Les nouvelles gÃ©nÃ©rations de pare-feu et les nouvelles dÃ©finitions politiques
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 18/4/2012 11:30:00

Nous sommes entrÃ©s dans lâ□□Ã¨re des applications qui, bien quâ□□elles apportent beaucoup de gains de productivitÃ© Ã la plupart des entreprises, entraÃ®nent aussi des risques. En plus de l'utilisation accrue des applications, une main-d'Å□uvre plus mobile et des menaces plus sophistiquÃ©es font Ã©voluer la faÃ§on dont les passerelles doivent Ãªtre sÃ©curisÃ©es.

C'est lÃ que la nouvelle gÃ©nÃ©ration de pare-feu (NGFWs) entre en jeu. Cependant, alors que les NGFWs vous fournissent une plus grande granularitÃ© de contrÃ´le, ils peuvent, aussi, Ã leur tour, accroÃ®tre la complexitÃ© de vos politiques et exiger une planification et des considÃ©rations supplÃ©mentaires.

L'avÃ¨nement des pare-feu de nouvelle gÃ©nÃ©ration

Les pare-feu traditionnels, qui bloquent les IP sources, IP destinations et les ports, ont Ã©tÃ© positionnÃ©s sur les passerelles depuis quâ□□elles existent. Bien qu'ils continuent Ã jouer un rÃ´le important dans la sÃ©curitÃ© de votre rÃ©seau, les attaquants ciblent les donnÃ©es et utilisent la couche applicative afin de les obtenir. La nouvelle gÃ©nÃ©ration de pare-feu va au delÃ du filtrage des ports 80 ou 443 et vous permet un plus grand contrÃ´le en vous fournissant la possibilitÃ© dâ□□effectuer un filtrage en fonction du type d'application et de l'identitÃ© de l'utilisateur. Avec cette plus grande granularitÃ©, vous pouvez dÃ©finir ce que certains groupes d'utilisateurs peuvent faire avec une application particuliÃ¨re, permettant ainsi dâ□□obtenir une meilleure sÃ©curitÃ© et, en consÃ©quence, un avantage concurrentiel (par exemple, l'Ã©quipe de marketing doit Ãªtre capable de poster sur Facebook, mais pas un dÃ©veloppeur).

ConsidÃ©rations concernant les politiques de pare-feu

Une plus grande granularitÃ© de contrÃ´le apporte plus de complexitÃ©. Plus vos politiques de rÃ©seau sont complexes, plus grande est la possibilitÃ© dâ□□avoir des pare-feu mal configurÃ©s. Et selon Gartner, 95% des violations de pare-feu sont causÃ©es par des erreurs de configuration â□□ et non par des dÃ©fauts de ces pare-feu. Si vous dÃ©finissez des politiques au niveau des applications, vous devez comprendre chaque application, sa valeur ajoutÃ©e pour les diffÃ©rents utilisateurs et les risques potentiels qui y sont associÃ©s.

Les dÃ©cisions politiques en matiÃ¨re de pare-feu ne sont plus entiÃ¨rement noires ou entiÃ¨rement blanches. Comme les ensembles de rÃ¨gles et les nombres de caractÃ©ristiques augmentent, la complexitÃ© augmente Ã©galement. Voici quelques questions que vous devez vous poser (et auxquelles il faut que vous apportiez des rÃ©ponses !) avant dâ□□exploiter des politiques par type d'application et par type dâ□□identitÃ© des utilisateurs que permettent les pare-feu de nouvelle gÃ©nÃ©ration :

â□¢ Combien de demandes de changement de plus par semaine devez-vous vous attendre Ã avoir Ã traiter ?

â□¢ Votre Ã©quipe existante peut-elle absorber la charge supplÃ©mentaire sans dÃ©gradation des dÃ©lais d'exÃ©cution ?

â□¢ Aurez-vous besoin dâ□□effectifs supplÃ©mentaires ?

â¢ Quel est l'impact si vous dÃ©finissez la politique par des rÃ¨gles telles que Â«bloquer les rÃ©seaux sociaux, le partage de fichiers et le streaming vidÃ©o, et autoriser tout le trafic Web restant Â» ?

Votre IT doit comprendre quelles sont les applications nÃ©cessaires pour quels utilisateurs et doit fournir un accÃ¨s - sans ralentir la productivitÃ© et sans ouvrir des failles de sÃ©curitÃ© qui provoqueraient des fuites de donnÃ©es ou des intrusions de logiciels malveillants.

Voici quelques recommandations Ã garder Ã l'esprit lors du dÃ©ploiement de politiques de pare-feu de nouvelle gÃ©nÃ©ration Ã granularitÃ© plus fine :

â¢ ExÃ©cutez vos NGFWs dans un Â« mode d'apprentissage Â» de sorte que vous puissiez voir ce pourquoi les applications sont utilisÃ©es dans votre environnement et par qui. Cela peut, pour commencer, vous fournir des informations essentielles pour dÃ©finir des politiques plus granulaires.

â¢ Simplifiez et automatisez la gestion de vos politiques de pare-feu de nouvelle gÃ©nÃ©ration en tandem avec vos politiques traditionnelles. Alors que les NGFWs fournissent plus de dÃ©tails et plus de contrÃ´le, vous voulez vous assurer que vous pouvez ajouter, mettre Ã jour, modifier, supprimer les politiques Ã travers tout votre domaine protÃ©gÃ© par les pare-feu de maniÃ¨re normalisÃ©e pour garantir la productivitÃ© et l'efficacitÃ© opÃ©rationnelle.

â¢ ExÃ©cutez des requÃªtes Ã risque contre des applications spÃ©cifiques, comme autre contrÃ´le de sÃ©curitÃ©, et dÃ©multipliez les risques tiers dans vos bases de donnÃ©es pour obtenir des informations prÃ©cises.

La nouvelle gÃ©nÃ©ration de pare-feu apporte, sans nul doute, des avantages supplÃ©mentaires par rapport aux pare-feu traditionnels. Mais pour vraiment tirer profit de ces avantages sans ajouter de la complexitÃ© et donc des Ã©lÃ©ments de risque, vous devez, Ã l'avance, Ã©laborer un plan de mise en Å uvre et un processus vous permettant de gÃ©rer ces politiques dans le temps et dans le cadre de votre environnement rÃ©seau au sens large affirme **Marc-Henri Guy**, Directeur RÃ©gional dâAlgoSec.

Â