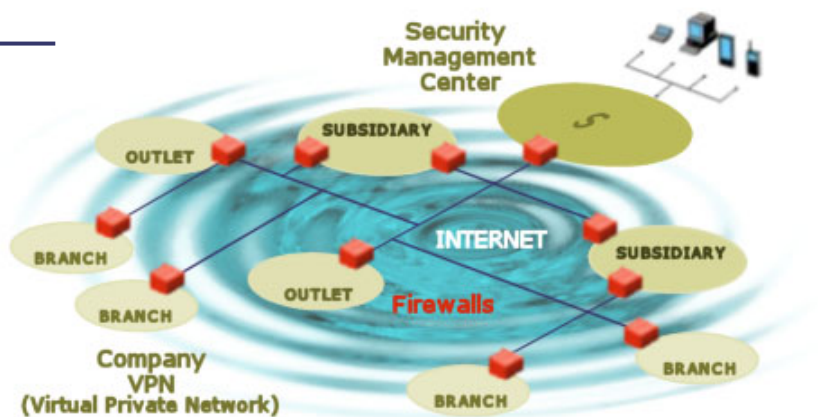


Cette étude de cas illustre l'apport clef d'une infrastructure de médiation pour construire une solution d'analyse de journaux de sécurité pour des réseaux virtuels privés de grande taille. Cette étude s'adresse aux Administrateurs de sécurité et aux Editeurs de logiciels de sécurité.

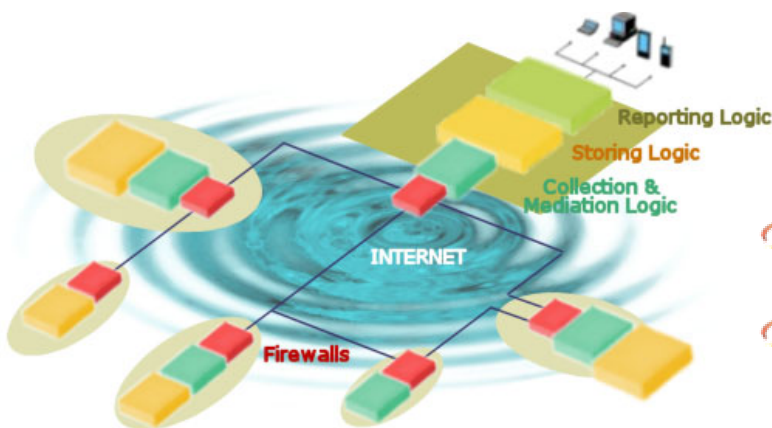
Bénéfices clients

L'analyse de journaux de sécurité est l'outil indispensable à un administrateur qui souhaite avoir une vue synthétique du fonctionnement de son installation sécurisée. L'infrastructure de médiation est la pierre nécessaire pour disposer à tout moment d'une information fiable, à haute valeur sémantique, en temps réel, sur un point unique d'administration alors que les équipements peuvent être fortement distribués sur un large territoire (agences, filiales, groupement régionaux, nationaux, ...). Elle s'adresse aux administrateurs de sécurité comme à l'éditeur du logiciel de sécurité :



L'administrateur de sécurité dispose d'un dispositif global de télésurveillance de son installation qui évite la duplication d'expertise sécuritaire sur chaque site géographique. A cette réduction des coûts d'exploitation s'ajoute la réduction des coûts matériels car l'infrastructure de médiation permet la décentralisation d'opérations coûteuses en matériel tels que l'archivage des journaux, la corrélation et fusion de données de sécurité. L'infrastructure de médiation permet aussi la consolidation des données multi-site pour fournir une information plus riche que la simple juxtaposition.

L'Editeur de logiciel de sécurité bénéficie de l'infrastructure SCAL AGENT pour enrichir son offre sans pour autant devoir maîtriser les technologies complexes d'architecture et de programmation distribuée. L'infrastructure ouverte de SCAL AGENT lui permet de reprendre ses propres composants métier existants, ou d'en construire rapidement de nouveaux, et de les proposer dans des configurations matérielles largement distribuées. Outil d'intégration, l'infrastructure SCAL AGENT s'insère facilement au sein de l'architecture logicielle de l'éditeur, pouvant inclure en particulier des outils de reporting ou des bases décisionnelles. Enfin la flexibilité des outils lui permet de répondre rapidement à l'émergence de nouveaux besoins, mais aussi de s'adapter à faible coût à la spécificité de ses clients.



Architecture de la Solution

- Logique de Collecte** : collecte le flux d'enregistrements de sécurité. Située au plus près de l'équipement de sécurité, elle garantit la fiabilité des données collectées.
- Logique d'Archivage** : conserve, archive et compresse les informations sur le long terme. Située au plus près de l'équipement de sécurité, elle est structurée en plusieurs niveaux permettant d'équilibrer le besoin de conservation sur le long terme et la place disque disponible. Elle est configurable pour s'adapter à la politique de sécurité du client. Elle peut également incorporer une intelligence propre, permettant l'adaptation automatique de la politique d'archivage en fonction d'événements externes comme l'éventuelle isolation prolongée suite à une coupure réseau.

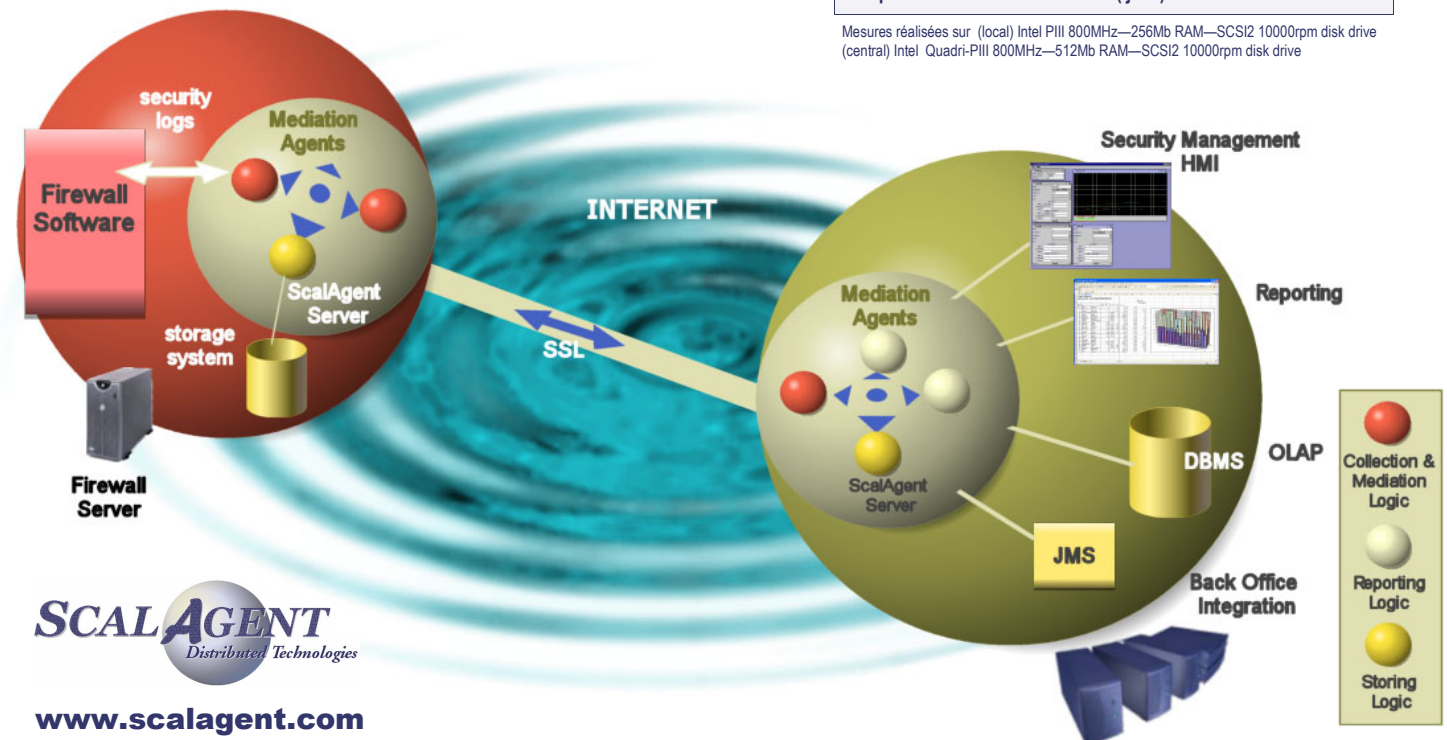


Logique de Médiation : Filtre, agrège, transforme, enrichit, corréle les enregistrements de sécurité pour divers usages. Elle permet ainsi le calcul d'indicateurs statistiques, d'indicateurs de surveillance temps réel, ou la détection de violation de règles de sécurité. Cette logique est répartie sur toute l'infrastructure réseau selon les critères définis par le fournisseur de service : temps de réponse, trafic réseau, capacité CPU, ... La solution sera d'autant plus scalable que le traitement est décentralisé près des sources de données. Ainsi le déport sur l'équipement de sécurité d'une partie du calcul des indicateurs statistiques permet de réduire de 20 fois le volume d'informations transmises au nœud central réalisant la consolidation des résultats. De même,

L'intégration technique

L'infrastructure de médiation **SCALAGENT** est l'outil d'intégration entre le pare-feu et les applications qui exploitent les données de sécurité. Le dialogue avec le pare-feu s'effectue par la récupération périodique des fichiers de logs du pare-feu correspondant. La fourniture des données calculées de sécurité s'effectue par une multitude de connecteurs :

- par fichier texte, CSV, XML, Excel, ...
- par chargement dans des SGBD : JDBC, Oracle, ...
- via JMS (Java Messaging Service)
- par intégration programmatique dans le logiciel de supervision métier.



SCALAGENT
Distributed Technologies

www.scalagent.com

E-mail: contact@scalagent.com
C/O INRIA - 655, Avenue de l'Europe
F-38334 St-Ismier Cedex - France
Tel. +33 4 76 61 52 56 Fax. +33 4 76 61 52 52

© 2002 ScalAgent Distributed Technologies S.A.
ScalAgent Distributed Technologies is a registered trademark. JMS™ and all Java-based products are trademarks or registered trademarks of Sun Microsystems Inc. in the U.S. and other countries.

des nœuds de consolidations intermédiaires peuvent être introduits pour réduire le besoin en puissance du nœud central. Par ailleurs, le déport d'une partie des traitements améliore la résistance de la solution en cas d'isolation de l'équipement.



Logique de Présentation : présente l'information produite à l'administrateur. Cette problématique métier peut aller au delà du domaine d'intervention de la médiation, qui exhibe alors ses fonctions d'intégration à destination de l'éditeur ou de l'intégrateur pour s'interfacier avec un outil externe (Oracle, WebTrends, Business Objects, infrastructures EAI). La médiation assure le formatage des données, et peut également activer l'outil externe.

Bénéfices techniques

L'usage de l'infrastructure **SCALAGENT** dans ce cas d'étude a permis d'apporter des caractéristiques techniques primordiales

- Flexibilité par le déploiement et redéploiement automatisé des chaînes de médiation
- Tolérance aux pannes et intégrité des données en cas de problèmes réseaux ou matériels
- Confidentialité par cryptage des données
- Performance par la décentralisation des traitements

Volumes de données brut (/jour)	1Go par pare-feu
Temps de traitement site local (/jour)	30min par pare-feu
Facteur de compression (entre le pare-feu et le site central)	x20
Volume de données transféré (/jour)	5Go sur central
Temps de traitement site central (/jour)	2h

Mesures réalisées sur (local) Intel PIII 800MHz—256Mb RAM—SCSI2 10000rpm disk drive
(central) Intel Quadri-PIII 800MHz—512Mb RAM—SCSI2 10000rpm disk drive