

[Concevoir une infrastructure de sécurité]

*Comment ouvrir son système d'information
en toute sécurité ?*

<http://securit.free.fr>

Sommaire

- **Comment ouvrir son système d'information vers l'extérieur ?**
- **Solution :**
 - Concevoir une infrastructure de sécurité logique.
 - Concepts associés.
- **Cas d'école**

[Concevoir une infrastructure de sécurité]

2

Problématique

Comment ouvrir son système d'information en toute sécurité ?



[Concevoir une infrastructure de sécurité]

3

Problématique

■ Contexte général

- L'ouverture des systèmes d'information vers l'extérieur devient incontournable :
 - Fourniture de service
 - Aux partenaires
 - Aux fournisseurs
 - Aux clients
 - Aux employés (utilisateurs internes dispersés, utilisateurs nomades et télé-travailleurs...)
 - ↳ Les limites de l'entreprise ne sont plus strictement identifiables et étanches
 - Time to market
 - Obligation de réactivité face aux contraintes du marché
 - Présence sur le média Internet indispensable
- Exigences fortes
 - Sécurité
 - Qualité de service
 - Intégration et évolutivité

[Concevoir une infrastructure de sécurité]

4

Problématique

■ Complexité des systèmes d'information

- Environnements hétérogènes
 - Ressources du système d'information (applications, données) sur des systèmes hétérogènes :
 - Grands systèmes (OS/390, AS/400, Tandem, GCOS...)
 - Unix (Solaris, HP-UX, AIX...)
 - Windows NT
 - Technologies hétérogènes (applications métier, applications de communication, applications de gestion...) :
 - Technologie *legacy* (ex. : émulation de terminal)
 - Technologie client/serveur
 - Technologie Inet (accès en mode Web aux applications Intranet/Extranet/Internet)
- Chaque application gère souvent son propre contexte
 - Mécanismes et bases d'utilisateurs spécifiques
 - Services de sécurité propres (authentification, habilitation, confidentialité...)
 - Sensibilité inégale des informations traitées

[Concevoir une infrastructure de sécurité]

5

Problématique

- Multiplication des contextes applicatifs
 - Gestion complexe de plusieurs bases d'utilisateurs
 - Difficulté d'administration et d'exploitation
 - Contrôle interne difficile à réaliser (suivi de la sécurité)
 - Multiplicité de procédures de connexion pour les utilisateurs et clients des différents services offerts
- **La sécurité : un élément essentiel**
 - Risques majeurs des systèmes ouverts (ex. : Internet)
 - Intrusion, rebond au sein du système d'information
 - Perte d'intégrité, de confidentialité, de disponibilité du patrimoine de l'entreprise (applications, données)
 - Risque financier (ex. : indisponibilité d'un service stratégique)
 - Risque juridique (ex. : fuite d'informations sensibles et personnelles, absence de preuves)
 - Risque d'image (ex. : détournement du service offert dans un but malveillant)
 - La sécurité est souvent mal maîtrisée, voire négligée et coûte cher !

[Concevoir une infrastructure de sécurité]

6

Solution

Concevoir une infrastructure de sécurité logique transversale !



[Concevoir une infrastructure de sécurité]

7

Infrastructure de sécurité logique

■ Principes essentiels

- La sécurité est structurante dans les stratégies d'ouverture vers l'extérieur.
- Une solution de sécurité mal conçue et mal pensée
 - Coûte cher,
 - Est inefficace,
 - Est souvent remise en cause ou difficilement intégrable !

■ Objectifs d'une infrastructure de sécurité transversale

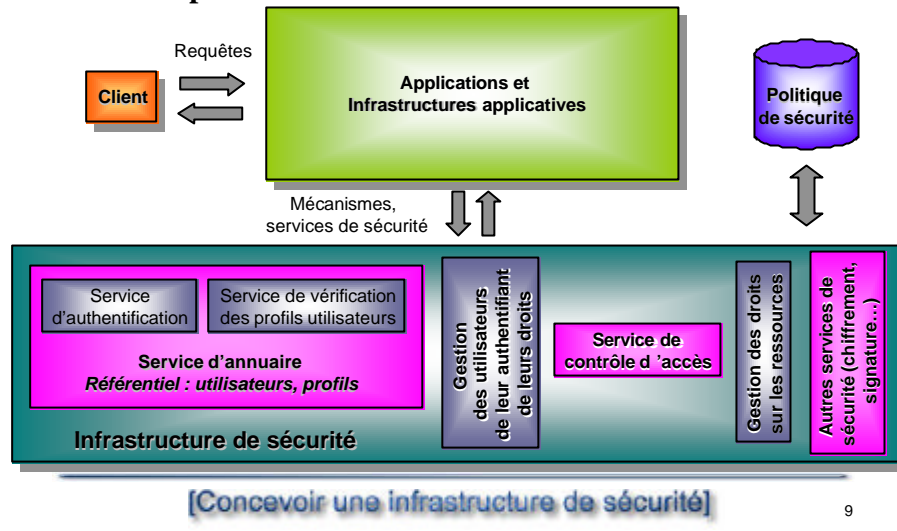
- Séparer totalement la sécurité, au sens large, de la logique applicative.
- Concevoir et mettre en place une solution de sécurité :
 - Globale et indépendante
 - Robuste, éprouvée, performante
 - Distribuée, modulaire, extensible
 - Évolutive, pérenne
 - Ouverte et normalisée

[Concevoir une infrastructure de sécurité]

8

Infrastructure de sécurité logique

■ Description fonctionnelle d'une infrastructure de sécurité



Infrastructure de sécurité logique

■ Éléments de qualification d'une infrastructure

- Couverture fonctionnelle : services de sécurité fournis
 - Identification, authentification (éventuellement *Single Sign On*)
 - Autorisation, habilitation
 - Contrôle d'accès
 - Disponibilité
 - Confidentialité
 - Intégrité
 - Preuve, non-répudiation
 - Contrôle, audit, traçabilité
- Qualité de la solution d'ensemble
 - « Administrabilité », exploitabilité
 - Intégration au sein du système d'information :
 - Au niveau de la sécurité existante (ex. : prise en compte de la sécurité RACF sur OS/390)
 - Avec les outils de supervision (ex. : HP-OV, Tivoli...)
 - Prise en compte des compétences disponibles

[Concevoir une infrastructure de sécurité]

10

Infrastructure de sécurité logique

■ Gains

- Pour l'entreprise
 - Meilleure protection de l'information
 - Rapidité et efficacité des échanges d'information sur tout type de réseau
 - Possibilité à termes de choisir des applications, produits et architectures uniquement sur leurs fonctionnalités, ergonomie et performances (critères intrinsèques) et non sur des aspects liés à la sécurité.
- Pour les administrateurs
 - Centralisation de la base de compte et de la stratégie de sécurité
 - Politique de sécurité évolutive, définie globalement, appliquée localement sur toute l'infrastructure
 - Contrôle et suivi de la sécurité plus efficaces, optimisés (moyens de contrôle interne, d'audit)
- Pour les développeurs
 - Logique applicative dissociée de la sécurité : gain de temps en développement de composants et paramétrage de ressources
 - Capitalisation sur l'utilisation des services de sécurité (interfaces de sécurité stables, uniques et maîtrisées)

[Concevoir une infrastructure de sécurité]

11

Infrastructure de sécurité logique

■ Démarche de conception d'une infrastructure de sécurité

- Processus classique
 - Identification des besoins et objectifs de sécurité
 - Définition des contours fonctionnels de l'infrastructure de sécurité
 - Études techniques
 - Architecture générale de la solution cible
 - Mise en œuvre
 - Maquette/prototype
 - Spécifications détaillées
 - Industrialisation
 - Pilote et mise en production
 - Suivi
- En parallèle, une réflexion essentielle doit porter sur
 - La mise en place d'une organisation adaptée
 - La définition de la politique de sécurité

[Concevoir une infrastructure de sécurité]

12

Cas d'école

Exemple de conception d'une infrastructure de sécurité

[Concevoir une infrastructure de sécurité]

13

Cas d'école - Problème

■ Énoncé du problème

- La banque B souhaite fournir à une partie de ses clients, les particuliers, l'ensemble de ses services via Internet en mode HTTP (consultation, gestion de comptes, trading au travers d'un navigateur...) et devenir une référence dans le monde des banques en lignes.
- La banque B souhaite également optimiser ses échanges d'informations bancaires avec ses partenaires, d'autres banques et établissements de crédits, en proposant un moyen de transfert d'informations formatées.

[Concevoir une infrastructure de sécurité]

14

Cas d'école - Problème

■ Données du problème

- L'ensemble des informations bancaires des clients de la banque B est, pour des raisons historiques, stocké en environnement grand système OS/390 sur un réseau SNA.
- De nombreux composants développés en COBOL assurent le traitement et la présentation de ces informations.
- Une partie des informations bancaires traitées par la banque B est extraite puis stockée en environnement Unix/IP, avec une base de données Oracle. Ces informations doivent être proposées aux clients de la banque, en consultation.
- Les échanges entre la banque B et ses partenaires (autres banques et établissements de crédit) se font par transferts de fichiers.
- La banque B privilégie deux éléments essentiels
 - La sécurité
 - La qualité de service

[Concevoir une infrastructure de sécurité]

15

Cas d'école - Solution

■ Objectifs de sécurité

- Protection du système d'information de la banque B vis-à-vis des risques liés à l'ouverture sur Internet
- Fourniture des services de sécurité aux clients :
 - Authentification forte
 - Habilitation
 - Contrôle d'accès
 - Confidentialité
 - Intégrité des flux échangés sur le réseau public
 - Preuve (transactions non répudiables)
- Modularité des services de sécurité
- Garantie de disponibilité des services offerts aux utilisateurs

[Concevoir une infrastructure de sécurité]

16

Cas d'école - Solution

■ Éléments au cœur de l'infrastructure de sécurité

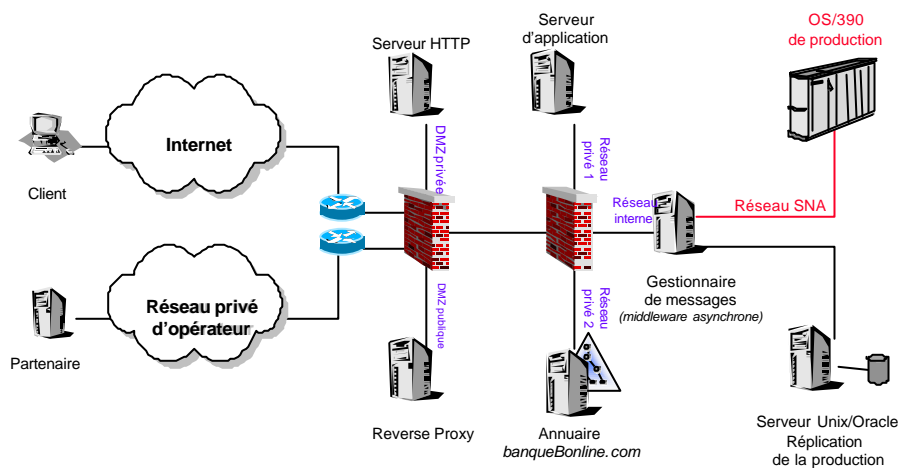
- Méta-annuaire
- Serveur d'application : architecture n-tiers
 - Tiers présentation : serveur Web
 - Tiers application : serveur d'application, gestionnaire de messages
 - Tiers données : bases de données et grands systèmes
- Logiciel de contrôle d'accès pour les applications Web
- *Optionnellement* : infrastructure de gestion de clés

[Concevoir une infrastructure de sécurité]

17

Cas d'école - Solution

■ Architecture cible



[Concevoir une infrastructure de sécurité]

18

Cas d'école - Solution

■ Lignes directrices dans le design de l'architecture

- Accès au service
 - Via Internet pour les clients (particuliers)
 - Via Internet ou un réseau privé d'opérateur assurant la qualité de service au niveau réseau et, optionnellement la sécurité (VPN), pour les partenaires à fortes exigences
- Distribution des éléments de l'infrastructure de sécurité
 - Une cascade de firewalls constitue l'épine dorsale de l'architecture réseau
 - Plusieurs sous-réseaux hébergent les différents composants de l'infrastructure :
 - [DMZ publique](#) : seul réseau accédé directement depuis l'extérieur, il regroupe les machines « publiques ».
 - [DMZ privée](#) : non directement visible de l'extérieur, ce réseau regroupe les serveurs Web.
 - [Réseau privé 1](#) : ce réseau héberge l'ensemble des serveurs d'application.
 - [Réseau privé 2](#) : ce réseau, sensible, héberge le service d'annuaire.
 - [Réseau interne](#) : réseau le plus sensible et le plus sécurisé, il héberge les données et est interconnecté avec le réseau privé de la banque B.
 - Objectifs : modularité, évolutivité, séparation élémentaire des services par zone

[Concevoir une infrastructure de sécurité]

19

Cas d'école - Solution

- Principes de sécurité mis en œuvre
 - Architecture dédiée, isolée logiquement du système d'information (principe d'étanchéité)
 - Pas d'accès direct en IP aux données de production :
 - Rupture de protocole IP/SNA pour accéder aux transactions sur OS/390
 - Accès IP à une base Oracle, réplique des données de production en consultation seule
 - Utilisation de plusieurs technologies différentes pour la réalisation des barrières de sécurité
 - Principe d'écluse
 - Les flux ne peuvent circuler qu'entre zones adjacentes (connexions de proche en proche)
 - Corollaire
 - Aucune machine ne doit être à la fois visible des réseaux sécurisés (regroupant les 2 réseaux privés et le réseau interne) et de l'Internet
 - Contrôle des flux :
 - Seuls les flux strictement nécessaires, identifiés strictement, doivent être véhiculés au sein de l'infrastructure
 - Nature des flux : mise en œuvre de flux contrôlables, à faibles risques de sécurité

[Concevoir une infrastructure de sécurité]

20

Cas d'école - Solution

■ Rôles des éléments de l'architecture

➤ Firewalls

- Une cascade de deux firewalls de technologies différentes est mise en œuvre.
- Firewall Internet : firewall à relais applicatifs
 - Contrôle les accès en provenance de l'Internet (ports, destinations)
 - Délimite les zones démilitarisées
 - Relaye et inspecte le contenu des flux autorisés à pénétrer la zone démilitarisée publique (contrôle le caractère inoffensif)
- Firewall Internet : firewall à filtre de paquets
 - Assure l'étanchéité du réseau sécurisé vis-à-vis de l'extérieur
 - Contrôle strictement le type de flux IP véhiculé vers le réseau sécurisé : identification des interlocuteurs, restriction des communications
 - Gère les accès en administration et exploitation de la plate-forme

➤ Reverse proxy

- Assure les fonctions essentielles d'authentification et de contrôle d'accès (mise en œuvre de listes de contrôle d'accès, ACL, sur les ressources et objets)
- Masque la structure de l'architecture et plus particulièrement le serveur Web
- Seule machine directement jointe depuis l'Internet, de manière transparente
- Garantit l'accès au serveur Web en provoquant une rupture de session

[Concevoir une infrastructure de sécurité]

21

Cas d'école - Solution

➤ Serveur HTTP

- Ne contient que quelques pages statiques (ex. page d'entrée d'un portail)
- Repose sur les services assurés par le reverse proxy

➤ Serveur d'applications

- Accessible aux travers des firewalls uniquement par le serveur Web
- Prend en charge et traite les requêtes utilisateurs
- Met en forme les informations pour délivrer la réponse au serveur Web

➤ Annuaire

- Contient les informations de sécurité et les règles de la politique de sécurité (contrôle d'accès aux ressources et objets). Il est donc extrêmement sensible.

➤ Middleware asynchrone

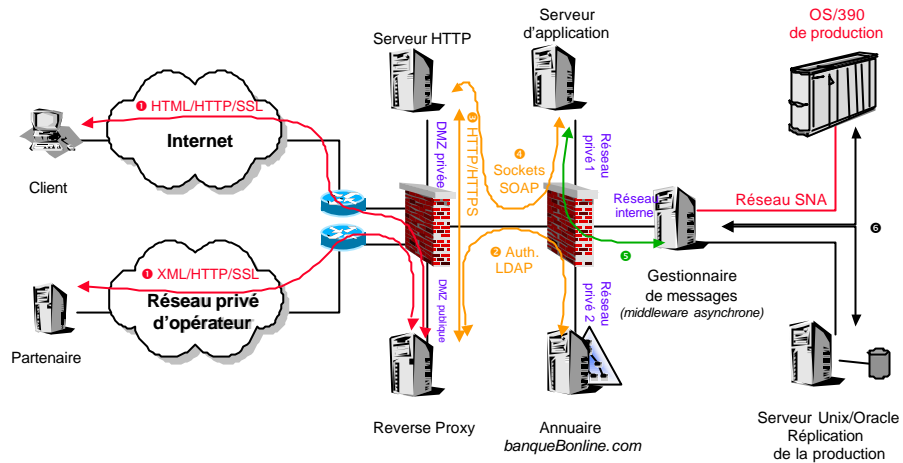
- Assure une rupture de protocoles : IP/SNA (niveau 3) ou niveau 7 pour les serveurs accédés directement en IP (données répliquées)
- Deuxième niveau de serveur d'application
- Rôle transactionnel : il intègre l'existant applicatif et la logique métier
- Accueille les connecteurs et le middleware pour l'accès aux données
- Constitue un bus fédérateur de messages asynchrones offrant un accès unifié au système d'information (OS/390, Unix...)

[Concevoir une infrastructure de sécurité]

22

Cas d'école - Solution

■ Cinématique des flux



[Concevoir une infrastructure de sécurité]

23

Cas d'école - Solution

■ Sécurité avancée

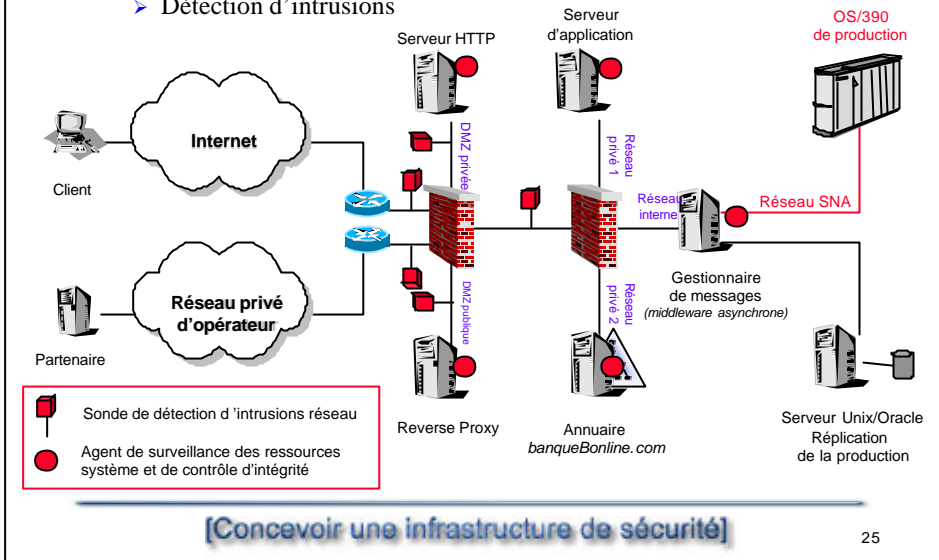
- Mise en œuvre du protocole SSL version 3 assurant
 - L'authentification mutuelle des correspondants (client et serveur) dans le cas de la mise en œuvre d'une IGC
 - La protection en intégrité des flux de données véhiculés
 - La protection en confidentialité des flux de données (chiffrement par algorithme à clé secrète)
 - Niveau de sécurité par ordre décroissant (*source* : Netscape)
 - Triple DES 168 bits et SHA-1 (autorisation SSSI nécessaire)
 - RC4 128 bits et MD5
 - RC2 128 bits et MD5
 - DES 56 bits et SHA-1
 - RC4 40 bits et MD5
 - RC2 40 bits et MD5
 - Pas de chiffrement, uniquement MD5

[Concevoir une infrastructure de sécurité]

24

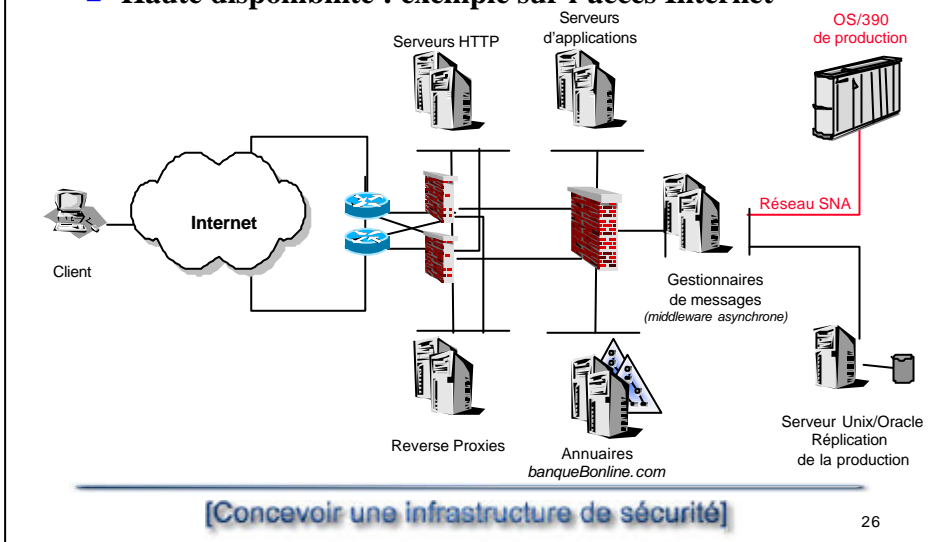
Cas d'école - Solution

➤ Détection d'intrusions



Cas d'école - Solution

■ Haute disponibilité : exemple sur l'accès Internet



Cas d'école - Solution

■ Administration

- Centralisée, depuis une plate-forme dédiée sur le réseau interne sécurisé
- Pour les serveurs en DMZ : plusieurs orientations
 - En local sur les serveurs en DMZ
 - Via une liaison série sur chacun des serveurs
 - Par un tunnel (ex. SSH, IPSec) depuis le réseau interne sécurisé
- Flux d'administration
 - Authentification forte des administrateurs (par carte à puce)
 - Flux sécurisés pour l'administration

■ Exploitation

- Remontée d'alertes via des protocoles sécurisés (ex. SNMP v2)
- Traitement centralisé des événements :
 - Centralisation et corrélation des logs et journaux d'évènements

[Concevoir une infrastructure de sécurité]

27

Cas d'école - Solution

■ Annuaire

- Élément essentiel de l'infrastructure de sécurité
- Stocke les informations de sécurité
 - Gestion des utilisateurs et des groupes d'appartenance
 - Gestion des authentifications (mot de passe, certificat) et des droits d'accès aux différentes ressources
- Exigences techniques
 - Utilisation du standard LDAP v.3
 - Disponibilité et sécurité élevée du service LDAP
 - Robustesse et performance du service d'annuaire pour supporter :
 - Un grand nombre d'utilisateurs
 - Le traitement des requêtes LDAP d'authentification et d'autorisation
- Schéma de l'annuaire
 - Domaine *banqueOnline.com* indépendant
 - Sous-domaine du domaine général *banqueB.com* administré par l'entreprise
 - Des échanges entre employés et clients de la banque B peuvent alors avoir lieu

[Concevoir une infrastructure de sécurité]

28

Cas d'école - Solution

■ Intégration d'une infrastructure à gestion de clés

- Les orientations prises dans l'élaboration de l'infrastructure permettent l'ouverture vers une IGC
 - SSL v3 permet l'échange des certificats
 - L'annuaire LDAP stocke les certificats et les listes de révocation des utilisateurs, et fournit un service de vérification
- Services de sécurité apportés par une IGC
 - Authentification du client par certificat (et non login/mot de passe sans IGC)
 - Service de signature (preuve, non-répudiation)
 - ↳ Usage adapté de la [carte à puce](#)
- Différents scénarios
 - Enregistrement des utilisateurs en ligne : autorité d'enregistrement (RA) accessible depuis Internet
 - Enregistrement des utilisateurs par les métiers de la banque B : RA hébergée au sein du système d'information
- Schéma de certification
 - Ex. : autorité de certification (CA) de *banqueOnline.com* dérivée de la CA principale de *banqueBcom*, isolée (modèle hiérarchique)
 - Intégration au sein d'une organisation d'IGC, Identrus, GTA (modèle croisé)

[Concevoir une infrastructure de sécurité]

29

Cas d'école - Conclusion

■ Confrontation de la solution aux besoins

- Niveau de sécurité global élevé
- Déportation et indépendance des services de sécurité vis-à-vis des applications
- Couverture complète des besoins de sécurité
- Accès à des environnements multiples par l'intermédiaire d'un middleware asynchrone
- L'architecture distribuée est reproductible en interne :
 - Interconnexion possible entre l'annuaire d'entreprise et l'annuaire des clients/partenaires
 - Le serveur d'application peut être déployé en interne pour gérer les développements applicatifs et les accès aux données, de manière homogène. Les composants sont alors identiques et ré-utilisables.
 - Si l'entreprise a déployé en interne sa propre IGC, celle-ci peut être interconnectée avec une IGC dédiée aux clients et partenaires.
- Extension de l'architecture vers d'autres services : ex. messagerie

[Concevoir une infrastructure de sécurité]

30

Conclusions

[Concevoir une infrastructure de sécurité]

31

Conclusions

- **Évolution de la sécurité dans les grandes entreprises**
 - Approche globale de la sécurité
 - La sécurité doit intervenir en amont des projets d'infrastructure et de développement.
 - **Les infrastructures de sécurité**
 - Stratégiques car structurantes dans l'évolution des systèmes d'information
 - Nécessitent des compétences et une démarche pointues dans :
 - L'expression du contour de l'infrastructure et des besoins de sécurité
 - Le choix de solution
 - L'intégration au sein du système d'information
 - Des offres matures existent et commencent à être implémentées.
- ☞ **Une infrastructure de sécurité permet d'aborder tous les aspects essentiels des problématiques modernes de sécurité.**

[Concevoir une infrastructure de sécurité]

32

Annexes

[Concevoir une infrastructure de sécurité]

33

Annexe A : solutions techniques

**Présentation des principales solutions du
marché**

(non exhaustif)

[Concevoir une infrastructure de sécurité]

34

Solutions techniques du marché

■ Annuaires

- ActiveDirectory de Microsoft
- Domino v5 Directory de IBM/Lotus
- Global Directory Server de Critical Path
- **Netscape Directory Server de IPlanet**
- Novell Directory Services eDirectory de Novell
- SecureWay Directory de IBM

■ Solutions de contrôle d'accès

- Contrôle d'URI (*Uniform Resource Identifier*) pour les applications Web
 - SiteMinder de Netegrity
 - **Policy Director de IBM**
 - DomainGuard de HP

[Concevoir une infrastructure de sécurité]

35

Solutions techniques du marché

■ Serveurs d'applications

- Inprise Application Server de Inprise
- Internet Application Server de Oracle
- **WebLogic de BEA**
- **WebSphere de IBM**
- **Windows 2000 Distributed Network Architecture de Microsoft**

■ Middlewares asynchrones

- **MQ Series de IBM**
- MSMQ Windows 2000 Advanced Server de Microsoft

■ Éditeurs d'infrastructure à clés publiques

- **Baltimore (UniCert)**
- **CS (WebP@ss et Sm@rtPKI)**
- **Entrust (EntrustPKI)**
- ID2
- Microsoft (PKI Windows 2000)

[Concevoir une infrastructure de sécurité]

36

Solutions techniques du marché

■ Firewalls

- Firewalls à relais applicatifs
 - FWTK sous licence GNU (Opensource)
 - Gauntlet de NAI
 - M>Wall de Matranet
 - NSM de Solsoft
 - **Raptor de Symantec (ex. Axent)**
- Firewalls à filtres de paquets
 - Cisco Secure PIX Firewall de Cisco Systems
 - **Firewall-1 de Checkpoint**
 - Linux IPFilter, Netfilter
 - Lucent Managed Firewall de Avaya (ex. Lucent Technologies)
 - Netwall de Evidian (ex. BullSoft)
 - SunScreen de Sun Microsystems

↳ Privilégier les solutions *appliance* (boîtes noires) avec firewall embarqué sur des systèmes d'exploitation allégés et sécurisés (ex. : IPSO de Nokia, NetScreen, Sonicwall, Firebox II de Watchguard)

[Concevoir une infrastructure de sécurité]

37

Solutions techniques du marché

■ Détection d'intrusions

- Sondes réseau
 - Cisco Secure Intrusion Detection System (ex. Netranger) de Cisco Systems
 - Kane Security Enterprise de Intrusion.com
 - NetProwler de Symantec (ex. Axent)
 - NFR de Network Flight Recorder
 - **RealSecure de Internet Security Systems**
 - SessionWall-3 de Computer Associates
 - Shadow de SANS Institute (Opensource)
 - Snort sous licence GNU (Opensource)
- Agents de surveillance système
 - CyberCop Monitor de Network Associates
 - **Kane Security Enterprise de Intrusion.com**
 - Intruder Alert de Symantec (ex. Axent)
 - RealSecure Agents de Internet Security Systems
 - Tripwire de Tripwire Inc.

[Concevoir une infrastructure de sécurité]

38

Solutions techniques du marché

■ Analyse de logs

- CMDS de **Intrusion.com**
- NetSecureLog de NetSecure Software
- WebTrends de WebTrends Inc.

■ Haute disponibilité, partage de charge

- Commutateur de sessions 5/7
 - **Content Services Switch** de Cisco Systems
 - **ACE Director** de Altéon (Nortel Networks)
 - FireProof de Radware
 - StoneBeat de Stonesoft

Remarque : ne sont pas référencées ici les solutions de cluster (ex. NLBS de Windows 2000)

[Concevoir une infrastructure de sécurité]

39