Pare-feu, proxy, antivirus, authentification LDAP & Radius , contrôle d'accès des portails applicatifs…

La haute disponibilité de la CHAINE DE SECURITE APPLICATIVE

1.1 La chaîne de sécurité applicative est un élément critique pour la qualité de service rendue aux utilisateurs

Il y a deux manières pour bloquer complètement l'accès de milliers d'utilisateurs à leur système d'information d'entreprise.

Soit vous bloquez un routeur par un mauvais paramétrage, par une panne hardware ou tout simplement un bogue logiciel. Ces éléments sont en général assez simples et peuvent être réparé et/ou remplacé très rapidement.

Soit vous bloquez les systèmes de contrôle d'accès que sont les pare-feux, les portails, les serveurs d'authentification. Les incidents associés à ces éléments sont plus complexes à détecter, diagnostiquer et réparer car ils s'appuient sur des environnements complexes multi-niveaux et peuvent déployer des protocoles de sécurité assez opaques. Ce sont souvent des applications de sécurité très compliquées.

La disponibilité **de la chaîne de sécurité applicative** est un facteur critique pour la qualité de service du système informatique.

1.2 La chaîne de sécurité applicative est composée de 5 types d'applications

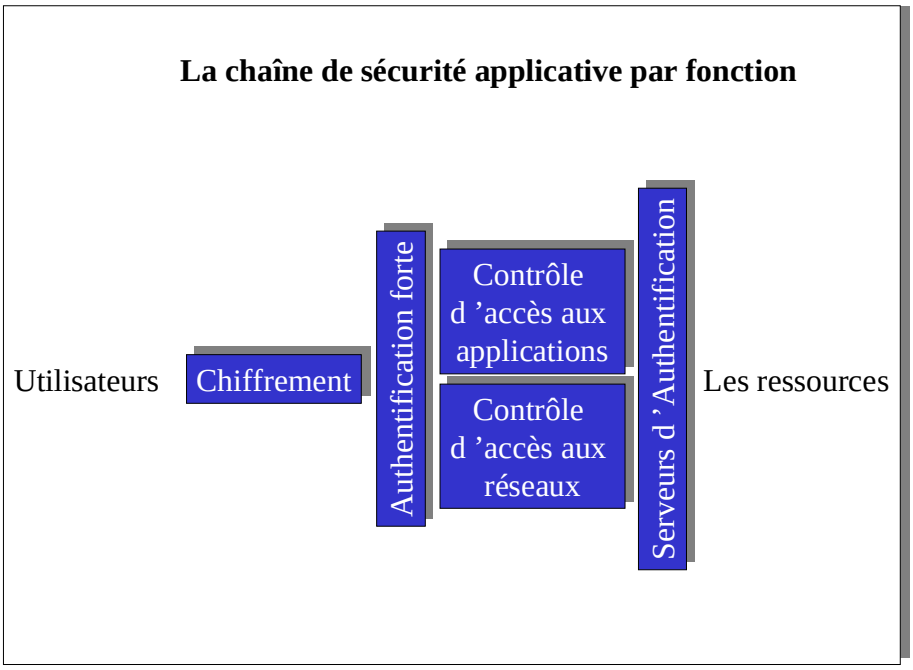
Les modules de chiffrement logiciel ou matériel des échanges qui permettent de protéger les échanges.
- VPN,
- SSL,
- chiffrement AES ou triple DES.

Les applications d'authentification forte qui permettent d'accroître la confiance dans l'authentification d'un utilisateur.
- les infrastructures PKI,
- les applications one time Password,
- les identifications biométriques,
- les identifications par carte à puce.

Les contrôles d'accès aux niveaux du réseau (incluant les applications couche basses) qui permettent de filtrer les types de flux qui peuvent circuler au sein de l'entreprise et de bloquer certaines attaques :
- firewall,
- proxy,
- antivirus.

Les contrôles d'accès aux niveaux de l'application finale qui gèrent les privilèges et les accès des utilisateurs finaux :
- portail web de sécurité,
- application de single sign-on (Web, Legacy, client/serveur…)

Les serveurs d'authentification peuvent s'interfacer avec toute application de sécurité qui a besoin d'authentifier une personne :
- LDAP,
- Radius,
- Annuaire X500.

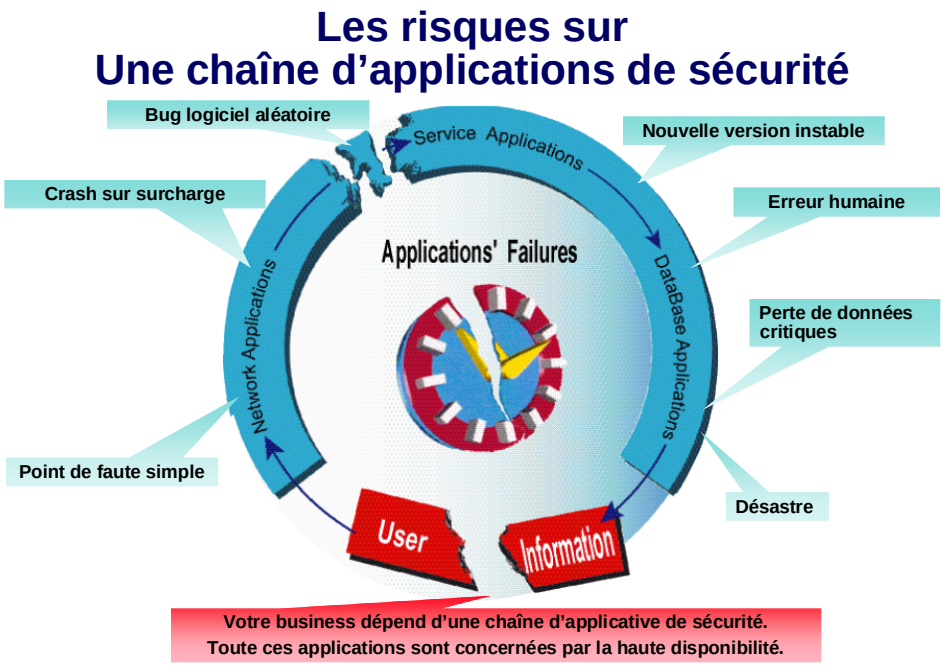


Cette **chaîne de sécurité applicative** recouvre complètement le Système d'Information de l'entreprise : si un maillon se brise, c'est toute la chaîne qui se brise.

1.3 Les opportunités de briser cette chaîne de sécurité applicative sont nombreuses

Selon le Gartner Group, l'indisponibilité d'un système informatique est aujourd'hui liée pour 20 % à des problèmes matériels et surtout d'environnement du matériel (incluant la panne globale à toute la salle machine), pour 40 % à des problèmes logiciels (régression sur évolution logicielle, indisponibilité par surcharge d'un service, bug logiciel aléatoire) et pour 40 % à des erreurs humaines (erreur d'administration et incapacité à redémarrer correctement un service critique).

Une chaîne de sécurité applicative peut donc être brisée pour de nombreuses raisons :
- si une application de sécurité s'exécute sur un seul serveur et si ce serveur est arrêté,
- si une application de sécurité n'est pas capable de supporter la charge,
- s'il y a un bug logiciel aléatoire arrêtant l'application de sécurité à n'importe quel moment,
- si la nouvelle version d'une application de sécurité est instable,
- si un administrateur commet une erreur et qu'il n'est pas capable de redémarrer correctement l'application de sécurité,
- s'il y a perte de données de sécurité,
- et dans le pire des cas à cause d'un désastre.

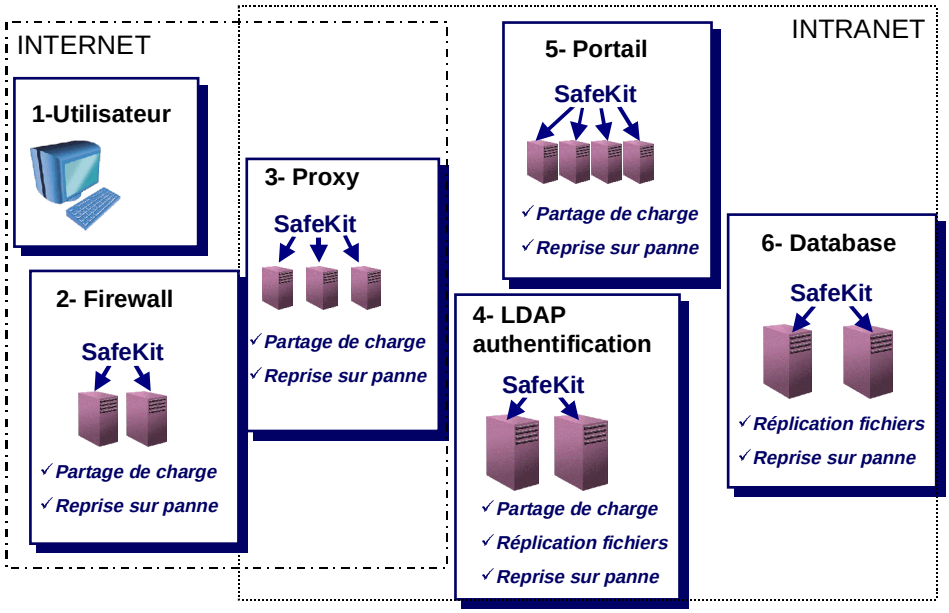


Au sein d'une entreprise, tout accès doit être contrôlé, tout utilisateur doit être identifié. Un seul goulet d'étranglement ou une défaillance ponctuelle dans votre infrastructure de sécurité, et un temps de réponse trop long ou une interruption de service peuvent vous coûter des clients

La solution logicielle, SafeKit, combinant le partage de charge, la réplication de données et la reprise automatique sur panne, vous fournit tout ce dont vous avez besoin pour assurer la haute disponibilité de n'importe laquelle de vos applications de sécurité.

1.4 Comment garantir le fonctionnement d'une chaîne de sécurité applicative

Exemple d'une chaîne de sécurité applicative rendue disponible 24H/24

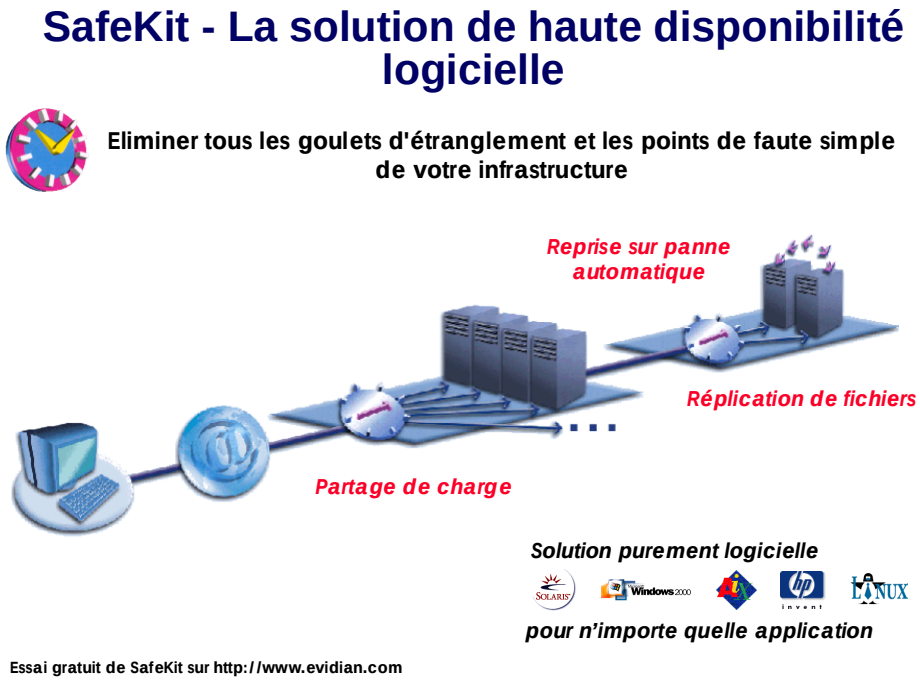


Typiquement, un utilisateur dans une entreprise (le poste de travail à gauche sur la figure précédente) accède à Internet pour réaliser une réservation. Il traverse un firewall et un proxy qui filtre les accès IP, puis ensuite arrive sur un service d'authentification utilisateur LDAP avec mot de passe unique. Une fois authentifié, l'utilisateur est connecté au portail d'entreprise qui lui présente le service de réservation et enfin la réservation est enregistrée dans une base de donnée relationnelle.

L'avantage de SafeKit est d'offrir une solution uniforme de haute disponibilité et de partage de charge tout au long de la chaîne applicative. La console java

d'administration centralisée de SafeKit permet d'avoir une vue et un contrôle uniforme de la chaîne en haute disponibilité.

1.5 La solution SafeKit



Avec SafeKit, vos applications deviennent de manière transparente résistantes à la montée en charge et aux défaillances. SafeKit est une solution purement logicielle qui apporte le partage de charge, la reprise automatique sur panne et la réplication de fichiers à toute application critique : pare-feu, services d'authentification, antivirus, proxy, Web, portails, Oracle, et n'importe quelle application métier.

Haute technologie logicielle

En offrant une adresse IP virtuelle et une mise en œuvre très efficace dans un 'driver' intermédiaire du système d'exploitation, SafeKit distribue le trafic du réseau sur le nombre de serveurs nécessaires pour supporter la charge liée à votre activité.

Avec sa réplication en temps réel des fichiers, n'importe quel type de fichier critique, de la base de données au simple fichier plat, est répliqué à travers le réseau standard. La détection d'erreur matérielle et logicielle ainsi que les procédures de reprise peuvent être personnalisées pour n'importe quelle application critique.

Solution plug&play purement logicielle

SafeKit ne nécessite aucun matériel dédié, comme des boîtiers réseau de partage de charge ou des disques partagés. Il s'adapte à votre architecture réseau et autorise l'utilisation des serveurs à distance pour la résistance au désastre. SafeKit supporte des plates-formes matérielles et des systèmes d'exploitation multiples. En utilisant vos plates-formes matérielles existantes, sans aucun investissement matériel spécifique, ni aucun développement logiciel, vous sécurisez vos applications critiques en quelques jours.

1.6 Les solutions de partage de charge et de haute disponibilité

Les solutions de partage de charge et de haute disponibilité

Solution de haute disponibilité	Dispatchers réseau Partage de charge	Cluster hardware Disponibilité des données	Logiciel Partage de charge & disponibilité des données
Cible	Fermes web	Base de données	Applications logicielles
Le mieux pour	Grand ISP	Grosse base de données	Applications petites et moyennes

Il existe deux grandes familles dans les solutions de haute disponibilité :

- Les boîtiers réseau de partage de charge ont pour principe de placer un équipement réseau en amont des serveurs pour le partage de charge, et d'ajouter un deuxième boîtier pour la reprise sur panne. Ce type de matériel dédié est adapté aux grands ISP avec des portails Internet très chargés mais il est moins bien adapté à une chaîne de sécurité, à cause de la multiplication des boîtiers réseau tout au long de la chaîne et dans les différentes DMZ. De plus, il n'y a pas de surveillance ni de redémarrage automatique des processus critiques d'une application de sécurité.

- Les clusters hardware des constructeurs de plate-forme ont pour principe de placer les données critiques sur un disque partagé et de récupérer le disque partagé en cas de défaillance. Ce type de matériel est adapté aux grosses bases de données et il peut être déployé dans le cadre d'une stratégie SAN. Malheureusement, le toolkit de haute disponibilité est mono-plateforme et il est délivré par le constructeur de la plate-forme. Il est donc mal adapté aux applications de sécurité.

SafeKit apporte en même temps **le partage de charge** et **la disponibilité des données** avec une solution purement logicielle (unique sur le marché). SafeKit ne requiert aucun matériel dédié, comme des boîtiers réseau dispatcher ou des disques partagés. Il peut gérer des plates-formes hétérogènes. En utilisant les plates-formes existantes, en évitant l'investissement dans du matériel dédié et des développements logiciels spécifiques, une application critique peut être sécurisée en quelques jours.

1.7 La technologie SafeKit

Comment fonctionne une solution purement logicielle…?

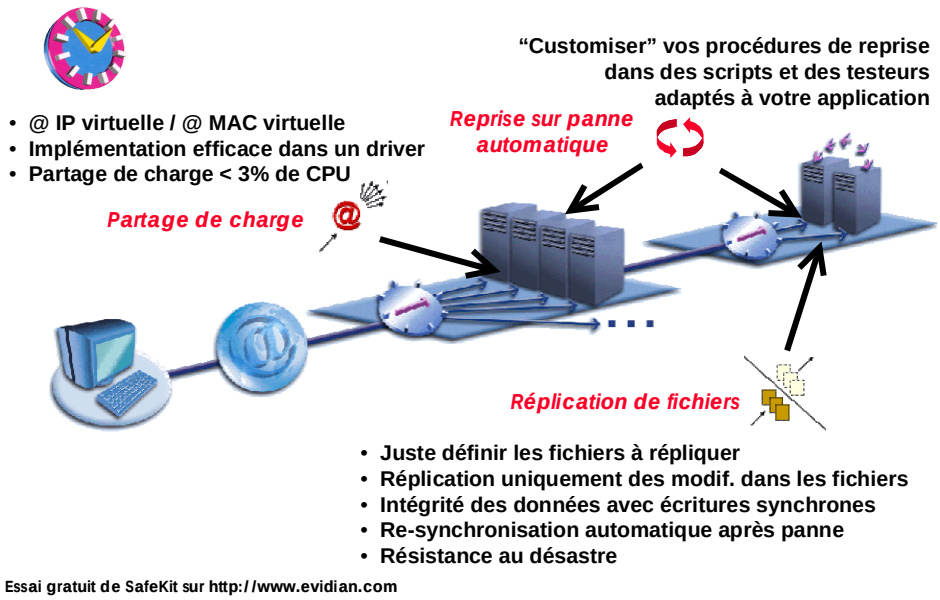
SafeKit combine trois technologies logicielles pour garantir la haute disponibilité de vos applications : le partage de charge, la réplication de fichiers et la reprise automatique sur panne.

Partage de charge efficace sur adresse IP virtuelle

Le trafic réseau en entrée est adressé à un ensemble de serveurs sous la même adresse IP virtuelle, puis distribué grâce à un filtre chargé dans le système d'exploitation de chaque serveur. Ce mécanisme de filtrage très efficace consomme moins de 3% de CPU, quel que soit le nombre de serveurs. La solution est très flexible : les serveurs peuvent être de puissance différente et recevoir plus ou moins de trafic. Si un serveur est défaillant, son trafic est automatiquement redistribué sur les autres serveurs.

Réplication en temps réel à travers un réseau LAN ou WAN standard

La réplication de fichiers est configurée simplement, en définissant les répertoires des fichiers à répliquer. Seules les modifications sont répliquées en temps réel à travers le réseau, limitant ainsi le trafic. Quel que soit le type de base de données, SafeKit assure la sérialisation des écritures sur les fichiers répliqués, l'intégrité des données et la récupération des applications. Après le redémarrage d'un serveur défaillant, SafeKit re-synchronise automatiquement les fichiers sans perturber les applications courantes. La réplication de fichiers est mise en œuvre sur le réseau standard et les serveurs peuvent être localisés dans des salles machines différentes pour résister au désastre.



Reprise automatique sur panne applicable à n'importe quelle application

SafeKit est une solution puissante pour la surveillance d'une application et son redémarrage automatique. Les procédures de démarrage et d'arrêt sont personnalisables, ainsi que les détecteurs d'erreur logicielle spécifiques. Une fois en place, cette configuration d'application ne change plus et peut être déployée facilement.

Administration simple pour minimiser les coûts

SafeKit est simple à configurer, maintenir et administrer. Basé sur une même solution de haute disponibilité globale, SafeKit peut être appliqué tout au long de votre chaîne applicative, tout en assurant une indépendance des pannes à chaque niveau. De plus, vous pouvez retirer un serveur pour maintenance ou mise à jour sans interrompre le service. Une solution SafeKit peut être administrée avec ses commandes en ligne, sa console java d'administration centralisée ou sa MIB SNMP avec les cartographies et les alarmes d'une console d'administration SNMP. Certaines actions spécifiques, telles qu'envoyer un mail sur basculement du service, peuvent être intégrées dans les scripts de SafeKit.

Personnalisation simple pour n'importe quelle application

SafeKit est déjà mis en œuvre comme une solution prête à l'emploi sur plus de 50 applications différentes, dans des domaines comme le Web (iPlanet, IIS, Apache, BEA Web Logic…), les pare-feu (Netwall, proxy, antivirus…), l'authentification (Radius, LDAP, PortalXpert, AccessMaster…), les bases de données (Oracle...).

Les intégrateurs, les revendeurs d'applications, les éditeurs de logiciels peuvent adapter SafeKit à toutes sortes de nouvelles applications en moins de 5 jours.

Environnements pris en charge

SafeKit supporte Solaris 7&8 (64 bits), AIX 4.3&5L, HP UX 11 (64 bits), Windows NT 4.0 service pack 5, Windows 2000 et Linux.

SafeKit est téléchargeable pour un mois d'essai gratuit à l'adresse http://www.evidian.com/safekit.

En savoir plus…

Dans le manuel de référence et dans le document 'release notes' que vous pouvez obtenir en téléchargeant l'essai gratuit de SafeKit, les caractéristiques avancées de SafeKit sont présentées :

- des adresses IP virtuelles en partage de charge ou primaire-backup, des mécanismes de détection des défaillances matérielles avec un ou plusieurs flux de contrôle réseau, des mécanismes de détection de défaillances logicielles sur mort anormale de processus, des détecteurs de panne d'interface réseau, de routeurs, de services TCP/IP et d'autres outils de combinaison des détecteurs d'erreur, des outils de reprise automatique sur panne avec redémarrage applicatif personnalisable par script, la notion de nom de machine virtuelle, des commandes d'administration en ligne, une console d'administration Java centralisée, une administration SNMP avec des alarmes personnalisables.