") tombe et que le pirate "écoute" le réseau, il ne pourra récupérer rien de confidentiel. Cette DMZ se construit autour d'une ou plusieurs infrastructures filtrantes (comme représenté dans le schéma précédent) qui possèdent au moins deux interfaces réseau.

La politique généralement adopté entre Internet, le réseau interne et la seule DMZ est la suivante :




Les DMZ et les solutions filtrantes offrent un mécanisme de protection du réseau interne vis-à-vis des menaces externes tout en offrant des services à l'extérieur. Ainsi, toutes les DMZ ne sont pas forcément "visibles" du monde public. On peut retrouver des DMZ frontales avec des serveurs publics (surtout le serveur Web dans notre cas), des DMZ invisibles de l'extérieur avec des serveurs protégés (surtout le serveur BD dans notre cas).

Nous avons partant préféré pour notre FDJeux une architecture à deux DMZ, dont la politique correspondante est représentée par le schéma qui suit :




Cette configuration nous semblait pertinente car elle permet de s'affranchir de la problématique d'ouverture du réseau interne en créant une seconde DMZ pour les serveur d'applications et les serveur de bases de données. Ce deuxième réseau permet de sécuriser de manière assez autonome ces serveurs vis-à-vis de la première DMZ publique et du réseau interne.

Nous avons choisi cette solution, malgré son coût élevé (ayant en tête qu'une entreprise comme la FDJeux a un colossal chiffre d'affaires) , car on y retrouve un "traçablilité" des échanges vis-à-vis de la base de donnée, une segmentation des réseaux en fonction de leur niveau de sécurité, sans laisser de portes ouvertes sur le réseau interne de l'entreprise.

## Le VPN

Une solution de PKI ("Public Key Infrastructure") assure la confidentialité et l'intégrité des données, ainsi que l'authentification. Elle permet d'assurer (plus ou moins!) qu'une information n'est pas lisible ni identifiable pendant son transport.

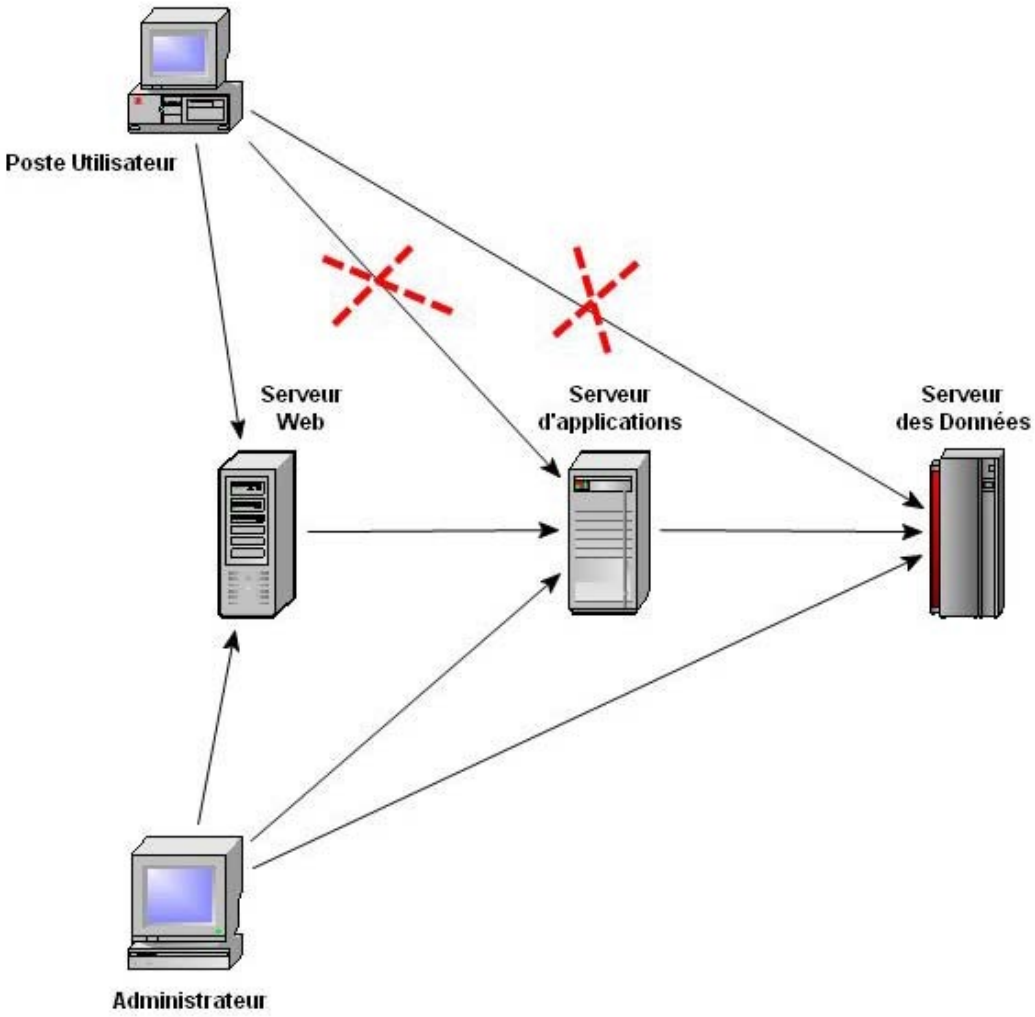
Les techniques de chiffrement des données sont souvent utilisées pour les données stockées. Nous avons prévu impérativement d'exploiter un chiffrement des échanges (aussi) pour notre FDJeux. Une telle technique est aussi mise en oeuvre pour les réseaux privés virtuels ou VPN.

Puisque toutes les transactions (et les mises-à-jour) des terminaux se font au travers du Web, nous avons prévu de "ressembler" ces terminaux dans un VPN émulant une liaison sécurisée entre les premiers et le siège, via un réseau non sécurisé tel que Internet. Au sein d'un tunnel VPN, les données sont cryptées pendant la transmission. Ce VPN ne doit absolument pas être interprété comme un contournement des systèmes de sécurité et de filtrage décrits précédemment (qui sont donc toujours utilisés!).

## Les différents serveurs

L'architecture Web de notre entreprise est composée au minimum de trois éléments : le serveur Web (plus couramment appelé serveur http), le serveur d'application et le serveur de base de données dans lequel on stocke tous les paris. Il est donc logique que chacun de ces éléments ce verra attribuer un niveau différent de sécurité. Le serveur Web de notre entreprise se verra oblige d'être accessible par tous les utilisateurs. En revanche, les internautes ainsi que les intranautes n'aurons pas l'accès au code de l'application ou à l'application à proprement parler, tout comme il n'est pas utile qu'ils puissent interroger la base de données en direct, car la base de donnée au siège ne sera accessible que par les administrateurs !

Le serveur d'application doit donc être accessible seulement par le serveur Web et le serveur de données par le serveur d'application. Ce seront donc que les administrateurs de notre entreprise qui auront le droit d'accéder aux machines de production (on veut dire par la les Serveur d'application, données et Web). Les équipes de développement se situant en province doivent uniquement interagir avec les serveurs de développement, permettant ainsi la programmation de différentes mises à jour des terminaux (voir schémas à la page suivante).




*Interaction administrateur-serveurs*

Connaissant ces règles il nous est donc possible d'adopter une politique de sécurité du réseau par la mise en place d'un firewall dont nous avons expliqué l'utilité et le mode de fonctionnement auparavant, ainsi que de zones démilitarisées.

## BIBLIOGRAPHIE

**"Sécurité des Réseaux"**, Merike Kaeo, Cisco Press, 2000

**"Sécurisez vos applications Internet"**, Christope Camborde, Dunod, 2004

**"Optimiser et sécuriser son trafic IP"**, Francis Ia & Olivier Ménager, Eyrolles, 2004

**"Les VPN"**, Rafael Corvalan & Ernesto Corvalan & Yoann Le Corvic, Dunod, 2003

La totalité des schémas ont été fait par nous en utilisant le logiciel gratuit **"Diagram Studio"**.

Merci à Madame L. Pierre et Monsieur J. P. Lips pour la gentillesse de nous avoir prêté des ressources.