JSSI 2002 – 09 Avril 2002

CONTRÔLE & AUDIT

La problématique de supervision

Présentée par : L. Delabarre

Les enjeux

- Au moins 60% des entreprises ont subi des infractions en 2000
- En 2003, 50 % des PME subiront une attaque via Internet
- 60 % des cibles ne sauront pas quelles ont été attaquées
- Les systèmes connectés à Internet subissent 17 scans de type netbios par jour

Source : Gartner Group, ***(enquête du Ministère du Commerce et de l'Industrie britannique, le Department of Trade and Industry)***

La solution

POUR CONTRÔLER et AUDITER :

VALORISER LA SUPERVISION

La problématique

Les questions

- Quels outils et services de supervision mettre en place pour atteindre le niveau de sécurité voulu ?
- Comment organiser l'exploitation de ces services pour garantir son efficacité et sa pérennité ?

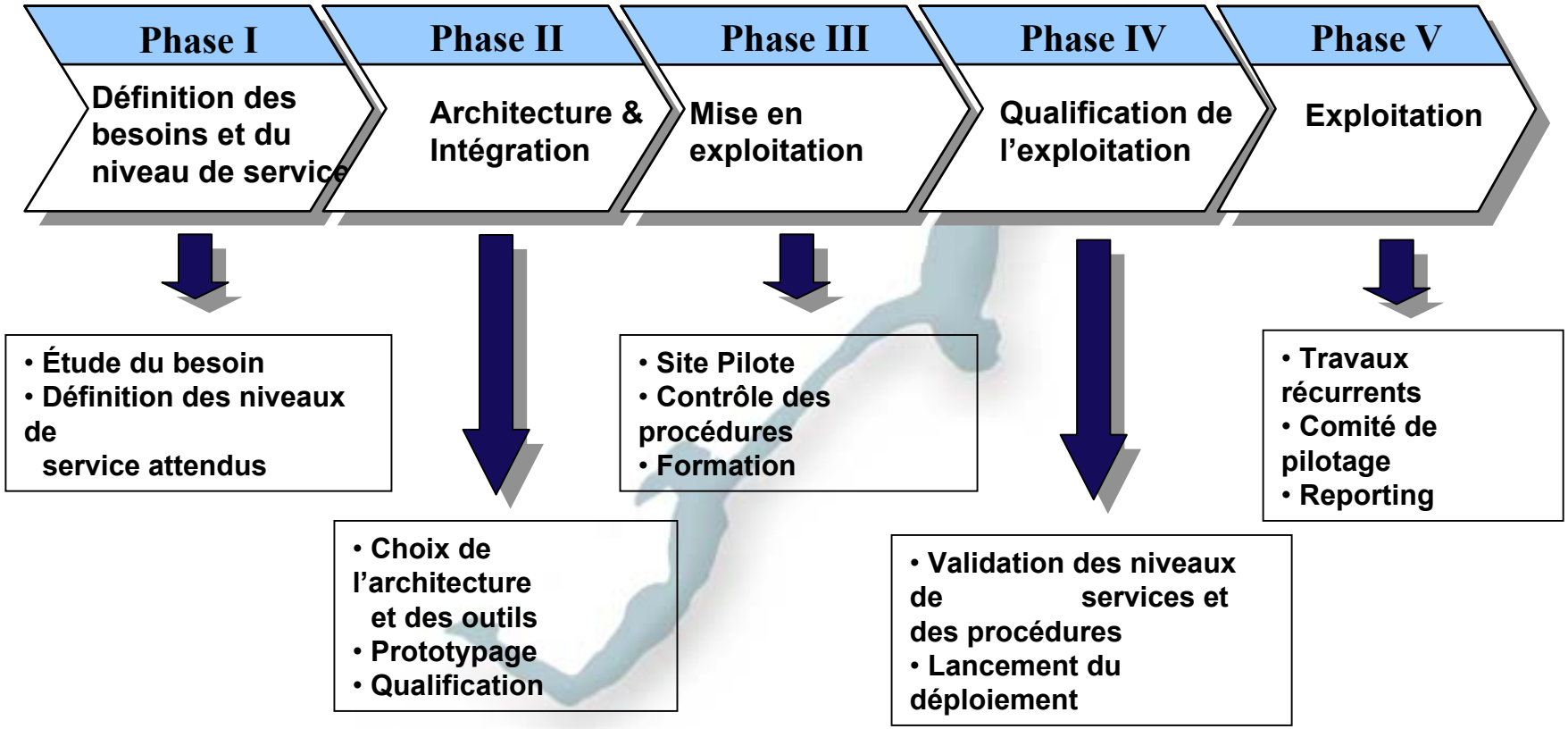
La problématique

- Disposer de ressources dédiées :
  - possédant des compétences pointues
  - disponibles pour réagir immédiatement
- Faire face à la complexité des outils à mettre en place
- Etre capable d'administrer une architecture multi-sites
- Disposer d'une veille technologique ciblée et cohérente
- Absorber des coûts d'exploitation élevés

La démarche de supervision en interne

- Une démarche en mode projet
  - Comité de pilotage
  - Une équipe
  - Un phasage du projet
  - Un budget
- Une activité récurrente
  - Un service dédié
  - Des experts sécurité
  - Une veille technologique
  - Un plan de réponses en cas d'incident

La démarche de supervision en interne



La démarche de supervision en interne

- *Hypothèse :*
  - 1 Firewall administré
  - Site unique
  - Politique de sécurité simple
  - Pas d'acquisition d'outils spécifiques pour l'administration et la supervision du Firewall
  - Veille technologique

La démarche de supervision en interne

Exploitation 5 jours par semaine

Exploitation en 8 x 5	Interne
Formation	10 K€
Outils d'analyse	5 K€
Assistance externe (10j)	10 K€
Total Investissement	**25 K€**
1 Ingénieur	100 K€
Total exploitation 3 ans	**325 K€**

Exploitation 24 x 7 x 365

- **2 ingénieurs + 5 techniciens**
- **Outils spécifiques pour l'administration et la supervision du Firewall**

Exploitation en 3 x 8	Interne
Formation	10 K€
Outils d'analyse	25 K€
Assistance externe (10j)	10 K€
Total Investissement	**45 K€**
2 Ing + 5 Techs	450 K€
Total exploitation 3 ans	**1395 K€**

Les outils

- Outils génériques
  - HP OV
  - Tivoli
  - Patrol
- Outils spécialisés
  - Logiciels de constructeurs
    - Checkpoint provider ONC
  - Outils dédiés à la sécurité
    - ex: Netforensics ; esecurity
- Outils internes
  - Développement spécifique

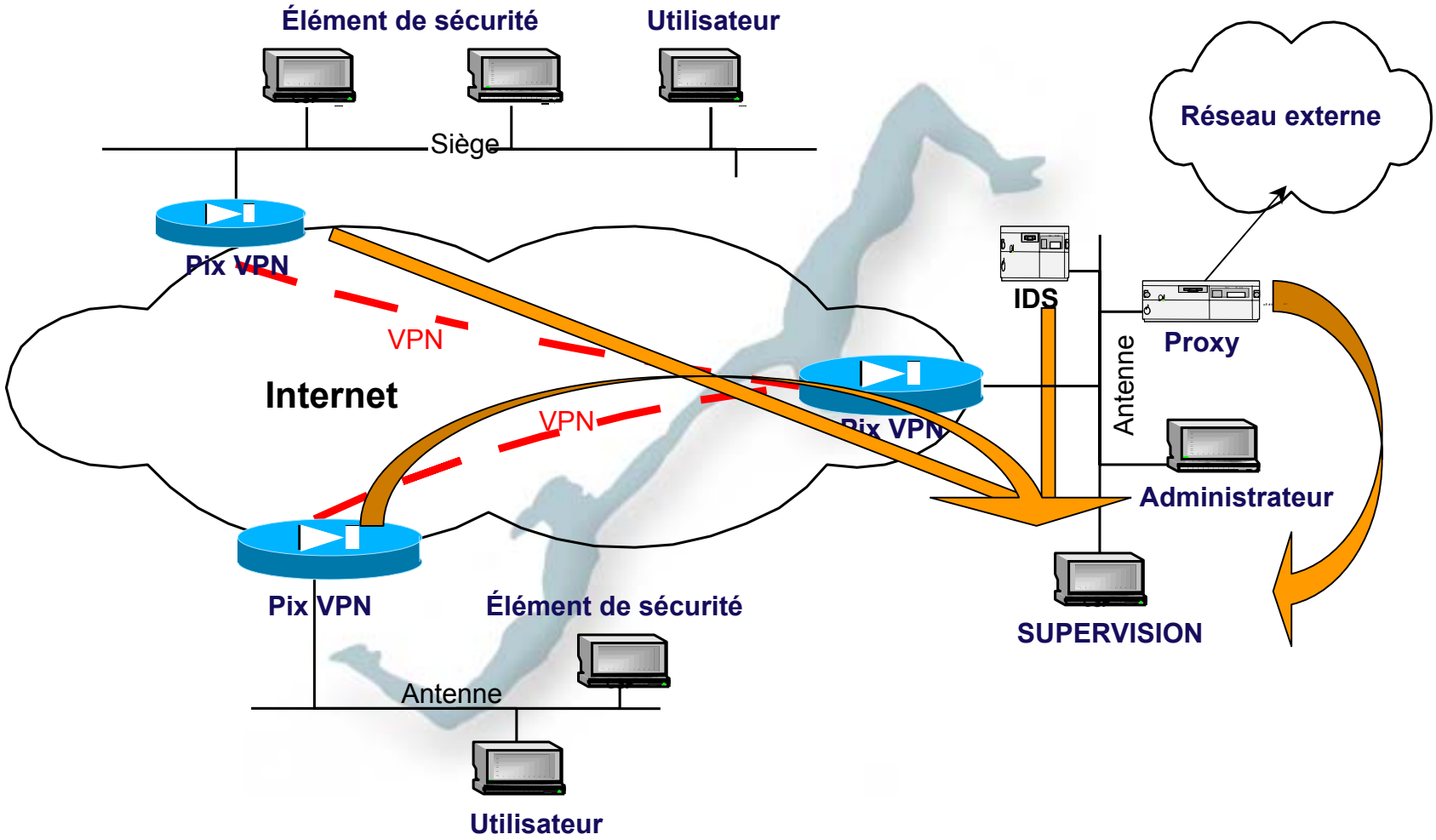
Avantages & inconvénients

- **Outils génériques**
  - (+) **Large possibilités**
  - (−) **La mise au point du produit**
    - modules propriétaires ex: KM patrol
    - Déploiement difficile
- **Outils spécialisés**
  - (+) **Intégration forte du produit aux besoins**
  - (−) **Multiplication des produits**
- **Outils internes**
  - (+) **Se cadre aux besoins spécifiques**
  - (−) **La maintenabilité**

Valoriser les compétences

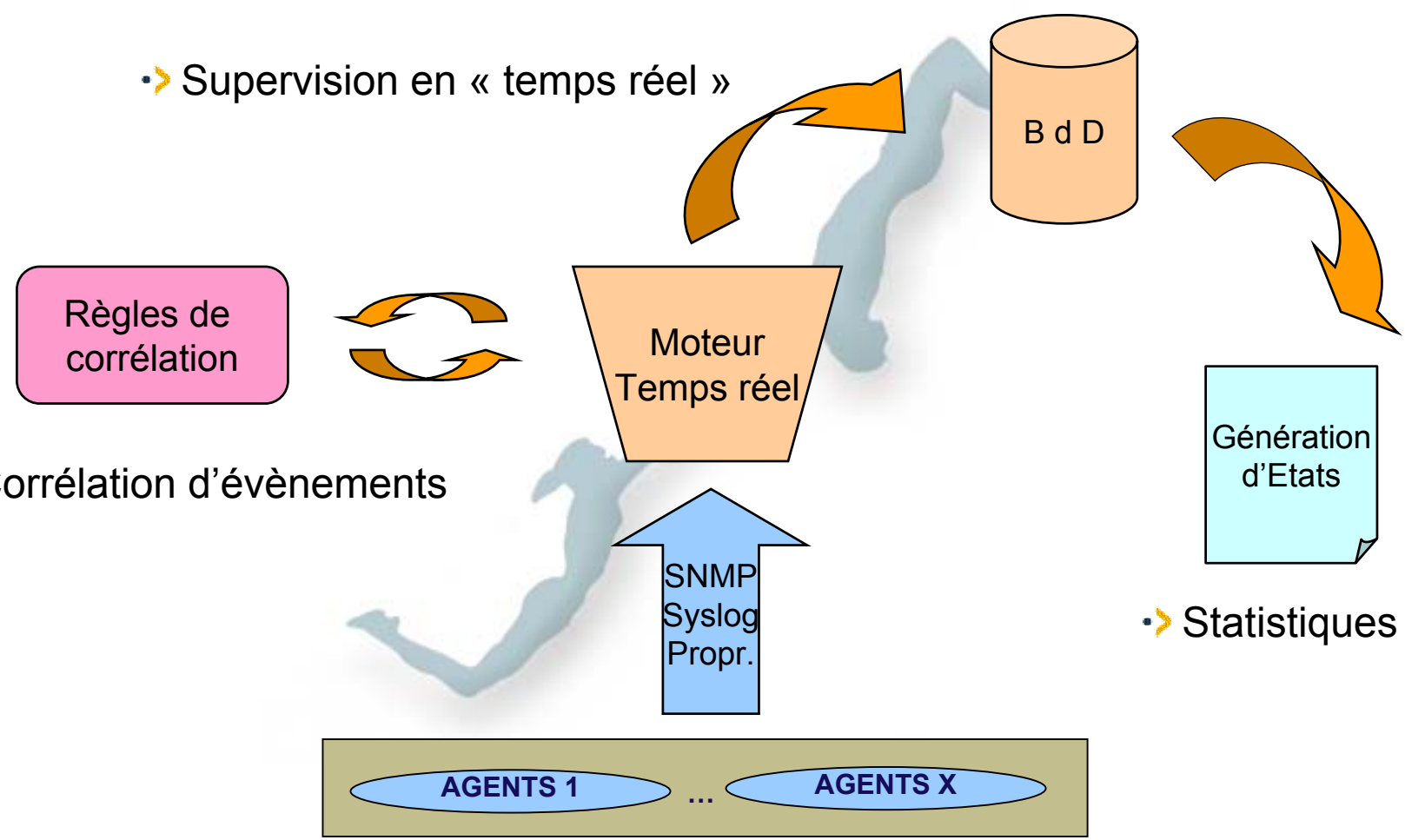
- Les éléments à superviser
- Mise en place d'une architecture de supervision
- Le déploiement de l'architecture
- La pertinence des traces
- La réactivité sur attaque

La supervision multi-sites



Le processus de monitoring

- Historisation
- Supervision en « temps réel »
- Corrélation d'évènements
- Statistiques



L'externalisation de la supervision

Recentrer l'entreprise sur son cœur de métier

- *Pourquoi externaliser ?*
- *Comment externaliser ?*

L'externalisation de la supervision

- Une interface unique vers le client
- HelpDesk accessible 24 / 7
- Comité de Pilotage régulier
- Rapports de supervision accessibles
- Engagement sur des niveaux de service
- Une compétence forte en sécurité
- *Coût*

Télé-administration

Un atout supplémentaire …

Gestion des règles de sécurité

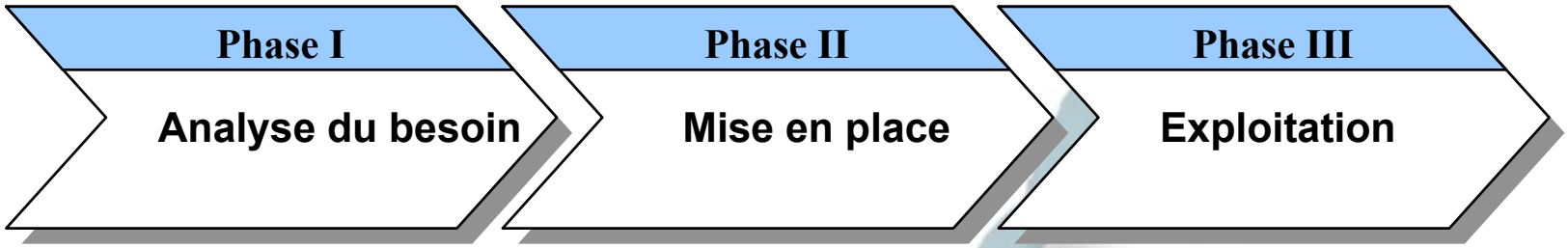
- Ajout, modification, suppression de règles
- Vérification de l'intégrité des règles
- Aide à la définition des règles

Gestion des patches urgents

Relais tiers mainteneur

- Prise de contact avec vos partenaires en cas de Problèmes

L'externalisation : la méthodologie



- Étude du besoin client
- Étude de l'architecture
- Définition des niveaux de service
- Définition des actions sur alarmes
- Définition du Reporting

- Modification du paramétrage
- Rédaction des procédures
- Adaptation des Reports

- Supervision et télé-administration
- Comité de pilotage
  - ✓ Statistiques
  - ✓ Examen des événements majeurs
- Help desk

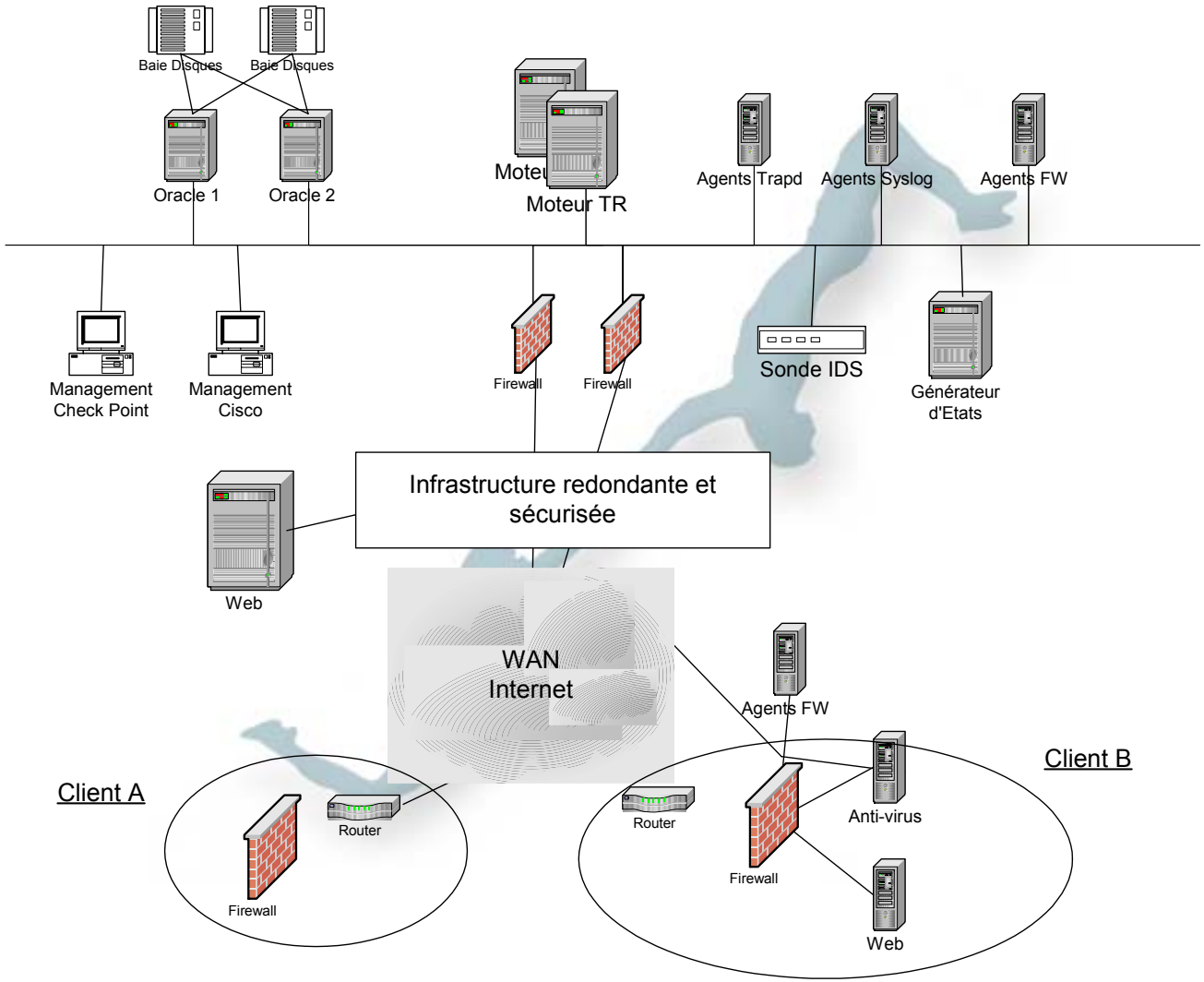
La sécurité de la supervision

- **Problématique :**
  - Besoins d'intégrité de l'information
  - Besoins de confidentialité
  - Besoin de haute disponibilité

- **Méthodes:**
  - Utilisations d'un canal sécurisé
    - Chiffrement
    - Authentification forte
  - Outil de détection d'intrusion
  - Cluster, redondance …

- **Implémentation d'une solution:**

Une architecture de supervision



Conclusion

- la réussite d'une supervision de la sécurité repose sur :
  - Une démarche projet
    - Une définition précise des besoins …
    - Une architecture technique de supervision
    - Des procédures d'escalade
  - Un service 24/7
  - Des compétences d'analyse
  - Une grande réactivité de réponse à
  - Une veille technologique
  - Des règles d'évolutivité