Technologies des réseaux et NTICs

La sécurité distribuée

Jeudi 11 juin 2009

Coordination scientifique :

- ***Jean-Claude Lambert (INSERM)***
- ***François Morris (CNRS)***

Amphithéâtre Gay-Lussac, École Polytechnique, Palaiseau

http://www.aristote.asso.fr Contact : **info@aristote.asso.fr**

Edition du 27 Prairial an CCXVII (*vulg.* 15 juin 2009)

ARISTOTE Association Loi de 1901. Siège social : CEA-DSI CEN Saclay Bât. 474, 91191 Gif-sur-Yvette Cedex.
Secrétariat : Aristote, École Polytechnique, 91128 Palaiseau Cedex.
Tél. : +33(0)1 69 33 99 66 Fax : +33(0)1 69 33 99 67 Courriel : Marie.Tetard@polytechnique.edu
Site internet http://www.aristote.asso.fr

Table des matières

Chapitre 1

Programme de la journée

1.1 Introduction

Chaque DSI constate quotidiennement, face à l'éclatement des modes de travail et de communication au sein des entreprises et des organismes publics, l'incapacité des modèles de sécurité classiques à s'adapter à ces nouveaux comportements et à offrir un niveau de sécurité suffisant. La vieille logique du bastion permettant de protéger l'ensemble du système d'information derrière un pare-feu est remise en question par des applications qui se veulent de plus en plus communicantes, des utilisateurs de plus en plus mobiles et des informations de plus en plus distribuées. La mobilité totale, tant à l'intérieur qu'à l'extérieur de l'entreprise entraîne un éclatement du périmètre de contrôle et exige donc de nouvelles manières d'aborder et d'organiser la sécurité. Des réponses seront apportées à travers des solutions présentées par des fournisseurs, des retours d'expériences et des analyses prospectives. Des acteurs comme Juniper ou Cisco proposent des solutions permettant de contrôler tous les flux et d'identifier chaque utilisateur venant de l'intérieur comme de l'extérieur à travers un tunnel SSL. De même Citrix a une approche globale et similaire associée à des terminaux légers. Les entreprises multisites ou travaillant avec des sous-traitants doivent partager et stocker leurs données sensibles sur plusieurs sites avec le maximum de confidentialité et d'intégrité. La société Active Circle apporte une solution innovante avec son logiciel Eponyme. Nous verrons également si la virtualisation qui envahit les salles serveurs et prochainement le poste client apporte un plus de sécurité ou de nouvelles problématiques. Sécuriser c'est aussi avoir une vision globale, temps réel, sur l'ensemble des flux venant de tous les matériels actifs, associée à une analyse comportementale et à la corrélation d'événements comme le propose Q1Labs. Des témoignages client autours des solutions de Trapèze et de Sparus Software démontreront qu'il est possible, maintenant, de gérer un vaste réseau Wifi ou une flotte de terminaux mobiles avec le même niveau de sécurité, de contrôle de flux et de qualité de service qu'avec une infrastructure câblée. On peut se demander si cet éclatement du système d'information et l'externalisation des données et des applications métier ne vont pas remettre en question les grands principes liés à la sécurité et à la possession des données.

1.2 Programme

9h00-9h30	*Accueil des participants*	
9h30-9h40		Ouverture du séminaire (par les organisateurs)
	Laurent Paumelle Juniper	Vers une manière plus intelligente de sécuriser les accès aux réseaux de campus
	Patrick Rohrbasser Citrix **Alain Poussereau** AB3F Consult	Les principes de la virtualisation et la vision de Citrix Systems Retour d'expérience de la CNAV et du domaine social
10h30-10h50	*Pause café*	
	Philippe Martinez Synchrotron Soleil **Philippe Boyon** Active Circle	Une solution stockage sécurisée et distribuée au synchrotron Soleil Construire son Cloud Storage et son Data Sharing facilement et en toute sécurité
	Nicolas Ruff EADS IW	Virtualiser pour mieux sécuriser ?
	Daniel Dezulier France Telecom Orange	Comment gérer la sécurité de tous les systèmes d'information de différents grands comptes avec méthode ?
	Raphael Marichez HSC	Les DSI du public et du privé face à la sécurité distribuée
13h30-14h30	*Repas* (salle «aquarium»)	
	Agostinho Rodrigues Interdata	Controle de l'activité et gestion des menaces dans un environnement réseau distribué
	Olivier Carbonneaux Trapèze **Jocelin Rajaona** IGR	Le wifi en tout lieu et en toute sécurité avec un retour d'expérience de l'Institut Gustave Roussy
16h00-16h20	*Pause*	
	Christian Claveleira CRU	eduroam : nomadisme sécurisé pour la communauté enseignement supérieur-recherche
	Cédric Blancher EADS	Les pare-feu nuisent-ils à la sécurité ? Quelques considérations autour du concept de dépérimétrisation
17h30——		Table ronde (avec les intervenants)

	Modifications	
	StoneSoft *Intervention annulée*	Les enjeux méconnus de la sécurisation d'un environnement virtuel à travers leur solution StoneGate Virtual IPS
	Sparus Software *Intervention annulée*	Comment gérer une flotte de terminaux mobiles avec le même niveau de qualité et de sécurité que des postes fixes. Un retour d'expérience autour de la solution Everywan Mobility Manager sera également proposé par Mondial Assistance

Pour ces conférences, nous publions les livres blancs qui illustrent les problématiques qui auraient dû être abordées.

Chapitre 2

Présentations

2.1 Laurent Paumelle (Juniper)

Vers une manière plus intelligente de sécuriser les accès aux réseaux de campus

Dans les entreprises actuelles, le réseau est de plus en plus le cœur de l'activité. Les utilisateurs qui accèdent aux ressources depuis un LAN dénué de contrôles des accès peuvent exposer l'entreprise à un grand nombre de menaces. Afin de satisfaire leurs exigences en matière de sécurité et de conformité réglementaire les entreprises doivent être en mesure d'identifier leurs utilisateurs et de contrôler leur niveau d'accès de l'intérieur comme de l'extérieur. Monsieur Serge Makowski présentera le point de vue de Juniper autour des solutions « Secure Access SSL VPN » et « Unified Access Control » ainsi qu'une étude approfondie sur les différents niveaux de contrôle appliqués à un client et à la sécurisation de ses accès.

Vers une manière plus intelligente de securiser les accès aux réseaux de campus

Juniper NETWORKS

The PR nightmare

Opportunistic…

InformationWeek

Fake Obama Web Site Reportedly Builds Botnet

January 20, 2009

The fake Web site looks just like the real thing and attempts to bait viewers into clicking a story titled "Barack Obama has refused to be a president."

Sure enough, the phishers and scammers have come out of the woodwork to try to exploit people's interest in America's new president

http://www.informationweek.com/news/security/government/showArticle=212901473

Devastating…

InformationWeek

Heartland Payment Systems Hit By Data Security Breach

January 20, 2009

The systems penetrated by a malicious keylogger could result in a data breach that rivals the parent company of TJ Maxx in 2007

Heartland Payment Systems, a leading payment processing company, reported on Tuesday that its systems had been compromised by malware in 2008

http://www.informationweek.com/news/security/attacks/showArticle.jhtml=212901505

ACCESS CONTROL
Why is this technology so important to customers??

- **Dynamic Network Boundaries – Location Complication**
  - Mobile Workforce
  - Wireless Networks
  - Contractors
  - Partners
  - Diversity of endpoints
- **Sophisticated Attacks**
  - Zero-Day Exploits
  - Rapid Infection Speed
  - Targeted Attacks (crimeware)
  - Rootkits, Botnets, Zombies and Back Doors
- **Harder to control/More demanding Applications**
  - IM/VoIP/VoD
  - Unenforceable policy
- **The Grey Network**
  - The Network you don't know you own!
- **The Usual Suspects**
  - Bad People
    - More Money for Attackers
    - Extortion, Identity Theft, Bank Fraud, Corporate Espionage,…
  - Careless People
    - Accidental agents of catastrophe

Market Expectations of Access Control

Must include this functionality

1. Evaluation of security state before connection
2. Quarantine and/or remediation for non-compliant users
3. Identity-based network admission control
   - Can you get on the network?
4. Policy and identity -based access control based on user identity
   - What can you get access to?
5. Evaluation of security state throughout the session
   - Threat management

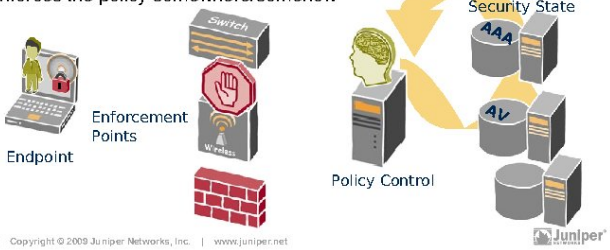
For these user groups

1. Guest users
   - Difficult to assess security state
   - Unmanageable devices
2. Contractors
   - Not onsite
   - Need access to a variety of enterprise-specific resources
3. Remote or mobile employees
   - Use the PC outside of the office
   - May be "careless"
   - May run unauthorized apps

Access Control
What IS Access Control and how to I get it?

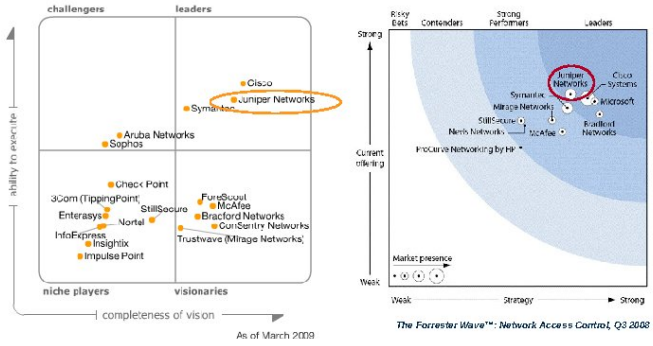
- **Incorporates a means to get the user's identity and the endpoint security state**
- Combines that information with access policy
- Enforces the policy somewhere/somehow

Combines user identity, endpoint security state, and device location with policy to make sure that the right people get the right access, while the network stays safe

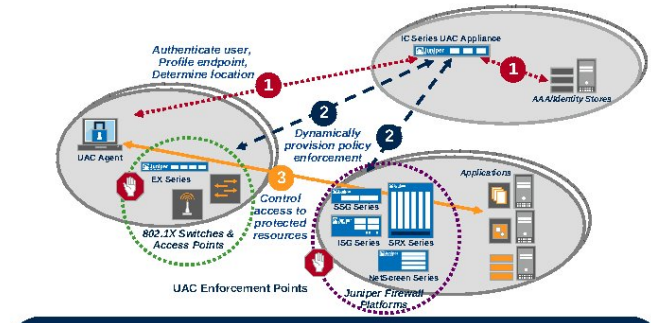


ABOUT JUNIPER'S UNIFIED ACCESS CONTROL

UAC – NAC Market Leader

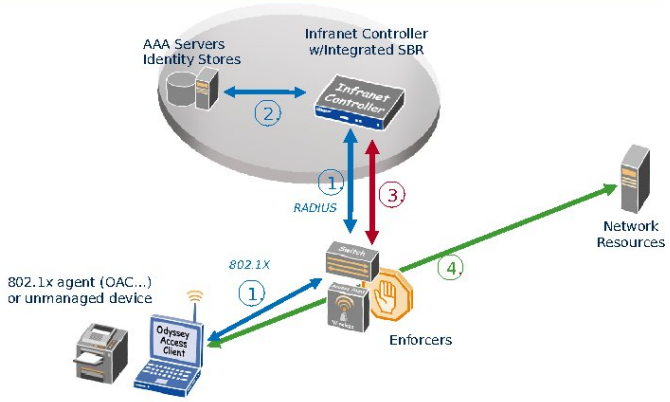


UAC – Identity Enabling Security and Access Control

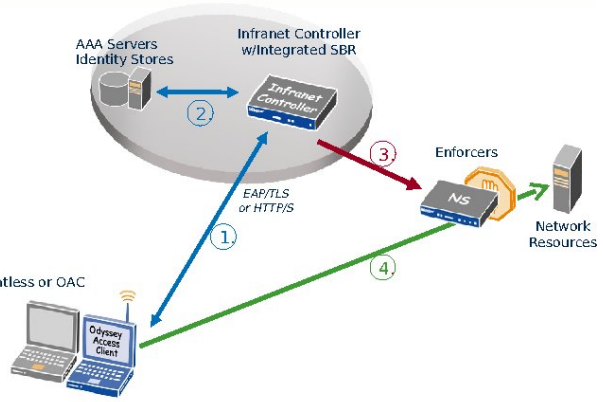


Comprehensive, vendor-agnostic, standards-based access control across heterogeneous environments delivering investment protection

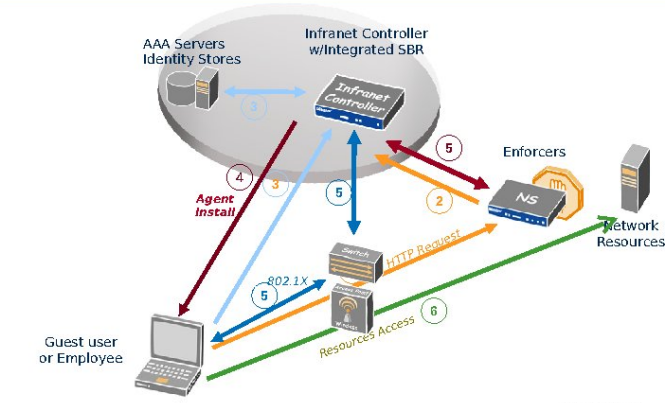
UAC – L2 Agent access (802.1x)



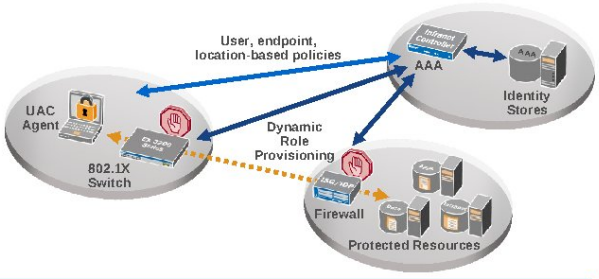
UAC – L3 Agent or Agenless access



UAC – Dynamically delivered Agent

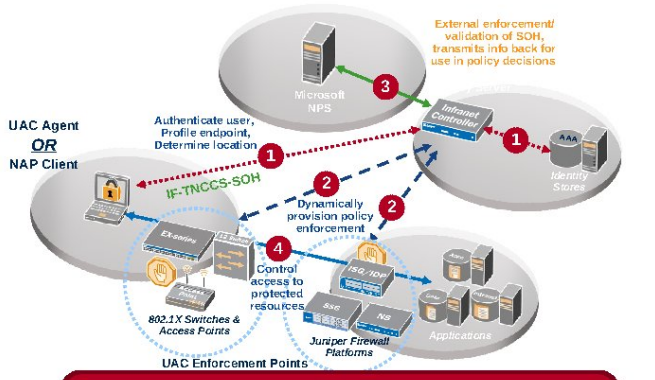


Unified Access Control & EX-series Ethernet Switches



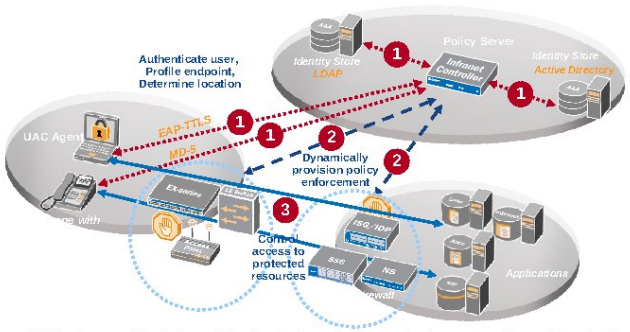
- Policy enforcement provided by EX-series switches and SSG/ISG/SRX Firewalls
- IC can push policy name to EX-series switches for dynamic configuration based on user or device
- Policy on EX-series can enforce specific QoS queuing or scheduling policies, VLAN assignment, or any other port configuration parameter

Windows Statement of Health (SOH) and Embedded NAP Agent Support



Streamlines deployments, while increasing deployment options

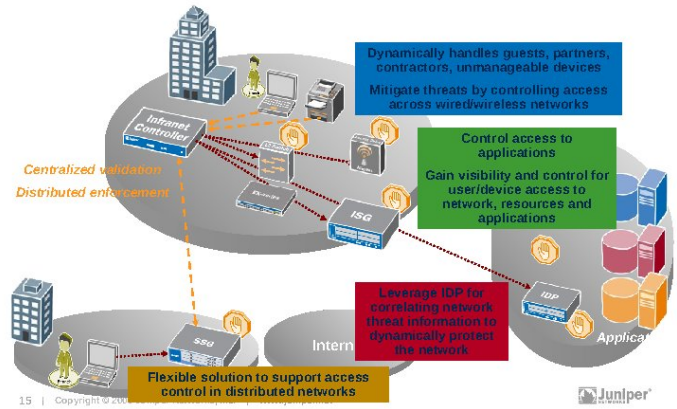
Automatic Realm Decisions Based on Authentication Protocols



- Configures the Infranet Controller to select a realm based on the authentication protocol in the connection request

Demystifies and simplifies a previously complex deployment, improving the administrative experience

Juniper Networks UAC Adaptable, Standards-based Access Control



ABOUT JUNIPER'S ACCESS CONTROL OPENNESS

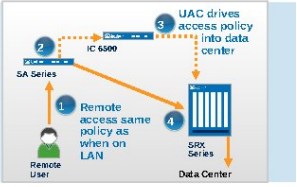
The *Only Enterprise-Wide* Access Control solution

Re-Defining Access Control:

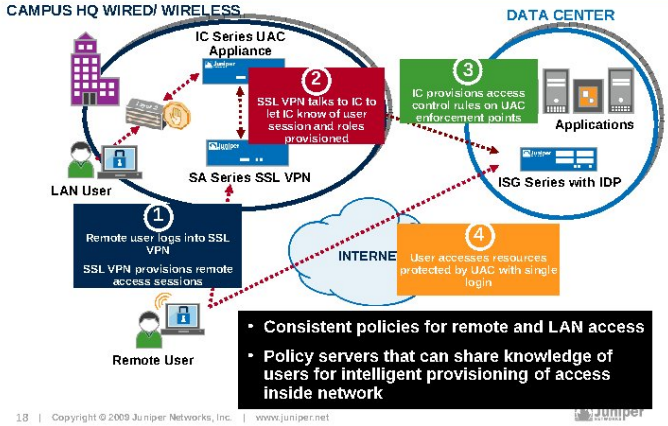
The Only Cooperative Local (UAC) and Remote (SSL VPN) Access Solution

- **Global, Shared "User/App" policies**
  - Cuts access control administration overhead by 50%
  - Ensures consistently enforced *global* policies
  - Effectively supports mobile user groups—policies "follow the user"

- **Federated SSL VPN and UAC sessions allows for true SSO with granular access control**
  - SSO across multiple UAC domains
  - Uses standard, IF-MAP

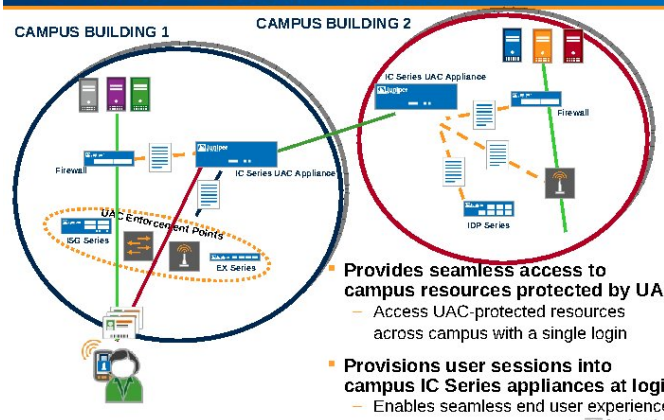


UAC-SA Federation Diagram



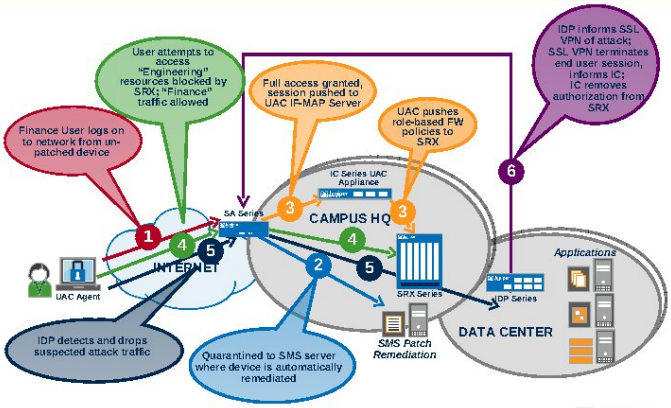
- **Consistent policies for remote and LAN access**
- **Policy servers that can share knowledge of users for intelligent provisioning of access inside network**

IC Series - IC Series Federation



- Provides seamless access to campus resources protected by UAC
  - Access UAC-protected resources across campus with a single login
- Provisions user sessions into campus IC Series appliances at login
  - Enables seamless end user experience

Enterprise-wide Access Control



What is Trusted Network Connect (TNC)

- Open architecture for Network Access Control (NAC)
- Completely vendor-neutral
- Strong security through trusted computing
- Full set of specifications available to all
- Products shipping for more than three years
- Developed by Trusted Computing Group (TCG)

TNC Includes All Kinds of NAC

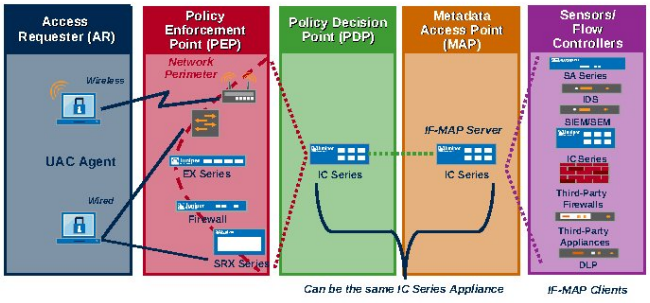
- Assessment options
  - Identity, health, and/or behavior
  - Optional hardware-based assessment with TPM
  - Pre-admission, post-admission, or both
- Enforcement options
  - 802.1X, firewalls, VPN gateways, DHCP, host software
- Clientless endpoints
  - No NAC capabilities built in
  - Printers, phones, robots, guest laptops
- Information sharing
  - Lets security devices share info on user identity and role, endpoint health, behavior, etc. (IF-MAP)

TNC Advantages

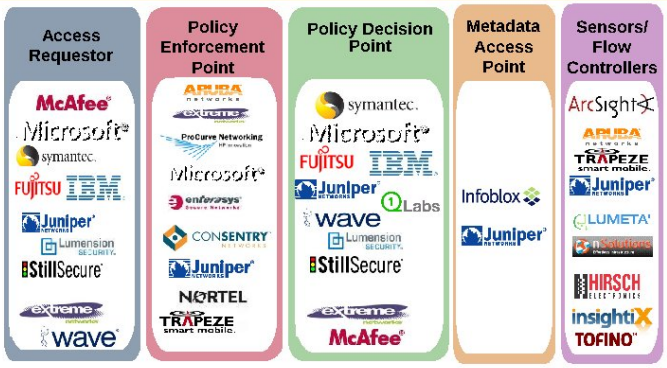
- Enables security throughout the enterprise
  - Beyond walls
  - Integrates all types of devices
- Open standards
  - Non-proprietary – Supports multi-vendor compatibility
  - Interoperability
  - Enables customer choice
  - Open source solutions
- Leverages existing network infrastructure
  - Excellent ROI
  - Supports Trusted Platform Module (TPM)

Products supporting TNC standards shipping today!

TNC Architecture



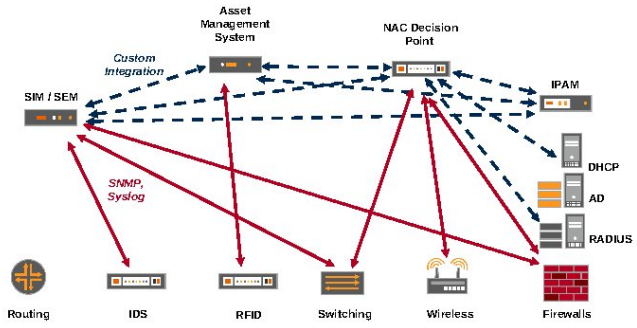
TNC Adoption



What is IF-MAP?

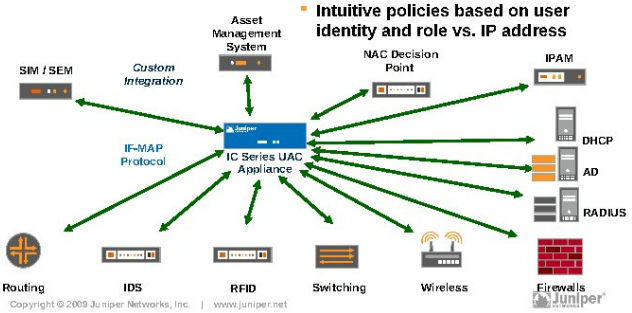
- Open standard for security and network coordination
  - Published in May 2008 by the Trusted Computing Group
  - Freely available for anyone to implement
  - Growing base of vendor and product support
- Shared database for security information
  - Who's connected to the network, what device are they using, what's the device state, what are its expected and actual behavior
  - "MySpace" for security systems
- Aggregates real-time information from many different sources
  - Both standard data types and vendor-specific extensions
- Designed to scale for machine-to-machine coordination

The Situation Today When Systems Want to Coordinate

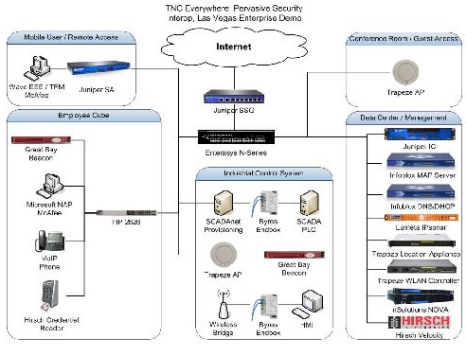


IF-MAP and UAC: Open, Interoperable Access Control

- UAC 3.0 adopts TNC's IF-MAP standard protocol
- Coordinated defense/response across multi-vendor device deployments
- Facilitates interoperability with and enforcement for third-party devices
- Enhances visibility into the network and its state
- Intuitive policies based on user identity and role vs. IP address



TNC's Pervasive Security

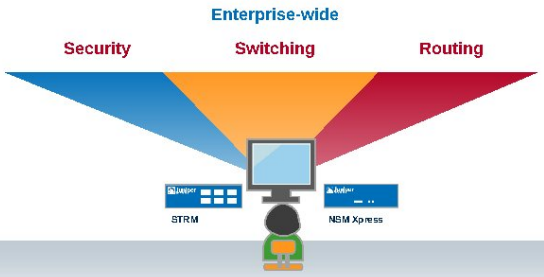


Summary

- TNC's Interface for Metadata Access Point (IF-MAP)
  - *The open standard for security and network coordination!*
  - Aggregator of real-time information from many different sources, providing a shared database for information on network devices, their state, and their activities
  - Has a growing list of adopters!
- UAC and IF-MAP
  - Enables standards-based, enterprise-wide access control with SA Series
  - Allows identity federation between UAC-SA, IC Series-IC Series
  - Simplifies user experience by providing SSO-like capability for access control
  - Empowers IC Series as IF-MAP server, collecting and leveraging network device data, state, and activity when making network security policy decisions

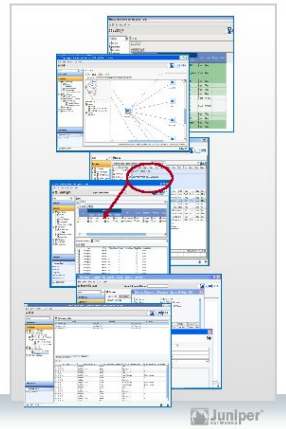
ABOUT JUNIPER'S ACCESS CONTROL MANAGEMENT

Consolidated network-wide management for high productivity with low risk



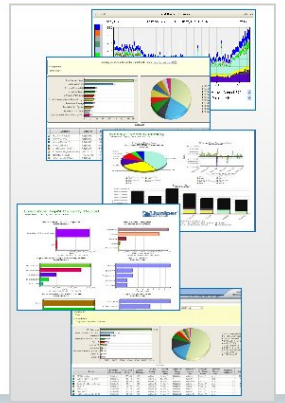
Network & Security Manager (NSM)

- Increase Productivity of your IT team
  - One provisioning system
  - Less to learn and maintain
  - Less mistakes—less wasted time
  - Coverage flexibility
- Usage pattern discovery and policy creation
  - Discover Applications and Applications usage
  - Correlate user to application
  - Protect network against application misuse
    - User "guest" → Block P2P traffic
    - User Role "Eng" → Rate-Limit on Web Traffic
- New device support
  - SRX
  - M / MX Series
  - EX8208
- New UAC and EX switch Management
  - Wizard
  - Tight EX and IC coupling

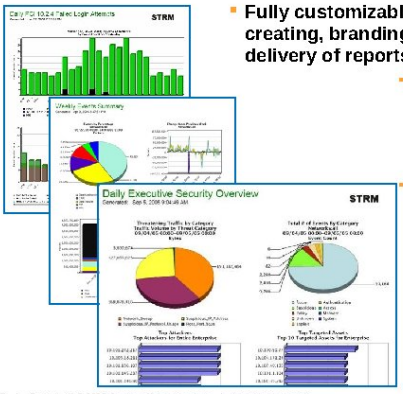


Security Threat Response Manager (STRM)

- IT Productivity gains
  - Integrated solution for
    - SIEM
    - NBAD
    - Application Visibility
    - Reporting and monitoring
  - Plug-n-Play appliance
  - Massive log reduction and prioritization
- New MSSP Offerings
  - Segregation of Data at device level
  - Granular control through user permissions
  - Horizontal permissions through the product
    - Event searching
    - Reporting
    - Offenses
- Now with over 500 template reports
  - Including new NAC and SA support
- New workflow system support



Compliance reporting



- Fully customizable reporting engine: creating, branding and scheduling delivery of reports
- Control Frameworks
  - CobiT
  - ISO/IEC 27002 (17799), ISO/IEC 15408
  - NIST special publication 800-53 revision 1
  - FIPS 200
- Regulations
  - PCI-DSS
  - HIPAA
  - SOX
  - GLBA
  - FISMA

THANK YOU

2.2 Patrick Rohrbasser (Citrix) et Alain Poussereau (AB3F Consult)

Virtualiser les ressources de l'entreprise par le biais d'une architecture totalement centralisée et sécurisée Retour d'expérience de la CNAV et du domaine social

Le poste client permet trop souvent à l'utilisateur d'installer des applications ou de pratiquer des opérations qui n'ont rien à voir avec son cœur de métier et sont souvent source d'insécurité. Le client léger, véritable poste passif ne propose à l'utilisateur que les applications métiers virtualisées qu'il est censé utiliser dans un environnement entièrement sécurisé. Un retour d'expérience sur la solution de virtualisation de bout en bout « XenApp » de Citrix sera présenté par Monsieur Patrick Rohrbasser.

CITRIX

LA SECURITE PAR L'ARCHITECTURE

L'offre Citrix – Patrick ROHRBASSER

Directeur des Régions et du Secteur Public

La consommation d'informations est incontrôlable

L'enjeu sécurité dans le SI ?

- Protéger la propriété intellectuelle
- Partager l'information
- Ne pas créer d'adhérence
- Assurer la traçabilité
- Veiller sur l'efficience des équipes et la perte de productivité

Sécurité ou Sécurité ?

Securité périmétrique
Mise en place de protections pour de prémunir d'attaques pouvant mettre en péril un organisation.

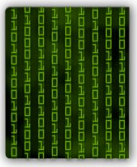
Sécurité d'accès
Fournir un accès sécurisé & contrôlé aux ressources pour que les collaborateurs de l'organisation puissent effectuer leur mission.

La sécurité vue par Citrix

- Comment sécuriser en permanence sans restreindre l'usage ?
  - Centraliser la propriété intellectuelle
  - Ne pas dupliquer l'information et les applications capable de la traiter
  - Sécuriser par l'architecture
  - Ouvrir les accès, les sécuriser et adapter la réponse
  - Etre en mesure de réagir vite
- Quelles sont les solutions qui peuvent s'appliquer globalement sans adhérence technologique et physique ?
  - Une architecture sans couture et virtualisée avec une visibilité de bout en bout

L'offre CITRIX XEN DELIVERY CENTER

Une infrastructure virtuelle complète pour mettre à disposition les ressources de l'entreprise



L'offre CITRIX XEN DELIVERY CENTER

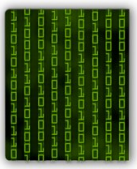
CITRIX WORKFLOW ORCHESTRATOR

CITRIX NETSCALER avec EDGESIGHT
CITRIX REPEATER
VYATTA

CITRIX XENSDESKTOP avec EDGESIGHT & PASSWORD MANAGER

CITRIX XENAPP avec EDGESIGHT & PASSWORD MANAGER

CITRIX ESSENTIALS FOR XENSERVER



Utilisateurs

Applications

CITRIX

Le retour d'expérience de la CNAV

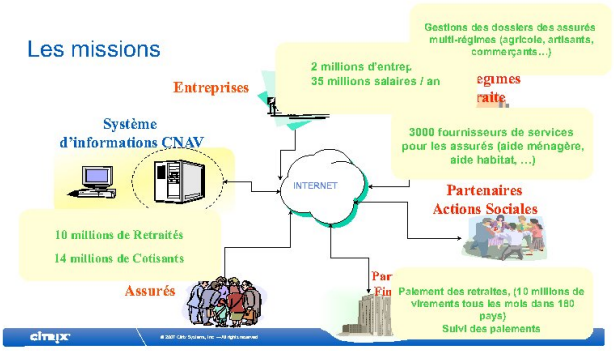
Alain POUSSEREAU
ex DSI de la CNAV

Dirigeant Associé du cabinet de conseil AB3F

Le cabinet AB3F Conseil

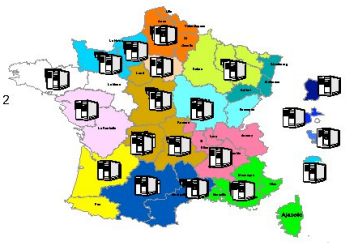
- Dirigé par le DSI de la CNAV (15 ans) et N°2 la dernière année.
- Expertise de haut niveau dans le domaine des affaires sociales.
- Les domaines de compétences touchent :
  - le management
  - la conduite de projet
  - le conseil stratégique auprès des Directions Générales
  - le conseil et accompagnement aux DSI
    - sur les schéma Directeurs
    - sur les stratégies d'infrastructures
    - la politique de sécurité
    - La recherche et la mise en œuvre de technologie

Les missions



L'environnement technique de la CNAV

- 21000 collaborateurs dont 1500 informaticiens
- Une organisation extrêmement décentralisée
- 20 centres de productions en 2002, 2 en 2010
- 2400 points d'accueil
- Des partenaires, des entreprises
- Des clients
- Des agents nomades
- Des structures temporaires



Pourquoi le choix Citrix ?

Impact utilisateur et organisation

- Amener l'utilisateur sur le SI plutôt que pousser le SI vers l'utilisateur
- Un accès unique quelque soit le type de connexion (interne / externe / partenaire / indéterminé)
- Homogénéité des applications et des technologies
- Un système d'information indépendant du poste de travail
- Meilleur contrôle du SI dans sa globalité

Impact sécurité

- Garder l'information dans l'organisation
- Une seule infrastructure, une seule porte, un seul SI, pour tous les scénarios d'accès
- Une identification rapide des problèmes avec réponse immédiate (service pack, …)
- Le poste, élément le plus sensible n'impacte pas la production
- La sécurité est renforcé à tous les niveaux

Le projet EMI sous l'angle sécurité

- Phase 1 : Virtualisation des applications
  - Sécuriser la propriété intellectuelle
    - Mise en œuvre d'une infrastructure commune sécurisée et sans couture
    - Préserver les investissements technologiques et applicatifs
    - Améliorer la performance et réduire les coûts
- Phase 2 : EMI 1 = Evolution des Moyens Informatiques (2004 à 2008)
  - Sécuriser la production
    - Consolidation et rationalisation des centres de production
    - De 20 centres à 4 centres
    - Mise en œuvre du PRA (actif / actif et actif / passif)
- EMI 2 (2009 …)
  - Sécuriser par l'unification des moyens
    - De 4 centres à 2 centres
    - Intégration du Web dans le processus de production

Conclusion sur la virtualisation Citrix à la CNAV

- Pas un seul virus détecté sur le SI de production depuis la mise en œuvre du projet EMI
- Aucune intrusion dans le système
- Mais vecteur d'ouverture du SI vers l'extérieur
- Et déterminant stratégique du télétravail
- Source de l'agilité du système et donc de réactivité face aux problèmes des montées de version et d'application de correctif
- Une infrastructure sans couture garante de la sécurité des données confidentielles du domaine social en France

CITRIX®

Une infrastructure de bout en bout

pour virtualiser

Serveurs, Applications,

Postes de travail & éléments actif du Réseaux

2.3 Philippe Martinez (Synchrotron Soleil) et Philippe Boyon (Active Circle)

Les entreprises multisites ou travaillant avec des sous-traitants cherchent souvent une manière simple et sécurisée de stocker ou de partager des fichiers entre plusieurs sites. La solution logicielle Eponyme de Active Circle est une solution de sauvegarde originale, robuste et sécurisée qui repose sur un ensemble de serveurs dédiés quelconques appelés cellules et formant un système de fichiers virtualisés qui appliquent également des classes de services dans un véritable Cloud Storage Privé. Monsieur Philippe Martinez viendra témoigner de son retour d'expérience avec cette solution utilisée sur le synchrotron Soleil à Saclay et sera accompagné par Monsieur Philippe Boyon de Active Circle pour les questions très techniques.

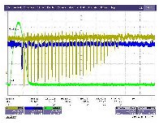
Une solution stockage sécurisée et distribuée au synchrotron Soleil ; Construire son Cloud Storage et son Data Sharing facilement et en toute sécurité

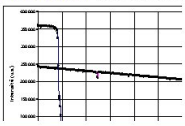
Une solution stockage sécurisée et distribuée au Synchrotron Soleil

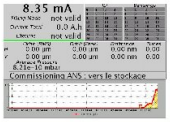
Philippe MARTINEZ
Informatique Scientifique – Groupe Systèmes et Réseaux – Division Informatique
philippe.martinez@synchrotron-soleil.fr

Historique du Synchrotron Soleil

- Début des années 1990 : initiation du projet (suite du LURE)
- 1996 - 1999 : mise en place d'une équipe CEA/CNRS pour l'étude de l'APD (Avant-Projet Détaillé)
- 11 septembre 2000 : Annonce de la construction de Soleil sur le plateau de Saclay par le ministre de la recherche
- 16 octobre 2001 : Création de la société civile
- Janvier 2002 : début de la construction
- Juin 2006 : 1ère accumulation d'électrons
- Septembre 2006 : 1er faisceau et **1er octet stocké**
- Janvier 2008 : 1ers utilisateurs







Philippe MARTINEZ
SYNCHROTRON SOLEIL

La société Synchrotron Soleil

- Société civile de droit français (CEA : 28 %, CNRS : 72 %)
- Partenaires : Le Conseil Général de l'Essonne et le Conseil Régional d'Ile de France

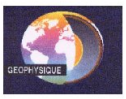
- Un grand projet national et européen :
  - Effectuer la recherche fondamentale dans tous les domaines qui requièrent l'utilisation du rayonnement synchrotron
  - Doter la France d'un outil de haute technologie au service de la Recherche, mais aussi des grands enjeux nationaux et de l'industrie (défense, environnement, santé …)
  - S'ouvrir aux utilisateurs français mais aussi aux utilisateurs européens et du monde entier

Philippe MARTINEZ
SYNCHROTRON SOLEIL

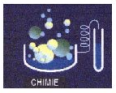
Les principaux domaines d'application

Détection de substances polluantes

Connaissance de la structure des matériaux



Exploration de la matière et connaissance de ses propriétés



Conservation des aliments

Elaboration de nouveaux matériaux

Recherche de nouveaux médicaments, imagerie des tissus osseux, étude de l'ADN, ...

Dans tous les domaines, un accueil est prévu pour les industriels

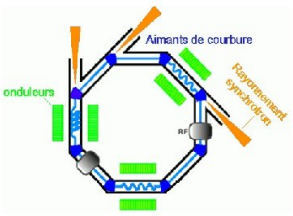
Philippe MARTINEZ
SYNCHROTRON SOLEIL

Qu'est-ce qu'un synchrotron ?

Philippe MARTINEZ
SYNCHROTRON SOLEIL

Le rayonnement synchrotron ?

- C'est un rayonnement très intense produit lorsque des électrons de très haute énergie sont soumis à l'action d'un champ magnétique et perdent leur énergie.

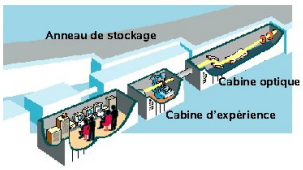


- Ces conditions sont réunies dans les accélérateurs circulaires où des électrons sont accélérés jusqu'à la vitesse de la lumière et forcés de suivre une trajectoire circulaire (aimants et éléments d'insertion).

Philippe MARTINEZ
SYNCHROTRON SOLEIL

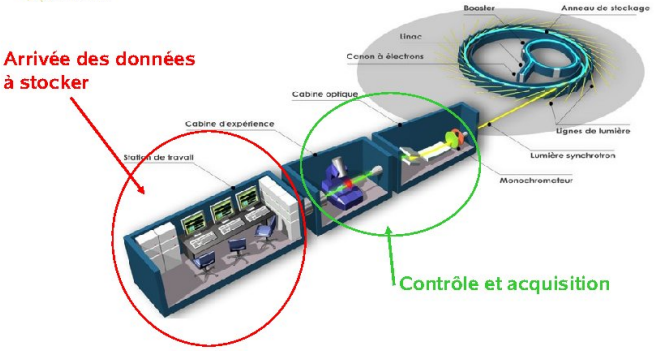
Le principe de fonctionnement

- Le rayonnement synchrotron sortant de l'anneau est concentré et dirigé par des systèmes optiques vers les installations expérimentales (les lignes de lumière).
- Grâce à des réseaux ou des cristaux, on sélectionne la longueur d'onde adaptée à l'expérience (plus elle est courte et plus on pourra étudier des objets de petite dimension).



- Le rayonnement illumine l'échantillon. Réfléchi, transmis ou absorbé, il est analysé par des détecteurs et, après traitement des informations, il permet d'appréhender les propriétés de l'échantillon étudié.

Périmètre de l'informatique

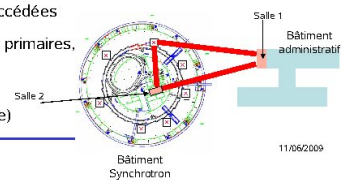


Les grandes étapes du projet "stockage"

- 1er semestre 2004 : recensement des besoins utilisateurs
  - compréhension du mode de fonctionnement de chaque ligne de lumière
  - identification et caractérisation des données
  - analyse du cycle de vie des données
- Janvier 2005 : lancement de l'appel d'offre
- Septembre 2005 : maquettage
- Fin 2005/début 2006 : choix de la solution
- Mai 2006 : début du déploiement
- Second semestre 2006 : premières mises en production
- Janvier 2008 : premiers utilisateurs extérieurs

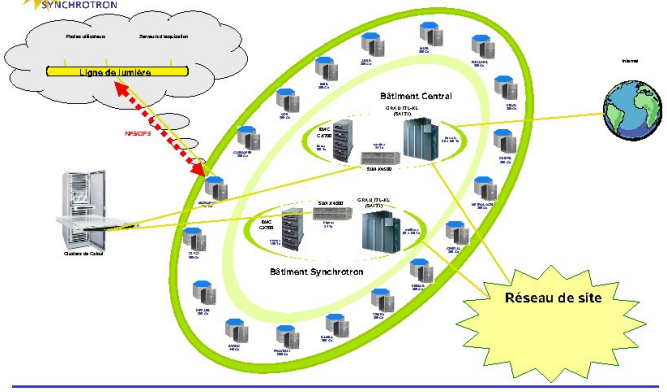
Synthèse des besoins

- Volumétries très différentes suivant les lignes de lumière (quelques Mo à quelques centaines de Go par jour)
- Durées de vie variables (de 2 semaines à "à vie" !)
  → Politiques de conservation différentes suivant le type d'utilisateurs (visiteurs ou scientifiques Soleil)
- Disponibilité permanente de l'accès aux données
- Accessibilité multi-réseaux
- Exportation des données pour les visiteurs : média ou réseau
- Archivage des données très peu accédées
- Hierarchisation (données critiques, primaires, secondaires, archives)
- Contrainte géographique (distances salles et lignesde lumière)



Objectifs

Architecture matérielle



Architecture matérielle

- Point d'accès des lignes de lumière sur serveurs autonomes (DELL), 300 Go à 1,8 To de disques SCSI
- Points d'accès salles informatique (DELL)
- Stockage des données primaires assuré par des baies de disques EMC (40 To puis 150 To)
- Stockage des données secondaires assuré par des librairies de bandes GRAU de 1344 slots : bandes LTO3 (400 Go à 800 Go) et SAIT1 (500 Go à 1300 Go)
- Réseau de stockage Gigabit IP dédié (fibre optique)

La politique de stockage

- Les données sont déposées sur les points d'accès des lignes de lumière ou depuis le cluster de calcul
- Elles sont copiées très vite sur les 2 baies de disques EMC et les 2 libraires de bandes GRAU
- La donnée reste dans le cache local 4 jours minimum
- Au bout de 100 jours, les 2 copies EMC expirent ; restent alors les 2 copies bandes
- Les 2 copies bandes expirent au bout de 1 à 5 ans suivant les systèmes de fichiers
- L'utilisateur demande alors au préalable un archivage de ses données s'il le souhaite
- A chaque "rupture de technologie", on reverra avec la ligne de lumière concernée si on pérennise ou pas les données.

Solution retenue

- Coeur de la solution = système de stockage cellulaire distribué ACTIVE CIRCLE
- Un seul noyau - identique sur toutes les machines - qui intègre :
  - ✓ sauvegarde en continu
  - ✓ réplication
  - ✓ stockage hiérarchique
  - ✓ stockage multi-sites
  - ✓ haute disponibilité

Raisons du choix

- Solution technique ayant le plus de perspectives intéressantes
- Evolutivité : architecture très extensible dans un environnement ouvert
- Robustesse : forte redondance offrant un niveau de réplication important, une sécurisation et une haute disponibilité des données
- Fonctionnalités : solution répondant à tous les objectifs, dont l'archivage intégré au format 'tar'
- À l'époque, capacité de DEVOTEAM à assurer la maîtrise d'oeuvre et à féderer les différents acteurs
- Meilleur prix au Téraoctet
- Capacité : des volumétries potentielles permettant largement d'anticiper les besoins

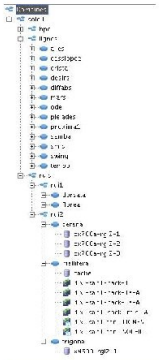
Mise en place

- Plateforme de référence utilisée depuis février 2006
- Début du déploiement en mai 2006
- Tests avec les premières lignes depuis septembre 2006
- Acceptance le 18 octobre 2006
- VSR signifiée le 18 décembre 2006 : validation de la disponibilité des données et de la fiabilité du matériel
- Début de la production des 7 premières lignes en janvier 2007
- Installation de 5 autres lignes début 2007
- Installation de 5 autres lignes 2nd semestre 2007
- … jusqu'à 24 à 26 lignes fin 2009

Bilan

- Engagements pris par ACTIVE CIRCLE respectés, même si parfois différés
- Très bonne réactivité grâce à des outils de debugging très complets qui permettent une compréhension rapide des problèmes
  --> corrections vite disponibles
- Bonne méthologie de travail : peu de régressions malgré le grand nombre de mises à jour et correctifs depuis 2 ans
- Dans la phase initiale, de nombreux bugs trouvés à la fois sur la plateforme de référence et celle de production, corrigés assez vite.
- La compétence, le sérieux et l'honneteté des intervenants a conforté notre confiance ; l'arrivée de Philippe Motet comme directeur technique en juillet 2006 a été très importante, à la fois dans les orientations techniques et dans l'organisation et la rigueur du support.
- Robustesse améliorée de jour en jour au cours des 2 premières années.

Situation chiffrée actuelle



- Version 3.1.2p29
- 28 cellules installées : 3 dans chaque salle informatique, 20 lignes de lumière, 2 contrôle machine
- ~ 5 millions de fichiers
- Plus de 16 Teraoctets, copiés 4 fois (sans historisation) et archivés 2 fois
- Près de 60 partages différents
- Plusieurs centaines de Go écrits/lus par jour quand le faisceau est disponible
- Pour chaque baie EMC : 150 To
- Pour chaque librairie GRAU :

LTO3	530 To à 1 Po
SAIT1	672 To à 1,7 Po

A venir ...

- Système de cache circulaire complet
- Encore de gros besoins d'outils d'exploitation plus ergonomiques : tableau de bord opérateur, statistiques, rechargement de configuration, centralisation de paramètres
- Meilleur ordonnancement des lecteurs de bandes
- Couche système de fichiers "vfs"
- Nécéssité d'avoir des outils d'analyse plus simples
- Optimisation du démarrage en parallélisant certaines taches

Conclusion

- Une solution novatrice : un choix "réfléchi" et mesuré entouré d'un nombre important d'engagements et garanties
- La mieux adaptée à notre architecture géographique et nos besoins : le « circle » colle bien à « l'anneau » !
- Un "cercle humain actif" au service du rayonnement de notre projet

ACTIVE CIRCLE

Système de Stockage Sécurisé et Distribué

Philippe Boyon

philippe.boyon@active-circle.com

ACTIVE CIRCLE – QUI SOMMES NOUS?

- Editeur français, spécialiste du stockage de fichiers et de la gestion de données
- Notre produit : un **système de stockage sécurisé et distribué** conçu pour aider nos client à stocker, protéger et gérer des volumes de contenu numérique en forte croissance
- Lignes directrices : simplifier le stockage, devenir indépendant du matériel, baisser les coûts
- Nos clients : IGN, Synchrotron Soleil, Orange, Beicip-Franlab, Observatoire de Paris …

ACTIVE CIRCLE

ACTIVE CIRCLE

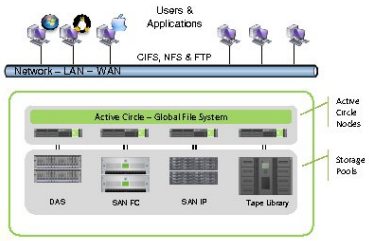
UNE PLATE-FORME LOGICIELLE CONÇUE POUR LE STOCKAGE, L'ARCHIVAGE ET LA GESTION DE GRANDS VOLUMES DE DONNÉES NUMÉRIQUES

Architecture

- Plate-forme logicielle compatible avec tout serveur x86
- Support de toute technologie disque ou librairie de bandes
- Architecture distribuée sur LAN ou WAN
- Accès via protocoles NFS, CIFS, FTP ou via API

Des Services embarqués

- Pour **protéger** les données
- Pour **gérer** le cycle de vie
- Pour **superviser** le stockage



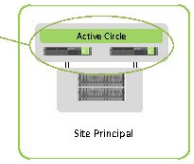
Active Circle –Storage for Digital Content Architecture

ACTIVE CIRCLE PROTÈGE LES DONNÉES

PROTECTION, HAUTE DISPONIBILITÉ ET PLAN DE CONTINUITÉ

Active Circle intègre les Services de protection des données

- Haute disponibilité du service

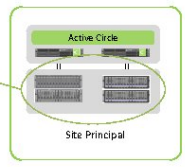


ACTIVE CIRCLE PROTÈGE LES DONNÉES

PROTECTION, HAUTE DISPONIBILITÉ ET PLAN DE CONTINUITÉ

Active Circle intègre les Services de protection des données

- Haute disponibilité du service
- **Haute disponibilité du stockage**

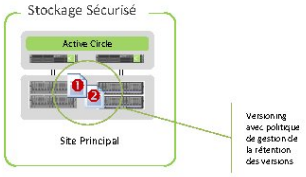


ACTIVE CIRCLE PROTÈGE LES DONNÉES

PROTECTION, HAUTE DISPONIBILITÉ ET PLAN DE CONTINUITÉ

Active Circle intègre les Services de protection des données

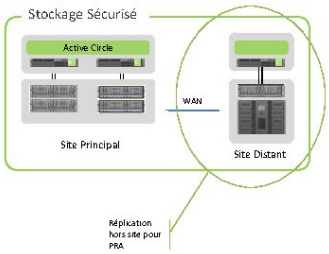
- Haute disponibilité du service
- Haute disponibilité du stockage
- **Protection en continu par versioning**



ACTIVE CIRCLE PROTÈGE LES DONNÉES
PROTECTION, HAUTE DISPONIBILITÉ ET PLAN DE CONTINUITÉ

Active Circle intègre les Services de protection des données

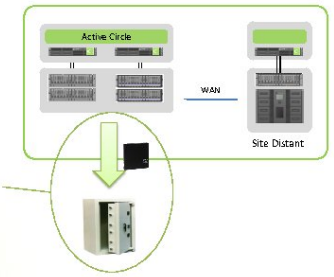
- Haute disponibilité du service
- Haute disponibilité du stockage
- Protection en continu par versioning
- **Réplication hors site pour plan de reprise d'activité**



ACTIVE CIRCLE PROTÈGE LES DONNÉES
PROTECTION, HAUTE DISPONIBILITÉ ET PLAN DE CONTINUITÉ

Active Circle intègre les Services de protection des données

- Haute disponibilité du service
- Haute disponibilité du stockage
- Protection en continu par versioning
- Réplication hors site pour plan de reprise d'activité
- **Export de données au format standard pour mise au coffre**

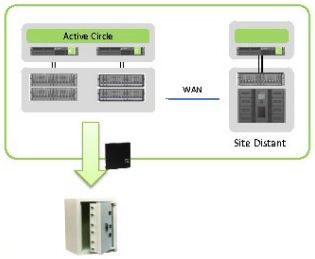


ACTIVE CIRCLE PROTÈGE LES DONNÉES
PROTECTION, HAUTE DISPONIBILITÉ ET PLAN DE CONTINUITÉ

Active Circle intègre les Services de protection des données

- Haute disponibilité du service
- Haute disponibilité du stockage
- Protection en continu par versioning
- Réplication hors site pour plan de reprise d'activité
- Export de données au format standard pour mise au coffre

Gestion entièrement automatisée par les Classes de Service

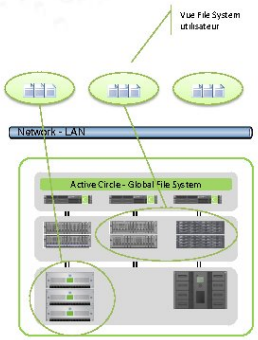


ACTIVE CIRCLE
GÈRE LE CYCLE DE VIE DES DONNÉES

Active Circle gère la localisation et le cycle de vie des données

- **Espaces de stockages sur pools rapides ou capacitifs**
- Espaces de stockage hiérarchisés
- Règles de déplacement sur critère de rétention
- Support du disque et de la bande

La gestion est automatisée par Classes de Service

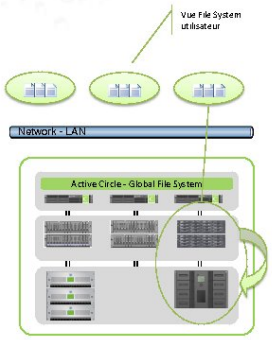


ACTIVE CIRCLE
GÈRE LE CYCLE DE VIE DES DONNÉES

Active Circle gère la localisation et le cycle de vie des données

- Espaces de stockages sur pools rapides ou capacitifs
- **Espaces de stockage hiérarchisés**
- **Règles de déplacement sur critère de rétention**
- **Support du disque et de la bande**

La gestion est automatisée par Classes de Service



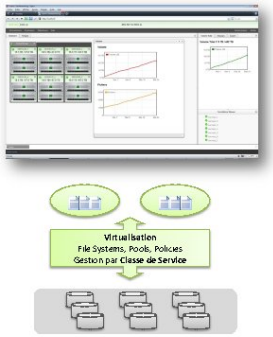
ACTIVE CIRCLE
SUPERVISION DES DONNÉES ET DU STOCKAGE

Le système Active Circle est auto-géré par des Classes de Service

- Gestion par règles, pas par action (placement des données, réplication, versioning, stockage hiérarchisé…)
- Système auto-réparant en cas d'incident
- Envoi d'alarmes et emails en cas d'incident ou de manque de ressource

Supervision des données et du stockage

- Un seul outil pour superviser les espaces de données virtualisés et les espaces de stockage
- Supervision des quotas, du remplissage, permettant d'anticiper (provisioning) et d'allouer de l'espace à la demande



EXEMPLES D'UTILISATION

Archivage Actif – Stockage de grands volumes de données

Consolider le service de fichiers

Partager des données sur plusieurs sites

ACTIVE CIRCLE

ARCHIVAGE ACTIF – STOCKAGE LONG TERME

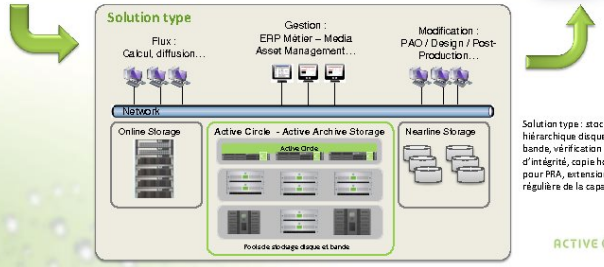
DE GRANDS VOLUMES DE CONTENU VIDÉO, AUDIO, IMAGES OU DONNÉES TECHNIQUES

Quels besoins ?

- Stockage très capacitif (10 TO – PO) et optimisé
- Archivage Actif : les données sont accessibles
- Garantie d'intégrité des données
- Evolutivité et scalabilité à chaud
- Si possible approche non propriétaire

Où? Exemples Clients

Audiovisuel, métiers de l'image, gros producteurs de données techniques, science et recherche



ACTIVE CIRCLE

CONSOLIDER LE SERVICE DE FICHIERS

POUR TOUS LES BESOINS DES UTILISATEURS ET DU SERVICE INFORMATIQUE

Quels Besoins ?

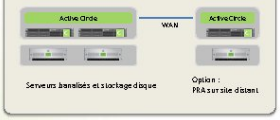
- Consolider le service de fichiers
- Stocker des fichiers utilisateurs, des exports de bases de données, des images de machines virtuelles… 1 à 10 TO
- Protéger les données via un outil de Backup
- Éventuellement Plan de Reprise d'Activité

Exemples Clients

Presse, collectivités territoriales, PME… qui stockent des données utilisateurs, des fichiers PAO, des sauvegardes

Solution Type → File Server Edition

Configuration type : serveurs banalisés, haute disponibilité, versioning, option PRA.



ACTIVE CIRCLE

PARTAGER DES DONNÉES

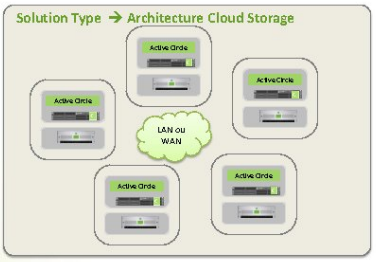
SUR PLUSIEURS SITES EN LAN OU WAN

Quels Besoins ?

- Stockage **local** pour accès immédiat et performant
- Réplication pour partage et sécurisation
- Réseau local ou distant
- Gestion des accès et des locks distribués

Solution type : nœuds de stockage sur LAN ou WAN, stockage disque, activation du Lock Manager

Solution Type → Architecture Cloud Storage



ACTIVE CIRCLE

ACTIVE CIRCLE – A RETENIR

Une Plate-forme Logicielle pour le Stockage de Fichiers

- **Virtualisée, distribuée et extensible** (Scalable)
- Compatible avec tout **type de matériel de stockage**

Avec des Services embarqués

- Pour **protéger** les données
- Pour **gérer le cycle de vie**
- Pour **superviser** le stockage

Utilisée pour

- **L'Archivage Actif** de grands volumes de données
- **Consolider et simplifier** le stockage de fichier
- **Distribuer et partager** les données sur plusieurs sites

ACTIVE CIRCLE

TÉMOIGNAGE UTILISATEUR SYNCHROTRON SOLEIL

ACTIVE CIRCLE

2.4 Nicolas Ruff (EADS IW)

Virtualiser pour mieux sécuriser ?

La virtualisation, sous ses multiples formes, envahit progressivement les différents domaines du système d'information. Sans être exempte de risque, chacune de ces solutions peut apporter, de façon différente, plus de sécurité aux utilisateurs et aux administrateurs de serveurs Les nouvelles offres, souvent gratuites comme, par exemple, le « Webmail », le « Software As A System » et le « Cloud Computing » posent un vrai problème de confidentialité, d'intégrité et de dépossession de ses propres données. Monsieur Nicolas Ruff, expert en sécurité, nous donnera un témoignage fondé sur sa propre expérience dans ce domaine ainsi qu'une connaissance beaucoup plus objective sur ces nouvelles technologies afin de ne pas succomber au chant des sirènes.

EADS

EADS INNOVATION WORKS

Virtualiser pour mieux sécuriser ?

Nicolas RUFF
nicolas.ruff (à) eads.net

EADS

Introduction

- La virtualisation est partout
  - Outils pour sécuriser la navigation sur Internet
  - Virtualisation d'applications
  - Virtualisation de systèmes
  - Infrastructures de *Cloud Computing*
  - Etc.
- La question de la sécurité est maintenant posée
  - N'est-ce pas un peu trop tard ?

EADS

Définition

- Comment définir la virtualisation ?
  - *"En informatique, on appelle virtualisation l'ensemble des techniques **matérielles et/ou logicielles** qui permettent de faire fonctionner sur une seule machine **plusieurs systèmes d'exploitation** et/ou **plusieurs applications**, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes."*
  - Source: Wikipedia
    - http://fr.wikipedia.org/wiki/Virtualisation
- Ceci étant dit …

EADS

Définition

Applicatif/Spécialisé
- Ne fonctionne que pour une application donnée, analysée en laboratoire
- Repose en général des points de contrôle précis à l'intérieur de l'application
- Ex. "bac à sable" pour Internet Explorer

Applicatif/Générique
- Fonctionne pour toute application en mode utilisateur
- Repose en général sur une interception des appels système
- Ex. Microsoft App-V, fonction native de Vista, …

Système/Spécialisé
- "Para" virtualisation
- Nécessite une adaptation de l'invité
- Ex. Xen

Système/Générique
- "Full" virtualisation
- Pas de modification de l'invité nécessaire
- Ex. VMWare, Hyper-V, Virtual PC/Virtual Server … mais aussi Xen, Bochs, KVM, VirtualBox, …

EADS

Définition

- A signaler aussi dans le panorama actuel (*liste non exhaustive*)
  - Google Native Client (NaCl)
    - Nécessite une recompilation des applications
    - Exécution de code vérifiable dans un "bac à sable"
    - Même principe qu'une machine Java ou .NET … mais pour du code natif x86
  - Isolation "en espace utilisateur"
    - Ex. V-Server, OpenVZ, SecComp …
    - Solutions explorées par le projet OLPC et par Google
  - Virtualisation sur architectures non x86/x64
    - Ex. Produit Trango de virtualisation sur processeur ARM (racheté par VMWare)

EADS

Virtualisation et sécurité

- Il existe deux usages de la virtualisation
  - Le mauvais:
    - Mutualiser des ressources de sensibilité différente sur le même matériel
      - Ex. *Cloud Computing* hébergé chez des tiers
      - Cf. passif de l'hébergement Web mutualisé
  - Le bon:
    - Confiner les applications dangereuses ou non maitrisées pour limiter l'impact d'une compromission
    - Concept de « défense en profondeur »

EADS INNOVATION WORKS

Virtualisation et sécurité

- Pas la peine de rêver …
  - La sécurité à 100% n'existe pas
    - Y compris dans le domaine de la virtualisation
  - Exemples
    - VMWare
      - Attaque "CloudBurst"
    - Hyper-V
      - Preuve semi-formelle de l'hyperviseur
      - … et pourtant il existe des bogues ! (cf. KB967902)
      - La partition "racine" est un bon vieux Windows (cf. KB970089)

EADS INNOVATION WORKS

Virtualisation et sécurité

- Projet ANR "SEC&SI"
  - Solutions proposées:
    1. Virtualisation applicative: Vserver
    2. Virtualisation système: Xen
    3. MAC
  - Note: des failles ont été trouvées dans toutes les solutions
- Affaire "LxLabs"
  - 100,000 sites compromis
    - http://www.theregister.co.uk/2009/06/08/webhost_attack/
  - Le développeur principal se suicide !
    - http://www.channelregister.co.uk/2009/06/09/lxlabs_funder_death/

EADS INNOVATION WORKS

Conclusion (sous forme d'analyse de risques)

- Les failles existent … et existeront
- Seul le fournisseur de la solution de virtualisation peut agir sur les risques
  - Sauf pour les solutions Open Source (ex. VirtualBox)
  - Il n'existe pas de logiciel de sécurité tiers intégrable à une solution de virtualisation
    - A venir: VMSafe
    - Mais ajouter un antivirus dans l'hyperviseur, est-ce vraiment une bonne idée ?
- Il ne faut pas que l'impact d'une « évasion » de la machine virtuelle soit catastrophique
  - Sinon ne virtualisez pas ☺

EADS INNOVATION WORKS

Questions ?

2.5 Daniel Dezulier (France Telecom Orange)

Comment gérer la sécurité de tous les systèmes d'information de différents grands comptes avec méthode ?

Monsieur Daniel Dezulier responsable sécurité du Système d'Information au sein du Groupe France Télécom Orange parlera des principes de bonne conduite appliqués en matière de sécurité à l'administration et à la gestion de l'ensemble des systèmes d'information de grands comptes hébergés dans les salles blanches de l'opérateur. Ces différents principes l'ont amené à mettre en place et à utiliser un véritable référentiel ITIL de la sécurité des systèmes d'information qu'il juge incontournable à ce niveau de responsabilité.

Gestion de la sécurité par la gestion du changement

Jeudi 11 juin 2009 - Séminaire Aristote - Ecole Polytechnique - Palaiseau

Daniel DEZULIER

Sommaire

- Le Groupe et sa transformation
- Etre leader : quelles contraintes ?
- Quelques chiffres pour comprendre
- Les réponses organisationnelles et opérationnelles
- Exemples

Le Groupe et sa transformation

« En 2006, le groupe France Télécom a concrétisé sa transformation par la mise en place d'une nouvelle organisation. Celle-ci s'appuie sur deux principes : placer le client au centre des priorités de chacun et accroître l'efficacité du groupe grâce à l'adoption d'une structure matricielle. »

« L'achèvement du plan NExT (Nouvelle Expérience des Télécoms) qui a couvert les années 2006 à 2008 confirme la réussite de la profonde transformation entreprise par France Télécom-Orange. La période actuelle se caractérise pour le Groupe par une accélération de la mutation de son écosystème, largement anticipée et intégrée dans la stratégie NExT et servie par une organisation adaptée »

« Avec Orange 2012, le Groupe confirme la validité de sa stratégie et adapte ses modes d'action pour atteindre un objectif ambitieux de génération de cash flow organique. Les actions mises en oeuvre dans ce cadre s'organisent autour de trois grands axes : simplicité, agilité et performance durable. »

Un Groupe Leader : des contraintes concurrentielles et règlementaires

- Contraintes règlementaires liées à la concurrence
- Contraintes règlementaires liées aux marchés LSF, SOX
- Contraintes juridiques liées aux contenus, aux usages
- Contraintes sécurité résultant de la position sur le secteur
- Contraintes sécurité résultants de la multiplicité et de l'évolutivité des supports de contenus

Nécessité d'introduire les contraintes au plus tôt dans tous les processus

Quelques chiffres pour comprendre

- Environ x 000 000 000 000 000 octets de stockage (péta-octets)
- 182 000 000 clients dans 30 pays
- 122 000 000 clients de l'offre mobile dans le monde
- 13 000 000 clients ADSL en Europe
- 180 000 stations dont 150 000 sous Windows
- 20 000 serveurs dont 3600 sous Windows
- 10 000 routeurs et commutateurs réseau
- 1400 applications interfacées
- 1200 sites dont 800 accueillant du public

Réponses organisationnelles et opérationnelles

- Maitrise du risque
- Convergence
- Normalisation
- Homogénéisation
- Exemples
- Résultats

Maitrise du risque : un enjeu

- Maitrise de la sécurité
  - Identification du risque ⇔ cartographie, analyse, stratégie
  - Identification des moyens d'action
    - Information et politique de sécurité ⇔ cohérence
    - Processus et acteurs ⇔ compétence
    - Architectures matérielles et logicielles ⇔ efficience
- Anticipation et suivi continu, externe et interne
  - Mise sous assurance qualité
  - Contrôle SOX
  - Contrôle Interne
  - Veille technologique internet et externe : CERT-IST

Convergence : une exigence économique

- Un grand nombre de pays, d'entités et de métiers
  - Une architecture unifiée et/ou compatible
  - Réduction du nombre de configurations (station / serveurs)
  - Centralisation des serveurs en Data Center, virtualisation
  - Achats « Corp. »
- Convergence : un retour sur investissement sensible
  - Réduction des coûts de développement et de maintenance matérielle et logicielle.
  - Gains réalisés par le choix de composants standards
  - Gains réalisés sur la durée du cycle de développement
  - Maitrise de la configuration logicielle sur le parc
  - Maitrise des paramètres relatifs à la sécurité
  - Amélioration de la qualité de service et du soutien

Normalisation du système d'information

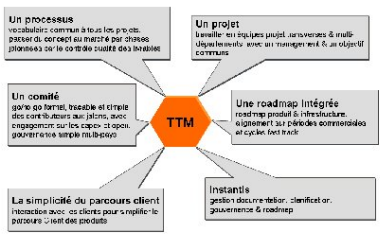
- Normalisation de l'architecture au niveau « Corporate »
  - Comité de validation des architectures, incluant la validation sécurité
  - Dossier d'architecture pour chaque projet, incluant les exigences de sécurité
  - Animation d'un collège d'architectes techniques et applicatifs
  - Création d'un « standard » serveur et d'un « standard » poste de travail : concept GCC ⇔ Group Core Component
  - Mise en place d'un réseau « sans couture » et de sa protection
- D'une informatique dispersée à une informatique distribuée
  - Création d'un référentiel applicatif;
  - Qualification systématique du logiciel et versionnage applicatif,
  - Mise en place d'une distribution des applications; utilisation de signatures applicative;

Homogénéisation des méthodes et prescriptions

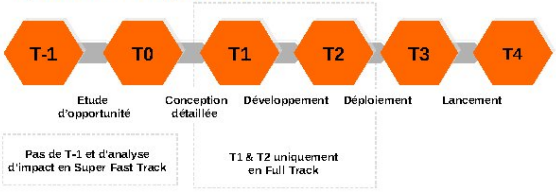
- **Homogénéisation des méthodes de conduite de projets**
  - 2000 -2006 : Projet « Agathone » ⇔ Normalisation de la conduite de projet, démarche qualité
  - 2006 - 2009 : Méthode Time To Market de pilotage de projet
- **Homogénéisation des règles de sécurité**
  - Rédaction et applications de règles ou prescriptions
  - Insertions des clauses sécurité dans les contrats et dans les dossiers d'architecture
- **Homogénéisation des bonnes pratiques de mise en production**
  - Convergence naturelle avec la Méthode ITIL de conduite du changement opérationnel
  - gestion globale commune du référentiel ⇔ CMDB

TTM Une réponse concrète au besoin de réactivité

- Méthode orientée réactivité fournisseur et satisfaction client



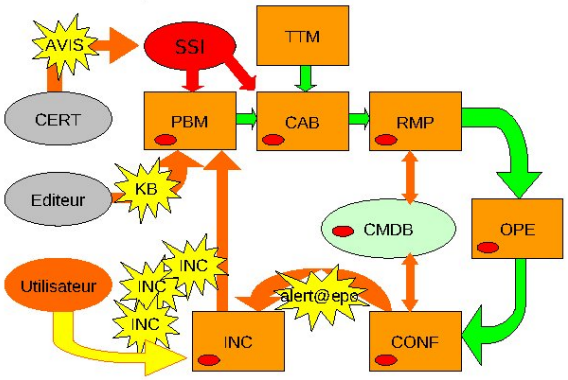
Simplicité : facteur de réussite
Cycle court : gage de réactivité



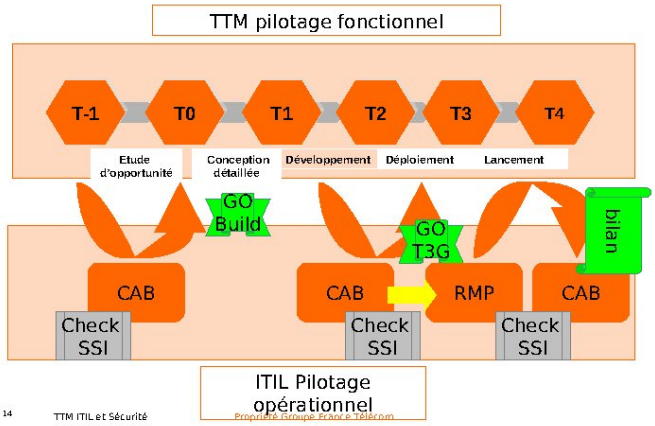
projets phasés
checklist de livrables
contrôles qualité à chaque jalon
options TTM adaptés à la complexité des projets

ITIL et fonction sécurité

Point d'ancrage/intervention de la fonction sécurité



Interopérabilité TTM ITIL



Organisation pour l'architecture technique sécurité pour le domaine France

- Maitrise d'ouvrage Groupe : Architectes Réseaux et Systèmes d'Information :
  - Choix des briques de sécurité et prescriptions de sécurité;
  - Evolution des briques tenant compte de l'évolution des menaces;
- Maitrise d'ouvrage sécurité poste de travail Direction de l'infogérance
  - Utilisation du GCC « eburo »
  - Utilisation des GCC Sécurité (antivirus, PKI groupe, ...)
  - Collecte des besoins métiers et utilisateurs
  - Promotion de nouvelles fonctionnalités et services, suivant l'évolution des métiers
  - Choix des réglages
  - Pilotage du changement
  - Suivi des incidents et amélioration de l'efficacité et du ressenti utilisateur
  - Supervision des incidents stations
- Maitrise d'œuvre, exemple Direction des Plateformes de Service
  - Préparation de l'infrastructure;
  - Mise en place des bases et requêtes;
- Exploitant de l'infrastructure Direction Technique France
  - Administration des bases
  - Exploitation des serveurs
  - Mise en production des requêtes
  - Supervision du service
  - Supervision des incidents serveurs

Exemples de gestion de la sécurité

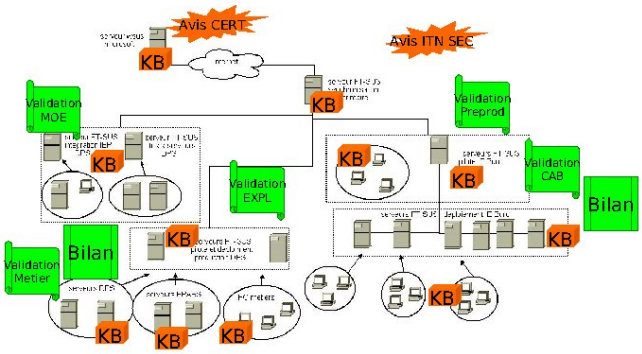
- Mise à jour programmée du système d'exploitation Windows
  - Request For Change Standard
- Protection contre les programmes malveillants
  - Demande de changement (RFC) systématique pour évolution du produits : nouvelles fonctionnalités face aux nouvelles menaces
- Prise en compte des avis de sécurité
  - Publication de nouvelles failles ou vulnérabilité
  - Publication d'avis d'exploitation des failles
  - Publication de correctifs ou de palliatifs
  - Analyse de risque et mise en œuvre d'une demande de changement urgent (Emergency CAB); incluant les préanalyses et tests en cycle court.

Sécurisation du système d'exploitation Windows

FTSUS = France Telecom Software Update System

- Homogénéisation du parc :
  - Une seule version cible Windows par socle (ex :station Windows XP + SP2 (SP3))
  - Un rattachement à une infrastructure d'alimentation
  - Des stratégies appliquées et verrouillées : par Active Directory
- Mise à jour automatique et pilotée :
  - Analyse continue des bulletins mensuels Microsoft et niveaux de criticité (Architecte, Infogéreur, Maitrise d'Œuvre, Exploitants)
  - Gestion du changement sous ITIL (CAB), pilotage Maitrise d'Ouvrage poste de ravail)
    - Test intégration de chaque correctif par la maitrise d'œuvre
    - Test pré-production de chaque correctif par l'infogéreur
    - Test complémentaire par chaque maitrise d'œuvre applicative
    - Pilote et bilan en CAB bas avant généralisation (jalon T3G)
    - Déploiement par zone de chalandise
    - Installation automatique ou manuelle négociée
    - Bilan du déploiement
- Gestion des alertes en Emergency CAB
  - Exemple : W32/Conficker gestion du changement en urgence pendant une période de « gel » des changements du système d'information (période de Noël)

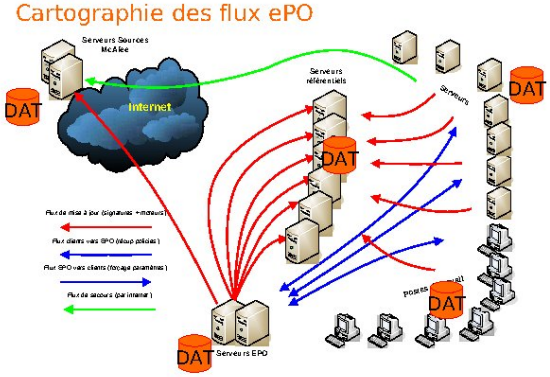
Sécurisation du système d'exploitation Architecture d'alimentation des correctifs



Protection contre les programmes malveillants des machines Windows

- Logiciel d'administration client serveur, push & pull
  - ePO : ePolicy Orchestrator (Mc Afee, Network Associates Inc.)
- Partie Cliente antivirus VirusScan ePO sur le poste de travail
  - Module antivirus
  - Module antispyware
  - Agent ePO supervise et administre les modules clients
- Partie Serveur ePO
  - Console ePO : supervise et administre les agents
  - Base SQL server
    - événements remontés par le parc
    - Stratégie de sécurité applicables aux parcs
    - description de l'organisation et droits associés
    - gestion des seuils et alertes
- Le référentiel (versions de logiciel, l'organisation)

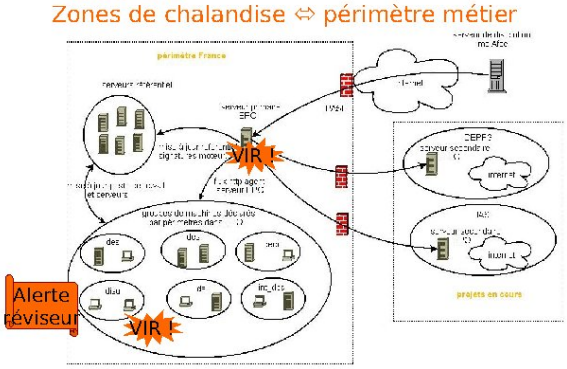
Protection contre les programmes malveillants Cartographie des flux ePO



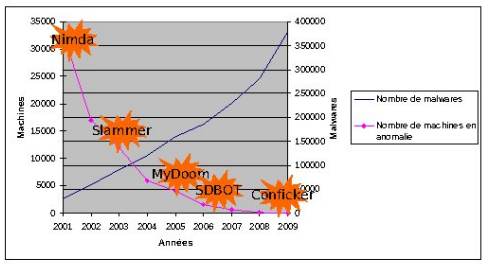
Pilotage ePO – processus SOX

- Le pilotage ePO est sous contrôle SOX dans le périmètre Infogéreur
- Réglages initiaux définis en mode projet (Infogéreur) : TTM + ITIL
  - Choix d'évolution des produits acquisition des nouvelles versions
  - Définition des stratégies,
  - Découpage des périmètres ou zones de chalandise (groupes de machines métier)
  - Inscription des responsables de zones : rôle de réviseur, délégation d'administration sur les groupes
  - Définition des stratégies par zones avec les responsables de zones
  - Définition des seuils d'alerte
- Gestion récurrente du changement (Infogéreur) : ITIL
  - Actualisation des stratégies,
  - Arbitrage des réglages des seuils de détection,
  - Amélioration continue du traitement des incidents,

Protection contre les programmes malveillants Zones de chalandise ⇔ périmètre métier



Convergence, normalisation, et méthodologie : des résultats probants



Autres exemples opérationnels de sécurité distribuée

- Interconnexion des partenaires et filiales
  - Filtrages spécifiques et « pack des services »
- Connexion des nomades (48000)
  - Business Everywhere : RTC; ADSL, WiFi, GSM, Edge, 3G
  - Certification PKI (Certetoo)
  - Chiffrement disque (postes sensibles) : Zone Central Primix
- Servers en Data Center
  - Authentification faible & Authentification forte
  - Relais applicatif
- Poste de travail en boutique (28000)
  - Terminal léger en déport d'écran
  - Pas de copie locale des données

Merci !

2.6 Raphaël Marichez (HSC)

Les DSI du public et du privé face à la sécurité distribuée

Monsieur Raphaël Marichez de HSC, au travers d'un bilan de la matinée, synthétisera les objectifs et les conséquences, en termes de sécurité de l'information, de la mise en oeuvre des solutions de sécurité distribuée. Au travers des habitudes, des cultures, et des principes directeurs des organismes du privé et du public, il présentera des méthodes utilisées par les DSI ou les RSSI pour optimiser l'emploi des solutions de sécurité dans leur structure. Quelques retours d'expériences choisis illustreront ensuite les différentes approches employées par les organismes publics et privés dans la prise en compte des évolutions de leur SI et dans la réponse aux incidents et aux risques SI, tant sur les aspects techniques que sur le management de la sécurité.

HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

aristote

La réponse des DSI et RSSI
à la sécurité distribuée

Raphaël Marichez
<Raphael.Marichez@hsc.fr>

Plan

- Bilan de la matinée
- Nouvelles technologies, nouveaux risques
- Une gestion de la SSI multi-acteurs
- Evolution récente et future du métier de RSSI

Les transparents seront disponibles sur www.hsc.fr

Bilan de la matinée

- Des méthodes répondant aux nouveaux besoins :
  - La gestion des utilisateurs
    - Besoin de mobilité et de souplesse
    - La politique de contrôle d'accès : selon le poste client ou l'utilisateur ?
  - La gestion du poste client
    - Une passoire
    - Séparer professionnel / privé : le poste client devient virtuel
- Distribuer pour mieux régner ?
  - Questions de fonds : Où ? Qui ? Responsabilités ?
  - A quand une gestion des prestataires de service ?

Bilan de la matinée

- Efficacité de ces méthodes ?
  - Risques résiduels
    - Etanchéité des VM, évasion, risques non traités par le prestataire...
  - Nouveaux risques
    - Mutualisation des ressources
      - Augmentation de la surface d'exposition
      - Augmentation de l'impact en cas d'incident
      - Traçabilité ?
    - Déposession des données
      - Localisation ?
      - Responsabilité ?
      - Traçabilité ?
  - Nouvelles méthodes
    - Bonnes pratiques, conformité, contrôle

Nouvelles technologies, nouveaux risques

- « Sécurité distribuée »
  - JRES 1999 Montpellier
- Complexité des infrastructures
  - Maîtrise de son activité ?
  - Dé-périmétrisation
    - Virtualisation des réseaux
  - Points d'accès externes
    - Télé-maintenance
      - « C'est quoi ce câble-là ? »
    - Prestataires / Partenaires
    - Infogérance

Nouvelles technologies, nouveaux risques

- « Infrastructures spontanées »
  - Ca **doit** marcher comme à la maison
  - La sécurite ne peut **plus** être un frein
    - => « Solution clé en main pour votre PRA »
    - => contournement de la DSI
    - => Google Apps, Services en ligne, BlueTooth, USB, ...

- Mélange des genres
  - Le test du PRA qui laisse un trou béant dans le firewall...
  - Un branchement de téléphone qui met à terre le réseau...
  - Un scanneur de vulnérabilités qui plante l'alarme incendie à 10.000 km...

- **Sécurité distribuée = sécurité diluée ?**

Nouvelles technologies, nouveaux risques

- Externaliser une partie de son activité
  - Externaliser les vulnérabilités
  - Distribuer pour être conforme
  - Titrisation de la sécurité
- Faites votre analyse de risques
  - On achète un produit... (site web)
  - ...qui intègre d'autres produits...
  - Hébergeur, backups, mail, DNS...
- Pyramide des risques
  - « Produits structurés » ?
- Perte de maîtrise : exemples
  - Sauvegardes externalisées
  - Test de vulnérabilité récurrent (TSAR) qui ne trouve jamais rien

Une gestion de la SSI multi-acteurs

- Le RSSI dans son organisme
  - Le RSSI est un vendeur
  - Il rend compte au DSI, ou au DG, selon le cas
    - De plus en plus souvent, au DG
    - Outils :
      - Appréciation de risques SI : **justification des budgets**
      - Guides de bonnes pratiques SSI reconnus
      - Système de management (SMSI) : amélioration continue (ISO 27001)
    - Moyens :
      - Point de vue externe (consultants) : indépendance ?
      - Faire mieux que les autres filiales / agences / régions / pays
      - Vulgarisation des risques SI (sensibilisation : ne pas oublier la DG)
      - Certifications (des personnes, des systèmes de management, des services)

Une gestion de la SSI multi-acteurs

- Le RSSI dans son organisme
  - Le RSSI est un acheteur
    - Produits, prestataires, infogérance
  - Marchés publics
    - Lourdeur : projets à échéance entre 9 mois et 2 ans
      - Mais la SSI a besoin de rapidité ! (deadlines : élections, ...)
    - Formalisme et dé-personnalisation de l'acte d'achat
      - Permet des relations plus cordiales avec les prestataires
      - Bien élaborer son CCTP sinon... c'est trop tard
  - Privé
    - Souple mais copinage possible

Une gestion de la SSI multi-acteurs

- Le RSSI en dehors de son organisme
  - Groupes sectoriels
    - Exemple : en milieu bancaire, les RSSI ont les mêmes problèmes
  - Associations
    - CLUSIF, OSSIR, Club 27001, …

  - Groupes restreints
    - GITSIS, Netfocus, …

  - Domaines connexes
    - Normalisation, FNTC...

    - Continuité d'activité, santé, données personnelles...
  - Associations régionales...

Une gestion de la SSI multi-acteurs

- Autour de l'organisme
  - La loi (pour tous)
    - Exemple : hygiène et sécurité au travail
  - La Défense
    - Protection pénale du secret de la Défense Nationale
    - Cascade HFDS → FSSI → AQSSI → RSSI → CFSSI
  - Le réglement sectoriel
    - Loi pour la Sécurité Financière, Bâle II, SOX, PCI-DSS...
    - La santé (CNAM, hôpitaux), les Douanes...
  - L'autorité ou la pression des clients, actionnaires ou utilisateurs
    - Certification, labellisation, contrôle ...

Evolution du métier de RSSI

- Distribution du SI
  - Le SI devient accessible depuis n'importe quel point du globe
  - Nombreux acteurs : les responsabilités sont ~~distribuées~~ diluées
  - Tous les métiers sont concernés
- Tout anticiper
  - Messagerie bloquée deux jours au Minefi pour un oubli sur l'anti-spam :

```
relaismsg.minefi.gouv.fr[194.250.149.46] said: 554 Service unavailable;
Client host [129.104.xx.xx] blocked using relays.ordb.org; ordb.org was
shut down on December 18, 2006. Please remove from your mailserver.
```

- Utiliser son budget
  - Justifier un budget précaire dans le privé
  - Optimiser l'emploi d'un budget rigide dans le public
- Avoir une vision long-termiste
  - vs. la vision « quarter » des CEO

Evolution du métier de RSSI

- Secteurs privés sensibles (banques, santé...)
  - Nombreux groupes de travail
- Collectivités locales
  - SSI très décentralisée, très en retard
  - Les RSSI des CG commencent à travailler ensemble... à imiter !
- Universités et recherche
  - Cas du CNRS : cadre SSI centralisé, réunions régulières des RSSI
  - RENATER impose un minimum de fait
- Dans tous les cas : **travaillez ensemble !**

Evolution du métier de RSSI

- Réaction à l'incident
  - Culture de la transparence vs. Culture du secret
  - Cas particulier en France : le CERT Renater
- Influences étrangères
  - Anglo-saxons : transparence, importance des données personnelles
    - En Californie : hôpital condamné à 250.000 $ d'amende le 15 mai dernier
    - Habitudes des utilisateurs : responsabilisation
    - Culture de l'intelligence économique

Evolution du métier de RSSI

- Le passé
  - La **conformité** : incite à déléguer (déplacer le problème)
  - Les rationalisations, les consolidations
  - → **Externalisation du SI**
    - Externalisation de la sécurité
- Aujourd'hui
  - La **Conformité** est progressivement remplacée par le **Contrôle**
    - Identifier les risques pour les **exprimer**
    - En prenant en compte la sécurité **externalisée**

Conclusion

- Le futur ?
  - Le RSSI dans un rôle central
    - De la sécurité des systèmes d'information à la **sécurité de l'information**
    - Quitte le giron de la DSI
  - Défense « en profondeur »
    - Pour réduire les risques encore et encore
  - Anticipation
    - **Connaître les risques et les réduire à un niveau acceptable**
  - **Demain : le RSSI distribué, mais pas dilué !**

2.7 Agostinho Rodrigues (Interdata)

Controle de l'activité et gestion des menaces dans un environnement réseau distribué

Pouvoir surveiller l'ensemble de la sécurité et activité des réseaux et permettre une détection en temps réel de toute anomalie grâce à une technologie basée sur l'analyse comportementale et la corrélation d'évènements (au niveau réseau et système). Monsieur Agostinho Rodrigues expert sécurité chez Interdata, présentera les avantages et bénéfices de la solution QRadar de Q1Labs, en particulier dans sa capacité à offrir une console de gestion unique pour l'analyse globale des évènements (Logs et Flows) et une détection intelligente des menaces de bout-en-bout sur le réseau.

Contrôle de l'Activité et Gestion des Menaces dans un environnement Réseau Distribué

INTERDATA – Présentation Q1Labs

Agostinho Rodrigues
Séminaire Aristote – 11 juin 2009

Les Problématiques Actuelles

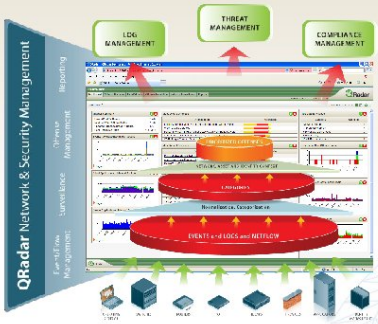
- **Volume d'informations provenant du SI**
  - Flux d'évènements provenant du réseau, des systèmes et des équipements de sécurité
  - Manque de compétence pour gérer des données disparates (multiples silos d'information)
- Menaces internes et externes en constante évolution
  - Malveillance interne, fraude, vol de propriété intellectuelle
  - Complexité croissante des attaques intégrées/distribuées
- Mise en conformité, Règlementations légales
  - Normes propres aux différents secteurs d'activité
  - Politiques internes de gestion des risques
- Coûts excessifs et croissants
  - Gestion manuelle, solutions inefficaces
  - Les offres de solutions SIEM de première génération sont coûteuses et complexes à mettre en oeuvre

La Réponse de Q1Labs

Vision Convergente du Réseau et de la Sécurité

- **Efficacité Opérationnelle:** Mise en oeuvre de contrôles du réseau et de la sécurité optimisés
- **Gestion des Menaces :** Détecter les nouvelles menaces que d'autres ne peuvent voir
- **Gestion des Evènements/Logs :** Collecte sécurisée, archivage, outils de recherche
- **Gestion de la conformité :** Respect des réglementations, politiques de sécurité

Architecture de la solution QRadar

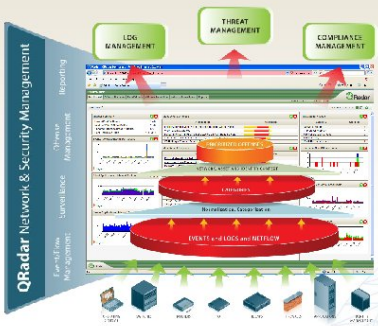


QRadar – Visibilité Réseau et Sécurité en temps-réel

- Collecte centralisée des données et visibilité globale
- Moteurs d'analyse et intelligence embarqués
- Classification/Priorisation des "Offenses"

Une solution efficace de gestion des évènements, des menaces et de la conformité

Architecture de la solution QRadar



QRadar – Visibilité Réseau et Sécurité en temps-réel

- Collecte centralisée des données et visibilité globale
- Moteurs d'analyse et intelligence embarqués
- Classification/Priorisation des "Offenses"

Une solution efficace de gestion des evenements, de gestion des menaces et de la conformité

---

1 - Gestion des Logs / Evènements

7

La Gestion des Logs

La collecte des évènements constitue l'élément fondamental d'une solution de Gestion Centralisée de **l'Activité** et la **Sécurité** du réseau

Les Défis:	Les Bonnes Pratiques:
➢ Volume de logs gigantesque	✓ Aggrégation de logs évolutive Archivage optimisé, intégrité des données
➢ Complexité des données	✓ Couverture la plus large des modèles et marques d'équipements, APIs souples pour intégrer les formats spécifiques
➢ Exigences Opérationnelles	✓ Flexibilité de déploiement et d'analyse, gestion de silos d'informations multiples

8

La Gestion des Logs: Les 5 principales exigences

1. Support des environnements Multi-Constructeurs
1. Profondeur d'analyse et de corrélation, réduction du "bruit"
   - Résultats directement exploitables
   - Taux de réduction significatif des évènements (aggrégation)
   - Filtres / Règles puissantes et faciles à personnaliser
2. Recherche, extraction de données
   - Fonctions intégrées de Reporting, Audit, Investigation
1. Simplicité d'évolution de l'architecture, Maîtrise des coûts
1. Flexibilité, évolutivité fonctionnelle
   - Capacité à répondre à d'autres besoins, non limité à une simple gestion des Logs

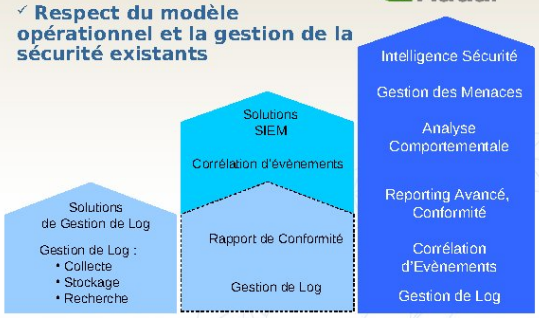
9

Solutions de Gestion des Logs: Evolution et Croissance

Bénéfices Qradar:

✓ **Gestion de Logs avancée, Richesse fonctionnelle**

✓ **Respect du modèle opérationnel et la gestion de la sécurité existants**



10

2 – Gestion des Menaces, Intelligence Sécurité

11

Au delà d'une simple Gestion des Evènements …

- Détection automatique des menaces en exploitant les informations et données traditionnellement disséminées :
  - Activité Réseau (commutateurs, routeurs)
  - Evènements de sécurité (Pare-feux, VPN, IDS/IPS, scanners de vulnerabilité …).
  - Monitoring et analyse applicative (Logs "flow" niveau réseau et application)
  - Identité, contexte utilisateur (annuaires AD, LDAP …)

Seule une Visibilité Totale et une "Intelligence Sécurité" peut garantir une détection et une réponse efficaces aux menaces sur votre réseau

12

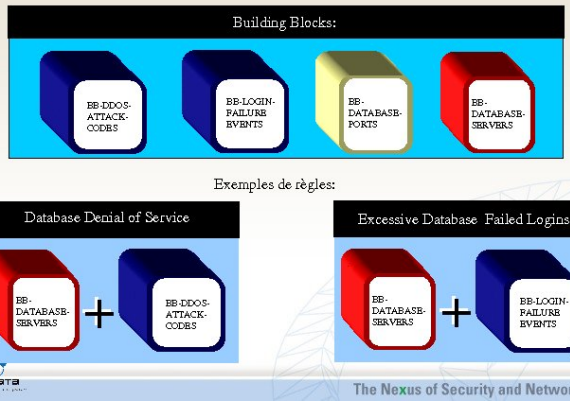
Moteurs d'analyse et Intelligence intégrée

Indispensable pour tirer profit de la richesse des données collectées

Les défis :	La réponse Qradar :
➢ Les règles de corrélation peuvent être complexes à gérer	✓ Gestion simplifiée par des jeux de règles et "building blocks" configurés et installés de base
➢ Diversité et évolution des formats de Logs constructeur	✓ Exploitation des données historiques et de modélisation (profiling) pour des résultats plus précis et plus fiables
➢ Réseaux en perpétuelle modification	✓ Exploitation des données historiques et de modélisation (profiling) pour des résultats plus précis et plus fiables

13

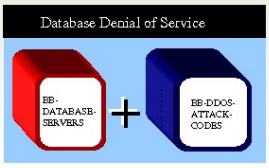
Intelligence intégrée: Règles & "Building Blocks"



14

Détection avancée des Menaces Actions et Réponses

Exemple de règle:

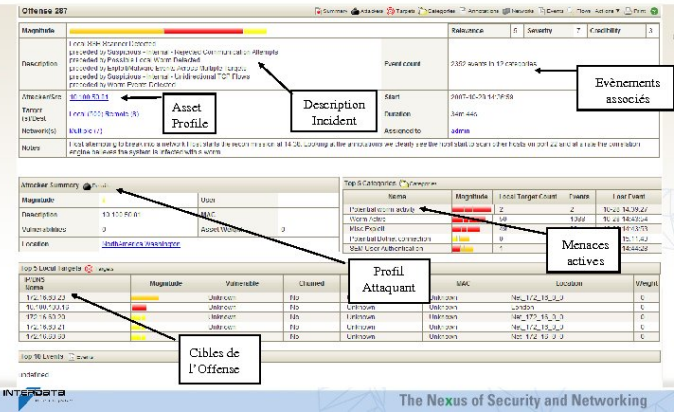


Les Actions/Réponses déclenchables au niveau des règles :

- Notification Administrateur
- Envoi d'email
- Création d'une "Offense"
- Remédiation de l' "Offense"

15

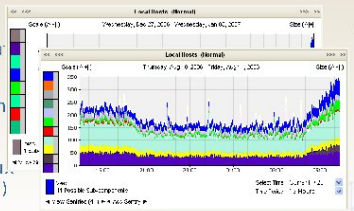
Gestion des "Offenses" : Contexte et historique d'une menace



16

Collecteurs de " Flow " Monitoring des flux réseau

- Améliore la découverte et la créa automatique des actifs réseau
- Détection d'éléments non référen ou "pirates"
- Surveillance de la matrice des flu (conforme à la politique établie ?)
- Traçabilité de tous les flux générés par un "attaquant" (qu'il ait ou non déclenché un événement/alerte)
- Détection d'attaques de type "zero-day" (non associées à une signature)



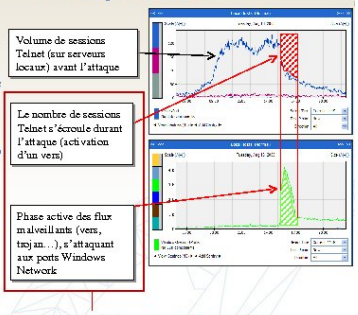
Meilleure Visibilité, Contrôle de l'activité réseau

17

Visibilité Réseau, Détection d'Anomalie

- Les messages "Flow" sont produits nativement par l'infrastructure réseau, et gérés par QRadar
  - Cisco, Juniper, Foundry, Extreme, Nortel, Alcatel-Lucent, HP, Enterasys
- Monitoring essentiellement L3-L4 (basé sur protocoles NetFlow, J-Flow, s-Flow, IPFix)
- Qradar: Facilité d'exploitation, visualisation contextuelle (drill-down…) pour investigations/audits simples et performants
- Analyse du comportement et détection des anomalies réseau
  - "Ecarts" de politique interne
  - Alertes selon des règles, seuils… (personnalisables)
- Visibilité globale, Analyse centralisée des "Flow" provenant de toute partie du réseau,

Un exemple de détection:



Corrélation des évènements => Détection d'une « offense » de type « Worm Outbreak »

18

QRadar " QFlow " Monitoring des Flux Applicatifs (L7)

- Complète la technologie Qradar de fonctions clés:
  - Détection des applications niveau 7
  - Analyse comportementale, détection d'anomalie
  - Contrôle de la politique interne (au niveau flux, sécurité…)
  - Fournit plus de contenu pour les recherches, investigations, audits
  - Intégrable avec des solutions "Flow" tierce-partie
- Basée sur le déploiement de sondes QRadar "Qflow" aux points stratégiques du réseau
- Enrichit la connaissance Réseau de la solution Qradar

Différentiateur majeur vis-à-vis des solutions concurrentes

19

QLabs

3 - Règlementation / Conformité

(Outils de Recherches & Reporting)

20

QLabs

Règlementations / Conformité

Règlementations	PCI HIPAA GLBA FISMA NERC SOX Fonctionnalités Compliance	Sécurité et Confor QRadarmité Bénéfices QRadar Total Network
Politiques de Sécurité	CobiT, ISO 17799, Interne ... Control Objectives	•Compliance workflow
Audits Reporting	Compliance Templates / Forensics Search / Policy Reporting	•Compliance reporting •Deep forensic analysis
Application de la Politique		•Auto remediate threats •Compliance based "offenses" •Enforce application policy
Analyse des Risques		•Integrated behavior analysis •Asset based profiling •Network, asset, & identity context
Gestion Des Logs	EVENTS and LOGS and NETFLOW	•Integrity - SHA hashing •Redundancy - Raid 10 •Reliability - Backup/restore
Collecte des Log / Evènements		•Unrivalled visibility •Secure data collection

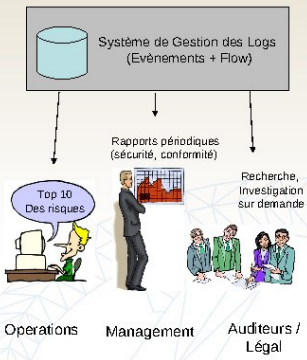
21

QLabs

Reporting & Audits

Fonctions intégrées de Reporting, Audit, et Recherche d'informations:

- Couvrent l'ensemble des besoins de l'entreprise
  - Réseau, Sécurité, Management, Direction, Auditeurs ...
- Outil de Création et Génération de Rapports simple et flexible
- Rapports d'analyse temps-réel et long-terme (suivi des tendances)
- Planification des rapports pour des informations
  - Automatisation de l'édition et de la diffusion
  - Génération ponctuelle (à la demande)

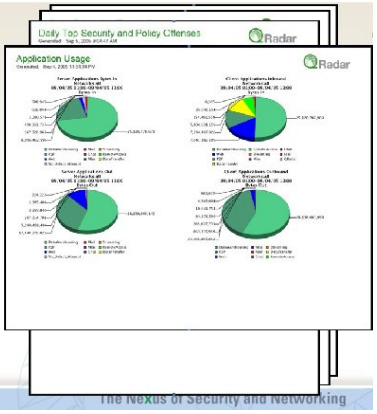


22

QLabs

Capacités de Reporting

- Reporting extrêmement flexible, basé sur des requêtes multi-critères
- Aggrégation dynamique des champs clés
  - Source, Destination
  - Protocole
  - Port
  - Username
  - Type d'évènement ...
- Aggrégation des données (compteurs) les plus importantes
  - Nbre d'évènements, Octets, Paquets
- Peuvent être pré-filtrés pour accélérer la génération des rapports, avec indexation automatique de tous les champs clé
- Rapports par groupe d'équipements



23

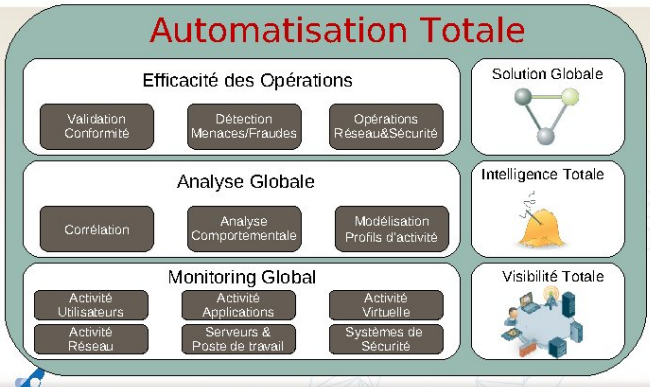
QLabs

En Résumé ...

24

QLabs

Intelligence Globale dans une Solution Unique



25

QRadar : Automatisation Totale

Exploitants: *Déploiement et Gestion automatique*

Analystes: *Priorisation automatique*

Auditeurs: *Reporting automatique*

Directions: *Réduction des coûts*

Monitor | Analyse | Action

- Auto-découverte des Log sources
- Auto-découv. des Applications
- Auto-découverte des Actifs
- Auto-groupement des Actifs
- Gestion des Logs Centralisée
- Auto-Tuning
- Auto-Détection des Menaces
- Milliers de Règles pré-définies
- Recherche d'évènements simple
- Moteur d'Analyse Sécurité Avancé
- Milliers de Rapports Pré-définis
- Priorisation basée sur les Actifs
- MAJ Auto des Menaces
- Réponses / Actions Automatiques
- Remédiation Ciblée

The Nexus of Security and Networking

26

Exemple de Cas Client: Supervision Sécurité Réseau Globale

Réseau d'Entreprise étendu:
- + de 20 000 serveurs
- 9000 Switchs & Routeurs

- ✓ 475 millions de logs (évènements & Flows) quotidiens, réduits à 10 offenses par jour
- ✓ Gains de Productivité en terme d'exploitation et supervision:
  - Nécessite moins de ressources pour les tâches quotidiennes
  - Optimise l'efficacité des équipes en place, sans obligation d'expansion
- ✓ Intégration dans leur outil de gestion des incidents de sécurité (tickets / workflow)
- ✓ Outil de référence pour répondre aux exigences des audits de conformité
  - Règlementations PCI, SOX , SCADA

The Nexus of Security and Networking

27

L'Offre QRadar

QRadar SLIM

Log Management :
- Gestion de Log simple "clé-en-main"
- Evolutive vers solution complète centralisée ou distribuée

QRadar 2100 | QRadar 3100

Network Security Management (SIEM) :
- Gestion Intégrée des Log, des Menaces et de la Conformité
- Monitoring de l'Activité / Flux Réseau

QRadar 3100

Architecture Distribuée Evolutive :
- Event Processors
- Flow Processors
- Distribution Géographique
- Croissance horizontale

QRadar QFlow Collector | QRadar VFlow Collector

Monitoring Activité Réseau & Applications :
- Monitoring Applicatif niveau L7
- Capture de contenu (paquets)
- Visibilité de l'activité réseau et applications basée sur les utilisateurs /identités
- Visibilité de l'activité en environnements Physiques et Virtuels

The Nexus of Security and Networking

28

En Résumé …

LOG MANAGEMENT

THREAT MANAGEMENT

COMPLIANCE MANAGEMENT

QRadar :

Contrôle de l'activité et la gestion de la sécurité sur votre réseau <u>en continu</u>

- ✓ **Visibilité Globale** - Réseau, Sécurité, Utilisateur, Applications - dans une plateforme **intégrée**
- ✓ **Corrélation avancée** pour la détection des "offenses" et aide à la résolution
- ✓ Solution de Gestion des Logs **efficace et sécurisée**, répondant aux exigences des **règlementations** et politiques de sécurité

The Nexus of Security and Networking

MERCI !

The Nexus of Security and Networking

2.8 Olivier Carbonneaux (Trapèze) et Jocelin Rajaona (IGR)

Le wifi en tout lieu et en toute sécurité avec un retour d'expérience de l'Institut Gustave Roussy

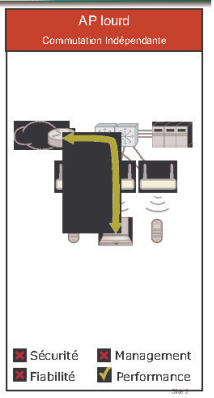
Il est devenu possible de construire et de gérer un ou plusieurs réseaux wifi, sur les mêmes antennes, avec autant de critères de sécurité, de contrôle de flux et de qualité de service qu'avec une infrastructure câblée. Un retour d'expérience sera présenté par Monsieur Jocelin Rajaona DSI de l'Institut Gustave Roussy et Monsieur Olivier Carbonneaux de Trapèze présentera les dernières innovations autour du contrôle d'accès et de la géolocalisation.

TRAPEZE NETWORKS
A BELDEN BRAND

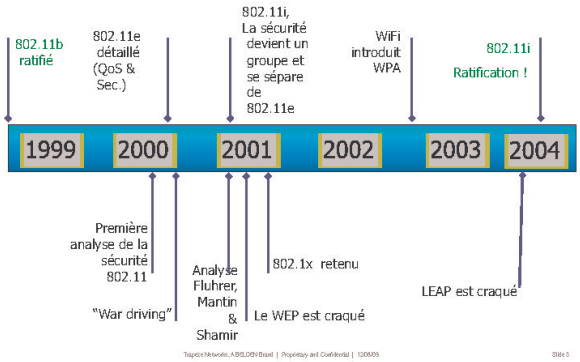
Le WiFi en tous lieux , en toute sécurité

Les points d'accès historiques

- Avant, avant…: « Narrow Band »
- Avant: 2.4Ghz
- 1997: 802.11
  - Pont Ethernet/radio 1Mb/s & 2Mb/s
- 1999: 802.11a, 802.11b
- 1999: WiFi
- 1999: Association ESSID/VLAN
  - Intrusif sur le filaire
  - Fuites sur le sans fil
  - VLAN dynamique : limitations
- 1999: Cisco achète Aironet
- 2003: 802.11g

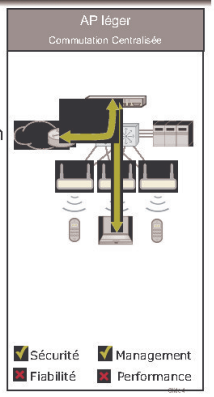


La longue marche de la sécurité



Architecture centralisée : une réponse

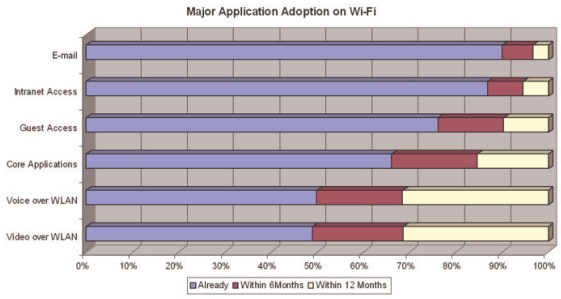
- Le point d'accès ne décide plus
  - Il exécute
- Le point d'accès n'a pas de microcode
  - Il le télécharge
- Le point d'accès n'a pas de configuration
  - Il la télécharge
- Le système devient intelligent
  - Adaptation canaux, puissances
- Les VLANs ne sont plus dispersés



Sécurité et Qualité de service : mariées

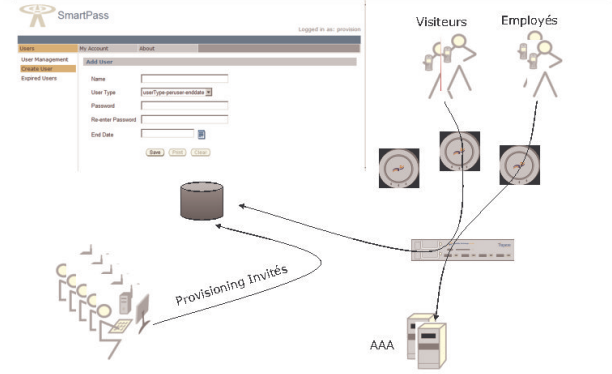
- Authentification forte (802.11i)
  - EAPs
  - PMK Caching, ou Opportunistic Key Caching
- Alignement 802.1p: 4 classes de service radio (802.11e)
- Gestion de l'alimentation (802.11e)
- Détection environnement
  - Embarquée dans les solutions, compatible QoS
  - Alerter l'administrateur
  - Recomposer le réseau
  - Brouiller les intrus: ad hocs, rogues
- Clustering des contrôleurs disponible
  - Moins de 100 ms : invisible pour les utilisateurs

Visiteurs : une forte attente, un fort risque



- Solution: le portail captif, type hot spot

Les invités dans un AAA !



Réseau WiFi

Direction du Système d'Information et Organisation

J. Rajaona
Juin
2009

9

Institut de cancérologie Gustave Roussy

Missions : Soins, Recherche et Enseignement
- 1er Centre de Lutte Contre le Cancer en Europe
- 400 lits, 1M Consultations externes jour
- 14 Unités de Recherche : IFR,INSERM, CNRS
- Enseignement : 4200 h de cours, Paris XI

Architecture Technique
- 2400 Utilisateurs – 1800 postes de travail
- 120 serveurs de production W2K3, OVMS, UNIX
- Backbone Ethernet 1Gbit
- 48 Locaux Techniques – 5000 points de connexions
- Accès Renater via plaque haut débit RUBIS

D.S.I.O.
- 35 ETP : Unité Technique, Etudes, Projets et Développement, Archives

10

Offres d'accès Wi_Fi

Accès S.I.H. : Mobilité
- Soins au chevet du patient Hopital De Jour, Réanimation, Post_Opératoire
- Stocks et délivrance Pharmacie décentralisée
- Imagerie salles du bloc opératoire

Accès Internet libre
- Patients en consultation externe, ambulatoire
- Accompagnants et visiteurs
- Partenaires industriels sur site
- Visiteurs professionnels
- Congressistes

11

Contraintes et solutions Wi_Fi

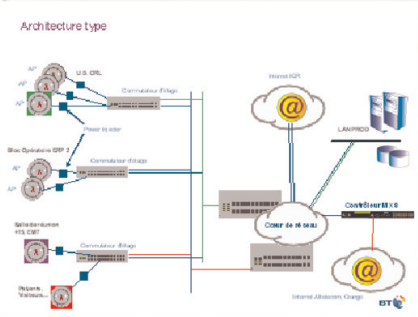
Accès S.I.H. : Mobilité
- Roaming
- Imagerie : Garantie de disponibilité, débit
- Maîtrise des accès sécurisés

Accès Internet libre
- Chartre RENATER
- Responsabilité Institutionnelle
- Accès simultané Wi_Fi et filaire postes IGR

Solution TRAPEZE NETWORKS
- Controleur MX et bornes AP
- Services et Profiles
- VLAN dédiés par profil
- Contrôle d'accès par MAC_Adress pour SIH
- Services d'accès gratuit ou payant

12

Architecture réseau et évolution



Il reste à traiter:

- Le déni de service
  - Les trames de management ne sont pas protégées
  - 802.11 fonctionne sur une méthode d'accès CSMA/CA
- Le service avancé aux « visiteurs »
  - Zéro configuration (SMTP, proxy, IP fixes…)
  - Logs légaux
- L'accès physique au réseau
  - Une place de parking est devenue une prise RJ45

Déni de service: réponses

- Le résultat du groupe de travail 802.11w
  - Attendu fin 2009
  - Va protéger les échanges de management
    - Trames de désassociations
  - Ne va pas résoudre le problème du « bavard »
    - Qui monopolise la ressource radio
- L'infrastructure doit pouvoir alerter l'administrateur
- L'infrastructure doit pouvoir localiser un émetteur
  - L'intervention physique est irremplaçable

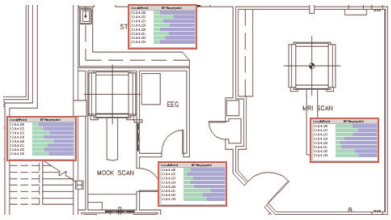
Service « invités »: réponse dédiée

- **IP Zéro configuration**
  - Support IP Fixes / Dhcp
  - SMTP Zéro configuration
  - Proxy Zéro configuration
- **Auto création compte**
  - Pour zone spécifique (zone réunion, exposition,…)
- **Gestion facilitée des obligations légales**
  - Log détaillés (AP, SSID, IP, Ports, heures, …)
  - Susceptibles d'évoluer

Netinary

L'absence de murs: la géolocalisation

- Utilisation de signatures radio des clients WiFi



- Pour:
  - Autoriser/interdire un accès (dedans/dehors)
  - Varier le profil (bureau/salle de réunion)
  - Pousser du contenu contextuel (commerces/services)

Le cas US Air Force

- **Besoins**: Sécurité multi-couches au dessus du WiFi
  - Authentification VPN
  - Intégration IDS filaire existant
- **Solution:** utiliser la position géographique du client comme variable d'authentification
- **Résultats**: Avec RF Firewall, Air Force détecte et se prémunit:
  - Antennes directives espionnes
  - Attaques Déni de Service
  - MAC spoofing
  - Rogue AP, ad-hocs

NEWBURY NETWORKS

2.9 Christian Claveleira (CRU)

eduroam : nomadisme sécurisé pour la communauté enseignement supérieur-recherche

Un chercheur en déplacement chez des confrères d'un autre laboratoire aimerait accéder à l'internet aussi facilement et avec la même confiance que lorsqu'il est dans son bureau, y compris à l'étranger. C'est le but du projet eduroam initié en 2003 par Terena. La présentation montrera comment quelqu'un peut se connecter sur le réseau d'un établissement où il n'a jamais mis les pieds avec son login et son mot de passe habituels sans craindre un espionnage ou un détournement de ses communications et sans intervention des administrateurs du réseau concerné. Les principes et l'architecture techniques seront expliqués ainsi que les relations de confiance nécessaires entre les différents partenaires pour y parvenir.

Nomadisme sécurisé pour la communauté enseignement supérieur-recherche

C. Claveleira
Comité Réseau des Universités

Séminaire Aristote – 11 juin 2009

Comité Réseau des Universités

- Petite structure universitaire ayant des missions nationales dans le domaine des réseaux pour la communauté enseignement supérieur/recherche publique
- Basée à l'université de Rennes 1
- Partenaires
  - Ministère de la recherche
  - Universités, grandes écoles
  - RENATER (réseau académique français)
  - Conférence des Présidents d'Universités

Comité Réseau des Universités

- Domaines de compétence :
  - Sécurité informatique
  - Fédération d'identités
  - Annuaires
  - IGC
  - Formations, conférences (JRES)
  - Services : universalistes, sourcesup, **eduroam.fr,** NTP, dépôt FTP,...

eduroam : contexte

- L'accès à Internet est devenu indispensable dans le cadre professionnel
- Les portables et le Wi-Fi se banalisent
- Le professionnel nomade aimerait avoir un accès simple et fiable lors de ses déplacements professionnels
- L'administrateur veut maîtriser son réseau à moindre coût
- Comment satisfaire tout le monde ?

eduroam : genèse

- Initiative de la TF Mobility de l'association Terena en 2003
- Étude des problèmes de sécurité des réseaux sans fil
- Recommandations pour solution(s) de nomadisme international pour les utilisateurs de réseaux académiques (NRENs)

eduroam : buts

- accès Internet aux utilisateurs nomades
  - Aisés mais contrôlés
  - Entraînant peu de surcroît d'administration
  - Sécurité comparable à un accès filaire
  - Facilement déployable à grande échelle

eduroam : solutions étudiées

- Authentification Web + Radius
  - déploiement facile
  - Déjà utilisé
  - Problèmes de sécurité
- VPN
  - Déploiement laborieux à grande échelle
  - Déjà utilisé
  - Sûr
- IEEE 802.1x + Radius
  - Déploiement facile à grande échelle
  - Sûr

eduroam : solution retenue

- Radius + 802.1x / EAP
- Première expérience de mobilité inter-NREN
- Pilote européen appelé EduRoam (devenu eduroam)
- Hiérarchie de serveurs Radius gérés par les NRENs ayant signé un agrément avec Terena
- Serveur racine géré par Terena

RADIUS : principes

- Remote Access Dial-In User Service :
  - Authentification
  - Autorisation
  - Accounting
- Pour contrôler l'accès d'utilisateurs à un réseau
- Historiquement beaucoup utilisé pour les accès asynchrones par modem
- Utilisable pour tout type d'accès (ethernet, Wi-Fi, applicatif,...)
- Stateless, sur UDP
- Transporte des paires attribut-valeur

RADIUS : relayage et authentification

- Notion de domaine (*realm*)
- Identifiants utilisateurs de la forme <user>@<realm>
  - Exemples : John@Paris, Paul.Dupond@solutionslinux.fr
- Le protocole est relayable (mode proxy) sur la base du *realm*
- Multiples backends d'authentification (fichier plat, base de données, LDAP, Unix,...)

RADIUS : aspects sécurité

- Secret partagé entre serveur et NAS et entre serveurs
  - Champ authenticator dans les paquets
  - Initialisé aléatoirement dans un Access-Request
  - Empreinte MD5 calculée sur ce champ, le contenu du message et le secret renvoyée dans les réponses
  - Utilisé pour chiffrer les mots de passe

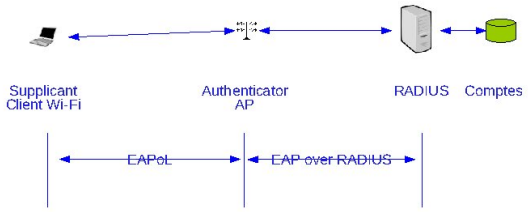
EAP

- Extensible Authentication Protocol
- Cadre général de transport d'authentification (messages)
- Supporte un certain nombre de méthodes d'authentification : MD5, OTP, SIM, TLS, TTLS, PEAP,...
- Chaque protocole utilisant EAP définit sa façon de l'encapsuler

802.1x

- Port Based Network Access Control
- Protagonistes :
  - supplicant (port, client WiFi)
  - Authenticator (AP)
  - serveur d'authentification (généralement RADIUS)
- Initialement conçu pour réseaux filaires (switches Ethernet)
- Définit les méthodes d'encapsulation de trames EAP entre port client (supplicant) et port authenticator : EAPoL

802.1x et 802.11x



802.1x est vulnérable

- Pas d'authentification mutuelle => MIM possible (faux point d'accès)
- Détournement de session : un attaquant peut déconnecter une station connectée (disassociate) et reprendre sa session en usurpant son adresse MAC

Problèmes de sécurité Wifi

- Accès Wi-Fi sujets à écoute, attaques MIM, session hijacking, DOS,...
- Pour prévenir le sniffing du trafic :
  - Chiffrement fiable au niveau des AP
    - Au minimum : WEP dynamique + rotation fréquente des clés
    - Mieux : WPA, WPA2
- Pour se prémunir contre les faux points d'accès :
  - Authentification du serveur d'authentification

Problèmes de sécurité Radius

- Modèle de sécurité RADIUS : *hop-to-hop* avec secret partagé
- Protection intrinsèque peu robuste
- => le trafic RADIUS doit être protégé (VLANs dédiés par ex.)
- Par défaut les mots de passe sont «déballés» et «ré-emballés» à chaque traversée de serveur
- => Sécurisation de l'authentification :
  - Méthodes à base de tunnels SSL de bout en bout
  - Authentification mutuelle

Autres aspects de sécurité

- Traçabilité
  - Journalisation des résultats d'authentification
  - Journalisation DHCP, NAT
  - Correspondance @IP <-> utilisateur en cas de besoin (abus)

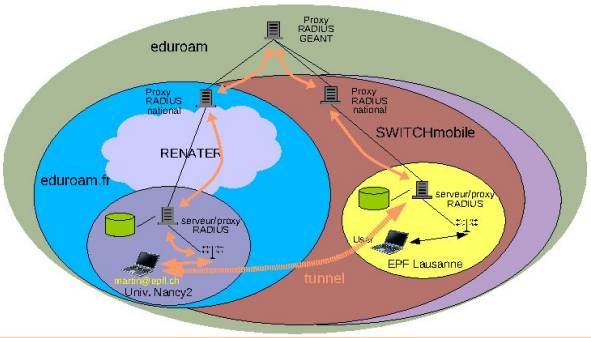
Méthodes EAP sécurisées

- Principe : établir un tunnel SSL entre le supplicant et le serveur d'authentification par-dessus EAP/RADIUS
- Une IGC peut ou non être nécessaire
- La disponibilité dépend des OS et des éditeurs
- Principales : LEAP, FAST, PEAP, SIM, TLS, TTLS

Principales méthodes EAP

- **EAP-FAST** : CISCO, successeur de LEAP. Nécessite un client CISCO.
- **PEAP** (Protected Extensible Authentication Protocol) : CISCO, Microsoft, RSA. Utilise un tunnel TLS. Mécanisme par défaut dans Windows. Authentification de l'utilisateur par mot de passe (MS-CHAP-V2) ou par certificat.
- **EAP-TLS** : authentification mutuelle par certificats X509 (nécessite une IGC). Méthode considérée comme la plus robuste.
- **EAP-TTLS** (Tunneled Transport Layer Security) : tunnel TLS, auth. du serveur par certificat, de l'utilisateur par mot de passe. Simple à mettre en oeuvre. Il existe des clients libres et/ou commerciaux pour tous les OS.

eduroam : architecture



eduroam : une question de confiance

- Intervenants : utilisateurs, sites d'origine, sites visités, les réseaux académiques, SA3/GEANT3
- Confiance des visiteurs dans les sites visités :
  - Disponibilité du service
  - Infrastructure réseau
  - Administration réseau
  - Administration des serveurs Radius
  - Chiffrement des liaisons sans fil

Une question de confiance, suite

- Confiance des sites visités dans les sites d'origine :
  - Validation, choix et sécurisation de l'authentification
  - Information de leurs utilisateurs
  - Configuration de leurs équipements
  - support
- Confiance dans les NRENs, à commencer par Renater
  - Fiabilité et sécurisation de leurs réseaux
  - Sécurisation et administration des proxies Radius

Formalisation des relations de confiance

- RENATER au centre des relations de confiance
- Acceptation du « eduroam service definition and implementation » par RENATER
  - Ses établissements agréés doivent s'engager sur de bonnes pratiques et sur l'éducation de leurs utilisateurs
  - Au moins un serveur proxy national doit être mis en oeuvre et sécurisé
  - De l'information sur le service doit être faite
  - Le service doit être surveillé
  - Le CERT est impliqué

Formalisation des relations de confiance, suite

- Signature de la charte eduroam.fr par les établissements (service mobilité de RENATER)
- Offrir le service conformément aux recommandations techniques eduroam.fr
- Administrer et sécuriser au moins un proxy RADIUS
- (In)former leurs utilisateurs sur le service et le respect des règles d'utilisation des réseaux visités
- Assurer leur support
- Journaliser les résultats d'authentification

Bilan de sécurité

- Confidentialité assurée par chiffrement radio fiable
- Authentification mutuelle utilisateur-établissement
- Protection des *credentials* par tunnel chiffré (EAP tunnelisé + identifiant externe anonyme)
- Confiance dans l'infrastructure utilisée par l'authentification du serveur RADIUS de l'établissement d'origine
- Traçabilité par remontée de l'identifiant de l'utilisateur au site d'accueil

eduroam.fr

- Frontend administratif fait par RENATER
- Service opéré par le CRU
- Un proxy national à Rennes, un deuxième à Strabourg
- Gestion des comptes, site web, listes de diffusion, configuration des proxies, monitoring, support
- >110 établissement adhérents
- >80 opérationnels

eduroam.fr spécifications techniques

- Ssid : eduroam
- Realms : *.fr (+ quelques .eu)
- 802.11g si possible
- WPA2, sinon WPA, sinon WEP 128 dynamique
- Accès ouvert sur l'Internet sinon liste de ports minimum
- Méthodes EAP : TLS et/ou TTLS et/ou PEAP
- Compte de test pour monitoring

eduroam.fr aujourd'hui

- > 30 réseaux académiques inter connectés en Europe, 4 en Asie
- Structure opérationnelle hébergée dans le cadre de GEANT3
- Composante française opérée par le CRU (au nom de RENATER) : **eduroam.fr**

eduroam : couverture européenne

eduroam.fr : carte

Conclusion

- *eduroam* permet un meilleur partage des infrastructures réseau académiques
  - En en étendant l'usage à toute la communauté
  - En en conservant la maîtrise par leurs administrateurs
  - À moindre coût
  - Avec une qualité de service (et de sécurité) garantie
  - Sans changer les habitudes des utilisateurs

Questions ?

2.10 Cedric Blancher (EADS)

Les pare-feu nuisent-ils à la sécurité ? Quelques considérations autour du concept de dépérimétrisation

Avec l'essor de la mobilité, les modèles de sécurité qualifiés de périmétriques sont mis à rude épreuve et montrent leurs limitent quand il s'agit de prendre en compte le nomadisme important des utilisateurs et des données. Ce qui amènent aujourd'hui certains à affirmer que ces pratiques nuisent à la sécurité des réseaux et prônent leur ouverture au nom de la sécurité. C'est ce qui se cache derrière cette tendance répondant au nom barbare de dépérimétrisation. Les choses ne sont évidemment pas aussi simples. S'il est clair pour beaucoup que la trop grande fragmentation des infrastructures réseau est un frein au déploiement de services sécurisés, une ouverture complète suppose cependant quelques pré-requis techniques et soulève nombre de questions techniques. Mais à l'heure où se développe le phénomène de Cloud Computing, il est certain qu'il faille au minimum remettre en cause le dogme du firewall et repenser notre approche de la sécurité réseau.

EADS

Les pare-feu nuisent-ils à la sécurité ?

Quelques considérations autour du concept de dépérimétrisation

Cédric BLANCHER

cedric.blancher@eads.net
EADS Innovation Works
Computer Security Research Lab

sid@rstack.org
Rstack Team
http://sid.rstack.org/

Séminaire Aristote - La sécurité distribuée
École Polytechnique Palaiseau - 11 juin 2009

EADS

La dépérimétrisation en quelques mots...

Tendance à l'ouverture des réseaux

- Ouverture des périmètres
- Suppression (ou presque) des firewalls
- Concentration sur la sécurité des données

Discours volontairement polémique, mais néanmoins intéressante

EADS

Agenda

1. La déperimétrisation
2. Différents points de vue
3. Conclusion

EADS

Agenda

1. La déperimétrisation
2. Différents points de vue
3. Conclusion

EADS

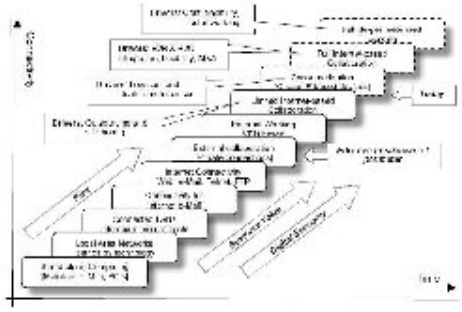
Jericho Forum

Think Tank poussant la déperimétrisation

- Les 11 commandements
- Business Case for Deperimeterisation
- Nombreux White Papers
- Présentations et exemples

EADS

Arguments (1)



EADS

Arguments (2)

Grosso modo

- Les mécanismes de sécurité réseau sont obsolètes
- Ils ne protègent pas de la plupart des attaques
- Ils sont contre-productifs
- Ils encouragent des comportements "incidentogènes"

Les pare-feu nuisent-ils à la sécurité ? — Cédric BLANCHER — 7/19

EADS

Arguments (2)

Grosso modo

- Les mécanismes de sécurité réseau sont obsolètes
- Ils ne protègent pas de la plupart des attaques
- Ils sont contre-productifs
- Ils encouragent des comportements "incidentogènes"

Solution

- Redonner au réseau son rôle de transport
- Rétablir la connectivité globale
- Remonter la sécurité vers les applications

EADS

Utopie ?

Une jolie collection de Yakafokons™© qui soulèvent plus de questions qu'ils n'apportent de réponses

- Faisabilité technique ?
- Ampleur des bénéfices ?
- Portée réelle du concept ?
- Applicabilité pratique ?
- Conditions, contraintes, limites, risques ?
- Etc.

EADS

Agenda

EADS

Point de vue du réseau (1)

Migration vers un réseau plus plat

- Moins de firewalls
- Plus de connectivité (cf. modèle IPv6)
- Sécurité de bout en bout

Les pare-feu nuisent-ils à la sécurité ? — Cédric BLANCHER — 10/19

EADS

Point de vue du réseau (1)

Migration vers un réseau plus plat

- Moins de firewalls
- Plus de connectivité (cf. modèle IPv6)
- Sécurité de bout en bout

Principe

- Chiffrement des flux applicatifs (SSL/TLS)
- Recentrage de la sécurité sur les données

EADS

Point de vue du réseau (2)

La segmentation du réseau est un problème

- Problèmes de NAT
- Configuration des pare-feu
- Mécanismes compliqués (cf. P2P)

Les pare-feu nuisent-ils à la sécurité ? — Cédric BLANCHER — 11/19

EADS

Point de vue du réseau (2)

La segmentation du réseau est un problème

- Problèmes de NAT
- Configuration des pare-feu
- Mécanismes compliqués (cf. P2P)

Apports de la connectivité globale

- Véritable sécurité de bout en bout
- Intégration de la mobilité
- Constitution d'overlays
- Etc.

EADS

Repérimétrisation

On ne supprime pas le périmètre, on le reconstruit...

- Périmètre plus ouvert physiquement
- Mais construction de domaines logiques
- Communication au sein de ces nouveaux périmètres

La dépérimétrisation transforme le périmètre physique en périmètre logique par la mise en place d'overlays

EADS

Point de vue système...

Axée connectivité, la dépérimétrisation apporte peu au système...

- Mêmes moyens de sécurité
- Menaces client-side exacerbées
- Problématiques de confinement

Les pare-feu nuisent-ils à la sécurité ? — Cédric BLANCHER — 13/19

EADS

Point de vue système...

Axée connectivité, la dépérimétrisation apporte peu au système...

- Mêmes moyens de sécurité
- Menaces client-side exacerbées
- Problématiques de confinement

Questions...

- Gestion de l'exposition des systèmes ?
- Assurance de la résilience ?
- Confinement par rapport au reste du périmètre ?

EADS

L'accès aux données

Problématique strictement identique

- Mêmes services
- Mêmes données
- Mêmes accès

EADS

L'accès aux données

Problématique strictement identique

- Mêmes services
- Mêmes données
- Mêmes accès

Problèmes

- Exposition accrue des clients
- Adaptation des applications

EADS

La dépérimétrisation pour tous ?

L'éclatement du périmètre ne veut pas dire mort du firewall

- Concept poussé par les besoins de mobilité
- Aucun intérêt pour les ressources fixes

EADS

La dépérimétrisation pour tous ?

L'éclatement du périmètre ne veut pas dire mort du firewall

- Concept poussé par les besoins de mobilité
- Aucun intérêt pour les ressources fixes

Mais aussi...

Votre dépérimétrisation profitera d'abord aux autres !

EADS

Agenda

EADS

L'accès aux données

Le fond du problème réside dans la gestion des données

- La valeur réside dans les données
- Comment protéger efficacement les données ?

EADS

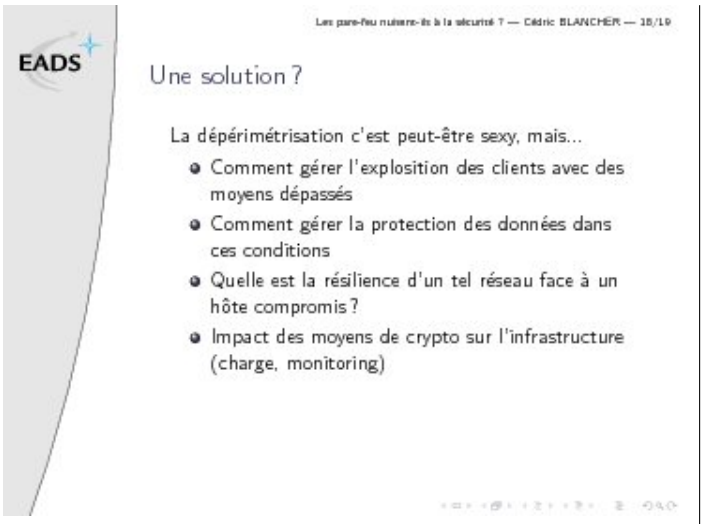
L'accès aux données

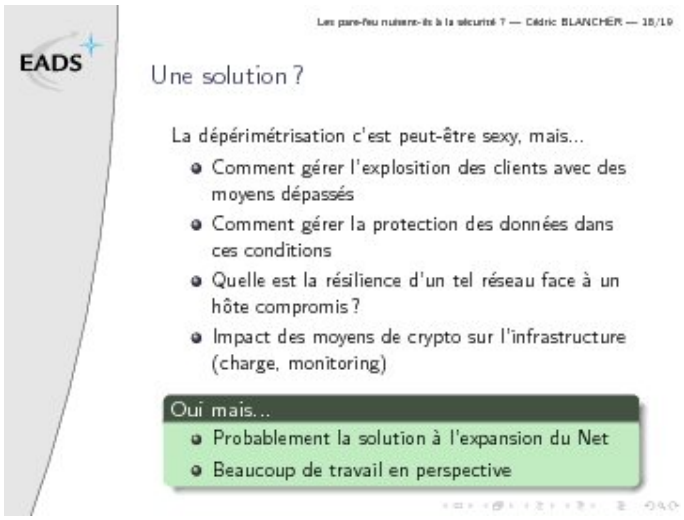
Le fond du problème réside dans la gestion des données

- La valeur réside dans les données
- Comment protéger efficacement les données ?

Problèmatiques

- De nombreuses données ne transitent pas sur le réseau !
- Distribution des données (e.g. Cloud Computing)


Les pare-feu nuisent-ils à la sécurité ? — Cédric BLANCHER — 18/19
EADS
Une solution ?
La dépérimétrisation c'est peut-être sexy, mais...
Comment gérer l'explosition des clients avec des moyens dépassés
Comment gérer la protection des données dans ces conditions
Quelle est la résilience d'un tel réseau face à un hôte compromis ?
Impact des moyens de crypto sur l'infrastructure (charge, monitoring)


Les pare-feu nuisent-ils à la sécurité ? — Cédric BLANCHER — 18/19
EADS
Une solution ?
La dépérimétrisation c'est peut-être sexy, mais...
Comment gérer l'explosition des clients avec des moyens dépassés
Comment gérer la protection des données dans ces conditions
Quelle est la résilience d'un tel réseau face à un hôte compromis ?
Impact des moyens de crypto sur l'infrastructure (charge, monitoring)
Oui mais...
Probablement la solution à l'expansion du Net
Beaucoup de travail en perspective


Les pare-feu nuisent-ils à la sécurité ? — Cédric BLANCHER — 19/19
EADS
That's all folks !
Merci pour votre patience...
Questions ?

Annexes : deux livres blancs

Nous mettons en annexe de ce document, les livres blancs communiqués par les sociétés Stonesoft et Sparus Software, leurs présentations ayant dû être annulées.

STONESOFT

Livre blanc

Les enjeux méconnus de la sécurisation d'un environnement virtuel

Sommaire

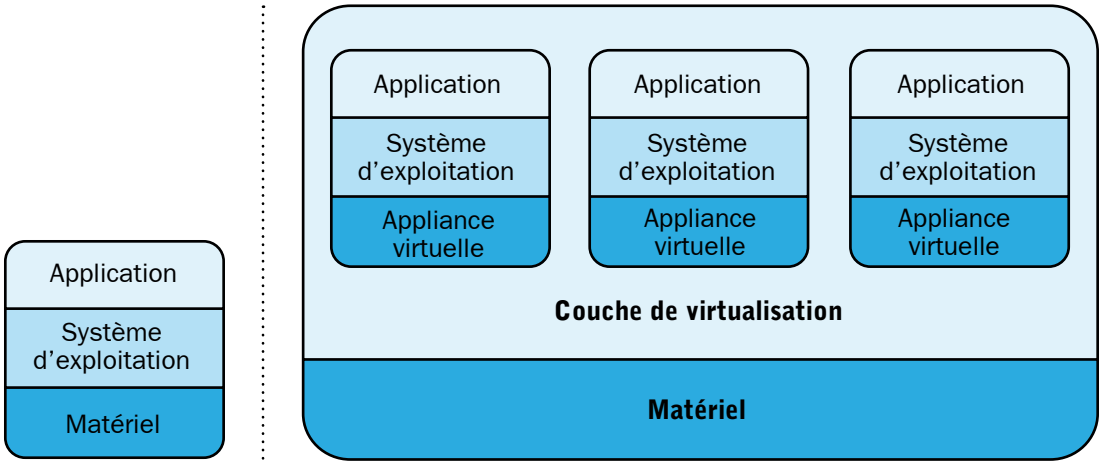
Synthèse

La virtualisation prend d'assaut l'industrie informatique. Selon un récent sondage du magazine InformationWeek, 70 % des personnes interrogées disposent d'au moins un serveur virtuel tandis que moins de 12 % d'entre elles ont une stratégie de sécurité adaptée à leur environnement virtuel. Où se situe votre entreprise par rapport à ces statistiques ?

Si vous avez déjà mis en œuvre une stratégie de virtualisation, ou si vous êtes en passe de le faire, la sécurité de votre entreprise risque d'être exposée à des menaces qui pourraient avoir un impact plus désastreux que jamais sur votre environnement d'exploitation. Étant donné que les systèmes de sécurité traditionnels ont recours à du matériel et à des systèmes d'exploitation spécifiques pour protéger votre environnement, ils perdent toute leur utilité dans un environnement virtuel où l'objectif consiste à réduire voire à éliminer le matériel.

Les meilleures pratiques classiques sont en outre remises en question puisque la segmentation physique et d'autres méthodes sont devenues presque impossibles à réaliser. Pour finir, en raison de la nature de l'environnement virtuel, la complexité du réseau augmente plus rapidement qu'avec des systèmes de gestion et de surveillance hérités, ce qui obscurcit nettement la visibilité sur les environnements virtuels et physiques. Dans le nouveau monde virtuel, les entreprises doivent réfléchir plus sérieusement à une nouvelle manière de sécuriser leurs réseaux et leurs données sensibles.

Ce livre blanc vise à donner aux professionnels de la sécurité et aux responsables informatiques une solide connaissance des risques potentiels qu'ils encourent s'ils n'incorporent pas de nouvelles technologies de sécurité à leurs environnements virtuels. Il explique pourquoi les systèmes traditionnels ne fonctionnent pas et contient une liste de questions à se poser pour s'assurer qu'un réseau est bien adapté aux environnements virtuels.



Architecture classique x86
» Un système d'exploitation par serveur
» Logiciel et matériel étroitement liés
» Une application par serveur
» Charge habituelle du serveur : 5 à 15 %

Architecture virtualisée
» Différents systèmes d'exploitation par serveur
» Séparation entre matériel et logiciel
» Plusieurs applications par serveur
» Charge habituelle du serveur : 50 à 70 %
» Ressources optimisées dynamiquement

Les enjeux liés à la sécurisation d'un environnement virtuel

Il est peu courant que des progrès technologiques entraînent un changement radical du mode de fonctionnement fondamental de l'informatique. Internet a eu un impact majeur, non seulement sur la manière d'accéder aux informations, de les stocker et d'interagir avec elles, mais aussi sur la façon dont les architectures applicatives et les réseaux sécurisent ces informations. La virtualisation révolutionne de manière similaire les environnements informatiques actuels.

Étonnamment, les environnements virtuels existent depuis plus de 30 ans. Pionnier dans le développement de ressources virtuelles avec le mainframe, IBM® offre à présent une large gamme de serveurs et d'architectures virtuels. La puissance de calcul ayant cependant augmenté exponentiellement ces dernières années, la vraie valeur ajoutée de la virtualisation est désormais à la portée d'organisations de toutes tailles. Avec l'avènement de VMware® , Parallels® , Xen™ et d'autres technologies de virtualisation, les entreprises d'aujourd'hui peuvent tirer profit de cette approche de machine virtuelle.

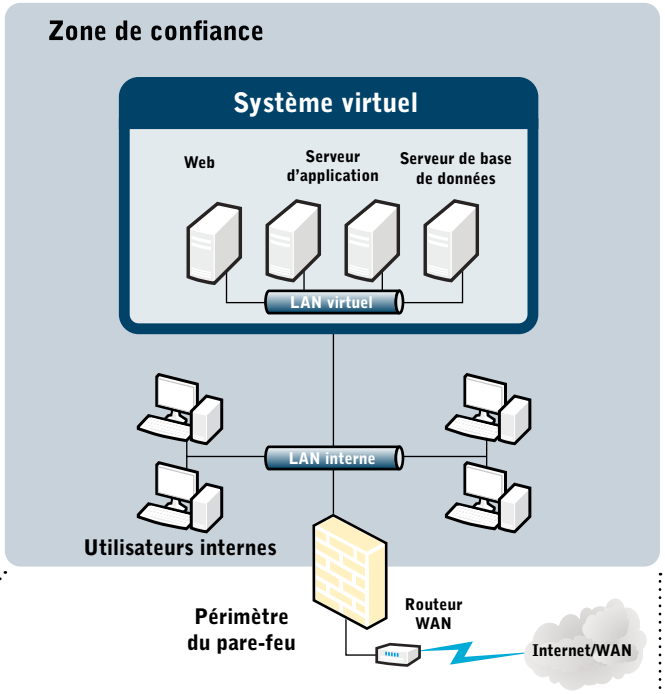
Maintenant que la virtualisation se généralise, de nombreuses entreprises s'y mettent sans prendre en compte tous les risques qu'elle comporte en termes de sécurité. Ces risques tiennent au fait que les nouveaux modes de travail sont sécurisés par des méthodes dépassées reposant sur un équipement inadéquat. Voyons à présent pourquoi les systèmes traditionnels de sécurité réseau créent des risques importants pour des milliers d'organisations.

Les solutions de sécurité matérielles traditionnelles perdent leur utilité

Au cœur de toute stratégie de virtualisation se situe la suppression ou la diminution des serveurs et du matériel. La majorité des solutions de sécurité traditionnelles, tels que les pare-feu et les systèmes de prévention des intrusions (IPS), sont basées sur le matériel, c'est-à-dire qu'elles résident sur une machine en amont du système qu'elles sécurisent. Lorsqu'il n'y a plus de matériel, le dispositif de sécurité est uniquement en mesure de jeter un voile protecteur sur l'ensemble de l'environnement virtuel, et non sur chaque composant individuel.

Pour compliquer encore le problème, la plupart des fournisseurs de solutions de sécurité utilisent du matériel ASIC, soit des systèmes conçus spécifiquement pour remplir une fonction bien particulière : assurer la sécurité. Ces circuits intégrés doivent être présents pour

Le principal problème de la virtualisation



Le principal problème de la virtualisation réside dans le fait qu'elle réunit les différents niveaux d'une architecture applicative classique en un seul système virtuel et qu'elle place ces derniers dans une seule zone de confiance accessible à l'ensemble des utilisateurs internes. Cet « aplanissement » de l'architecture expose le système à des menaces de la part des utilisateurs internes et supprime toute possibilité de protéger les données les plus stratégiques en cas d'infraction.

que ces solutions fonctionnent. Or dans un véritable environnement virtuel, il n'y a pas de place pour des circuits intégrés spécialisés supplémentaires.

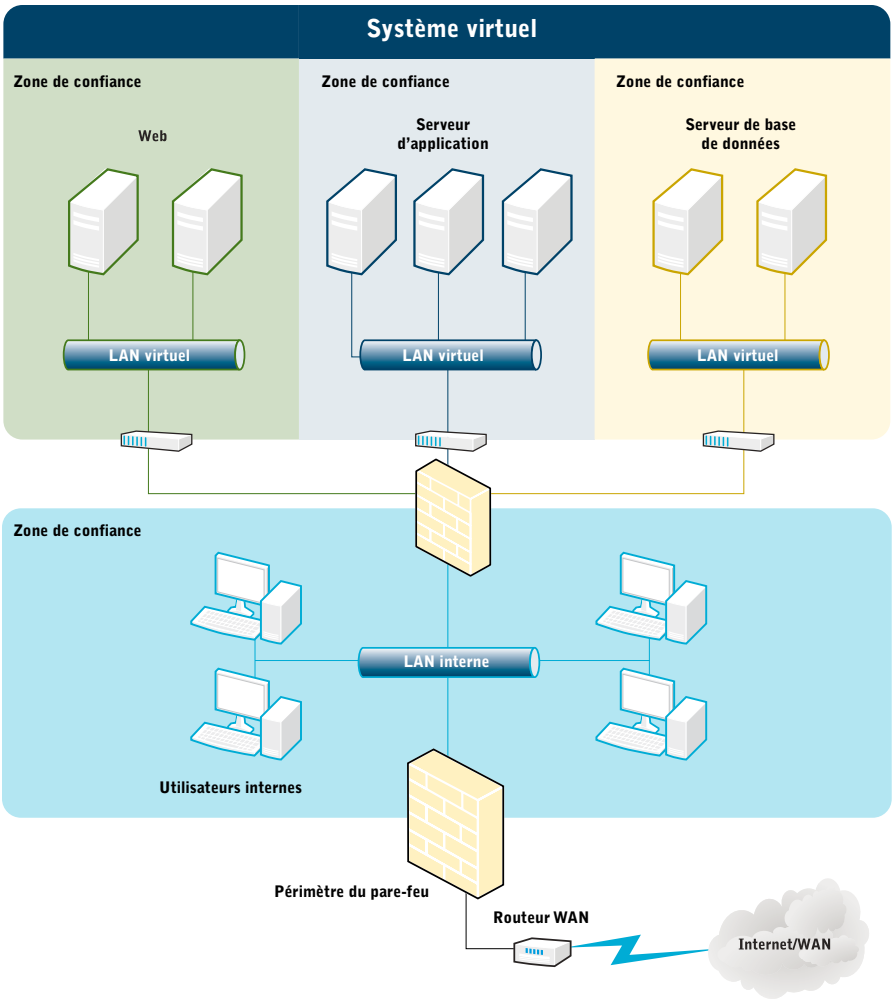
Enfin, les solutions de sécurité matérielles étant généralement placées à la périphérie de l'environnement, elles exposent davantage les organisations aux attaques venant de l'intérieur, lesquelles représentent 59 % de toutes les attaques selon une enquête réalisée par le CSI en 2007.

Les modèles traditionnels de contrôle de la sécurité sont remis en cause.

Toute architecture informatique possède au moins trois niveaux : 1) la base de données d'arrière-plan qui contient les données stratégiques sur les clients ou l'organisation, c'est-à-dire la mine d'or à laquelle la plupart des hackers tentent d'accéder ; 2) le middleware applicatif qui permet à l'utilisateur final d'agir comme il l'entend sur les données ; 3) les serveurs Web frontaux qui permettent au monde extérieur d'interagir avec les deux précédents niveaux.

Pour que l'application puisse fonctionner comme prévu, les dispositifs de sécurité sont généralement placés en amont des serveurs Web et configurés pour laisser passer le trafic Web. Or, selon de nombreux analystes, près de 80 % de toutes les failles dans le système de sécurité proviennent d'attaques lancées par le biais de protocoles Web. Lorsqu'un serveur

Virtualisation externe du pare-feu

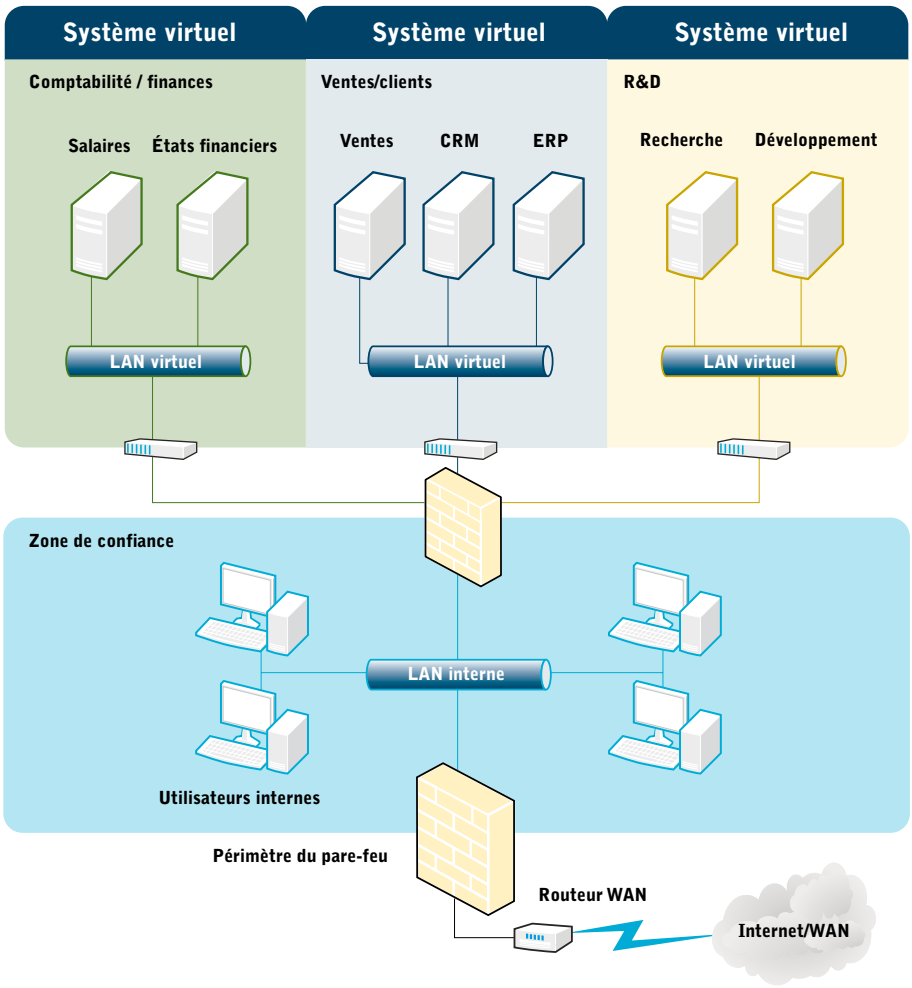


Les organisations cherchant à améliorer la sécurité de la virtualisation ont dû envisager l'utilisation de produits matériels extérieurs à l'environnement virtuel. Les composants de sécurité réseau ne pouvant toutefois être virtualisés, l'organisation ne peut toujours pas voir à l'intérieur de l'environnement virtuel, ce qui induit des difficultés supplémentaires en termes de conformité et d'audit. En outre, l'architecture ne tire pas pleinement profit des avantages de la virtualisation, générant ainsi des coûts supplémentaires dus à la complexité, à l'électricité, à la ventilation, etc.

Web a été infiltré dans le modèle traditionnel, ce serveur et son application restent les seuls concernés par l'intrusion.

Dans un environnement virtuel, en revanche, où de multiples applications et serveurs résident sur un seul serveur, une fois que le hacker a pénétré cette couche, il a accès à tout ce qui se trouve dans des dizaines voire des centaines de systèmes, d'applications et de bases de données. En outre, les contrôles habituellement placés autour de chaque application n'existent pas dans un environnement virtuel. Par conséquent, la capacité d'une organisation à déterminer qui a accédé aux différentes informations et à quel moment est sérieusement compromise. Résultat : des préoccupations parmi les auditeurs et le risque de générer des « faiblesses matérielles » dans le rapport de conformité d'une organisation.

Systèmes virtuels multiples



Pour tenter de résoudre les problèmes de sécurité liés à la virtualisation, il convient de créer de multiples zones de confiance en ayant recours à plusieurs systèmes virtuels, chacun d'eux ne virtualisant qu'un seul aspect de l'architecture. Des dispositifs physiques basés sur le matériel sont utilisés en tant que produits de sécurité réseau traditionnels pour protéger les systèmes. Cette approche augmente néanmoins aussi le matériel physique, ce qui peut nettement réduire le retour sur investissement (ROI) que la virtualisation aurait pu générer. Elle accroît également la complexité, les besoins en électricité et en refroidissement ainsi que d'autres facteurs, tel que l'encombrement du centre de données.

Les stratégies de segmentation classiques deviennent inefficaces.

La plupart des responsables informatiques sont conscients de l'importance de la segmentation, notamment ceux des entreprises cotées en bourse qui sont tenues de respecter les directives strictes de la loi Sarbanes-Oxley et d'autres exigences réglementaires.

Les meilleures pratiques en termes de conformité prônent une segmentation ou un « partionnement » des fonctions clés de l'entreprise, comme les RH, la R&D et les salaires, au sein

de l'infrastructure informatique. Nombre d'organisations appliquent également des stratégies de segmentation en créant des zones de confiance pour se protéger des menaces internes et externes. Ces tactiques aident à éliminer le risque que des personnes non autorisées accèdent à des informations qui ne leur sont pas destinées.

Dans les environnements virtuels qui dépendent encore de solutions de sécurité héritées, la segmentation est plus complexe car elle oblige les responsables informatiques à installer de multiples serveurs physiques pour exécuter différents environnement virtuels – un pour chaque domaine, comme les RH, la R&D ou les salaires. Cette situation met en péril l'objectif numéro un de la virtualisation, à savoir réduire le matériel, les coûts et la complexité. Par ailleurs, la rentabilité de la mise en commun est compromise, l'espace sur le serveur reste problématique et les complexités du réseau créent un risque encore plus important en termes de sécurité et de disponibilité.

Les consoles de gestion classiques ne suffisent pas.

Si les systèmes de sécurité réseau basés sur le matériel ne peuvent résider entre les serveurs virtuels ou dans les applications virtuelles sur ces serveurs, les consoles de gestion, quant à elles, ne sont pas en mesure d'offrir une visibilité sur l'activité de l'environnement virtuel. Ainsi, les dispositifs de sécurité hérités placés en amont du système virtuel ne peuvent détecter le volume de trafic réseau transitant entre les systèmes virtuels. Ils ne peuvent avertir l'administrateur si le système physique est sur le point d'atteindre sa capacité maximale ou s'il doit être reconfiguré. Sans ces informations vitales, les responsables informatiques ont beaucoup de mal à déterminer si une attaque est en cours ou si la capacité maximale est atteinte. En conséquence, l'entreprise est davantage sujette à des pannes réseau.

Comment s'assurer qu'une solution de sécurité réseau est adaptée aux environnements virtuels

Au vu des difficultés décrites plus haut, nous pouvons conclure que les solutions de sécurité logicielles représentent la seule option pour protéger votre infrastructure informatique virtuelle ainsi que les avantages que vous espérez retirer de vos initiatives de virtualisation.

Stonesoft est une entreprise d'envergure mondiale qui, depuis près de 20 ans, aide les organisations à sécuriser leur flux d'informations grâce à des solutions de pointe en matière de sécurité réseau et de continuité de service. Depuis 2002, elle propose des solutions logicielles de sécurité qui ont fait leurs preuves dans des environnements virtuels. Avec les solutions StoneGate, les entreprises peuvent tirer pleinement profit des avantages offerts par la technologie de serveur virtuel tout en étant assurées que leurs réseaux restent sécurisés et disponibles.

Assurer la sécurité de l'environnement virtuel pour les MSP

La sécurité, la convivialité et la flexibilité sans précédent offertes par les solutions StoneGate peuvent aider à jeter les bases d'une consolidation des serveurs pour tout type d'organisation. Néanmoins, la virtualisation revêt un intérêt particulier pour les fournisseurs de services gérés (MSP) qui comptent des centaines de clients, de pare-feu en clusters et d'appliances IPS. Au lieu de devoir mettre en place des environnements avec des dizaines de serveurs, les MSP peuvent désormais gérer de multiples environnements utilisateur au moyen d'un seul ordinateur.

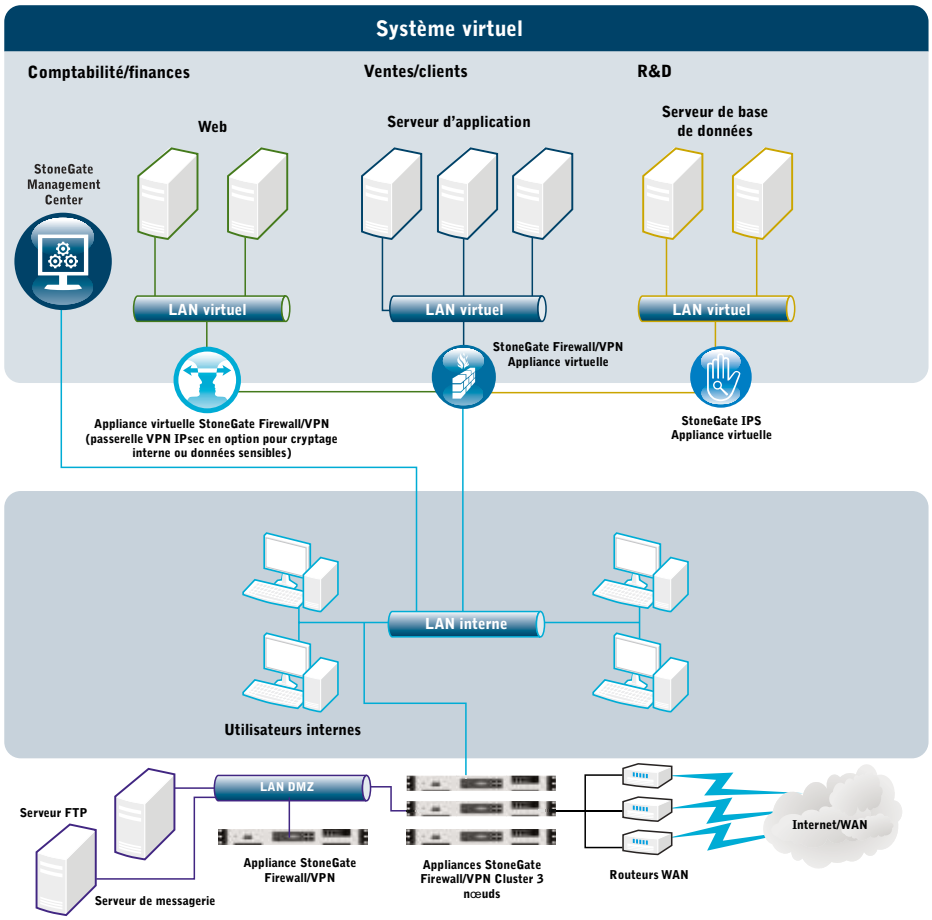
Pour savoir si votre solution actuelle est adaptée aux environnements virtuels, passez en revue les questions suivantes avec votre fournisseur de sécurité réseau :

1. Vos produits actuels peuvent-ils prendre en charge un environnement virtuel ? Si oui, comment faut-il procéder et quels composants supplémentaires faut-il acheter pour bénéficier du niveau de sécurité que nous offrent actuellement nos produits matériels ?

Les solutions StoneGate sont conçues de bout en bout pour être des systèmes logiciels sécurisés, ce qui signifie que la capacité à fonctionner dans un environnement virtuel est déjà intégrée. Elles n'induisent aucun coût supplémentaire dans le cadre de la mise en place d'un environnement virtuel. Avec plus de cinq ans d'expérience dans la virtualisation, StoneGate offre une gamme d'appliances virtuelles certifiées VMware pour pare-feu/VPN, IPS et SSL VPN.

La solution StoneGate Firewall/VPN fonctionne selon un principe simple : tout ce qui n'est pas expressément permis est refusé. La solution StoneGate IPS autorise le trafic normal et stoppe le trafic nuisible en cours de route. StoneGate fournit des systèmes virtuels avec pare-feu d'inspection dynamique, VPN, IPS et SSL VPN qui allient la puissance des signatures à l'analyse des anomalies. StoneGate Firewall/VPN intègre en outre une fonction d'inspection multicouches grâce à laquelle le pare-feu peut soit fonctionner comme filtre de paquets de base ou comme pare-feu d'inspection dynamique, soit effectuer une inspection approfondie des paquets au niveau de la couche application – chaque option étant sélectionnée au cas par cas par l'administrateur.

La virtualisation avec StoneGate



Les appliances virtuelles de la solution StoneGate de Stonesoft permettent de protéger les réseaux virtuels à l'aide d'un pare-feu virtuel/VPN et d'ajouter une protection supplémentaire pour les serveurs de bases de données via un système de prévention d'intrusions virtuel intégré. La solution StoneGate Management Center, qui réalise une gestion robuste et centralisée de tous les composants StoneGate, peut également être virtualisée. Elle permet ainsi à une organisation de tirer pleinement profit des avantages de la virtualisation tout en ayant l'assurance que le nouvel environnement est à l'abri des attaques internes et externes. Qu'ils soient physiques ou virtuels, les dispositifs de sécurité sont gérés à partir de la même console.

Exploitant les fonctionnalités VMware, les appliances virtuelles StoneGate sont extrêmement simples à mettre en œuvre.

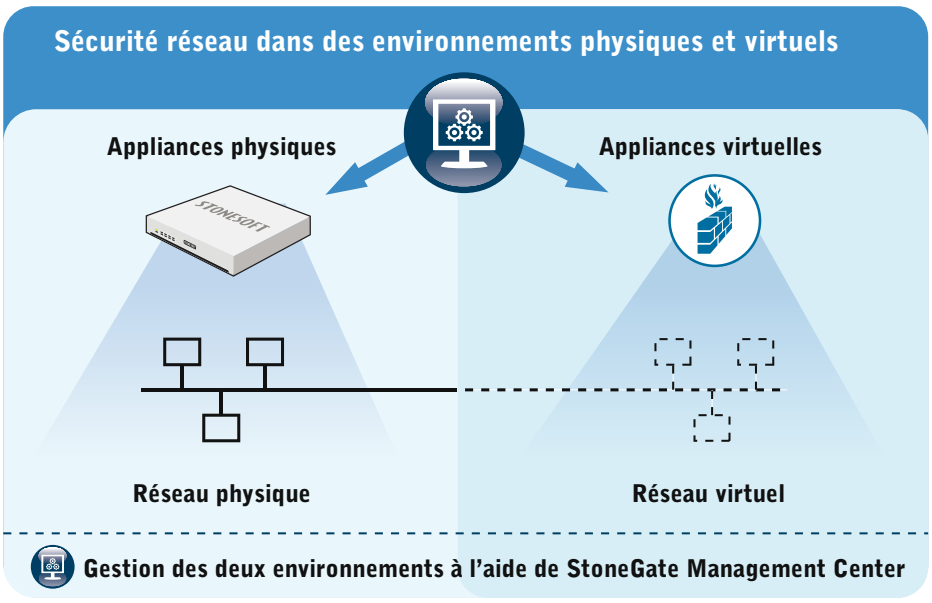
Étant donné que les solutions StoneGate Firewall/VPN, IPS et SSL VPN intègrent leur propre système d'exploitation sécurisé, il n'est pas nécessaire d'en installer un au préalable dans la machine virtuelle. Cette intégration du système d'exploitation ne simplifie pas seulement le processus d'installation. Elle réduit également les temps de gestion. En effet, elle évite toutes les tâches associées à l'installation du système d'exploitation, comme la suppression des progiciels, applications, services, utilisateurs, groupes et fichiers parasites, la vérification des autorisations du système de fichiers et des téléchargements ou l'installation des correctifs et des service packs.

Les appliances virtuelles de la solution StoneGate de Stonesoft permettent de protéger les réseaux virtuels à l'aide d'un pare-feu virtuel/VPN et d'ajouter une protection supplémentaire pour les serveurs de bases de données via un système de prévention d'intrusions virtuel intégré. La solution StoneGate Management Center, qui réalise une gestion robuste et centralisée de tous les composants StoneGate, peut également être virtualisée. Elle permet ainsi à une organisation de tirer pleinement profit des avantages de la virtualisation tout en ayant l'assurance que le nouvel environnement est à l'abri des attaques internes et externes. Qu'ils soient physiques ou virtuels, les dispositifs de sécurité sont gérés à partir de la même console.

2. Votre produit est-il en mesure de surveiller avec précision les activités des environnements virtuel et physique à partir d'une seule console de gestion ?

La flexibilité de l'architecture StoneGate, qui lui permet de s'intégrer aussi bien dans les environnements virtuels que physiques, profite également aux organisations qui souhaitent gérer l'ensemble de leur réseau de manière centralisée à partir d'une seule plate-forme. Ainsi, la solution StoneGate Management Center peut gérer des instances de dispositifs StoneGate virtuels et physiques, des clusters de dispositifs StoneGate virtuels et physiques, et des versions logicielles s'exécutant sur du matériel x86 standard. Elle permet également, pour chacun de ces éléments, une gestion unifiée des politiques. Les administrateurs ont la possibilité de surveiller, de contrôler et de changer les versions logicielles pour les clusters du périmètre sur des serveurs x86, les appliances StoneGate sur des sites distants et les machines virtuelles VMware, le tout à partir d'une interface utilisateur et d'un centre de gestion uniques.

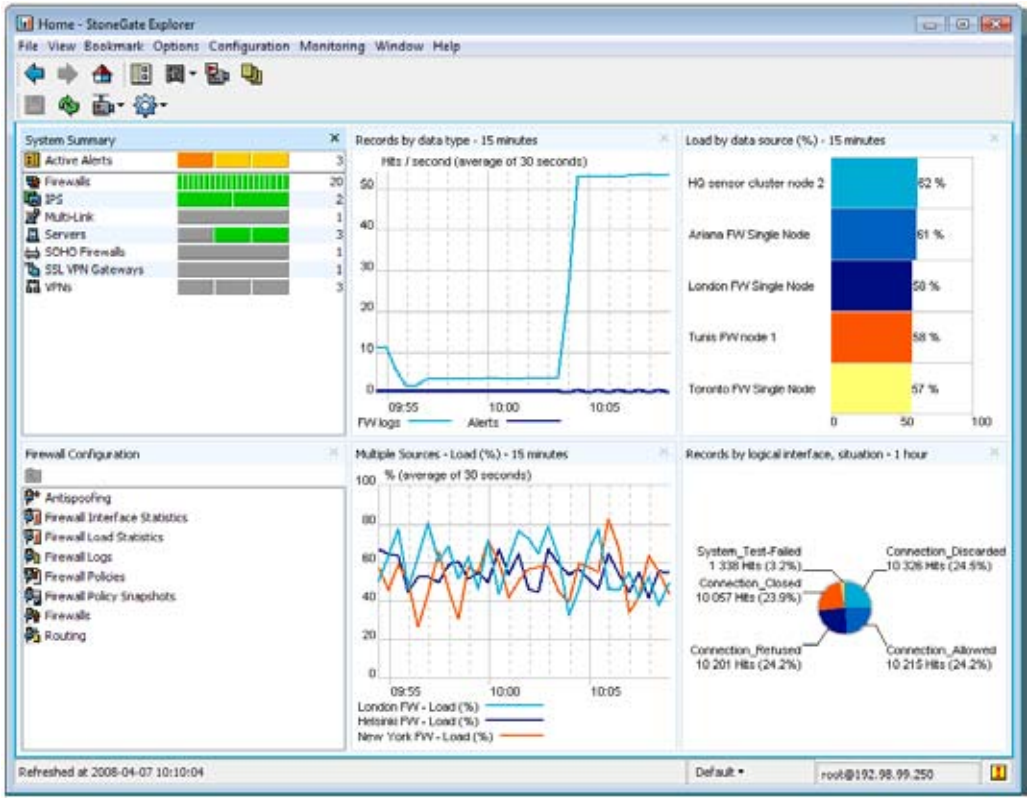
Solution de sécurité StoneGate pour environnements virtuels



3. Comment votre produit m'aide-t-il à atténuer les menaces en temps voulu sur l'ensemble de mon environnement virtuel ?

Grâce à ses fonctionnalités intégrées de journalisation et d'audit, StoneGate peut encore renforcer la sécurité du système virtuel en fournissant des journaux du trafic à l'entrée et à la sortie du système, et entre les machines virtuelles et les réseaux. Les fonctions de filtrage puissantes permettent à l'administrateur d'isoler rapidement les entrées qu'il recherche en fonction d'un certain nombre de critères, comme l'adresse IP source ou de destination, les informations d'authentification de l'utilisateur, l'heure, ou autre. Les fonctions d'audit surveillent l'accès et les modifications apportées aux politiques de sécurité et aux éléments réseau, notamment les propriétés et les informations de routage des dispositifs firewall/VPN et IPS. Associées à différents rôles et autorisations d'administrateur, ces fonctions permettent à une organisation d'exercer un contrôle très strict sur la sécurité de ses systèmes, qu'ils soient virtuels ou physiques.

StoneGate Management Center



Conclusion

La virtualisation étant en passe de se généraliser, les professionnels de la sécurité et les responsables informatiques doivent également veiller à ce que ces nouveaux environnements soient tout aussi sécurisés que les anciens systèmes physiques. Pour ce faire, ils doivent considérer sous un nouvel angle les stratégies de sécurité réseau, les systèmes et les outils de gestion/surveillance. Stonesoft est l'une des seules sociétés à fournir une suite de solutions logicielles de sécurité réseau et de continuité de service. Elle est idéalement positionnée pour accompagner des entreprises de toutes tailles dans la sécurisation de leurs infrastructures informatiques virtuelles.

À propos de Stonesoft

Stonesoft Corporation (OMX : SFT1V) est un fournisseur novateur de solutions de sécurité réseau intégrées. Ses produits sécurisent le flux d'informations à l'échelle d'entreprises distribuées. Les clients de Stonesoft sont notamment des entreprises dont les besoins croissants requièrent une sécurité réseau avancée et une connectivité professionnelle permanente. La solution de connectivité sécurisée StoneGate™ fusionne les aspects de la sécurité réseau que sont le pare-feu (FW), le réseau privé virtuel (VPN), la prévention d'intrusion (IPS), la solution de réseau privé virtuel à technologie SSL (SSL VPN), la disponibilité de bout en bout, ainsi qu'un équilibrage des charges plébiscité, au sein d'un système dont la gestion est centralisée dans des environnement physiques et virtuels. Les principaux avantages de la solution de connectivité sécurisée StoneGate se traduisent notamment par un coût total de possession faible, un excellent rapport prix/performances et un retour sur investissement élevé.

La solution SMC (StoneGate Management Center) permet une gestion centralisée des solutions StoneGate Firewall with VPN, IPS et SSL VPN. Les solutions StoneGate Firewall et IPS fonctionnent en synergie pour fournir une défense intelligente à l'échelle du réseau de l'entreprise toute entière, tandis que la solution StoneGate SSL VPN renforce la sécurité dans le cadre d'une utilisation mobile et à distance.

Fondé en 1990, Stonesoft Corporation a son siège mondial à Helsinki, en Finlande, et un autre siège social aux États-Unis, à Atlanta, en Géorgie. Pour plus d'informations, visitez notre site Web, www.stonesoft.com.

À propos de l'auteur

Architecte solutions senior chez Stonesoft Inc, Mark Boltz a effectué des présentations lors de conférences et de salons professionnels sur la sécurité des informations. Ainsi a-t-il notamment tenu des séminaires sur la virtualisation de la sécurité pour SHARE, dirigé des colloques sur les protocoles de routage dynamique pour SANS, présenté la gestion de la sécurité réseau pour RSA et exposé la sécurité de la voix sur IP lors de l'Internet Telephony Conference and Expo. Parmi ses contributions écrites, on peut citer des articles sur la sécurité des informations et la planification de la continuité de service pour l'International Legal Technical Association (ILTA) ainsi que sur la sécurité de la virtualisation pour CSO. Mark Boltz possède plus de 18 ans d'expérience dans le domaine des technologies de l'information, dont plus de dix ans consacrés spécifiquement à la sécurité de l'information. Instructeur StoneGate agréé (CSGI), il est également titulaire de la certification CISSP des experts en sécurité des systèmes d'information, de la certification CISA (certified information systems auditor) et de l'IEM de la NSA. Résidant dans le nord de la Virginie, il est membre de l'Information Systems Security Association (ISSA) chapitre Virginie du Nord, du programme Infragard du FBI, de la League of Professional Systems Administrators (LOPSA), de USENIX-SAGE, de l'IEEE Computer Society, du Computer Security Institute (CSI) et de l'ISACA.

STONESOFT

Stonesoft Corporation

Itälahdenkatu 22 A
00210 Helsinki
Finland
tel. +358 9 476 711
fax. +358 9 476 712 34

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338, USA
tel. +1 770 6681 125
fax. +1 770 6681 131

IDC
Analyze the Future

WHITE PAPER

L'administration et la Sécurité des Terminaux Windows Mobile.
« Un investissement indispensable et rapidement rentabilisé.»

Sponsored by: Sparus Software

septembre 2007

IDC OPINION

Associant les bénéfices de l'intégration de différents outils de gestion des ressources (aussi bien du côté des terminaux mobiles que du Système d'Information), les solutions de Mobile Device Management (MDM) deviennent indispensables au déploiement rapide d'applications métiers en situation de mobilité.

Il est aujourd'hui clair que les entreprises accélèrent le déploiement de solutions de mobilité auprès de leurs employés pour leur offrir la possibilité de se connecter de n'importe où au système d'information de l'entreprise, par l'intermédiaire des terminaux de poche communicants (PDA et smartphones) et des connexions sans fil des opérateurs mobiles. Dans ce contexte, l'enjeu réside dans la fourniture d'un service sophistiqué et de haute performance dans un environnement business mis à l'épreuve 24h/24 et 7j/7.

Les solutions de MDM qui offrent une réponse adaptée à cet enjeu vont rapidement se développer dans les entreprises dans les années à venir. Ainsi selon IDC, le marché des solutions de MDM qui s'est élevé à près de 230 millions de dollars en 2006 sera porté par une croissance annuelle moyenne de 29% au cours des cinq prochaines années.

Le marché des applications mobiles a démarré avec des solutions permettant uniquement l'accès aux messageries électroniques, aux agendas et à la gestion des contacts. Il évolue maintenant vers les applications de Sales Force Automation et Field Force Automation (SFA, FFA), et autres services web. Ces solutions interagissent avec les applications critiques des entreprises, si bien que les besoins de fiabilité et de sécurité sont renforcés.

Acteur central du marché des plates-formes mobiles, Microsoft n'a pas toujours été perçu comme un fournisseur de solutions de gestion des terminaux mobiles performantes. De ce fait, certains acteurs se sont positionnés sur ce segment de marché avec des offres très spécifiques, en complément de l'offre de Microsoft.

L'exemple de l'offre développée par Sparus montre que nous assistons à un tournant pour les solutions de MDM. A l'image d'EveryWAN Mobility Manager, les offres les plus structurées reposent sur cinq dimensions fonctionnelles : une gestion étendue des actifs, le paramétrage des terminaux, des fonctions de télédistribution d'applications, une sécurité renforcée et des fonctionnalités innovantes telles que le tunneling applicatif et l'intégration avec les outils de gestion du système d'information.

124, Bureaux de la Colline 92213 Saint-Cloud Cedex, France Tél: 01 55 39 61 00 Fax: 01 55 39 61 01

Elles permettent aux entreprises de proposer un service de haut niveau aux utilisateurs de terminaux de poches communicants en assurant :

- Une optimisation des performances des applications mobiles: la partie réseau mobile constitue sans nul doute le talon d'Achille de ces applications. Assurer la continuité du service en cas de problèmes de couverture, d'utilisation dans des conditions difficiles, de déconnexion, de latence des réseaux sans fil est au cœur de la réussite des projets.

- Un niveau de sécurité en adéquation avec la stratégie générale de l'entreprise. Les solutions de MDM doivent être alignées avec la politique de sécurité de l'entreprise en proposant des fonctionnalités d'authentification des terminaux et des utilisateurs nomades, de cryptage des flux, de protection des données stockées sur le terminal et de protection des attaques extérieures (virus, spams…).

- Une réduction de la complexité de la gestion du parc et des utilisateurs : la diffusion des terminaux mobiles à un plus grand nombre de collaborateurs et la possibilité d'accéder à des applications métiers renforcent les besoins en support de la part du helpdesk. Les fonctionnalités des solutions de MDM permettent de réduire la durée des interventions et de faciliter l'adoption des applications mobiles par les employés concernés dans l'entreprise.

- Une contribution à la réussite financière des projets de mobilité : les solutions de MDM exercent une action significative sur l'économie des projets de mobilités en réduisant les coûts de helpdesk, de mise en route des terminaux (provisioning), de distribution d'applications et les dépenses auprès des opérateurs grâce à une diminution des consommations en bande passante. En outre la réduction du nombre d'incidents et des durées de dépannage permet d'augmenter la productivité des employés.

Ce livre blanc, rédigé par IDC et sponsorisé par Sparus Software, traite des principaux éléments à prendre en compte dans le choix d’une solution de MDM et les bénéfices associés. Les cas clients fournissent des illustrations des bonnes pratiques retenues par les entreprises.

Lars Vestergaard, Research Director, Wireless Services

Généralisation de la mobilité et des terminaux de poche communicants

Du fait de la montée en puissance des performances des réseaux mobiles et des terminaux, une évolution accélérée des processus d'entreprises et des modèles d'organisation se réalise, tirant partie de la mobilité des employés. Dans un environnement en mutation, les entreprises étendent l'accès aux outils de mobilité à une part toujours plus importante de leurs employés. L'objectif est de leur permettre de se connecter de n'importe où et à tout moment au système d'information de l'entreprise.

Ce mouvement a démarré par les personnels itinérants : en premier lieu les dirigeants, puis les commerciaux et consultants, et plus récemment s'est étendu aux techniciens (maintenance, service après vente).

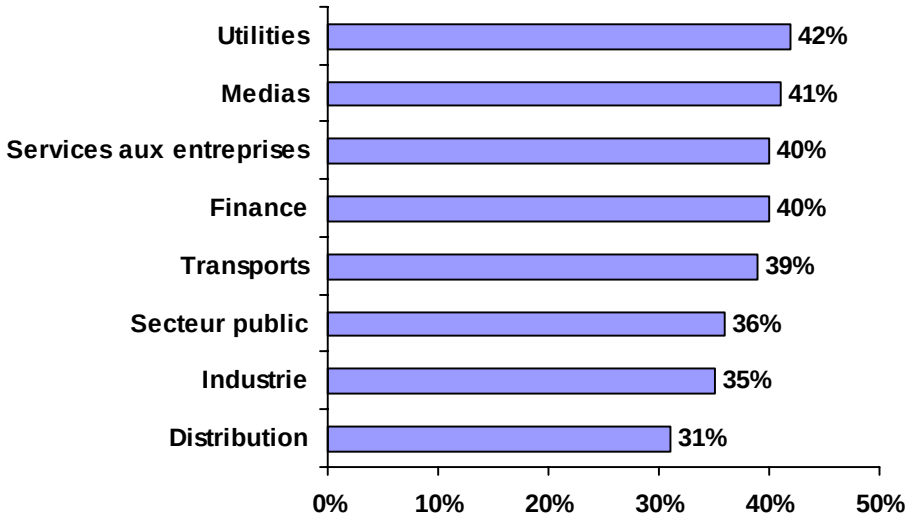
La dynamique s'étend aujourd'hui au-delà des seuls personnels itinérants pour atteindre une population plus large composée principalement de cadres, ce qui accélérera la croissance du marché. Ainsi, IDC estime que dans le monde entier la population des employés mobiles passera de 708,5 millions (23,1% des employés) en 2005 à 878,2 millions (27,3%) en 2009 (source : Worldwide Mobile Worker Population IDC). En 2011, les livraisons de terminaux de poche communicants en entreprise (smartphones et PDA communicants) s'élèveront à plus de 82,3 millions d'unités, soit une croissance annuelle de près de 54%. IDC estime qu'en 2011, Microsoft livrera 24,2 millions de ces unités, soit une part de marché de plus de 29% sur le segment entreprise.

Toutes les entreprises sont concernées, même les plus petites. Ainsi, selon une enquête réalisée par IDC auprès des entreprises françaises de plus de 50 salariés, la part des entreprises équipées en solution de mobilité est passée de 39% au début de l'année 2006 à 46% au début de l'année 2007.

FIGURE 1

Part des entreprises européennes de plus de 50 salariés ayant mis en place une solution de mobilité data

Question : votre entreprise a-t-elle mis en place une solution de mobilité data?



Source: IDC, 2007

Développement et spécialisation des usages

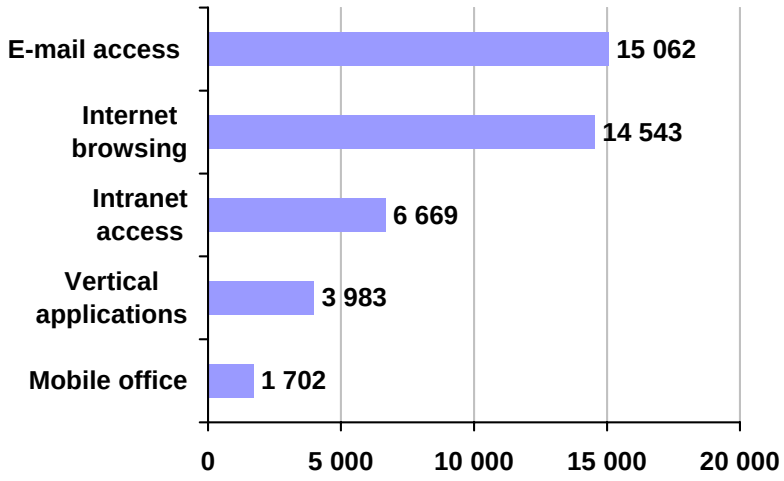
Les terminaux de poche communicants sont en premier lieu utilisés pour l'accès à la messagerie et l'utilisation d'Internet. Bien que l'accès aux applications métier soit encore peu répandu, il représente un développement majeur des applications data mobiles en Europe tant du côté de la demande que de l'offre. La démarche consistant à proposer sur des terminaux de poche des solutions métiers constitue une rupture déterminante par rapport aux pratiques classiques du marché. Elle implique de proposer à l'utilisateur un usage de plus en plus spécialisé de son terminal lié à la fonction qu'il occupe.

Les entreprises sont amenées à répondre à plusieurs types de besoins :

- Les équipes dirigeantes et les cadres : ces populations doivent rester joignables et accéder aux documents en tout lieu et tout moment.
- Les équipes commerciales : il s'agit d'améliorer la relation client, d'accélérer les cycles de vente et de réduire le temps consacré aux tâches administratives. Ces populations doivent être en mesure de consulter les dossiers clients et d'accéder aux bases de données produits.
- Les équipes logistiques : il s'agit d'optimiser les tâches (optimisation des tournées), de réduire les risques d'erreurs et d'améliorer la satisfaction client.
- Les équipes techniques : les enjeux portent sur la facilitation des conditions d'interventions, la réduction des tâches administratives et l'amélioration de la qualité de service.

FIGURE 2

Nombre d'utilisateurs data mobile en Europe par type d'applications (en milliers)



Source: IDC, 2007

Solutions de MDM : une prise de conscience progressive

Dans ce contexte d'évolution très rapide, la gestion des terminaux de poches communicants est une donne essentielle pour les entreprises qui doivent livrer un service sans faille aux utilisateurs. Les outils de MDM (Mobile Device Management) ouvrent la possibilité de gérer des parcs complexes de terminaux hétérogènes, utilisés pour divers usages par différents profils d'utilisateurs. Les solutions de MDM peuvent être mises en place par toute entreprise pour laquelle la gestion efficace de la mobilité des employés est une priorité. IDC estime que moins de 30% des entreprises ont déployé une solution de MDM. Parmi elles, on trouve principalement des entreprises qui doivent gérer des centaines, voire des milliers de terminaux. Les entreprises ayant moins de 50 terminaux mobiles n'ont pas encore déployé ce type de solution.

La notion centrale et structurante du concept de MDM est l'intégration des outils et fonctionnalités concourrant à la gestion des ressources, des usages et des flux d'informations. Les solutions de MDM reposent sur cinq dimensions fonctionnelles et technologiques.

Gestion des actifs

La gestion des actifs permet de faire l'inventaire global des ressources disponibles : type de terminal, de logiciel, ressources mémoires, batteries. Elle offre également des possibilités de gestion des licences présentes sur les terminaux. De plus elle permet de contrôler l'utilisation des logiciels et les droits d'accès des utilisateurs.

Paramétrage

Le paramétrage à distance des terminaux est un point essentiel lors du provisioning initial et des mises à jour. Cette fonction inclut notamment les paramètres de connexion sur les réseaux sans fil (réseaux WiFi ou réseaux cellulaires des opérateurs mobiles) et les profils des utilisateurs.

Télédistribution d'applications

La télédistribution d'applications consiste à installer une application ou un patch sur un ou plusieurs terminaux mobiles "over the air". Elle s'appuie sur les fonctions d'inventaires de terminaux qui fournissent les informations nécessaires : caractéristiques des terminaux et des logiciels déjà installés. Un de ses avantages est qu'elle permet d'augmenter la vitesse de déploiement de nouvelles applications. Elle diminue également les coûts de maintenance en évitant le retour des terminaux aux centres techniques et les installations manuelles répétitives.

Sécurité

La plupart des solutions de MDM intègrent des fonctions de protection sous forme de mot de passe, d'authentification des utilisateurs, de blocage des terminaux. Il est cependant essentiel de proposer également des technologies d'encryption des données, de chiffrement SSL, d'authentification par certificat. D'autres fonctionnalités sont parfois proposées telles que des antivirus et antispams.

Fonctionnalités avancées

Plusieurs types de fonctionnalités avancées sont parfois proposés par les fournisseurs de solutions de MDM :

- Gestion des déconnexions, compression des flux et tunneling applicatif afin d'améliorer le fonctionnement des applications mobiles sur les réseaux sans fil des opérateurs mobiles.
- Prise en main des terminaux à distance et établissement d'une communication vocale avec l'utilisateur en encapsulant un canal VoIP dans un canal data.
- Intégration avec l'infrastructure informatique en place : annuaires d'entreprise, infrastructure réseau (pare-feu, réseau privé virtuel…), outils de gestion, de supervision et de customer care.
- Fonctions de backups d'applications, de configurations ou de fichiers.

Principaux enjeux dans la mise en place de solutions de MDM

Si la mise en place d'une solution de MDM est critique pour la réussite d'une démarche de mobilité en entreprise, les questions soulevées par l'existence d'un parc installé et par la justification économique sont au cœur de chaque projet.

- Croire qu'il est facile de mettre en place une solution de MDM après le déploiement d'une flotte de terminaux mobiles est une erreur. Cela est possible mais loin d'être optimum dans la gestion du projet. IDC préconise de mettre en place une solution de MDM en même temps que le déploiement initial des terminaux et des applicatifs. Cela permet d'éviter des coûts supplémentaires, des disfonctionnements et des risques liés à la sécurité.

- Croire qu'une solution de MDM engendre de la complexité et augmente les coûts d'exploitation est également une erreur. Au contraire, en facilitant la gestion des terminaux mobiles et des applications, les solutions de MDM interviennent surtout sur les OPEX qui peuvent représenter jusqu'à deux tiers des investissements globaux dans le cadre d'un projet de mobilité.

  - Ainsi les solutions de MDM diminuent les consommations en bande passante en réduisant le transfert de données grâce aux mécanismes de reprise au "paquet près" lors d'incidents de réseau et en comprimant les données. Les économies réalisées peuvent atteindre 50% à 80% du trafic sur les réseaux sans fil.

  - Les coûts de support aux utilisateurs sont également minimisés. En cas d'incident, la prise en main à distance permet de réduire les temps d'interventions du helpdesk et de supprimer un grand nombre de retour de terminaux en panne. Les temps de traitement d'un incident sont diminués de 50% à 70%. Les économies réalisées sur le personnel du helpdesk sont proches de 30%.

  - Les fonctions de télédistribution des applications permettent de réduire les coûts de configuration initiale ainsi que les coûts liés à la mise à jour des applications. La télédistribution permet de réduire l'ensemble de ces coûts de près de 50%.

- Selon les différentes études de cas analysées par IDC, le remboursement de l'investissement (payback) pour une solution de MDM se fait en moyenne entre 6 et 9 mois.

TABLE 1

Checklist : les sept points à vérifier

Chaîne de valeur	Points à contrôler	Indicateurs de performances clés
Installation	Mise en place de la solution en minimisant les développements	Délais Coûts de développement et d'intégration Coûts de training
Activation des terminaux	Provisioning initial et paramétrage	Temps moyen d'activation
Réseaux mobiles	Gestion des déconnexions, compression des flux et solutions de tunneling applicatif	Taux d'incidents Bande passante Productivité par utilisateur
Helpdesk	Prise en main à distance	Taux de retours de terminaux Temps moyen de résolution d'incident Durée d'immobilisation de l'utilisateur
Mise à jour des applications	Fonction de télédistribution "over the air"	Taux de retours de terminaux Temps moyen d'installation
Sécurité	Gestion des identités, gestion des intrusions	Taux de perte de terminaux Temps moyen de restauration
Intégration avec l'infrastructure informatique	Compatibilité avec l'infrastructure existante	Coûts de développement et d'intégration Coûts de saisie et de mise à jour Coûts de modification des processus en place

Source: IDC, 2007

L'APPROCHE DE SPARUS SOFTWARE VIS A VIS DES ENJEUX DU MDM.

Sparus Software est une entreprise française créée en 2003. Sparus est certifiée Microsoft Gold Partner dans les domaines d'expertise ISV/Software solutions et Mobility Solutions.

Sparus propose une suite logicielle de gestion et de sécurisation centralisée de terminaux mobiles communicants. EveryWAN Mobility Manager offre des fonctions de tunneling applicatif, de compression à la volée des paquets de données et de reprise en état d'avancement. En outre EveryWAN facilite les installations et mises à jour d'applications grâce aux fonctions d'installation et de configuration "over the air".

Sparus a tenu à effectuer le processus de certification « Designed for Windows Mobile » de Microsoft pour son agent logiciel, de manière à assurer une compatibilité maximale avec la large gamme de terminaux proposés sur le marché et une installation possible quel que soit le modèle de sécurité imposé par les opérateurs cellulaires.

Pour répondre aux besoins de support des utilisateurs, Sparus propose EveryWAN Remote Support qui permet au helpdesk de prendre en temps réel le contrôle des terminaux à distance et d'établir une communication vocale avec l'utilisateur grâce à une fonction de Voix sur IP. EveryWAN Remote Support accède à l'ensemble des informations du terminal, assure le transfert des fichiers et l'installation des logiciels sur les terminaux et permet de redémarrer les terminaux à distance.

Sparus a renforcé les fonctions de sécurité d'EveryWAN en proposant l'option EveryWAN Secure Device qui intègre les services de chiffrement en AES des flux en tunnel SSL, d'authentification mutuelle forte serveur-terminal, de déploiement "over the air" de certificat client et de chiffrement des données locales sur le terminal.

La solution de Sparus, comme toute solution de MDM, est principalement destinée aux équipes d'exploitation des infrastructures informatiques. Sparus a apporté beaucoup d'attention à l'ergonomie et au fonctionnement intuitif de sa solution, qui doit être mise en œuvre et utilisée rapidement et simplement, sans faire appel à des équipes spécialisées dans le développement logiciel.

CAS CLIENTS

TABLE 2

Synthèse des cas clients

Entreprise	Secteur d'activité	Enjeux de la mobilité	Apports de la solution Sparus
CEGEDIM	Conception de bases de données et de logiciels pour le monde de la santé.	Assurer aux visiteurs médicaux un accès performant aux applications de CEGEDIM	Mécanisme de prise en main à distance Compression des données Utilisation dans plusieurs pays et sur les réseaux de plusieurs opérateurs
Deloitte France	Audit et conseil	Connections aux messageries et agendas	Interfaçage avec l'annuaire de l'entreprise Mécanisme de prise en main à distance Gestion du parc Télédistribution
e.l.m. leblanc	Chauffage au gaz	Gestion des tournées, envois des comptes rendus d'intervention, commandes de pièces	Synchronisation Fonctions de télédistribution Mécanisme de prise en main à distance
M6	Chaîne de télévision généraliste	Connections aux messageries et agendas et de manière plus marginale à des serveurs applicatifs	Amélioration de la sécurité Mécanisme de prise en main à distance
VELUX France	Commercialisation de fenêtres de toit, de stores intérieurs, de volets et stores d'extérieur…	Gestion des plannings d'intervention	Synchronisation Mécanisme de prise en main à distance Télédistribution

Source: IDC, 2007

CEGEDIM

Depuis 1969, CEGEDIM conçoit des bases de données exclusives et des solutions logicielles à forte valeur ajoutée en direction des professionnels du monde de la santé et de l'assurance santé. En 2006 CEGEDIM a réalisé un chiffre d'affaires de 541 millions EUR. Après l'acquisition au début 2007 de Dendrite (spécialiste des solutions à destination de l'industrie pharmaceutique sur le continent américain et en Asie Pacifique), le chiffre d'affaires 2006 en base annuelle pro-forma s'établirait à 877 millions EUR. CEGEDIM exerce ses activités dans plus de 80 pays et emploie près de 7 500 collaborateurs.

Enjeux des solutions de mobilité : améliorer la productivité des visiteurs médicaux

CEGEDIM gère un parc de 25 000 PDA qui équipent une population de visiteurs médicaux. Les terminaux PDA ont été retenus pour leurs coûts moins élevés que des PC portables. Les visiteurs médicaux utilisent principalement les applications dédiées au monde de la santé développées par CEGEDIM. Elles sont généralement couplées à la messagerie. La solution de CEGEDIM a été historiquement développée sur Palm en 2002 avant que le choix ne s'oriente vers Windows Mobile, en raison de l'évolution du marché. Les connexions des terminaux au système d'informations se font via GPRS.

Pour la gestion de son parc de PDA, CEGEDIM se heurte à plusieurs difficultés :

- Des problèmes de couverture réseau dans certains pays.
- L'hétérogénéité des PDA due aux différents rachats effectués par CEGEDIM ainsi qu'à la disponibilité selon les pays des terminaux et des OS.
- L'intégration de la solution data mobile avec la solution d'authentification Radius en place dans l'entreprise.

Bénéfices de la solution EveryWAN : fiabilisation des connexions, réduction des coûts et support aux utilisateurs

La solution proposée par Sparus est déployée à partir de juillet 2006, prioritairement dans les zones où les clients de CEGEDIM étaient insatisfaits des conditions réseau. Le déploiement de la solution est également en cours au Mexique. EveryWAN répond à plusieurs exigences :

- Compatibilité avec l'infrastructure actuelle : l'adoption d'EveryWAN n'implique aucune modification des applications développées par CEGEDIM.
- Utilisation d'EveryWAN dans un contexte multi-opérateurs et multi-réseaux.
- Fiabilisation des connexions grâce au mécanisme de reprise sur incidents qui permet de réduire les volumes de données transmises et les coûts associés.
- Mécanisme de compression des données qui permet de faire face à l'augmentation de la volumétrie et de mieux maîtriser les budgets. En particulier lors de ses premiers déploiements en France et au Mexique, CEGEDIM a constaté une réduction du trafic data de 64%.
- La fonctionnalité de prise en main à distance est un atout non négligeable dans la résolution des incidents et contribue à améliorer la qualité du service fourni par les quatre personnes dédiées à l'exploitation des plates-formes hébergées.
- A moyen terme, CEGEDIM envisage d'utiliser EveryWAN pour le cryptage des données des PDA.

Deloitte France

Deloitte France est un cabinet d'audit et de conseil, membre du réseau international Deloitte Touche Tohmatsu qui compte parmi les « Big Four ». Avec 6.000 collaborateurs en France, Deloitte exerce ses activités dans deux grands domaines :

d'une part l'expertise comptable, d'autre part l'audit, le conseil et les services juridiques pour lesquels les effectifs s'élèvent à près de 3 000 personnes.

Mobilité des collaborateurs et communication à distance : au cœur des enjeux de l'entreprise

Les métiers de l'audit et du conseil nécessitant une présence permanente auprès des clients, la mobilité des collaborateurs et les moyens de communication sont au cœur des enjeux de l'entreprise. En 2005, après un test auprès d'un groupe d'utilisateurs, Deloitte choisit d'équiper ses collaborateurs de « téléphones communicants » dotés du système d'exploitation Windows Mobile qui offre une interface graphique adaptée aux habitudes des utilisateurs et d'intéressantes perspectives d'évolution. Malgré l'attention portée sur le choix initial de la solution et les efforts déployés, Deloitte est confronté à des problèmes récurrents de synchronisation et peine à assurer un support à distance efficace. Au bout de deux ans, l'entreprise décide de revoir sa stratégie mobile et l'organisation de son support.

Bénéfices de la solution EveryWAN : améliorer la gestion du parc, la qualité du support et bénéficier de fonctions de télédistribution

Début 2007, Deloitte lance un appel d'offres et renouvelle ses abonnements voix et données, la gestion de la flotte et le support. Mille cinq cents terminaux sont déployés pendant l'été auprès des collaborateurs qui ont le choix entre trois modèles HTC : le S720 retenu par 55 % de la population, le S620 pour 30% et le PDA Touch Phone pour les 15% restants. Les associés disposent d'abonnements de 50 Mo et reçoivent leurs messages en mode Push. Les collaborateurs disposent d'abonnements de 5 Mo avec une synchronisation de leur messagerie en mode pull, tout en étant parallèlement dotés de cartes 3G+ qui leur permettent de se connecter en permanence au système d'information sans limite de temps ou de volume de données.

Tous les téléphones ont été équipés de la solution EveryWAN de Sparus. Plusieurs facteurs ont justifié le choix de Sparus lors de l'appel d'offres :

- EveryWAN est interfacé avec l'annuaire de l'entreprise (Active Directory) mis à jour automatiquement par l'application de gestion des ressources humaines. Ce point est fondamental : il permet aux administrateurs systèmes de s'appuyer sur les mêmes groupes de sécurité de l'annuaire et d'éviter les double-saisies.

- EveryWAN améliore le support utilisateur grâce à la prise de main à distance. D'une part les délais de résolution sont largement réduits ; d'autre part l'utilisateur final apprécie particulièrement la possibilité offerte par Sparus de dialoguer avec le technicien pendant la session de prise de main à distance (en encapsulant un canal VoIP dans un canal data).

- EveryWAN offre une gestion efficace de parc à moindre coût. Deloitte a défini des paramètres de base qui sont désormais distribués, vérifiés et restaurés en cas de besoin.

- Grâce à la fonction de télédistribution, les mises à jour des fonctionnalités et des versions de logiciels peuvent être réalisées sans rappel des terminaux. Cette fonction justifie à elle seule l'investissement d'EveryWAN.

- En outre la solution de Sparus permet de mesurer précisément les consommations et les usages, ce qui permet de revoir les types d'abonnement et

de préparer dans les meilleures conditions les futurs appels d'offres auprès des opérateurs mobiles.

Deloitte envisage maintenant de porter des applications métiers sur les terminaux mobiles (gestion du temps et indicateurs stratégiques). A cette occasion, Deloitte pourra profiter des fonctions de compression et de tunneling applicatifs d'EveryWAN.

e.l.m. leblanc

Filiale du groupe Bosch depuis 1996, e.l.m. leblanc est l'un des leaders sur le marché français des systèmes de chauffage au gaz et de production d'eau chaude sanitaire. Cette entreprise possède aussi son propre service après vente, fort de 300 techniciens.

En 2006 Cette société a réalisé un chiffre d'affaires de 121 millions EUR. et emploie près de 700 personnes.

Enjeux des solutions de mobilité pour les techniciens : optimisation des tournées et contrôle des coûts grâce au projet e-dépanneur

En 2003, e.l.m. leblanc a lancé le projet e-dépanneur pour ses 300 techniciens. e-dépanneur comportait plusieurs objectifs : réduire le temps de traitement des dossiers, optimiser les réapprovisionnements, suivre en quasi-temps réel l'activité des techniciens, proposer le paiement par carte bancaire en remplacement des chèques, augmenter la qualité des travaux et renforcer l'image de marque d'e.l.m. leblanc.

Depuis juin 2007, la première génération d'équipement informatique « PDA grand public et imprimante portable » a été remplacée par des terminaux Intermec CN3 équipés de lecteur de piste magnétique pour paiements par carte bancaire ainsi que d'une imprimante Zebra RW420 avec connexion Bluetooth. Ces équipements ont été choisis en raison de leur robustesse et de leur autonomie. L'application a été développée en utilisant le framework .NET qui permet des évolutions de versions logicielles à moindre coût et dans des délais très courts. Les terminaux fonctionnent sous Windows Mobile 5.

Grâce à e-dépanneur, les techniciens reçoivent chaque matin leur plan de tournée mis à jour. Ils ont accès aux fiches clients, aux fiches appareils et aux contrats de maintenance. A l'issue de l'intervention, le paiement par carte bancaire est proposé et une facture ou un devis sont imprimés. Les comptes rendus d'intervention sont envoyés lors des synchronisations. Les techniciens ont la possibilité de faire des commandes automatisées en cochant les cases de réapprovisionnement. Ils peuvent également effectuer l'inventaire des équipements dans leurs véhicules grâce à un lecteur de code barre.

Lors du passage des réseaux fixes commutés et GSM aux réseaux GPRS/EDGE à la fin 2006, e.l.m. leblanc s'est trouvé confronté à des problèmes de synchronisation. En effet les techniciens évoluent parfois dans des zones où le signal est faible. De plus, ils effectuent parfois des synchronisations dans leurs véhicules alors qu'ils circulent.

Bénéfices de la solution EveryWAN : synchronisation et fonction de télédistribution

e.l.m. leblanc a adopté la solution EveryWAN à la fin 2006. Plusieurs facteurs ont fait pencher la balance en faveur de Sparus :

- EveryWAN permet de résoudre le problème de synchronisation. La solution développée par Sparus permet de masquer les coupures de réseau vis-à-vis de l'application mobile, EveryWAN jouant le rôle de "buffer".

- Les fonctions de télédistribution facilitent les mises à jour des versions des logiciels à moindre coût.

- La prise en main à distance permet d'améliorer le support aux utilisateurs, de réduire les temps d'intervention et de diminuer le nombre des retours de terminaux.

- Grâce au passage aux réseaux GPRS/EDGE et à l'utilisation d'EveryWAN, e.l.m. leblanc a constaté une baisse moyenne des consommations de plus de moitié et une diminution de plus de 50% des incidents de synchronisation. Les gains constatés devraient augmenter avec le passage à la synchronisation différentielle prévue en 2008.

- e.l.m. leblanc est extrêmement soucieux de la sécurité car les paiements peuvent être effectués par carte bancaire. Les techniciens ne peuvent faire aucune modification sur l'application. Si des modifications étaient effectuées, EveryWAN se charge de remettre les paramètres ad hoc automatiquement.

- Grâce à la solution EveryWAN, e.l.m. leblanc est en mesure d'améliorer le suivi des consommations afin de vérifier si les forfaits sont bien adaptés.

EveryWAN participe à la réussite du projet e-dépanneur pour lequel e.l.m. leblanc a consenti un effort financier important : près de 1% du chiffre d'affaires. Les principaux gains se mesurent en termes de réduction des délais pour traiter un dossier (il fallait parfois 20 jours auparavant), en frais postaux, en frais de saisie, en augmentation de chiffres d'affaires lié à la réduction des erreurs… L'ensemble des gains a permis une rentabilité globale du projet en moins de 24 mois.

M 6

M6 est une chaîne de télévision généraliste dont le principal actionnaire est le groupe RTL. En 2006, M6 a réalisé un chiffre d'affaires de 1,283 milliard EUR, soit une hausse de près de 19% par rapport à l'année précédente. Cette croissance est le résultat de la hausse de l'audience, des activités Internet et de l'activité Vente à Distance. M6 emploie près de 1 600 personnes. L'essentiel des sites est situé en région parisienne. Le groupe dispose de quelques décrochages régionaux qui correspondent à des rédactions locales.

Enjeux des solutions de mobilité : améliorer les communications et l'accès distant aux serveurs

La DSI de M6 gère 3 types de populations nomades : les VIP, les commerciaux ainsi que certains informaticiens et consultants. Ces populations ont été équipées de 200 ordinateurs portables et de 100 PDA dont le nombre augmentera dans les années à venir. Tous les terminaux peuvent se connecter au réseau WiFi de l'entreprise et aux réseaux cellulaires GPRS, EDGE ou 3G. Pour les connexions cellulaires, M6 a retenu des forfaits data illimités. Les ordinateurs portables équipent les 3 types de populations nomades.

Les PDA: équipements et usages

- Les PDA équipent deux populations : les VIP et les informaticiens qui ont besoin de travailler à distance. A l'origine, M6 avait choisi les terminaux Treo de Palm. Lors du renouvellement du parc, M6 s'est aperçu que Palm allait de plus en plus utiliser le système d'exploitation Windows Mobile. M6 a donc délibérément opéré le choix de Windows Mobile, seul OS compatible avec l'infrastructure de M6 en l'état. M6 a fait le choix de terminaux HP IPAQ 6915 pour l'ensemble des utilisateurs. Ce choix sera reconsidéré car ces terminaux sont trop riches pour les VIP qui ont besoin d'une ergonomie renforcée mais pour des usages simples.

- Les usages des VIP concernent les applications de messagerie, de navigation sur Internet et de consultation d'agenda. Les informaticiens utilisent les PDA pour se connecter à un serveur applicatif.

Principales difficultés

Le principal enjeu porte sur la sécurisation de ces nouveaux points d'entrée dans le système d'informations, mais également de faire accepter de nouvelles règles aux populations équipées de ces terminaux, notamment les VIP.

Bénéfices de la solution EveryWAN : crypter les flux et améliorer le support aux utilisateurs en attendant d'utiliser l'ensemble des fonctionnalités

M6 a retenu Sparus au dernier trimestre 2006 essentiellement pour deux bénéfices principaux :

- Améliorer la sécurité et le support aux utilisateurs : contrôler à distance les terminaux avec cryptage des flux est essentiel pour améliorer l'aide aux populations nomades en cas d'incidents et pour accroître la sécurité. M6 considère que le premier objectif de gains de productivité, d'efficacité et de confort a été atteint. En particulier, le travail de la ressource dédiée aux solutions mobiles (environ une personne en équivalent temps plein) dans l'équipe en charge de l'assistance aux utilisateurs, s'en trouve facilité.

- Tunneling applicatif : M6 a également fait le choix d'EveryWAN pour ses fonctionnalités de tunneling applicatif. Jusqu'à présent, elles ne sont pas utilisées mais M6 tirera la quintessence de cette solution à partir de 2008 lorsque M6 déploiera des applicatifs spécifiques.

VELUX France

VELUX France est une filiale du groupe danois VELUX A/S. VELUX France commercialise des fenêtres de toît, des raccordements d'étanchéité, des habillages intérieurs, des stores intérieurs, des volets et stores d'extérieur, des commandes électriques et des capteurs solaires. VELUX France ne vend pas directement ses produits aux consommateurs mais à des grossistes et à des grandes surfaces spécialisées. VELUX France emploie environ 250 personnes.

Enjeux des solutions de mobilité pour les techniciens du service d'après vente : optimiser les tournées d'intervention

Les techniciens du Service Après Vente sont munis de PDA grand public Qtek et d'imprimantes légères. Grâce aux PDA, les techniciens ont accès aux applications

métiers SAP où se trouvent les plannings d'intervention. Les comptes rendus d'intervention sont directement rédigés sur les PDA et envoyés au système d'intervention de l'entreprise par synchronisation.

Lors du lancement du projet, VELUX France a rencontré des problèmes de synchronisation. Un meilleur réglage du "time out", diagnostiqué grâce à EveryWAN, a permis de régler une partie des problèmes mais pas totalement. En outre, il était nécessaire de proposer aux techniciens un support, utilisant une prise en main à distance, comparable à celui proposé aux commerciaux sur leurs PC portables.

Bénéfices de la solution EveryWAN : améliorer la gestion du parc et bénéficier de fonctions de télédistribution

Afin de répondre aux objectifs de synchronisation et de prise de main à distance, VELUX France a choisi EveryWAN et l'a déployé à la fin 2005. Sparus a contribué à la réussite du projet qui se solde par un retour sur investissement plus rapide que prévu : 18 mois au lieu de 24 mois. VELUX France se félicite d'avoir dorénavant 93% des lignes d'interventions confirmées sur PDA, que le temps de traitement des rapports d'intervention soit passé de 5,5 jours à 0,5 jour et que le chiffre d'affaires par technicien ait augmenté. Au bout de plus d'un an et demi d'utilisation, VELUX France peut également dresser un bilan de l'utilisation d'EveryWAN.

- Un taux de compression des données synchronisées d'environ 70%, qui réduit ainsi les coûts de communication.
- L'utilisation de la fonction de télédistribution d'EveryWAN permet les mises à jour de logiciel, tandis que la restauration du PDA repose sur un clone stocké sur carte SD.
- Pouvoir accéder directement au PDA et en même temps parler avec le technicien facilitent grandement le diagnostic et la résolution des problèmes. Chaque prise en main à distance (un appel sur deux) est un gain de temps pour la hot line et le technicien, et évite le retour de matériels en atelier.

ARISTOTE Association Loi de 1901. Siège social : CEA-DSI CEN Saclay Bât. 474, 91191 Gif-sur-Yvette Cedex.
Secrétariat : Aristote, École Polytechnique, 91128 Palaiseau Cedex.
Tél. : +33(0)1 69 33 99 66 Fax : +33(0)1 69 33 99 67 Courriel : Marie.Tetard@polytechnique.edu
Site internet http://www.aristote.asso.fr