



RSA

Solution RSA

**Sécuriser les VPN SSL avec
l'authentification forte à deux
facteurs RSA SecurID®**

Il est essentiel que seuls des utilisateurs habilités puissent accéder à nos systèmes stratégiques...

Les entreprises doivent de plus en plus souvent fournir à leurs salariés, partenaires et clients des accès mobiles ou distants à leurs applications et ressources internes dans un environnement simple et performant. Dans ce contexte, il est essentiel que seuls des utilisateurs habilités puissent accéder à ces systèmes stratégiques. Pour garantir une réelle sécurité réseau, le mode d'accès lui-même doit être à toute épreuve et de robustes contrôles doivent permettre d'identifier toute personne sollicitant l'accès aux ressources réseau.

L'association de la technologie SSL (Secure Socket Layer) aux solutions d'authentification forte à deux facteurs de RSA permet aux entreprises de toutes dimensions de protéger leurs réseaux tout en offrant aux utilisateurs habilités des accès distants économiques et simples. RSA, la Division Sécurité d'EMC, propose une solution éprouvée d'authentification à deux facteurs pour maximiser la protection des réseaux VPN SSL. RSA SecurID® présente en effet tous les gages de flexibilité, d'extensibilité et de simplicité d'administration pour fournir des accès mobiles et distants aux réseaux VPN SSL préservant parfaitement les informations et applications.

Les nouveaux challenges de l'accès distant

Dans un contexte d'internationalisation, les environnements de travail ont évolué - passant d'un modèle centralisé et contrôlé à celui de la mobilité et de la performance. Face au rapide développement du télétravail et de l'itinérance, les entreprises doivent s'équiper de technologies plus efficaces pour maximiser la productivité de leurs collaborateurs, où qu'ils se trouvent, tout en conservant une sécurisation supérieure des informations stratégiques. Cette nouvelle exigence d'ouverture peut faire courir des risques considérables aux entreprises qui ne prennent pas d'indispensables mesures de protection.

Disposant souvent de ressources informatiques limitées pour administrer un nombre croissant d'utilisateurs distants, elles sont en effet confrontées à des réseaux VPN trop complexes pour garantir une protection appropriée des données critiques. Il est donc essentiel d'avoir recours à des technologies innovantes, simples à intégrer à l'existant et offrant aux utilisateurs des outils de support en libre-service pour améliorer leur qualité d'expérience et alléger la

charge du support technique. En synthèse, les outils de sécurisation des accès distants doivent répondre aux exigences suivantes...

Des équipes toujours plus mobiles

Le nombre de collaborateurs distants et mobiles continue d'augmenter — une grande partie d'entre eux travaillant occasionnellement à domicile. Les entreprises doivent donc rendre leurs informations sensibles accessibles, de partout et à tout moment, à leurs salariés, clients et partenaires — tout en assurant l'authentification des utilisateurs et la protection des ressources.

Des accès distants à partir de systèmes non gérés

Les collaborateurs doivent accéder aux informations utiles où qu'ils se trouvent ; ils emploient pour cela divers appareils et systèmes en dehors du périmètre d'administration de l'entreprise : téléphones intelligents, assistants personnels, accès sans fil depuis des hôtels, des aéroports, etc. Les entreprises sont soumises à une pression croissante pour accepter ces accès — sans risquer d'intrusion.

De nouveaux impératifs de conformité

De multiples lois et règlements imposent aujourd'hui aux entreprises de protéger l'accès aux informations et leur confidentialité : Sarbanes-Oxley, Gramm-Leach-Bliley, Bâle II, PCIDSS (Payment Card Industry Data Security Standard), HIPAA (Health Insurance Portability and Accountability Act), etc. Pour s'y conformer, elles sont tenues de contrôler et journaliser les accès et de documenter leurs pratiques de conformité conformément aux dispositions légales qui leur sont applicables.

Des menaces de plus en plus sophistiquées

La prévention des accès illicites n'est pas uniquement une exigence métier ; elle est également essentielle pour préserver l'image de marque et la réputation de l'entreprise. Les pirates sophistiquent constamment leurs attaques pour détourner des informations et ternir l'image des entreprises auprès du public.

Un impératif de continuité

Comme on a pu le constater récemment, les catastrophes naturelles, par essence imprévisibles, exigent une résilience supérieure des infrastructures de communication — pour que tous ceux qui en sont victimes puissent informer leurs proches, pour organiser les secours, etc. Il est donc crucial, à la suite d'un scénario catastrophe, de disposer d'un mode de collaboration sécurisé pour assurer la continuité métier et la viabilité de l'entreprise. Cela exige d'être capable de récupérer rapidement et de reconnecter l'ensemble des intervenants afin de maintenir la productivité. Malheureusement, plus de 60 % des entreprises ayant subi une telle catastrophe sont incapables de maintenir leurs activités et mettent la clé sous la porte au cours de l'année qui

suit. Au vu de ces sombres statistiques, les entreprises comprennent aujourd'hui que leurs plans de continuité métier doivent être intégrés à la planification globale de leurs accès distants.

Des implications métier fortes

Les entreprises doivent développer une stratégie aboutie de protection des accès distants pour :

- garantir la sécurité des données en transit ;
- valider l'identité des utilisateurs finaux demandant l'accès aux informations ;
- auditer l'accès aux ressources.

Les entreprises doivent faire en sorte que leurs collaborateurs distants et mobiles disposent de toutes les prérogatives d'accès nécessaires pour atteindre une productivité optimale (sans compromis de sécurité) et qu'ils accèdent librement aux réseaux pour accomplir sereinement leur mission — où qu'ils se trouvent. Ainsi, les entreprises doivent en permanence jongler entre sécurité et productivité en fournissant à leurs utilisateurs — partout et en permanence — des accès à leurs réseaux privés par Internet.

Les réseaux VPN Internet éliminent une bonne part des dilemmes administratifs et financiers liés aux réseaux étendus (WAN) et améliorent indiscutablement la productivité des collaborateurs distants et mobiles. Si des mesures suffisantes sont prises pour renforcer la sécurité des accès, ces gains de producti-

Les entreprises doivent s'assurer que leurs collaborateurs distants et mobiles disposent de toutes les prérogatives d'accès nécessaires pour atteindre une productivité optimale – sans compromis de sécurité.

tivité ne sont pas contrebalancés par des risques supérieurs de sécurité ni d'intégrité des systèmes internes.

Considérations relatives aux accès distants

Dans un passé relativement récent, la collecte d'informations exigeait du temps et des ressources ; elle est aujourd'hui librement accessible à toute personne disposant d'une connexion Internet. Cette omniprésence d'Internet a permis de redistribuer les cartes plus équitablement, en offrant à des entreprises de toutes tailles des possibilités égales de compétitivité. Les accès distants, mobiles et en temps réel étaient l'apanage de grandes entreprises disposant d'infrastructures, de budgets et de ressources suffisants pour les sécuriser ; des solutions innovantes permettent aujourd'hui à tous les acteurs du marché de capitaliser sur Internet pour sécuriser leurs connexions.

Les réseaux VPN permettent ainsi d'envoyer et de recevoir des données de manière totalement sécurisée et privée sur des réseaux qui ne le sont pas (comme Internet). Le standard IPSec de l'IETF définit les principes d'authentification de la couche réseau, de contrôle d'accès, de cryptage, d'intégrité des messages et de protection des rediffusions afin de sécuriser les communications entre appareils et applications réseau. IPSec analyse les paquets IP émis/reçus par l'interface réseau et ne laisse passer que ceux qui répondent à la politique de sécurité configurée. Cette solution, était utilisée pour les

premières implémentations VPN jusqu'à l'apparition de la technologie SSL.

En effet, les réseaux VPN IPSec répondent aux exigences de connectivité intersites mais laissent subsister de nombreux challenges dès qu'il s'agit de gérer des points de terminaison multiples et les accès dynamiques de collaborateurs distants ou mobiles. Les réseaux VPN sous IPSec offrent solution adaptée pour gérer un nombre raisonnable d'utilisateurs de confiance, connectés avec des ordinateurs gérés par l'entreprise, et pour les connexions intersites à travers un accès transparent au réseau local. La technologie SSL est un protocole réseau éprouvé pour sécuriser les transmissions de documents par Internet utilisant une clé de cryptage privée. Prise en charge par tous les navigateurs Web, c'est le standard de sécurisation de fait des transactions en ligne.

Les réseaux VPN SSL sont adaptés pour administrer n'importe quel nombre d'utilisateurs, où qu'ils soient et quels que soient les appareils qu'ils utilisent ou leurs prérogatives. Ils permettent de sécuriser le transport sur Internet sans logiciel client spécialisé et offrent une flexibilité supérieure grâce à des interfaces Web pour PC, téléphones intelligents, PDA, etc.

La technologie SSL, plus simple à déployer et administrer qu'IPSec, offre un accès distant sécurisé

Il est indispensable que les utilisateurs soient clairement authentifiés pour s'assurer qu'ils sont effectivement ceux qu'ils prétendent être avant de leur ouvrir tout accès au réseau VPN.

Authentification à deux facteurs

Le changement du code toutes les 60 secondes implique que le mot de passe de l'utilisateur final change également toutes les 60 secondes.



Quelque chose que vous savez...

Quelque chose que vous détenez...

aux applications avec n'importe quel navigateur Web standard et présente des gages supérieurs de contrôle administratif, de flexibilité et de gestion à forte granularité des accès aux ressources d'entreprise.

Avec les réseaux VPN SSL, les entreprises peuvent sécuriser les accès distants aux e-mails et autres applications de l'ensemble de leurs collaborateurs — où qu'ils se trouvent et quel que soit le système qu'ils utilisent. Ils permettent également de protéger les portails et Extranets et de simplifier l'accès des partenaires commerciaux.

Coûts totaux d'exploitation (TCO)

Le coût total d'exploitation se définit comme le coût d'acquisition augmenté des charges cumulées d'utilisation et de maintenance dans le temps. La plupart des entreprises y attachent une importance critique — notamment lors de l'achat d'une solution VPN. Il est également important d'évaluer précisément les coûts d'utilisation et de maintenance pour s'assurer que ses coûts récurrents d'exploitation ne seront pas trop élevés. En d'autres termes, son TCO (Total Cost of Ownership) doit être aussi faible que possible tout en maximisant la productivité des utilisateurs grâce au support des ressources existantes et à la fourniture d'accès distants ergonomiques.

Dans un contexte de pénurie de ressources, la nécessité d'installer, de configurer et de supporter un logiciel client sur les postes des utilisateurs, puis de les former, joue en la défaveur des réseaux VPN IPSec.

Sécurité

Cependant, la sécurité demeure une considération cruciale. Un tunnel VPN IPSec ouvert est un point d'entrée sur le réseau local de l'entreprise. Certes, le tunnel lui-même est crypté et sécurisé, mais cette protection est **considérablement affaiblie** si l'une des extrémités de la connexion reste ouverte sur le monde extérieur (notion de "split-tunneling"). Si dans le cas d'une connexion intersite, on peut raisonnablement présumer que la connexion VPN s'effectue entre deux entités connues ; tel n'est pas le cas des utilisateurs distants empruntant un tunnel LAN. Les risques de sécurité pesant sur les accès distants concernent essentiellement les entrées provenant du tunnel — à travers des sessions VPN laissées ouvertes par les utilisateurs. Quelle que soit la taille d'une entreprise, même une brèche mineure de sécurité peut avoir de multiples conséquences : du préjudice irréversible d'image de marque à la fermeture pure et simple de l'entreprise. Si les réseaux VPN protègent les données pendant la transmission, il est essentiel d'authentifier les utilisateurs pour s'assurer qu'ils sont bien ceux qu'ils prétendent être avant d'activer leur accès VPN.

Mots de passe – La parole aux utilisateurs ...

Les mots de passe ne sécurisent pas les réseaux ...Les organisateurs d'InfoSecurity Europe ont mené à Londres une étude informelle, démontrant que :

- 71 % des utilisateurs échangeaient leurs mots de passe contre une barre chocolatée !
- Un utilisateur en retient en moyenne quatre — un malchanceux indique même devoir en retenir 40 !
- Les personnes en utilisant plusieurs reconnaissent les avoir notés ou cachés dans leur bureau ou sur leur ordinateur.
- 34 % indiquent le mot/groupe de mots utilisé si on leur demande s'il est lié à un animal ou un enfant.
- Les mots de passe de tous les sondés étaient inspirés de noms de famille, d'animaux ou d'équipes de sport.
- 80 % des répondants sont lassés des mots de passe et préféreraient un autre moyen de connexion.

Sécurité d'entreprise

Les réseaux VPN SSL s'appuient sur Internet et sur certains protocoles intrinsèques à son utilisation. Le cryptage SSL a été développé pour sécuriser les transactions financières en ligne et reste un composant fondamental de l'e-business. Le logiciel client — qui initialise des transferts sécurisés de données — est intégré à tous les navigateurs standards et donc disponible sur les PC et systèmes mobiles de tous les utilisateurs. Selon Gartner : "Avant 2008, les réseaux VPN SSL constitueront la méthode principale d'accès à distance pour plus des deux tiers des collaborateurs distants, des trois quarts des sous-traitants et pour 90 % des accès occasionnels de collaborateurs."

Les entreprises doivent donc arbitrer entre le verrouillage des informations sensibles et l'indispensable ouverture de certaines données aux collaborateurs mobiles et non-techniciens dans le respect des bonnes pratiques de sécurité afin qu'ils accomplissent efficacement leur mission. Une solution de sécurité performante doit intégrer ces deux dimensions pour éliminer les risques liés aux accès distants et mobiles. Selon une étude réalisée par Forrester Research, le principal challenge pour gérer des effectifs distants et mobiles en forte croissance est de garantir des niveaux supérieurs de sécurité sans nuire à la transparence ni à la productivité d'utilisation.

Limites des mots de passe

Les mots de passe ne sont pas suffisants pour protéger les accès aux réseaux VPN SSL. Simples à créer et à utiliser, leur prolifération les rend aujourd'hui passablement coûteux alors même qu'ils laissent subsister des vulnérabilités qui engagent les entreprises à se tourner vers des solutions d'authentification forte. Les vols et autres utilisations frauduleuses des mots de passe sont fréquents ; les utilisateurs ayant naturellement tendance à les noter

sur des feuilles volantes ou dans des fichiers — exposant ainsi leur entreprise à des risques considérables d'accès illicites.

Ils soulèvent également de sérieuses préoccupations de conformité vis-à-vis des exigences légales, dans la mesure où ils ne permettent pas de certifier l'identité de la personne se connectant à distance. La frustration des utilisateurs est également un facteur à prendre en compte : tant pour ceux qui souhaiteraient une méthode d'authentification plus simple et cohérente ; que pour le management, déplorant les risques qu'ils font courir, les coûts croissants d'administration qui en découlent et les pertes de temps et de productivité liées à leur apprentissage (erreurs, appels aux services d'assistance, etc.).

De façon générale, la gestion des mots de passe est extrêmement coûteuse si l'on totalise l'inactivité des utilisateurs et les dépenses de support. Les demandes de réinitialisation de mot de passe peuvent représenter jusqu'au tiers des charges d'assistance — une dépense récurrente qui pourrait pourtant être évitée.

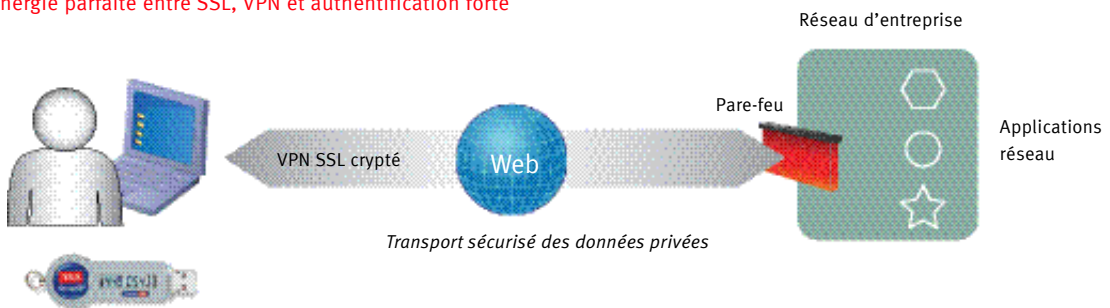
Frustration des utilisateurs, pertes de temps et de productivité, multiplication des appels de support, inquiétude des responsables, inflation des coûts de maintenance, autant d'inconvénients des mots de passe qui mettent en péril la sécurité des réseaux VPN SSL — dans l'incapacité de fournir une identification certaine de l'appelant avant de lui donner accès aux ressources critiques de l'entreprise.

Pour sécuriser les accès distants

L'authentification forte nécessite de fournir deux éléments d'identification pour corroborer l'identité de chaque demandeur d'accès au réseau VPN SSL. Toute entreprise envisageant de déployer un VPN pour protéger ses données en transit doit également s'assurer que les utilisateurs qui s'y connectent sont bien ceux qu'ils prétendent être. Grâce à son approche multiniveau, l'authentification à deux facteurs renforce la sécurité en évaluant l'état du point de terminaison avant toute connexion.

RSA SecurID® est une plate-forme d'authentification forte permettant de certifier l'identité des utilisateurs se connectant à distance aux VPN SSL en exigeant qu'ils fournissent une information qu'ils connaissent (leur numéro personnel d'identification ou code PIN),

Synergie parfaite entre SSL, VPN et authentification forte



Etablissement d'une identité de confiance

Une approche multiniveau de la sécurité

- Authentification forte avant établissement du réseau VPN
- Une couche additionnelle simple à ajouter (PKI / AD / LDAP)
- Evaluation de l'état de sécurité du point de terminaison avant établissement du VPN

et une autre changeant constamment (le code généré par la clé matérielle RSA SecurID ou par l'authentificateur logiciel). RSA Authentication Manager peut être déployé en central pour gérer le moteur d'authentification de RSA SecurID ou s'appuyer sur la solution matérielle RSA SecurID Appliance (en format rack) pour offrir une solution complète et intégrée .

L'accès n'est accordé qu'après la saisie par l'utilisateur d'un mot de passe RSA SecurID valide. Le framework d'authentification prend ensuite le relais pour gérer ou restreindre les accès aux seules ressources habilitées. Avec les solutions d'authentification à deux facteurs de RSA, les entreprises peuvent pleinement capitaliser sur la mobilité de tous leurs collaborateurs avec le même système physique. Cette organisation maximise la productivité en leur permettant d'accéder aux ressources utiles de partout et à tout moment dans un contexte parfaitement sécurisé et aide les entreprises à intégrer des pratiques de conformité au meilleur état de l'art (contraintes légales et réglementaires, protection des informations sensibles, etc.).

Un des principaux avantages des réseaux VPN SSL réside dans l'absence de logiciel client et dans la possibilité de s'y connecter de n'importe quel point d'accès public sans fil. Cette ouverture est

naturellement génératrice de vulnérabilités. En effet, si les réseaux VPN SSL assurent la confidentialité et l'intégrité des données (statiques ou en mouvement) par cryptage, ils ne peuvent pas garantir l'identité de l'appelant ni interdire que des données soient communiqués à des personnes mal-intentionnées.

Exigences fonctionnelles

Le système d'authentification RSA SecurID a été développé spécifiquement pour sécuriser les connexions des collaborateurs distants ou mobiles. Les solutions RSA bénéficient de références incomparables et l'authentification RSA SecurID est compatible avec les applications et environnements existants (pare-feux, appliances, serveurs VPN, etc.). La sécurisation des accès RSA est une solution idéale pour les entreprises de toutes tailles, pouvant librement évoluer en cas d'ajout de nouveaux utilisateurs distants — auxquels il suffira d'indiquer leur identifiant (PIN) et le code changeant constamment de leur authentificateur RSA SecurID pour accéder au réseau dans les mêmes conditions que si leur PC y était physiquement connecté.

Les authentificateurs RSA SecurID sont proposés en plusieurs formats matériels et logiciels pour s'adapter aux différents périphériques de connexion (PDA, téléphones intelligents, etc.). Les utilisateurs n'ont plus besoin de retenir des mots de passe abscons pour s'identifier simplement sur le réseau et établir un tunnel crypté sous SSL ; la solution d'entreprise de RSA s'intègre en toute transparence aux infrastructures et bases de comptes existantes pour maximiser la sécurité et les performances des accès distants.



Les différents formats de RSA SecurID®

Coûts totaux d'exploitation (TCO)

La solution d'authentification à deux facteurs VPN SSL de RSA est tarifée pour s'adapter aux besoins et aux budgets de toutes les entreprises — quelle que soit leur taille. Les authenticateurs RSA SecurID épargnent aux entreprises les coûts et l'inconfort liés à la réinitialisation des mots de passe et suppriment les risques qu'ils laissent subsister — par exemple, quand les utilisateurs les recopient pour s'en souvenir... Il suffit en effet de fournir son identifiant et le code en cours indiqué par la clé.

Les solutions d'authentification à deux facteurs de RSA éliminent également les coûts de support liés aux pertes ou aux oublis de mot de passe et établissent une identité unique par utilisateur pour de multiples applications. Pour ajouter un utilisateur, il suffit d'indiquer son nom, ses habilitations et contrôles d'accès ou d'utiliser les répertoires existants. Aucune configuration additionnelle n'est requise et un processus simple et rapide d'activation permet d'émettre une nouvelle clé SecurID.

Sécurité

La technologie SSL repose sur un cryptage fort qui reste un standard mondial pour les transactions sensibles. Les solutions d'authentification à deux facteurs de RSA protègent les extrémités des tunnels SSL en certifiant positivement l'identité du demandeur. Elles peuvent être intégrées aux moteurs centraux de politiques applicables aux différents groupes d'utilisateurs ainsi qu'aux bases de comptes et aux autres mesures de sécurisation des points de terminaison applicables aux accès distants et mobiles.

Extensibilité

Les solutions d'authentification RSA SecurID pour réseau VPN SSL répondent aux besoins d'accès distants actuels et futurs, grâce à des modalités simples, rapides et économiques d'ajout de nouveaux utilisateurs.

Les solutions d'authentification RSA SecurID pour réseaux VPN SSL répondent aux besoins d'accès distant actuels et futurs des entreprises.

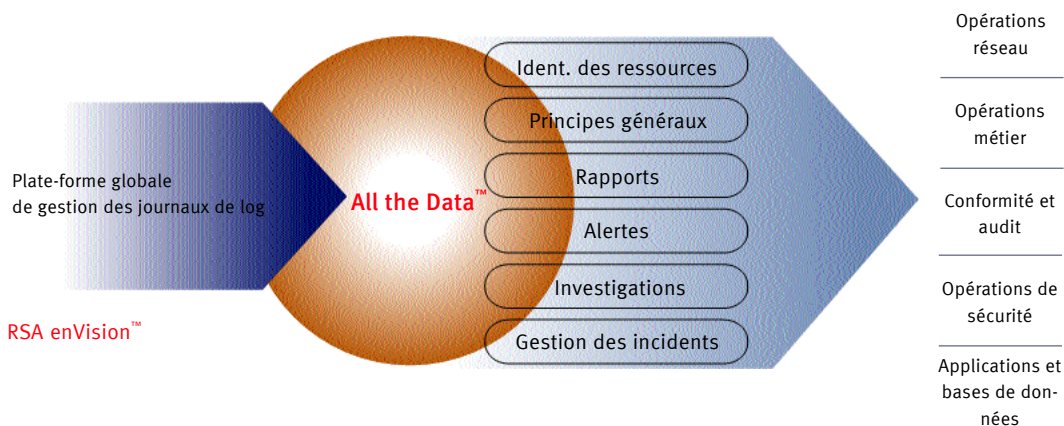
Administration des journaux VPN SSL

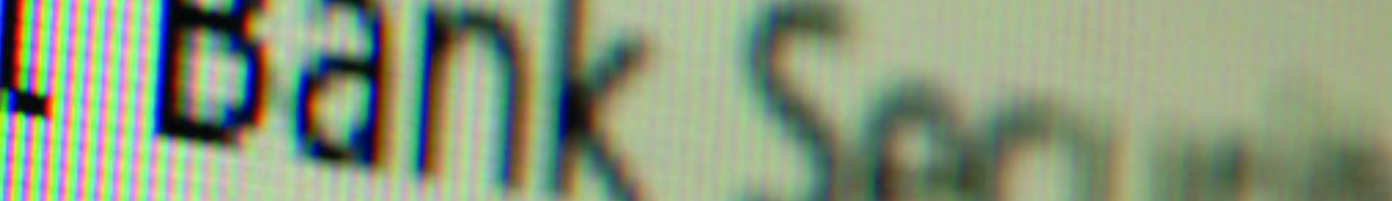
Les appliances RSA EnVision™ réunissent dans une plate-forme unique une puissante trame VPN SSL et une solution d'authentification pour optimiser les opérations de sécurité et de conformité. Selon un rapport du cabinet Gartner :

“Les accès utilisateur doivent faire l'objet d'audits et de contrôles selon une politique prédéfinie. Les informations sur les flux sortant des appareils VPN (événements de connexion, paramètres en vigueur à la connexion, etc.) doivent être inclus dans les solutions de suivi, de journalisation et d'administration des informations et événements de sécurité. Des rapports et alertes doivent également être générés pour contrôler les activités, identifier les violations d'accès ou de politique et surveiller les accès privilégiés et les tentatives d'accès. Les données d'accès VPN doivent être corrélées aux annuaires, aux journaux de log des systèmes d'exploitation et des applications et à d'autres outils de suivi, pour identifier et traiter les incidents de sécurité liés aux activités des utilisateurs.”

Pour garantir une analyse la plus précise possible et une conformité vérifiable, il est nécessaire de procéder à une collecte complète de données. La technologie RSA enVision assure une collecte et une protection efficaces de toutes les données (*All the Data™*) depuis n'importe quel appareil IP, quelle que soit la taille de l'environnement, sans filtrage ni agent. A partir de la base de données IP LogSmart™, les appliances RSA enVision capturent et enregistrent des centaines de milliers d'événements par seconde pour fournir une vue intégrale de l'activité d'un nombre quelconque de sources (appareils réseau, systèmes d'exploitation, applications propriétaires).


Les exigences de conformité et d'investigation nécessitent de conserver des volumes croissants de données. Avec ses outils de collecte et de protection à haute disponibilité et ses solutions d'optimisation du stockage multiniveau, RSA enVision offre aux entreprises une plate-forme économique pour gérer cette considérable quantité de données de façon différenciée selon l'évolution de sa valeur métier. Ses performances éprouvées, ses fonctionnalités de collecte et d'analyse, son extensibilité incomparable et sa capacité à gérer le cycle de vie des informations font de RSA enVision une plate-forme répondant à tous les challenges de conformité et de sécurité. Elle permet en effet de récupérer les données des différents appareils et plates-formes VPN, de corréler les menaces potentielles et de transformer automatiquement les données brutes en informations exploitables de sécurité et de conformité.





Synthèse

RSA propose une puissante solution de sécurité présentant des caractéristiques exceptionnelles de flexibilité, de simplicité d'administration et de robustesse. Sa technologie d'authentification à deux facteurs a été adoptée par des milliers d'entreprises et des millions d'utilisateurs dans le monde. Les solutions RSA SecurID permettent de sécuriser les réseaux VPN SSL afin d'ouvrir des accès simples et sécurisés aux utilisateurs distants. Les entreprises peuvent implémenter ces solutions pour déployer en toute sécurité des réseaux VPN SSL et protéger l'accès à leurs informations. Elles peuvent ensuite collecter, analyser et corréler les données des plates-formes VPN et d'autres appareils réseau à l'aide de RSA enVision. Les solutions RSA permettent de déployer en toute sécurité et à des coûts réduits des réseaux VPN SSL tout en protégeant les données d'entreprise et en assurant l'authentification centralisée des utilisateurs distants avant tout accès aux informations à travers ces réseaux.



RSA, votre partenaire de confiance

RSA, la Division Sécurité d'EMC, est un expert de la sécurité centrée sur l'information et de la protection différenciée des données tout au long de leur cycle de vie. RSA offre à ses clients des outils économiques pour sécuriser leur patrimoine informationnel et les identités en ligne des utilisateurs – où qu'ils se trouvent et sur l'ensemble du trajet – et pour administrer l'intégralité des données et événements de sécurité afin d'assurer leur conformité et leur légalité.

RSA propose des solutions leaders de certification des identités et de contrôle d'accès ; de gestion du cryptage et des clés numériques ; d'administration de la conformité et des informations de sécurité et de lutte contre la fraude. Cette large gamme de solutions certifie l'identité de millions d'utilisateurs dans le monde et des données qu'ils génèrent lors de leurs transactions quotidiennes. Pour plus d'informations, veuillez consulter www.RSA.com et www.EMC.com.

©2006-2007 RSA Security Inc. Tous droits réservés.
RSA, RSA Security, SecurID, enVision, LogSmart et le logo de RSA sont des marques ou marques déposées de RSA Security Inc. aux États-Unis et/ou dans d'autres pays. EMC est une marque déposée d'EMC Corporation. Tous les autres produits et services mentionnés sont la propriété de leurs détenteurs respectifs.

SSLVPN SB 0707



www.rsa.com