



Gestion d'identité

Les chantiers IAM

Etat des lieux

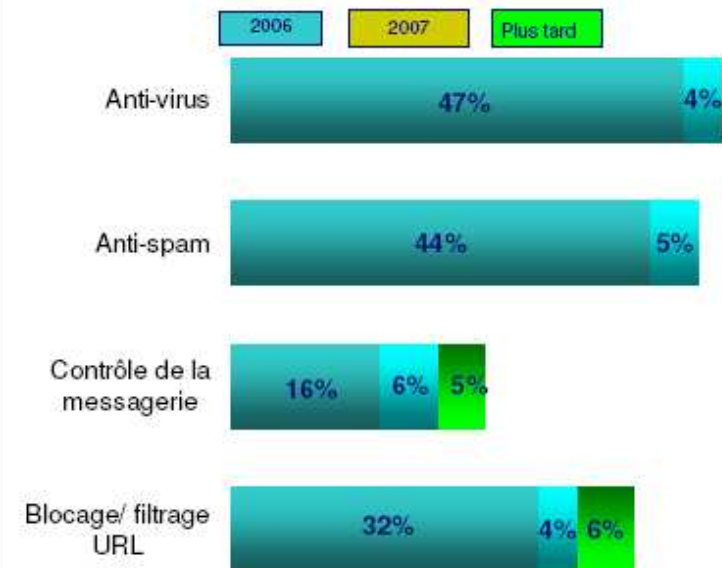
Jean-Louis MARTIN – SSI-Conseil

ENE 13 décembre 2006

Evolution des menaces du malware....



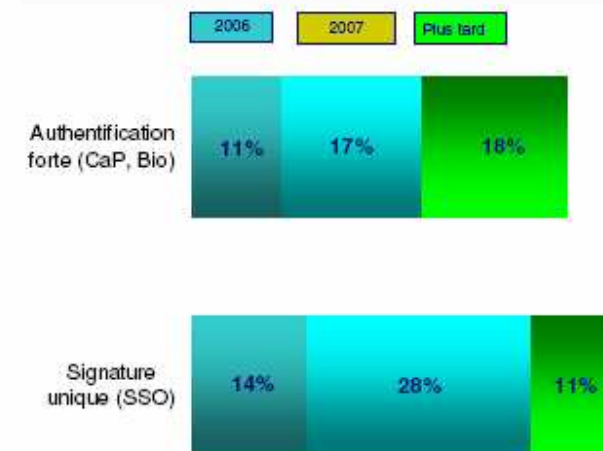
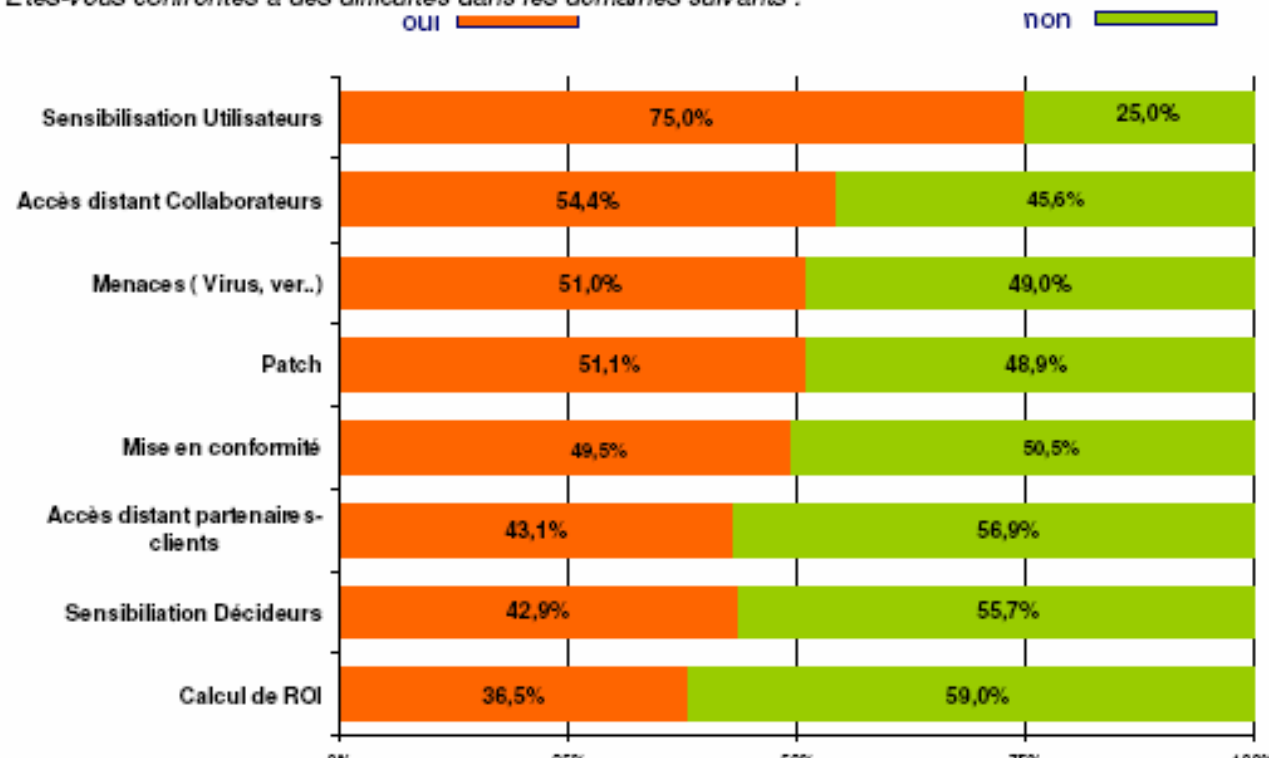
Prévoyez-vous les investissements suivants ?



IDC Etude Etat des lieux marché de la Sécurité - Assises de la Sécurité et des systèmes d'information, Octobre 2006

à l'utilisateur... en 2007... peut-être

Etes-vous confrontés à des difficultés dans les domaines suivants :



IDC Etude Etat des lieux marché de la Sécurité - Assises de la Sécurité et des systèmes d'information, Octobre 2006

Prévoyez-vous des investissements dans les domaines suivants ?

IAM : Demain, c'est loin !

Les chantiers IAM

Etat de lieux :

- Une nécessité : retour sur les enjeux
- Les réponses du marché : limite des solutions techniques
- Caractéristiques des projets IAM
- Retours d'expériences et bonnes pratiques
 - ❖ Stratégie
 - ❖ Tactique
- Nouvelles voies
- Conclusion

Retour sur les Enjeux de la gestion d'identité



Enjeux : Une nécessité *d'Aristote à l'IAM*



Qui ?
Quoi ?
Quand ?
Où ?
Comment ?
Pourquoi ?
Combien ?

Enjeux :

« *nouvelles frontières et patrimoine étendu :
L'entreprise en réseau d'expose.* »

- Les frontières du SI ont éclaté
 - ❖ Personnels et nomades, partenaires, fournisseurs et invités,...etc
 - ❖ Web services et Portails d'accès web aux applications (SOA / OASIS)
 - ❖ Peut concerner des millions d'identifications

Mais ...

- La construction en silo perdure et s'accroît:
 - ❖ Sources de données et d'applications hétérogènes
 - ❖ Annuaires dédiés et incohérents
 - ❖ Contenus incompatibles
- Les anciennes applications (client/serveur d'entreprise, ERP,...etc) doivent être amorties

Enjeux : techniques ou organisationnels ?

Les frontières de l'entreprise éclatent

- Complexité des entreprises (Groupes, filiales, fusions, acquisitions, partenariats, sous-traitants, ...etc)
- Complexité des organisations (ex: 5000 profils pour 8000 collaborateurs chez Natexis, ramenés à 500 après implication des responsables métiers)
- Complexité des rôles: plusieurs casquettes pour un même individu => impact sur les contrôles basés sur les rôles
- Agilité et réorganisations fréquentes
- Pression réglementaire (Conformité LSF, SOX, Sectorielle)
 - ❖ Qui a fait quoi, quand, avec quel niveau d'habilitation, et quel contrôle ?

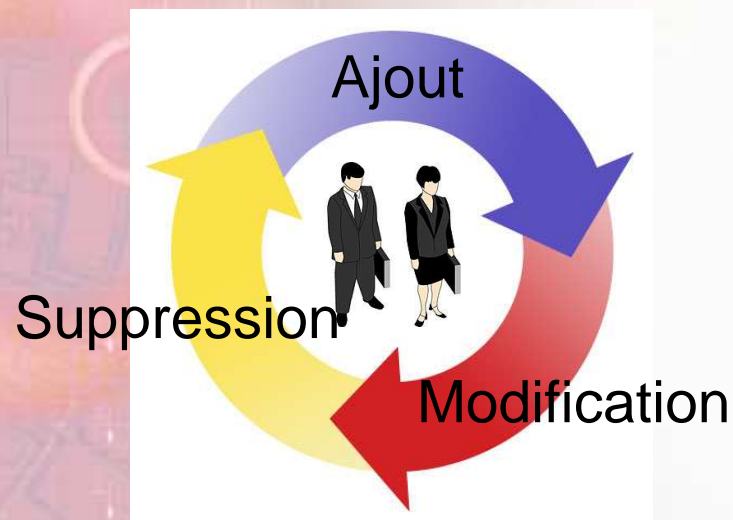
Enjeux : Que cherche-t-on à faire ?

Ce qui est recherché :

- Renforcer la Sécurité :
 - ❖ Gestion centralisée et automatisée des identités et des droits d'accès
- Répondre aux contraintes de conformité :
 - ❖ Traçabilité et obligations réglementaires et juridiques
- Contribuer à la productivité :
 - ❖ Workflow,
 - ❖ Provisionnement, synchronisations
- Simplification, réactivité et réduction des coûts de l'administration
- Satisfaction des utilisateurs :
 - ❖ SSO
 - ❖ Self-service utilisateurs

Les réponses du marché

Solution complète pour gérer les profils et les autorisations des utilisateurs tout au long du cycle de vie

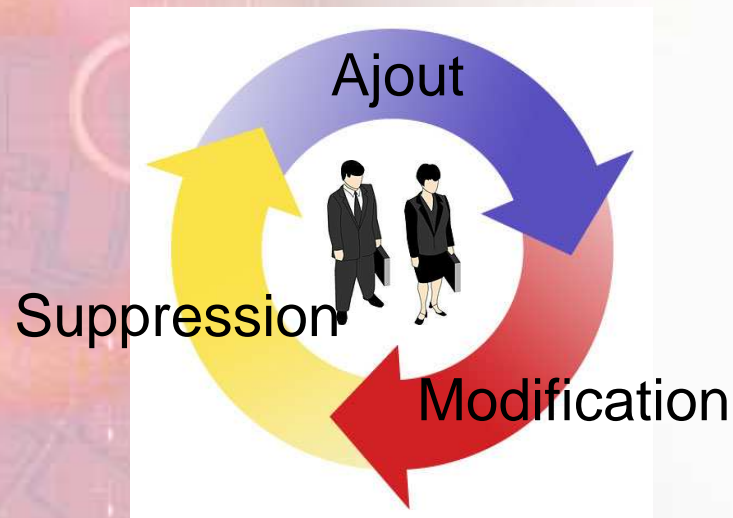


- ✓ Services d'annuaires
- ✓ Services de gestion du cycle de vie des identités
- ✓ Services de gestion d'accès,
- ✓ Services d'audit

- Sécurité renforcée
- Coûts réduits
- Productivité améliorée

Les réponses du marché

Solution complète pour gérer les profils et les autorisations des utilisateurs tout au long du cycle de vie



- Sécurité renforcée
- Coûts réduits
- Productivité améliorée

- Approvisionnement automatisé des utilisateurs pour une plus grande efficacité opérationnelle et une sécurité accrue
- Gestion des mots de passe sécurisée et automatisée pour une meilleure qualité de service et une réduction des coûts
- Administration déléguée et services en accès libre pour diminuer les coûts de support
- Synchronisation automatisée des données pour réduire la charge de travail associée à la gestion des modifications
- Architecture flexible et non intrusive pour accélérer les déploiements et le ROI
- Audit et rapport complets pour améliorer la sécurité

Réponses du marché : les limites techniques (1/2)

Les limites des solutions techniques : fédération d'annuaires

- N'apportent pas les réponses toutes faites aux problématiques organisationnelles,
- Facteur de complexité technique
 - ❖ Virtualisation des annuaires un must, mais quel contenu ?
 - ❖ Approvisionnement automatisés et auto-découverte
 - ❖ Limites des techniques de synchronisation complexes
 - ❖ Limite des connecteurs « universels et non-intrusifs »
 - ❖ Change management des agents
 - ❖ Limite des outils d'habilitation (finesse des profils d'habilitations)
 - ❖ Limite des « clonages » de profils
 - ❖ Nécessité de développements complémentaires

Réponses du marché : les limites techniques (2/2)

Les limites des solutions techniques suite :

- Limite des aspects sécurité couverts
 - ❖ Allocations de ressources et RBAC*
 - ❖ État sanitaire et contrôle d'admission au réseau
 - ❖ Comportement sur le réseau
- Limite des outils d'audit
 - ❖ Qui a fait quoi pendant quelle période avec quels privilèges ?
- Complexité de mise en œuvre des projets IAM
 - ❖ Coût et ROI
 - ❖ Effet tunnel

* Standard Role Based Access Control

Caractéristiques des projets IAM



Caractéristiques des projets IAM (1/3)

Projet Transverse

- Concerne tous les métiers
- Doit être sponsorisé par la DG
- Ne peut être conduit par la technique
- Les RH doivent s'impliquer dans les processus du cycle de vie des employés
- Les métiers doivent s'impliquer dans les définitions et mises à jour des rôles et habilitations fines
 - ❖ Exemple : Implication des achats pour contractuels et fournisseurs

Caractéristiques des projets IAM (2/3)

Projet Transverse (suite)

- C'est un projet d'intégration organisationnelle
 - ❖ Définitions de fonctions et de rôles
 - ❖ Modélisation des processus métiers
 - ❖ Cartographie des droits
 - ❖ Formaliser le processus d'habilitation des personnes



Partenaires



Employés



Clients



Employés
temporaires

Caractéristiques des projets IAM (3/3)

Projet Transverse (suite)

- C'est un projet d'intégration technique
 - ❖ Annuaire de référence (virtuel => quel contenu ?)
 - ❖ Urbanisation des référentiels
 - ❖ Paramétrage d'un workflow
 - ❖ Architecture des méta annuaires
 - ❖ Stratégie de provisionnement
 - ❖ Synchronisation
 - ❖ Fédération
 - ❖ Développements complémentaires

Les Chantiers IAM

- Retours d'expériences et bonnes pratiques
 - ❖ Stratégie
 - ❖ Tactique



Retour d'expériences et bonnes pratiques : Stratégie : par étapes courtes (1/4)

1- Initialisation :

- Cartographier :

- ❖ Les processus critiques
- ❖ Les applications (C/S et WeB)
- ❖ Les sources d'identification authentification
- ❖ Le cycle de vie des identités

- Évaluation les enjeux juridiques et réglementaires

- ❖ S'appuyer sur RH, Juridique et Finance

Retour d'expériences et bonnes pratiques :

Stratégie : par étapes courtes (2/4)

1- Initialisation : (suite)

- Identifier les populations à risques
 - ❖ Personnel, par métiers par processus
 - ❖ Clients,
 - ❖ Invités temporaires
 - ❖ Partenaires
 - ❖ Sous-traitants ponctuels
- Identifier les risques par typologie d'accès
 - ❖ Lan / Wan / VPN / Wifi
 - ❖ Intranet /Internet

Retour d'expériences et bonnes pratiques : Stratégie : par étapes courtes (3/4)

2- Préparation : Définir des lots pilotes par processus homogènes

- Définir les étapes de migration rechargement
 - ❖ Par applications processus critiques
 - ❖ Par typologie d'utilisateurs

3- Evaluation des technologies disponibles


- POC, tests, validations, visites de références

Retour d'expériences et bonnes pratiques : Stratégie : par étapes courtes (4/4)

4- Cahier des charges (Spécifications générales fonctionnelles et techniques, Lotissement)

- choix des technologies cibles pour chaque étape (voir tactique)
- choix d'un intégrateur indépendant (optionnel mais recommandé)

5- Planification des déploiements par lots

- 
- Pilotes, recettes, déploiement
 - Conduite du changement, assistance, validation, déploiement pour chacune des étapes définies.

Retour d'expériences et bonnes pratiques :

Tactique : Pas de Big Bang (1/3)

Démarrer petit et ne pas négliger les pilotes pour assurer la vente interne

Phase 1 :

- Choisir un périmètre réduit
 - ❖ Obtenir l'adhésion de la RH et des Directions métiers
 - ❖ Et celle des utilisateurs concernés
- Définir l'annuaire de référence pour le périmètre choisi
- Choisir un outil d'administration avec IHM assurant sa visibilité RH, son intérêt pour les métiers, sa compréhension pour la DG
- Rodage des processus via une implémentation du Workflow
- Puis mise en place des services d'annuaire pages blanches, pages jaunes, organigrammes....

Retour d'expériences et bonnes pratiques : Tactique : Pas de Big Bang (2/3)

Démarrer petit et ne pas négliger les pilotes pour assurer la vente interne

Phase 2 :


- Mise en place du SSO avec
 - ❖ qualité de service visible
 - ❖ retour sur investissement rapide sur le help desk
- Mesures, Bilan et communication des bénéfices obtenus

Retour d'expériences et bonnes pratiques : Tactique : Pas de Big Bang (3/3)

La DG est alors « mure » pour sponsoriser les étapes suivantes du projet IAM (pluri-annuel)

Phase 3 : Déploiement progressif de l'IAM sur la base de solutions de fédération neutres vis à vis des annuaires en place,

Travailler par domaines homogènes (cartographie) et étapes à court terme en mode projet

- 
- En priorité sur les applications nouvelles
 - Étendre progressivement aux autres applications
 - Objectifs visibles, mesurables, atteignables
 - En cohérence avec les étapes initiales

Nouvelles Voies ?



Nouvelles voies ?

NAC NAP et politiques d'accès aux ressources:

Limite de la sécurité périmétrique

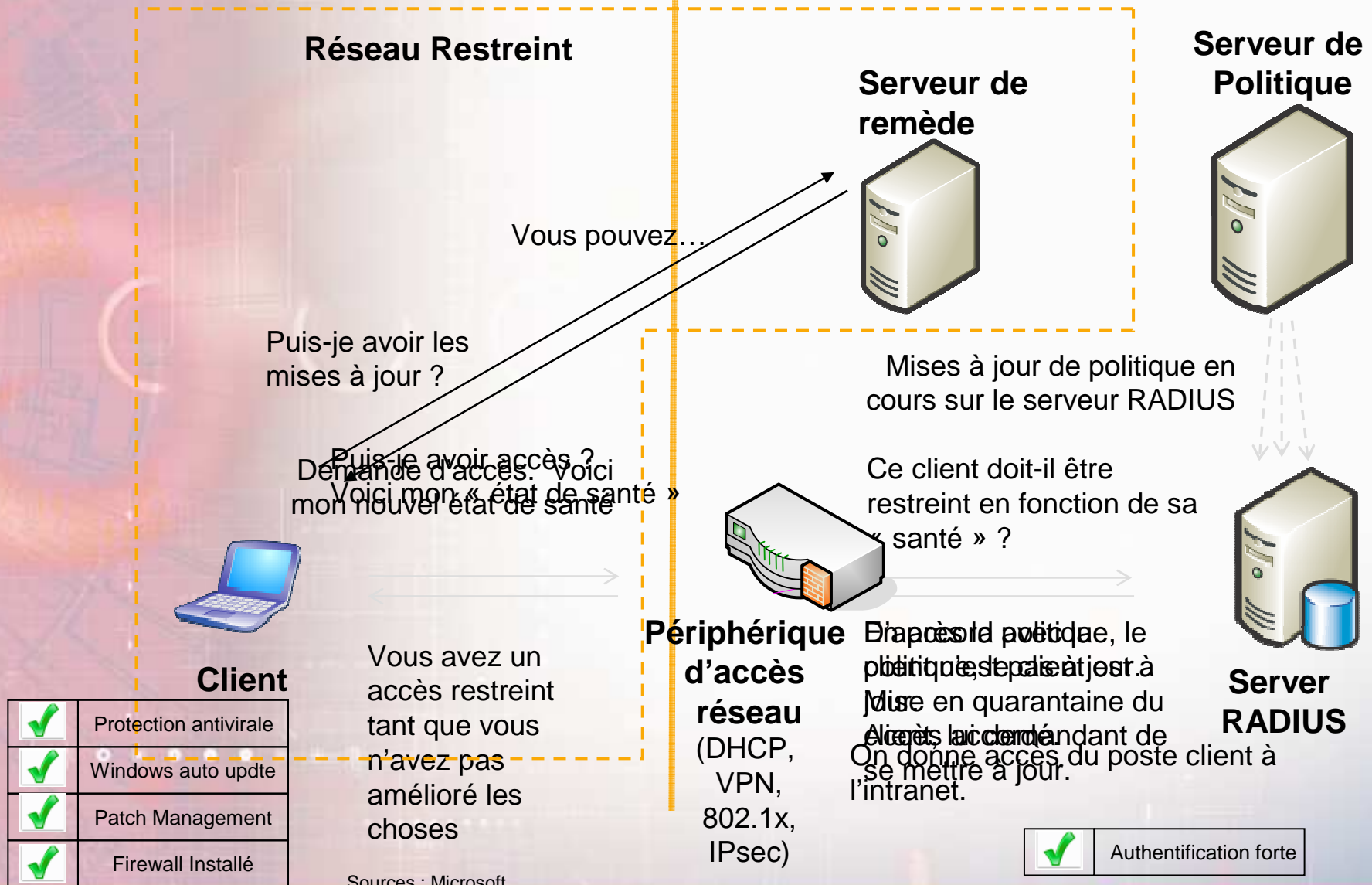
- Depuis les vers SQL Slammer, MS Blaster, Sobig nimba, etc... => Les menaces internes enfin prises au sérieux

Passage d'une sécurité de type forteresse à une sécurité de type aéroportuaire :

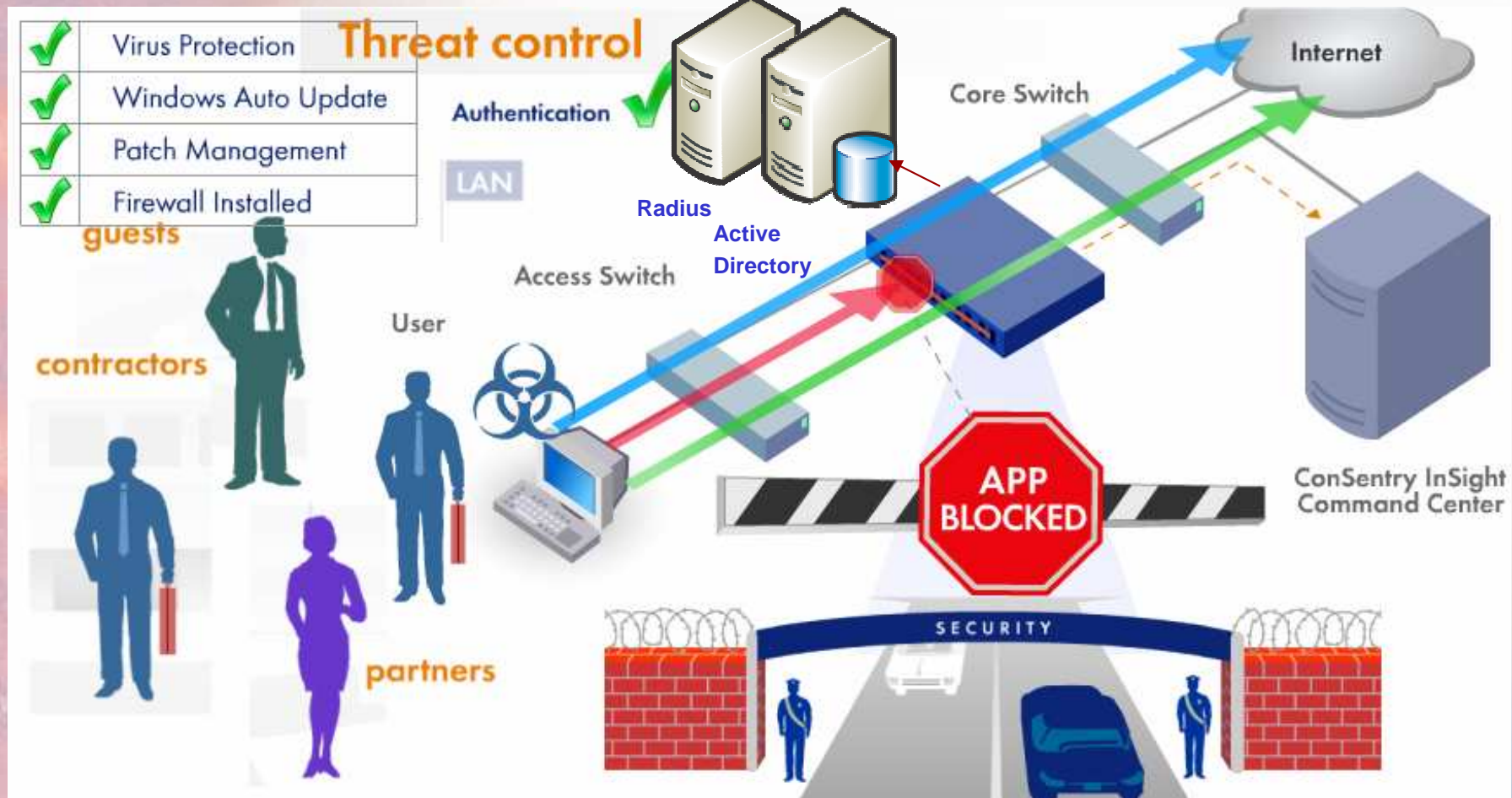
- Passer d'une analyse d'identité à une analyse d'accès au réseau de confiance de l'entreprise et de comportement à l'intérieur de ce réseau
- Nécessite une capacité à imposer dynamiquement les politiques de contrôles « sanitaires » en complément
- Nécessite une analyse de niveau 7 en complément aux autres niveaux de contrôle des flux (Puissance des équipements)

Protection d'accès au réseau

Réseau de l'entreprise



Couplage RBAC et NAC sur un contrôleur de type « appliance »



Sources : d'après Consentry

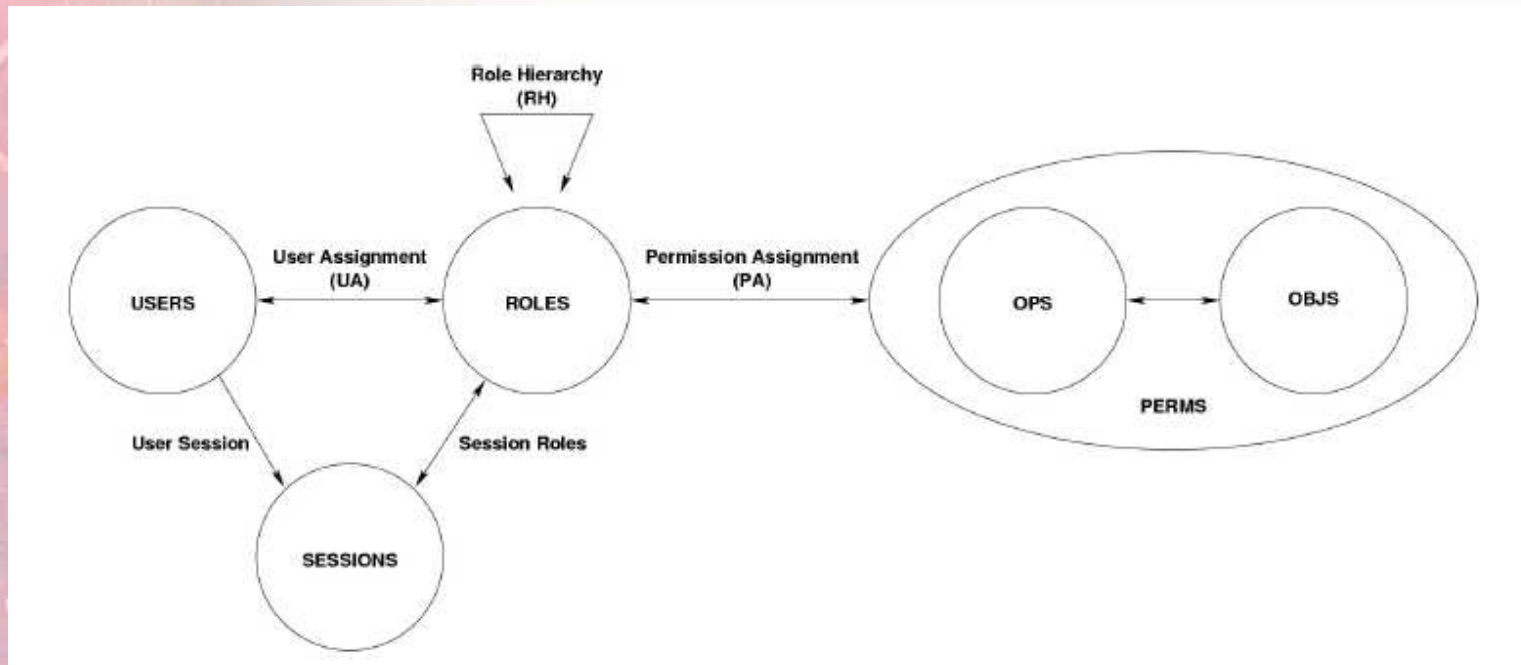
Conclusion

La gestion des identités et le contrôle d'accès réseau sont deux pivots de la réussite d'une politique de sécurité d'accès

- La gestion des identités est un préalable aux projets de sécurité
- Les technologies actuelles sont matures la difficulté de leur mise en œuvre tient à la sous-estimation de la complexité de la situation technique et organisationnelle initiale
- Les projets de déploiement IAM sont des projets d'intégration **longs à forte composante organisationnelle**
- Ils doivent faire l'objet d'un découpage par étapes et bénéficier d'une préparation stratégique et tactique soignées
- Le sponsoring DG et la communication sont un must.

Modèle RBAC

Standard proposé par le NIST en 2001



<http://www.nsa.gov/selinux/download3.html>