



Yannick Michel, Ingénieur réseau et sécurité auprès d'une banque privée à Genève

Simplifier la gestion et optimiser les coûts grâce au firewall virtuel

La gestion des firewalls, et en particulier celle de leurs règles de sécurité, peut s'avérer un vrai casse-tête dans les architectures de réseau complexes. Comment éviter la prolifération des règles de sécurité, parfois contradictoires ? Gérer les problèmes d'administration ? Maîtriser les coûts de hardware et de maintenance ?

Ce problème, la succursale genevoise d'une banque privée y est confrontée. Le groupe bancaire dans son ensemble est actif dans les domaines de la banque commerciale, privée et internationale. La succursale de Genève est très autonome. Son implication dans l'hébergement des services informatiques d'autres succursales est grande et va en augmentant. Cela représente une responsabilité importante au niveau du groupe dont elle est pour ainsi dire le pôle technique.

Yannick Michel est Ingénieur réseau et sécurité dans la succursale de Genève : « *Le projet est né il y a environ deux ans. La succursale de Genève hébergeait toujours plus de services informatiques pour d'autres succursales de la division international banking. Avec plus de 300 règles de sécurité par firewall, la situation devenait intenable, tant au niveau de l'administration des nombreux firewalls que de leur maintenance et des coûts engendrés.* »

« Avec plus de 300 règles de sécurité par firewall, notre situation devenait intenable, tant au niveau de l'administration des nombreux firewalls que de leur maintenance et des coûts engendrés. »

Solution

Pour résoudre ce problème, l'équipe informatique avait d'abord pensé qu'il suffirait de passer en revue toutes les règles existantes afin de les optimiser et de les simplifier. Yannick Michel : « *Comme un certain nombre de règles de sécurité étaient imposées au niveau du groupe, nous n'avons pas pu procéder à une simplification suffisante. La démarche a échoué.* » Le problème demeure, et l'équipe informatique continue sa réflexion : « *Nous avons cherché le moyen de simplifier la situation. Un firewall par groupe de services aurait permis de minimiser le nombre de règles par firewall. C'est alors que nous avons eu l'idée de virtualiser notre architecture.* »

« Nous faisons des économies de frais de maintenance Check Point, des économies en frais de hardware et nous gagnons en flexibilité. »

L'équipe teste plusieurs solutions de firewalls virtuels : Cisco, Check Point et Juniper. « Les trois solutions étaient toute très bonnes et répondaient au « cahier des charges » initial. Notre architecture de sécurité étant en grande partie basée sur des environnements Checkpoint, nous avons naturellement opté pour la solution VSX. Ceci nous permettait une utilisation des objets déjà existants dans notre serveur de management et diminuait de fait la charge de travail liée à la migration vers une architecture virtuelle. De plus grâce à l'offre de trade-in, la solution Check Point était de loin la plus attractive. Avec un peu de recul, nous sommes complètement satisfaits de ce choix. »

VPN-1 Power VSX est un portail de sécurité virtualisé permettant de créer jusqu'à 250 systèmes virtuels (firewalls, VPN, filtrage URL et fonctionnalités de prévention d'intrusions) dans un environnement réseau virtuel, sur une plate-forme hardware unique. Les réseaux gérés par VSX peuvent être interconnectés facilement avec des ressources partagées, internet ou des DMZ.

L'installation est simple, mais c'est surtout à l'usage que la solution VSX s'avère extrêmement efficace. Yannick Michel : « Virtualiser les firewalls nous a permis de diminuer les règles de sécurité à gérer par firewall et d'avoir une administration simplifiée. Nous faisons des économies de frais de maintenance Check Point, des économies en frais de hardware et nous gagnons en flexibilité. A titre d'exemple, la création d'un cluster de firewalls virtuels se fait en trois clicks de souris. »

Les systèmes de sécurité de l'entreprise, qu'ils soient virtuels ou physiques, sont tous gérés de manière centrale par un cluster de serveur de management, SmartCenter ou Provider-1. Yannick Michel : « La possibilité donnée par la solution VSX de garder notre infrastructure de management déjà opérationnelle nous a également permis de consolider et de capitaliser l'existant. Durant cette période transitoire de migration, le support et l'expertise de Navixia nous ont été très précieux. »

« Aujourd'hui, la solution VSX associée à une politique de filtrage nous a de passer de 300 règles par firewall à une quinzaine seulement ! »

Amélioration de la performance

La performance du système dans son ensemble a pu être améliorée : « Après l'installation du VSX, nous avons multiplié le nombre de firewalls actifs. Nous avons donc revu notre politique de filtrage afin d'éviter que les mêmes règles soient répétées sur chaque firewall. En effet, la multiplication des règles consomme les ressources du firewall, ce qui représente une perte de performance et une charge en termes d'administration. Aujourd'hui, la solution VSX associée à une politique de filtrage nous a permis de passer de 300 règles par firewall à une quinzaine seulement ! »

A ce jour, le trafic généré par 2000 utilisateurs passe par le portail de sécurité VPN-1 Power VSX. Mais le système doit être en état de fonctionner 24h sur 24, en raison des différents fuseaux horaires des succursales desservies. Deux systèmes fonctionnent donc en parallèle pour assurer la redondance. Yannick Michel : « Pour éviter que l'un des systèmes soit constamment en fonction pendant que l'autre reste

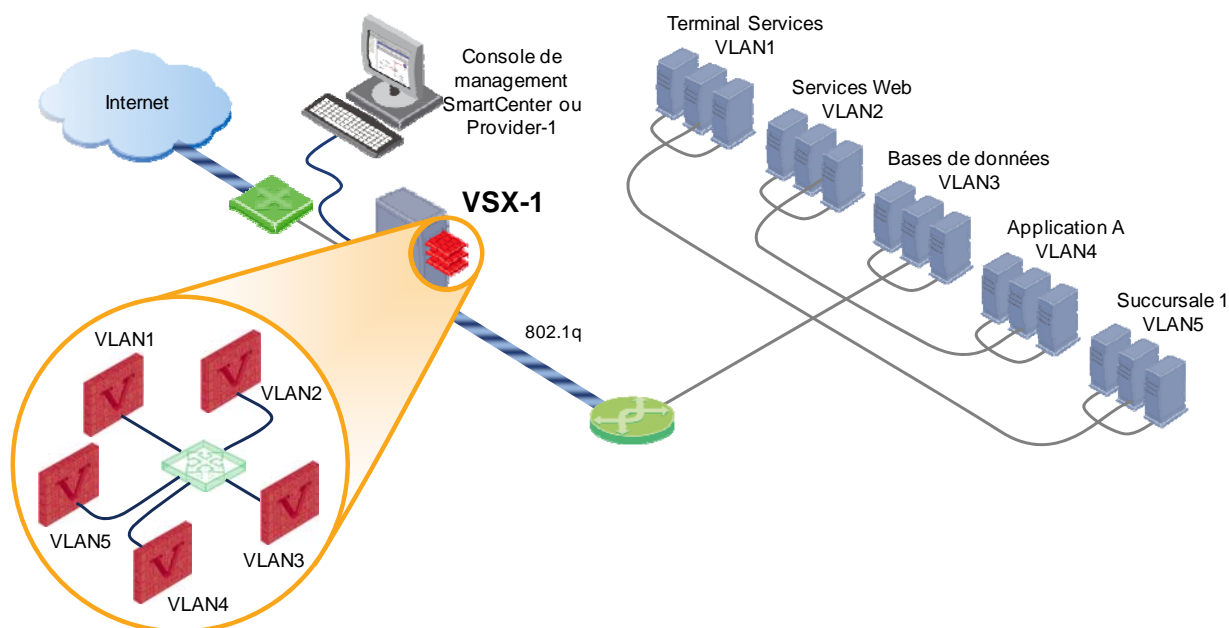
Nous avons pu diminuer le budget de fonctionnement et d'investissement tout en améliorant la performance.

inactif, nous avons fait en sorte que des firewalls virtuels soient activés des deux côtés. Nous pouvons effectuer la bascule du système en pleine journée sans impacter nos utilisateurs et ainsi procéder à des maintenances durant les heures de production. »

Plus d'une année après la mise en service du système, Yannick Michel et la banque sont très satisfaits : « *Nous avons pu diminuer le budget de fonctionnement et d'investissement tout en améliorant la performance. Nous apprécions aussi la flexibilité de la solution. Pour nous, il est important de disposer d'outils et d'une infrastructure souples permettant de répondre à tout moment, sans surcoût, à l'augmentation des besoins éventuels. »*

La solution VPN-1 Power VSX est intéressante pour toute entreprise qui souhaite simplifier la gestion et l'administration de ses firewalls, bénéficier d'une solution facilement modulable et réduire ses coûts d'exploitation et d'investissement.

Exemple d'architecture



Navixia SA

Route du Bois 1
CH - 1024 Ecublens

Tél. :
41 (0)21 324 32 00

Fax :
41 (0)21 324 32 01

E-mail :
info@navixia.com

Web :
www.navixia.com

VPN-1 Power VSX

- Solution de sécurité virtualisée, incluant firewall, VPN, filtrage URL et IPS
- Environnement réseau virtualisé
- Amélioration des performances
- Réduction des coûts d'exploitation et d'investissement
- Administration simplifiée
- Disponibilité, souplesse et évolutivité
- Nécessite peu d'espace physique