StoneGate™ : Solution firewall et clustering

StoneGate est une solution logiciel de firewall et de clustering particulièrement bien adaptée aux services E-serenity de aComm. StoneGate à été conçu dés le départ avec la haute disponibilité et la performance à l'esprit. Cette solution E-Serenity gère tous les aspects de déploiement de plate-formes d'hébergement pour applications critiques. Les bénéfices de la tolérance de panne sont fourni dans ce cadre de manière particulièrement avantageuse.

Les prestations E-Serenity sont née du constat des contraintes associées à la disponibilité et à la sécurisation des sites web et autres services en ligne. Toute interruption de service, qu'elle soit due à une panne, à l'intrusion d'un code malicieux ou à une saturation du serveur d'hébergement, se traduit par une perte parfois considérable et souvent irréversible de chiffre d'affaires. Sites portails, de commerce électronique et plus généralement tous les fournisseurs de services Internet développent un besoin critique de plates-formes hautement disponibles et capables de suivre une montée en charge. Les prestation de service E-Serenity répondent à ces problématiques par des architectures en clusters (ou grappes) de serveurs d'applications profitant ainsi d'un savoir faire acquis par la gestion et le déploiement de services E-business critique. Afin d'illustrer une réalisation d'une mission sur des systèmes critiques, au stade de la conception bien avant l'installation et le déploiement de la solution il faut se poser les questions suivantes:

- Quelle est l'importance des services qui vont être mis en ligne
- Combien d'autres services dépendent du service qui va être déployé? Que se passe-t-il si un système ou un processus logiciel tombe en panne?
- Quelles conséquences financières ?
- Quelles conséquences en terme de perte d'image pour la société?

La réponse à ces questions impliquent souvent la mise en place d'infrastructures à tolérance de panne.

À cet égard StoneGate est une nouvelle race de firewall conçu depuis le départ avec des capacités de clustering. Deux type d'installations de base peuvent êtres conçues : Comme un site simple avec VPN, les fonctionnalités StoneGate suffiront pour répondre à des besoins de niveau de départ. Si le site protégé grandit et les mouvements d'exigences vers un firewall renforcé avec une architecture distribuée de pointe, la solution de site initiale simple peut être étendue pour inclure un cluster de haute disponibilité, l'équilibrage de charge pour connexion Internet multiples et des services de réseau virtuel privé (VPN) redondant . Jusqu'à 16 moteurs peuvent être regroupés pour former une entité unifiée employant un réseau de contrôle consacré.

Un cluster StoneGate fournit des fonctionnalités d'équilibrage de charge, signifiant que tout le trafic est distribué aussi également que possible entre les moteurs dans un cluster. Chaque fois qu'un node se connecte ou se dé-connecte pour une raison ou une autre, la charge est redistribuée à travers les nodes actifs. L'option d'équilibrage de charge dynamique permet aussi de déplacer une partie du trafic réseau d'un moteur surchargé aux nodes restants sans perdre l'information d'état ou de connexion.

StoneGate a un système de gestion à trois niveau. Les administrateurs y ont accès via l'interface graphique de gestion éloignée, qui est connecté à un serveur de gestion et des serveurs de log. Les serveurs de gestion mettent à jour les règles de configuration et de sécurité sur les moteurs firewall et les serveurs de log récupèrent l'information de log des firewalls. Des serveurs de log multiples peuvent être déployés si nécessaire pour des raisons de performance ou architecturales, bien que chaque cluster ne puisse s'enregistrer que sur un seul serveur de log.

Le serveur de log fournit un service consacré au firewall, qui permet au système de fournir le dépistage en temps réel et l'analyse statistique. Le GUI de gestion est basé sur Java et inclut des outils pour la maintenance des modèles de base de règlements ainsi que des capacités de filtrage et d'élision approfondies des logs . Le GUI est séparé du serveur de gestion lui-même et de multiples sessions du GUI peuvent avoir accès à un seul serveur de gestion à distance, si exigé. Il met aussi en oeuvre des niveaux d'administrateur multiples, permettant de limiter différents administrateurs à différentes tâches.

Le système de gestion comprend quelques options d'automatisations, telles que le traitement de données log automatisé et les capacités de backup des données et des fichiers de configuration. Toutes les communications entre les systèmes de gestion et les moteurs firewall sont encryptées et les données de configuration sont entièrement protégées.

La définition des règles suit un chemin semblable à des firewalls de filtrage de paquet ou d'inspection d'état. Chaque ligne de la base des règles contient un jeu des paramètres qui sont comparés aux paquets qui passent par le firewall et un jeu d'agents de protocole est aussi fourni pour accorder le filtrage de trafic selon les protocoles utilisés. Là où une correspondance est trouvée pour l'adresse IP, le numéro de port et le protocole, alors une ou plusieurs actions sont effectuées. L'action spécifie si le paquet peut passer à travers le firewall, s'il est refusé, abandonné, ou si un tunnel VPN doit être créé.

L'action peut aussi être "continuer", qui force une comparaison de règle plus approfondie à être exécutée, ou un saut à un groupe "de sous-règles" peut être effectué. Cette dernière particularité est une capacité très utile qui est conçue pour accélérer le processus de comparaison pendant la traversée du firewall, puisque des sections entières de la base de règle peuvent être supprimées du processus de correspondance en se basant sur les résultats d'une règle. Cela rend les grandes et complexes bases de règle beaucoup plus facile de suivre, un peu comme les routines rendent les programmes informatiques plus faciles de lire. Une fois définie, la même base de règle doit être partagée par chaque node d'un cluster de firewall après son chargement dans le moteur. L'édition et la mise à jour des bases de règle sont faites selon des privilèges d'administrateur et des permissions. La cohérence à travers le réseau est fournie par l'utilisation de modèles des bases de règle qui peuvent être "verrouillées" par l'administrateur principal.

Les règles contenues dans les modèles ne sont pas éditables par d'autres administrateurs, mais chaque modèle contient un point d'insertion où de nouvelles règles et sous-règles peuvent être ajoutées pour s'adapter aux exigences individuelles de différents firewalls.

Les données de log sont produites à partir de multiples moteurs de firewall et rassemblées par le serveur de log depuis plusieurs gateway hosts. Les données dans le serveur de log peuvent être vues et traitées immédiatement après leur réception en employant le navigateur de log.

aComm

La Chocolatière 26

CH - 1026 Echandens

Tél. +41 21 706 06 06

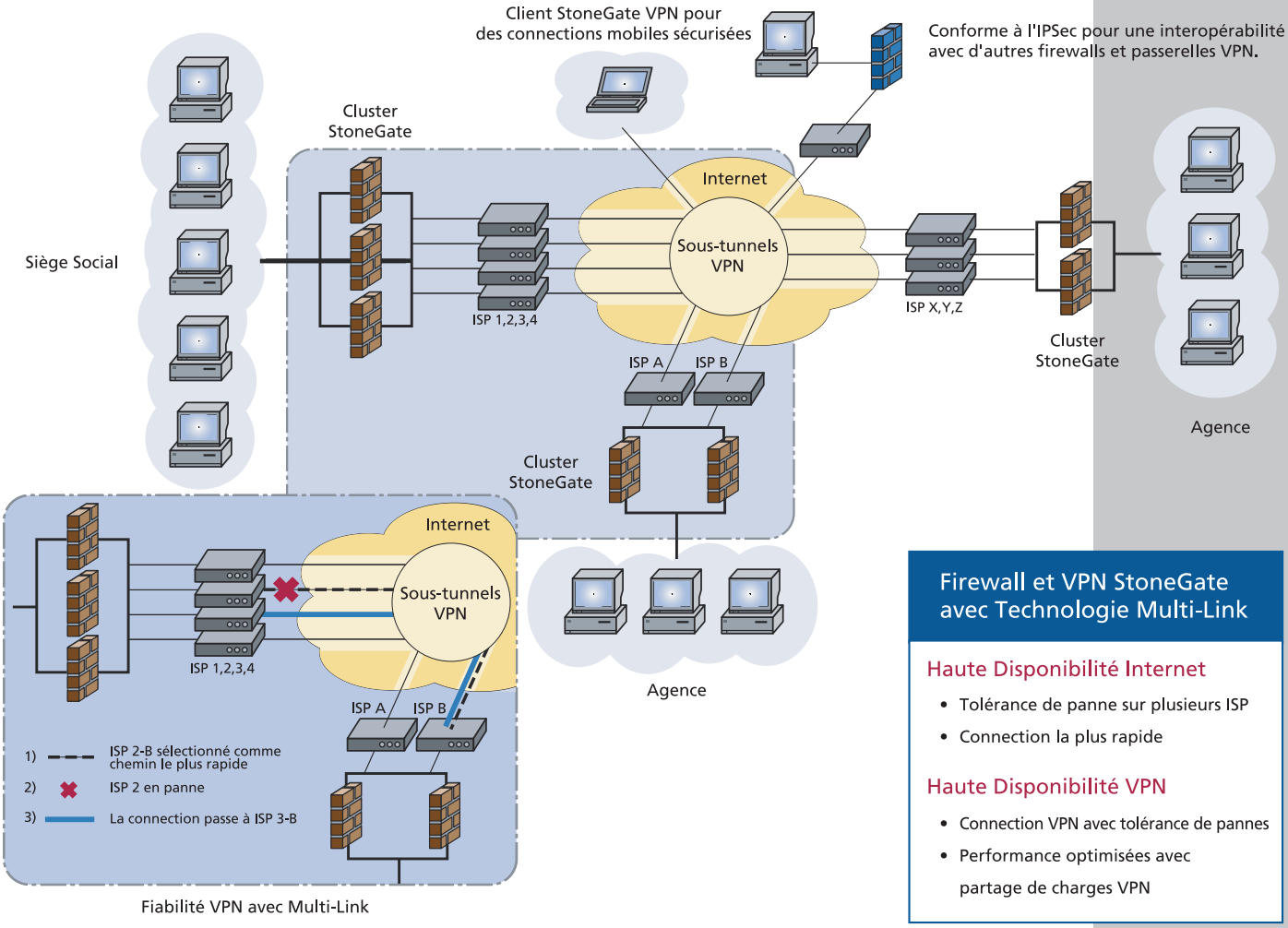
Fax +41 21 706 06 00

info@acomm.ch

www.acomm.ch

STONESOFT
Value-Added Reseller
Premium

Sun microsystems
AUTHORIZED PARTNER



Fiabilité VPN avec Multi-Link

Firewall et VPN StoneGate avec Technologie Multi-Link

Haute Disponibilité Internet

- Tolérance de panne sur plusieurs ISP
- Connection la plus rapide

Haute Disponibilité VPN

- Connection VPN avec tolérance de pannes
- Performance optimisées avec partage de charges VPN

Présentation du Firewall et VPN de haute disponibilité StoneGate

En tant que première solution de sécurité de réseau de ce type, StoneGate établit une nouveau standard. StoneGate inclut "un firewall renforcé," une architecture de firewall distribuée ultra-moderne, pour la protection de réseau, qui est entièrement intégrée avec le clustering de haute disponibilité, l'équilibrage de charge des connexions Internet et les services de réseau virtuel privé (VPN) redondant.
Firewall Renforcé : Puissante sécurité de réseau avec haute disponibilité incorporée et équilibrage de charge pour un firewall continuellement opérationnel.
Réseau Virtuel Privé : Haute disponibilité VPN bénéficiant de la Technologie Multi-Link™ assurant une connection internet redondante à plusieurs fournisseurs d'accès Internet (ISP).
Fonctionnalités de haute disponibilité : Clustering personnalisable pour un équilibrage de charge toujours opérationnel du firewall, des connexions à Internet, du VPN, des serveurs du Web et d'autres services d'information.

	StoneGate	Avantages StoneGate
Haute disponibilité incorporée (HA)		Sécurité toujours active
Inclue dans le firewall	✓	Fiabilité Internet et VPN pour applications commerciales critiques
HA pour Internet et connections VPN	✓	
Sécurité de qualité supérieure		Elimination des risques de sécurité provenant d'erreurs d'installation OS
OS incorporé	✓	Inspection de paquets améliorée pour une sécurité de performance et de proxy
Inspection Multicouches	✓	Mise en oeuvre, maintenance et audit de règlements de sécurité facile
VPN Intégré	✓	
Base de règle hiérarchique	✓	
Base de donnée log incorporée	✓	
Administration unifiée		Flexibilité de la gestion des règlements de sécurité d'entreprise distribuée
Administration centralisée pour infrastructure firewall	✓	Frais d'IT excédentaires réduits avec une solution d'une seule pièce pour l'installation et l'administration
Installation et configuration simple	✓	
Etablissement des logs et rapports amélioré avec base de donnée incorporée	✓	
Rapport performance/coût		Coût total de propriété réduit dû à une conception de réseau simplifiée
Haut débit sur hardware standard	✓	Coût du support et de la maintenance limités
Equilibrage de charge incorporé pour firewall, connections Internet multiples VPN et serveur Web	✓	Conversion du matériel standard en "unités ouvertes" à haut débit (gigabit)
		Trafique Internet et VPN optimisés d'où réduction des dépenses de télé-communication

acomm
La Chocolatière 26
CH - 1026 Echandens

Tél. +41 21 706 06 06
Fax +41 21 706 06 00

info @ acomm.ch
www.acomm.ch