

# VPN AUGMENTÉ

Optimisation de la sécurité du réseau,  
efficacité des performances et des coûts

# SOMMAIRE

Résumé	3
Connexions Améliorées	4
Une bande passante toujours disponible	7
Votre business, toujours prioritaire	9
Des coûts toujours plus faibles	10
Les trucs en plus (de sécurité)	12
Intelligence Artificielle et Augmented VPN	13
Evaluer les possibilités	14
Le protocole BGP (Border Gateway Protocol)	14
Répartiteurs externes de charge	15
Conclusion	16

# RÉSUMÉ

Comparer un VPN augmenté à un VPN classique revient à confronter un GPS à une carte routière. Tous deux se basent sur les mêmes informations, mais sont séparés par un fossé technologique. Le système GPS intègre de nombreuses options comme la géolocalisation, les informations sur le trafic, des fonctionnalités de recherche, la possibilité de localiser certains services, le suivi d'itinéraire et bien d'autres fonctionnalités correspondant à cette évolution technologique.

Un phénomène semblable est en train de se développer sur le marché du Réseau Privé Virtuel (VPN). Au début de la mondialisation, une entreprise pouvait se contenter de connecter ses bureaux et ses sites de production avec un simple VPN ou un circuit dédié point à point. Cependant, depuis ce temps là, la situation a énormément changé.

Aujourd'hui, les entreprises sont confrontées à trois problèmes principaux :

1. Les systèmes de production sont en ligne/connectés et doivent être disponibles en permanence et ce, de n'importe où. Un directeur technique a déjà comparé le stress engendré par une panne de son système à une heure de négociation avec son ex-femme pendant son divorce. En vérité, de nombreuses sociétés ne peuvent pas fonctionner sans applications en ligne comme un ERP, l'email ou des services hébergés dans le Cloud, comme Salesforce.com. Existe-t-il une façon efficace de fournir des connexions de secours si le réseau MPLS tombe en panne ?

*« Le stress engendré par une panne du système équivaut à une heure de négociation avec mon ex-femme pendant mon divorce. »*

2. La connectivité internet est constamment limitée et paradoxalement son utilisation est en pleine expansion. Comment faire la différence entre le trafic essentiel et les autres types de trafic ? Comment allouer suffisamment de bande passante pour les activités commerciales essentielles tout en autorisant d'autres types de trafic lorsque la bande passante est disponible ? Existe-t-il une façon de rediriger uniquement les flux de production via le réseau MPLS et d'utiliser une connexion moins chère pour le reste des flux ?

3. Les coûts de connexion réseau sont trop élevés. Beaucoup d'entreprises sont implantées dans le monde et ont besoin de connexions fiables et rapides entre les sites de production et les différents bureaux. Un réseau MPLS permet, par exemple, de relier de façon efficace les sites mais se révèle beaucoup plus cher lorsqu'il faut relier plusieurs pays.

Vous trouverez dans ce Livre Blanc des réponses à ces trois problèmes et des conseils de sécurité par ailleurs.

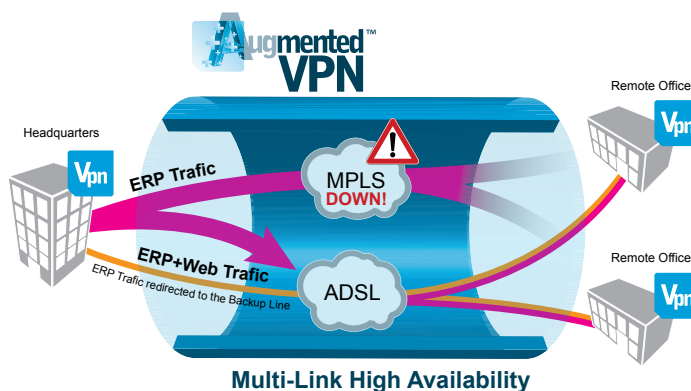
# CONNEXIONS AMÉLIORÉES

Prenons pour exemple une société dont les sites de production étaient basés aux Etats-Unis (sur le continent) et les bureaux commerciaux aux Bermudes. Leur problème : en termes de connexion, les bureaux situés aux Bermudes étaient totalement dépendants des sites de production. La société ne disposait que d'une seule connexion entre les sites de production et les sites des Bermudes. Le CIO était d'autant plus inquiet que les Bermudes sont fréquemment touchées par des ouragans. Un gros ouragan risquait de perturber les lignes télécoms et priver la société de son business pour un long moment.

La société s'est alors mise à comparer plusieurs options, dont des connexions satellites de secours accompagnés d'une connexion MPLS supplémentaire assurée par un autre ISP utilisant le BGP. Toutes les solutions envisagées se sont révélées non seulement complexes mais également très coûteuses. La société a fini par choisir la solution StoneGate Multi-Link Firewall/VPN reposant sur deux connexions MPLS fournies par deux ISP différents. Ils ont ainsi pu éviter d'opter pour la configuration BGP et bénéficier désormais de connexions hautement disponibles.

Environ un an après, un ouragan de catégorie 4 a frappé les Bermudes et a emporté avec lui l'un des principaux ISP de l'île. Après avoir entendu la nouvelle dans les journaux télévisés, un technicien du support Stonesoft a contacté le responsable informatique de la société afin de savoir si ce dernier s'était rendu compte que l'un de ses ISP avait été touché par l'ouragan. Le responsable informatique a répondu qu'il ne s'était rendu compte de rien et que leurs connexions fonctionnaient sans souci. Ceci n'est qu'un petit exemple illustrant la puissance de StoneGate Multi-Liens. Le trafic transitant sur la connexion qui rencontrait des problèmes a été automatiquement redirigé vers la connexion toujours valide. Le business a continué, comme si de rien n'était.

Le nombre de sociétés dont l'activité repose sur Internet augmentant constamment, les connexions doivent être fiables et les services disponibles en permanence. Les risques qu'impliquent les pannes forcent les entreprises à rendre leurs réseaux hautement disponibles en y installant des passerelles, des pare-feux, des commutateurs, des routeurs et d'autres



composants réseaux redondants. Malgré tout, les réseaux ainsi équipés restent exposés aux pannes, notamment si un lien réseau vers Internet ou vers un autre site de production est rompu.

Les ISP savent fournir différents types de liens réseaux mais ces derniers sont tous sujets aux pannes. Même un lien MPLS est vulnérable. Une panne d'ISP peut prendre différentes formes. Un ISP peut par exemple, être la cible d'une attaque par Déni de Service (DoS) ou d'un virus ou d'un vers. La mauvaise configuration du routage côté ISP peut également provoquer une panne, ce qui prendra du temps à être non seulement localisé mais surtout corrigé. Parfois, une panne peut subvenir pour des raisons n'ayant aucun lien avec la « technique » : des travaux, une faillite ou même des catastrophes naturelles telles qu'un tremblement de terre, un glissement de terrain, une éruption volcanique ou une inondation. Peu importe les raisons, les résultats sont les mêmes. Malgré les efforts que déploieriez pour assurer la haute-disponibilité de votre réseau, celui s'arrêtera brusquement, quoi qu'il arrive.

Pour éliminer le risque que représente l'ISP unique, de nombreuses entreprises ont dû déployer des dispositifs redondés (routeurs externes, commutateurs...). Ces dispositifs nécessitent des protocoles de routage complexes comme le BGP ou l'HSRP et la mise en place d'accords de peering entre les ISP. D'autres entreprises trouvent cette approche trop chère et trop complexe, puisqu'elle exige une redondance hardware, des routeurs plus chers, des logiciels supplémentaires et des accords financiers avec les ISP... et ce, au début ! Une fois mise en place, pour conserver cette haute-disponibilité, les administrateurs doivent configurer et assurer la maintenance sur un réseau complexe.

Approfondissons le BGP : le BGP est un protocole de routage conçu pour permettre la création d'itinéraires redondants sur un ensemble de réseaux. Cependant, le BGP est non seulement complexe à gérer mais cher. Il nécessite des adresses IP indépendantes de l'ISP et un nombre de systèmes autonomes (ASN), ce qui risque d'être impossible pour les adresses IPv4 aujourd'hui. L'ASN est une identité unique qui sait repérer les réseaux d'entreprises sur les routeurs d'Internet et permet à d'autres routeurs de comprendre qu'il existe plusieurs chemins pour accéder à un réseau. Pour mettre en place des adresses indépendantes de l'ISP, l'entreprise doit négocier des accords avec au moins deux ISP différents pour le routage de leur ASN. Pour les PME et même de plus grandes entreprises, cet accord est difficile à mettre en place. De plus, les entreprises ayant des budgets réduits doivent également supporter les frais d'upgrade des routeurs (mémoire et logiciels supplémentaires) permettant de mener à bien le routage complexe et dynamique qu'est le BGP.

Les entreprises doivent pouvoir rendre une connexion redondante avec une solution unique, sans recourir à des logiciels ou du matériels onéreux, sans avoir à gérer des configurations compliquées ou à établir une collaboration entre deux ISP. La solution idéale devra également savoir relever les défis tels qu'assurer la sécurité des systèmes, les VPN tolérants aux pannes, la répartition de charge, l'évolutivité, la possibilité d'upgrader et la facilité d'administration.

L'Augmented VPN de Stonesoft permet de créer très facilement une redondance ISP et d'assurer une connectivité internet permanente. Il permet de se passer de solutions matérielles et logicielles tierces chères et complexes et de rendre l'administration réseau beaucoup plus facile. Grâce à StoneGate, l'accès Internet et le VPN ne sont plus les points critiques du réseau en cas de panne.

Grâce à Stonesoft Augmented VPN, les entreprises peuvent facilement additionner plusieurs connexions internet à leur réseau en passant par différents ISP, par des lignes louées ou un ensemble des deux. Ceci leur permet de :

- Assurer la disponibilité de leur connexion réseau, même si l'ISP rencontre des difficultés ou connaît une panne.
- Améliorer les performances d'Internet et de la bande passante
- Faciliter la migration d'un ISP à l'autre
- Migrer progressivement à partir de lignes louées et onéreuses avec la possibilité, malgré tout, de les conserver en backup, si nécessaire
- Améliorer la satisfaction client

Stonesoft Augmented VPN permet d'éviter qu'Internet soit le point critique du réseau en cas de panne en donnant la possibilité aux entreprises de mettre en place plusieurs liens internet très facilement et avec un excellent rapport qualité prix. L'ensemble des liens est actif et utilisé. Dans le cas où un lien tombe en panne, le trafic est automatiquement transféré vers les liens restants. L'Augmented VPN sait supporter tout type de liens internet, comme l'ISDN (un type de lien ADSL), des lignes louées, des connexions modem et même satellites. Avec Stonesoft Augmented VPN, les entreprises savent que la connectivité internet sera toujours disponible lorsqu'ils en auront besoin.

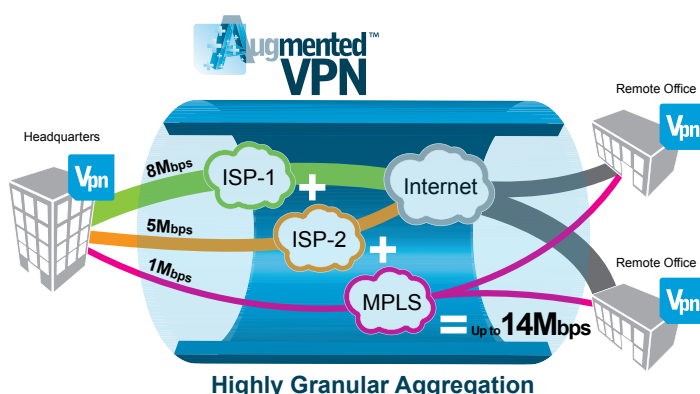
Grâce à la technologie Multi-Liens StoneGate, les entreprises n'ont plus à s'inquiéter si leur ISP est la cible d'une attaque par déni de service ou d'un virus. Si une pelleteuse détruit un câble ISP, ils resteront malgré tout connectés. Si leur ISP met en place une mauvaise configuration, fait faillite ou est touché par une terrible catastrophe, l'activité du réseau continue grâce à StoneGate et les connexions sont redirigées vers les liens réseaux restants.

Même si les problèmes que l'Augmented VPN sait résoudre sont complexes, l'installation du produit est extrêmement simple et rentable. A l'inverse des solutions classiques, l'Augmented VPN ne nécessite aucun matériel ou logiciel spécialisé, ce qui permet de réduire considérablement les coûts d'installation et de maintenance. Par ailleurs, Stonesoft Augmented VPN offre la redondance ISP, sans qu'aucun accord de peering ne soit nécessaire entre deux ISP concurrents. Les ISP n'ont pas à communiquer, ce qui permet de simplifier l'installation, la maintenance et la résolution de problèmes.

# UNE BANDE PASSANTE TOUJOURS DISPONIBLE

Voici un autre exemple. Une entreprise avait des problèmes de capacité de leur connexion internet. Le trafic principal concernait le CRM, hébergé dans le Cloud. Ils disposaient initialement d'une connexion MPLS, mais la bande passante est rapidement arrivée à saturation à mesure que le trafic internet augmentait et que les employés utilisaient des réseaux sociaux comme Facebook ou LinkedIn. Les réseaux sociaux faisaient partie du service client et de la stratégie marketing, la direction ne pouvait donc pas les interdire. Ils ont augmenté la capacité de la bande passante de leur réseau MPLS à 8Mbps et cela les a dépannés pendant quelques temps. Bien entendu, peu de temps après toute cette bande passante était de nouveau utilisée à 100 %.

Leur ISP offrant jusqu'à 8 Mbps via des lignes (cuivre) de téléphone classiques, la décision d'investir qu'ils devaient prendre était bien plus significative. Pour les débits supérieurs à 8 Mbps, ils avaient deux possibilités : demander une connexion fibre à leur ISP ou un lien radio sans fil. Le débit via une connexion fibre peut atteindre plusieurs dizaines de gigabits par seconde. Quant aux liens radio sans fil, ils peuvent atteindre jusqu'à 100 Mbps par seconde. Chacune de ces options impliquait du matériel supplémentaire et des frais de mise en place, l'ISP devant installer des nouveaux équipements dans les locaux de la société. Aucune de ces options n'étaient réalisables dans l'immédiat, aussi, le délai d'installation allait varier de cinq semaines à deux fois. L'entreprise trouvait ce délai trop long. Ce besoin en bande passante était urgent.



Cette société utilisait heureusement l'Augmented VPN de Stonesoft, qui permet d'ajouter plusieurs lignes low cost pour n'en faire qu'une seule et unique, résiliente et haute-capacité. Deux lignes ADSL de 5 Mbps peuvent s'ajouter pour n'en former qu'une seule de 10 Mbps. La société en question a souscrit auprès de son ISP deux abonnements à des lignes de 5 Mbps afin de répondre immédiatement à ses besoins en bande passante. Ils peuvent désormais, s'ils le souhaitent, ajouter de nouvelles lignes low cost, dans le cas où leurs besoins en bande passante augmentent encore. L'un des autres avantages de Stonesoft Augmented VPN est la très haute disponibilité, les lignes supplémentaires apportant la redondance en cas de panne.

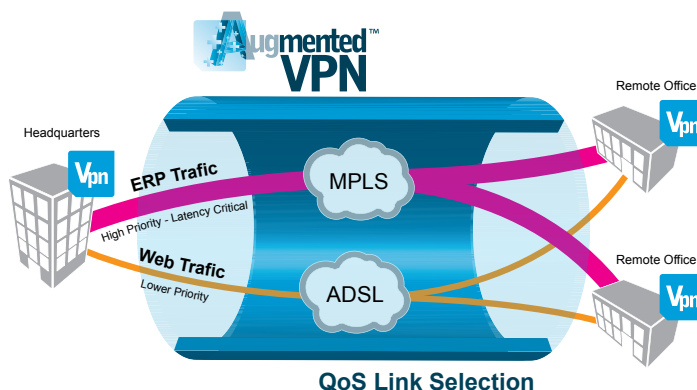
### **EXEMPLE DE CONFIGURATION VPN :**

- Trafic du CRM = priorité 1 = forcé sur le lien MPLS, ligne de secours ADSL1
- Trafic HTTP = priorité 4 = forcé sur les connexions actives ADSL 1 et ADSL 2

Parce qu'il choisit toujours le chemin le plus rapide pour les connexions utilisateurs, StoneGate Augmented VPN permet d'améliorer considérablement les performances. Il permet notamment aux connexions de choisir en toute transparence les différents liens VPN en fonction de la quantité de trafic et de l'état du réseau. Le trafic essentiel du CRM peut par exemple passer par le lien le plus rapide. Le trafic de moindre importance peut lui être redirigé vers les liens actifs afin que la bande passante soit toujours préservée pour le trafic essentiel. Augmentation de la bande passante et réduction du temps de latence signifient que des nouvelles technologies telles que la Voix sur IP et la visioconférence sont bien mieux supportées. De plus, les clients de ladite société sont satisfaits, l'expérience utilisateurs est nettement plus agréable.

# VOTRE BUSINESS, TOUJOURS PRIORITAIRE

Prenons l'exemple d'une société de retail qui utilisait une connexion MPLS pour se connecter au site central où était situé un système SAP. Le problème venait du fait que le trafic SAP ne trouvait pas toujours de bande passante disponible. Celle-ci était en effet consommée par d'autres types de trafic (email, navigation internet etc...) qui transitaient également via la même connexion MPLS. La société de retail souhaitait que ces autres trafics ne passent plus par la ligne MPLS, afin d'être sûr que le trafic SAP aurait toujours suffisamment de bande passante disponible. La société étant composée de nombreuses représentations, cela revenait bien trop cher d'installer une deuxième connexion MPLS dans chaque bureau. Il a également été envisagé d'augmenter la capacité de la connexion MPLS mais cela était également très onéreux. Par ailleurs, le risque que tout soit concentré sur le MPLS et qu'en cas de panne, tout s'arrête n'était pas éliminé. Même si le contrat de service qui liait la société à son ISP était intéressant, les dédommagements maximums couvrant une panne informatique correspondaient à ce que la société avait déjà payé pour son abonnement. Ces frais, en cas de panne ne couvraient en rien les pertes en termes de production. La société voulait donc mettre en place une connexion de secours et financièrement abordable dédiée au trafic SAP.



Cet exemple est emblématique de ce que rencontrent les entreprises actuellement. La société de retail a trouvé une solution à son problème via le VPN Augmenté. Ils ont fait l'acquisition d'une ligne ADSL supplémentaire pour chaque bureau, une façon peu chère et efficace de rajouter de la bande passante. Ils ont ensuite eu recours à la solution StoneGate Augmented VPN pour la répartition de charge du trafic entre les lignes ADSL et MPLS. Le trafic http classique est automatiquement redirigé vers la connexion ADSL. Ils se sont reposés sur la fonctionnalité de QoS pour mettre en priorité le trafic SAP. Le trafic SAP est donc désormais prioritaire sur le réseau MPLS et que les autres types de trafic transitent via la connexion MPLS de moindre priorité. Dans le cas où une partie de la ligne MPLS est libre, l'autre trafic y est également redirigé. La connexion haute qualité MPLS est donc utilisée à son maximum, en permanence et la ligne ADSL fournit de la capacité supplémentaire, si besoin.

## EXEMPLE :

- Trafic SAP = priorité 1 = haute priorité sur la ligne MPLS
- Trafic http = priorité 4 = utilise normalement l'ADSL et priorité basse sur la ligne MPLS

# DES COÛTS TOUJOURS PLUS FAIBLES

Une société mondiale de textile souhaitait réduire ses coûts Internet afin d'assurer la connectivité entre les sites de production et les bureaux commerciaux. Ils avaient des exigences contradictoires :

- Les entités de production étaient situées dans des pays en voie de développement où les coûts de production sont faibles mais où les infrastructures ne sont pas équipées de connexions internet fiables, ou lorsque c'est le cas, sont très chères.
- Le système ERP demandait des connexions avec des taux de latence bas, une ligne MPLS avec un SLA très strict, si possible
- L'utilisation d'un service de VoIP à tout endroit possible, afin d'économiser les coûts
- L'infrastructure réseau (800 sites) devait pouvoir être administrée de façon centralisée par 2 à 3 personnes

Dans les pays en voie de développement, les connexions filaires n'existent soit pas, soit elles ne sont pas fiables et de mauvaise qualité. Cependant, il y a de fortes chances que le wifi y soit disponible. Grâce à l'Augmented VPN de Stonesoft, il est possible d'utiliser par exemple, des connexions 3G et d'y ajouter des lignes filaires plus tard, lorsqu'elles sont prêtes. Si les connexions filaires sont rompues ou en panne, l'Augmented VPN de Stonesoft s'appuiera sur la 3G comme connexion de secours.

Une connexion MPLS coûte moins cher lorsqu'elle ne concerne qu'un seul pays. Si le besoin en MPLS devient global, alors le prix augmentera proportionnellement à la distance entre les sites. Dans ce cas, le système ERP a besoin d'un taux de latence bas et le MPLS sait répondre à ces besoins. Cependant, si le système ERP ne consomme que peu de bande passante, Internet et la VoIP, eux, en consomment beaucoup.



La société de textile a donc décidé d'utiliser une faible bande passante MPLS pour le trafic ERP et a redirigé tout autre type de trafic vers des lignes ADSL low cost. Ainsi, ils ont administré le tout via la solution Augmented VPN de Stonesoft qui sait, en toute transparence, combiner différentes connexions ISP.

Administrer 800 sites est une tâche ardue sans gestion centralisée. La console d'administration StoneGate Management Center de Stonesoft offre une visibilité sur l'ensemble des infrastructures VPN et permet d'administrer de façon centralisée l'ensemble des équipements VPN. Actuellement, la société en question administre ses 800 sites avec seulement 2 administrateurs.

Les VPN offrent aux entreprises un moyen moins cher de sécuriser leurs communications, en comparaison avec d'autres solutions comme la location de lignes. Cependant, les connexions VPN se sont révélées fragiles et présentent donc un risque pour les communications sensibles de l'entreprise. L'Augmented VPN de Stonesoft sait résoudre ce problème en ajoutant la tolérance de pannes et le basculement automatique transparent vers les tunnels VPN.

L'Augmented VPN permet de faire encore plus d'économies en donnant notamment la possibilité aux entreprises de migrer de lignes louées et onéreuses vers des solutions plus intéressantes financièrement. Cette migration se fait très simplement, notamment car les entreprises peuvent conserver leurs connexions existantes et finaliser la migration après avoir testé les nouvelles lignes et terminé la configuration.

# LES TRUCS EN PLUS (DE SÉCURITÉ)

L'Augmented VPN de Stonesoft délivre un excellent niveau de sécurité déjà intégré à la solution. Une très grosse proportion du trafic qui transite via l'Augmented VPN est sensible, le chiffrement est donc absolument essentiel. Bien que les connexions MPLS soient réputées fiables, elles ne sont pas chiffrées. Le flux de trafic est visible à l'intérieur du réseau de l'ISP. Souvent, l'Augmented VPN est utilisé pour chiffrer le trafic MPLS afin de s'assurer que le trafic n'est pas intercepté par un tiers sur le réseau.

L'Augmented VPN possède des fonctionnalités d'inspection en profondeur du trafic, d'anti-virus, d'anti-spam, d'anti-spyware et de tests anti-évasions. Stonesoft en tant que pionnier dans la recherche anti-évasions sait fournir une protection inégalée contre ces menaces.



# INTELLIGENCE ARTIFICIELLE ET AUGMENTED VPN

Répartir les trafics entre différents ISP n'est pas aussi facile que ce que l'on s'imagine. Il peut notamment être très difficile de gérer plusieurs situations problématiques en même temps. L'Augmented VPN de Stonesoft repose sur plusieurs technologies de pointe, dont la logique floue, pour solutionner les problèmes de répartition de charge VPN et de haute-disponibilité.

Ci-dessous, quelques exemples de problèmes pouvant survenir si la répartition de charge ou la résilience ne sont pas faites correctement.

- Le trafic n'est redirigé que sur un lien ISP alors que de nombreux autres liens actifs sont disponibles
- Le trafic est redirigé vers un lien de qualité médiocre alors qu'un lien de meilleure qualité est disponible
- Le trafic transite par un lien provisoire alors que des liens actifs fonctionnent
- Le basculement vers un lien provisoire prend trop de temps

La logique floue sait tout à fait répondre à ces problématiques : c'est en effet une logique polyvalente. Elle ne repose pas sur 0 ou 1 mais sur plusieurs valeurs. Ceci signifie que des données imprécises et donc la logique floue sont nécessaires. Elle peut utiliser des données imprécises et malgré tout calculer des degrés de vérités, répondant ainsi à des questions du type :

- La charge est-elle haute ?
- Sommes-nous près du basculement ?

Pour donner sa réponse, la logique floue s'appuie sur des grandeurs d'entrée, des ensembles flous, des grandeurs de sortie, des règles et de la défuzzification. Grâce à la logique floue, l'Augmented VPN fonctionne de façon optimale même dans un environnement imprévisible et soumis à des changements rapides. En plus d'utiliser la logique floue, l'Augmented VPN repose sur la technologie Multi-Liens de Stonesoft. Elle lui permet de toujours choisir la ligne ISP la plus rapide. Pour en savoir plus sur le Multi-Liens, nous vous invitons à consulter notre Livre Blanc « StoneGate Multi-Liens, assurer une connectivité permanente à moindre frais ».

# EVALUER LES POSSIBILITÉS

Comme expliqué ci-dessus, il existe d'autres technologies que l'Augmented VPN de Stonesoft pour supporter les multiples connexions ISP. Cependant, ces autres technologies n'affichent pas les mêmes performances que celles de l'Augmented VPN. Par exemple, le routage BGP des connexions exploite un algorithme capable de déterminer le chemin le plus court, calculé en fonction du nombre de « bonds » (routeurs) entre la source et sa destination. Les protocoles VRRP et HSRP sont utilisés pour la haute-disponibilité des routeurs. Tous ces protocoles spécialisés, qu'ils soient utilisés pour la redondance des routeurs ou pour choisir le chemin le plus court, ne sont pas obligatoires mais peuvent coexister sur le réseau avec l'Augmented VPN de Stonesoft.

## LE PROTOCOLE BGP (BORDER GATEWAY PROTOCOL)

Les entreprises ayant souscrit plusieurs connexions internet pour la haute disponibilité utilisent souvent le protocole BGP. Voici les caractéristiques principales de ce dernier :

- Le BGP est une technologie de routage qui définit le chemin des paquets chez tous les ISP disponibles
- Le BGP peut être configuré pour utiliser le partage de charge statique. Il ne répartit pas la véritable charge. Par exemple, des réseaux configurés de façon statique utilisent toujours un lien A et d'autres réseaux toujours un lien B.
- Le BGP choisit des porteurs sans évaluer leurs performances. Lorsque le BGP choisit des porteurs lents ou encombrés, les performances réseaux sont affectées.

## LES LIMITES DU BGP

Le BGP est une solution dédiée ISP. Il n'est pas conçu pour être déployé par des clients finaux et nécessite par conséquent des ressources chez l'ISP et surtout des équipements spécifiques. Mettre en place du routage BGP nécessite par exemple un panel d'adresses IP indépendantes de l'ISP, ce qui représente des risques considérables d'interruption de service. Ces mêmes interruptions de service risquent de provoquer du routage incorrect à moins que l'utilisateur ne négocie une collaboration commune entre les deux ISP concurrents. La mise en place en tant que telle est un processus complexe, composé de plusieurs étapes qui vont bien au-delà de la simple configuration logicielle. L'équipe chargée du projet doit d'abord négocier des accords entre deux ISP, acheter et configurer le hardware et les plans de routage et savoir programmer impeccablement le BGP.

Comparativement, l'Augmented VPN de Stonesoft est une solution unique qui ne nécessite aucun matériel ou logiciel supplémentaire ou spécifique. En termes d'implémentation, elle se fait bien plus facilement et les coûts de maintenance sont ainsi réduits. L'Augmented VPN sait sélectionner la connexion dotée du débit le plus rapide ; le BGP, lui, ne sait pas distinguer si un chemin avec davantage de rebonds est plus rapide qu'un chemin encombré mais comptant moins de rebonds. Enfin, l'Augmented VPN s'appuie sur la passerelle StoneGate et ne nécessite aucune capacité de traitement ou matériel supplémentaire. Le BGP, lui, s'appuie sur les routeurs et exige de la capacité de traitement supplémentaire pour calculer le chemin le plus court. En d'autres termes : des dépenses en plus.

## **RÉPARTITEURS EXTERNES DE CHARGE**

Les répartiteurs externes de charge sont des appliances localisées devant une passerelle réseau. Ils ne dépendent ni du BGP, ni d'aucun autre protocole de routage et utilisent des méthodes similaires au Multi-Liens pour traiter différents ISP.

### **LIMITES DES RÉPARTITEURS EXTERNES DE CHARGE**

Les répartiteurs externes de charge exigent des équipements spéciaux et une maintenance permanente. Cependant, même dans le meilleur des cas, ils ne s'intègrent pas à un réseau VPN sans ralentir les performances réseau.

A l'instar du BGP, si le client souhaite installer des répartiteurs, il doit faire l'acquisition de matériel spécialisé. Pour avoir recours à plusieurs ISP, les répartiteurs externes de charge impliquent des composants réseaux spécifiques comme deux passerelles et deux répartiteurs de charges (pour ajouter la haute-disponibilité) : ceci ne fait qu'augmenter les coûts de mise en place.

Les répartiteurs externes de charge doivent être constamment surveillés, administrés, mis à jour en plus des coûts de maintenance qu'ils sous-entendent déjà. Les administrateurs doivent également configurer séparément la passerelle et s'assurer que la répartition est cohérente. L'administration n'en est que plus complexe.

# CONCLUSION

L'Augmented VPN est une solution simple et efficace pour créer des connexions rapides, sécurisées et de haute-capacité entre les sites et assurer une connectivité internet ininterrompue. Conçue avec la facilité d'utilisation en tête, l'installation de l'Augmented VPN ne nécessite aucun équipement spécifique, aucun logiciel ou accord entre deux ISP. L'Augmented VPN de Stonesoft permet aux organisations d'intégrer sans difficulté plusieurs ISP, donnant ainsi naissance à des connexions hautement disponibles et tolérantes des pannes, le tout sans avoir à modifier leur infrastructure réseau.

Pour un réseau disponible en permanence, les organisations ont habituellement recours à plusieurs fournisseurs d'accès internet ou points d'accès WAN afin d'assurer une connectivité ininterrompue et augmenter la bande passante tout en gardant un TCO relativement bas. L'Augmented VPN de Stonesoft permet d'agrèger l'ensemble des liens Internet de vos ISP. L'agrégation de liens est une fonctionnalité unique qui permet aux entreprises de combiner différents liens ISP afin d'obtenir une ligne unique, résiliente et de haute-capacité.

Les études montrent que de plus en plus, les employés utilisent des applications comme Skype, MSN et Facebook dans l'environnement professionnel. Ce phénomène a un gros impact sur la bande passante qui devient alors sollicitée généralement pour des activités n'étant pas essentielles au business, ce qui met donc en péril les applications critiques et la productivité de l'entreprise. L'Augmented VPN de Stonesoft permet d'établir des priorités dans les flux réseaux et de définir des portions de bandes passantes dédiées à différents types de flux. Les applications essentielles à l'entreprise peuvent avoir la priorité sur des connexions Internet haute-qualité et le reste du trafic peut, lui, transiter sur des connexions moins chères.

Les VPN offrent le meilleur rapport qualité/prix pour des communications sécurisées, toutefois le manque de fiabilité des liaisons VPN représente un risque pour les communications métiers des entreprises. La technologie Augmented VPN de Stonesoft résout ce problème en ajoutant une vraie répartition de charge des tunnels VPN et une tolérance de pannes à l'aide d'un basculement automatique transparent vers vos tunnels VPN encore actifs ou de secours.

En comparaison avec des solutions ISP multi-connexions, l'Augmented VPN de Stonesoft améliore les performances en offrant notamment une véritable répartition de charge ISP, une grande souplesse d'installation et une réduction significative des coûts d'administration. Le Multi-Liens permet quant à lui d'augmenter considérablement la fiabilité et les performances des VPN. Seul le Multi-Liens possède cette capacité de faire basculer les VPN sur plusieurs ISP.

## 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 commerciaux 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), le VPN SSL, la disponibilité de bout en bout, ainsi qu'un équilibre des charges plébiscité, au sein d'un système dont la gestion est centralisée et unifiée. Les avantages clés d'une solution de connectivité sécurisée StoneGate sont notamment un coût total de possession faible, un excellent rapport prix/performances et un retour sur investissement élevé.

La solution SMC (StoneGate Management Center) fournit une gestion unifiée 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, tandis que la solution StoneGate SSL VPN renforce la sécurité dans le cadre d'une utilisation mobile et à distance.

Fondée en 1990, l'entreprise Stonesoft Corporation a un siège social à Helsinki, en Finlande, et un autre aux États-Unis, à Atlanta, en Géorgie. Pour plus d'informations, visitez notre site Web, [www.stonesoft.com](http://www.stonesoft.com).



**STONESOFT FRANCE SAS**  
38, Rue de Villiers  
FR-92300 Levallois, France  
tel. +33 (0)1 47 58 48 05 | fax. +33 (0)1 47 58 56 17  
[info.france@stonesoft.com](mailto:info.france@stonesoft.com)

**STONESOFT**  
Network Security

**STONESOFT CORPORATION**  
Itälahdenkatu 22 A  
FI-00210 Helsinki, Finland  
tel. +358 9 4767 11 | fax. +358 9 4767 1349  
[www.stonesoft.fr](http://www.stonesoft.fr)