Pare-feu de nouvelle génération
Guide de l'acheteur

7 raisons pour lesquelles Hillstone Networks est le prochain pare-feu à regarder!

Le monde a radicalement changé au cours de la dernière décennie, voire des cinq dernières années, et du point de vue de la cybersécurité, il devient de plus en plus risqué. Notre dépendance absolue à l'égard de l'internet est incontestable. Les organisations d'aujourd'hui sont tellement liées à la technologie que la simple idée de perdre des données donne des sueurs froides à n'importe quel informaticien.

Certains pays investissent aujourd'hui des sommes considérables dans la cyberguerre et, malheureusement, des victimes innocentes sont touchées ou piratées entre deux feux. Tout cela alors que le cybercriminel moyen a accès à un énorme catalogue d'outils et à un réseau d'équipes sur le Darkweb.

Cela signifie que le département de sécurité informatique moyen doit être très vigilant. Il doit être à la pointe du progrès et disposer d'une multitude d'outils intelligents pour protéger son organisation. Pour mieux comprendre la situation dans laquelle ils se trouvent, il est important de connaître certaines statistiques et le contexte :

- Dans 60% des cas, les pirates informatiques peuvent compromettre les victimes en quelques minutes ! ①
- Chaque seconde, plus d'une nouvelle menace est développée ! ②
- Toutes les 5 minutes, une intrusion se produit !
- 67% des systèmes ne parviennent pas à se protéger contre les attaques !
- 55% des organisations ne savent pas qu'elles ont été compromises !
- 6% des attaques sont détectées !
- Il faut plus de 200 jours pour être détecté, en moyenne !

Information personnelles (GDPR)

La conformité des informations personnelles devenant une réalité, il est essentiel que les organisations comprennent ces statistiques et fassent tout ce qui est en leur pouvoir pour ne pas devenir une statistique !

Données critiques pour l'entreprise

Les données critiques des organisations sont devenues si sensibles que leur perte ou leur compromission peut signifier la fin de l'organisation. Si ce n'est pas le cas, cela peut au moins signifier la fin de l'équipe de direction, y compris le DSI et le RSSI. Il est temps de prendre très au sérieux les menaces qui pèsent sur l'organisation et l'entreprise.

Prix de la sécurité informatique

En raison de la gravité des répercussions des attaques, les organisations sont poussées à acquérir des solutions de sécurité par souci de protection. C'est là que l'organisation doit se méfier des dépenses inutiles, voire du gaspillage. Les éléments suivants doivent être pris en considération:

- Aujourd'hui, une astuce courante des fournisseurs consiste à vendre une bonne solution avec une remise initiale excessive, puis à réduire les remises pour la maintenance et les abonnements des années suivantes. Pour vous assurer que cela ne vous arrivera pas, demandez une proposition de coût total de possession (TCO) sur trois ans.
- Lorsqu'une solution est nettement moins chère que la concurrence, assurez-vous que ce que vous obtenez a toujours de la valeur et qu'elle protège réellement l'organisation tout en fonctionnant conformément aux spécifications, avec toutes les fonctionnalités activées. Par exemple, il n'est pas logique que l'antivirus doive être désactivé pour obtenir le débit correct pour l'organisation.

① Verizon 2015 DBIR

② Ponemon & IBM, 2015; Verizon, 2016

- Acheter la marque la plus chère n'est pas toujours la meilleure. Certaines de ces marques existent depuis plus longtemps et sont considérées comme les meilleures en raison de leur durée de vie. Testez-les avec les marques les moins chères et assurez-vous qu'il y a une bonne raison d'acheter. Il se peut que ces marques compensent des coûts de marketing considérables. Méfiez-vous des rapports de recherche et de conseil qui font ressortir ces marques, car ils ne tiennent pas compte de l'état actuel des choses ; ils regardent tous en arrière.
- Soyez prudent lorsque vous achetez toutes vos solutions de sécurité auprès d'un seul fournisseur. Cela devient très courant et va à l'encontre d'une stratégie de "défense en profondeur ". Par exemple, la protection des points d'extrémité est assurée par la même marque que le pare-feu de l'entreprise. Cela revient à s'appuyer sur la même équipe d'ingénieurs pour deux solutions et cette équipe d'ingénieurs devient le "point de défaillance unique" de votre stratégie de sécurité.

Ne laissez pas la taxe sur la sécurité informatique engloutir tout votre budget. Il existe d'excellentes solutions qui garantissent que vous disposez d'un budget pour chaque partie du cycle de vie de votre sécurité..

Hillstone Networks Next Generation Firewall

Outre son prix très compétitif, le pare-feu de nouvelle génération (NGFW) de Hillstone Networks a de nombreuses autres raisons convaincantes pour lesquelles le marché prend cette solution de sécurité au sérieux. En voici les raisons :

1. Un pare-feu de nouvelle génération complet

C'est simple. Conformément à la définition du pare-feu de nouvelle génération, Hillstone Networks dispose d'une visibilité et d'un contrôle complets des applications. Hillstone Networks fait état de plus de 3 000 applications différentes. Un contrôle plus poussé des différents sous-ensembles ou fonctions des applications, comme le chat Facebook au sein de Facebook, permet un contrôle approfondi de l'accès des utilisateurs. Hillstone utilise l'inspection complète des paquets pour obtenir une visibilité précise des applications. Le décryptage et le contrôle de SSL et SSH garantissent l'inspection de l'ensemble du trafic. Même les utilisateurs ou les applications malveillantes qui tentent des techniques de contournement seront contrôlés. En outre, les pare-feux Hillstone sont dotés de la technologie IPS (Intrusion Prevention System) recommandée par NSS Labs, qui offre une protection inégalée contre les menaces sans compromettre les performances.

2. Technologie avancée brevetée de détection des menaces

Tout bon pare-feu doit protéger contre les menaces connues et inconnues. Un examen plus approfondi de l'approche de Hillstone Networks permet de comprendre pourquoi il s'agit d'une solution aussi complète. Le moteur de détection des menaces avancées (ATD) de Hillstone compare d'abord des échantillons de logiciels malveillants connus au code suspect. Grâce à l'apprentissage automatique, Hillstone utilise le regroupement de logiciels malveillants pour comprendre à quelles souches le code pourrait appartenir. Hillstone Networks traite ensuite les logiciels malveillants inconnus à l'aide d'un moteur d'apprentissage du comportement des logiciels malveillants qui détecte les modèles de comportement des logiciels malveillants inconnus. Les nouvelles variantes de logiciels malveillants sont ensuite partagées avec l'ensemble de la communauté mondiale de Hillstone Networks, ce qui profite à tous et les protège.

Mais ce n'est pas tout. Selon les statistiques, il faut en moyenne 220 jours à une organisation pour se rendre compte qu'elle a été piratée. Le NGFW de Hillstone Networks comprend un moteur de détection des comportements anormaux (ABD) pour atténuer ce défi. ABD procède d'abord à l'apprentissage du comportement et à la modélisation des serveurs et des hôtes. ABD analyse des centaines de dimensions comportementales dans les couches 4 à 7. D'autres analyses en temps réel sont effectuées pour détecter les comportements anormaux. Les niveaux de risque et de certitude de la menace aident l'ingénieur en cybersécurité à décider des mesures à prendre. Le NGFW atténue aussi automatiquement la menace en fonction de la politique.

3. La "cartographie de la chaîne de la mort" et l'analyse criminelle des attaques sont des outils essentiels dans cette lutte

La chaîne d'exécution est le processus ou les tâches qui doivent être accomplies pour qu'un pirate informatique atteigne son ou ses objectifs. Si ces tâches sont exécutées au sein de votre organisation, Hillstone Networks indique visuellement où en est le processus. Grâce à la chaîne d'exécution, il est possible d'atténuer la menace dans certains domaines. Il est très impressionnant de voir ce processus à l'œuvre, car les étapes suivantes sont indiquées : Exploitation initiale, livraison, commandement et contrôle, monétisation, reconnaissance interne, mouvement latéral et enfin exfiltration (que vous ne voulez pas voir au sein de votre organisation). Nous espérons que vous n'êtes pas en train de vivre cela au moment où vous lisez ces lignes !

4. Les meilleurs flux de renseignements sur les menaces

Hillstone Networks dispose d'un système de détection des menaces avancées qui arrête la plupart des menaces. Le problème est qu'il y a toujours une menace qui est plus évasive, plus rusée que les autres. Pour cela, Hillstone Networks propose une solution de bac à sable en nuage (Cloud Sandbox) intégrant Lastline. Lastline est sans doute la meilleure solution de bac à sable disponible, car elle est la seule à avoir obtenu un taux de blocage de 100 % lors de l'évaluation du bac à sable par NSS Labs. Le bac à sable exécute essentiellement un code suspect dans un environnement contrôlé, en le testant dans différents environnements de systèmes d'exploitation et dans différentes versions. Il convient de noter que les logiciels malveillants sont de plus en plus sensibles aux bacs à sable et que le bac à sable que vous mettez en place doit être capable de détecter les techniques d'évasion des bacs à sable. Le partenariat avec Lastline est un exemple de technologie de pointe permettant d'offrir une détection et une protection complètes contre les menaces.

5. Une solution de pare-feu bimode à la pointe de l'industrie

De plus en plus d'entreprises s'appuient sur la disponibilité des applications 24/7/365, et la conception de centres de données redondants avec basculement des applications est donc une obligation. Hillstone s'attaque de front à ce problème avec sa fonction Firewall Twin-Mode, qui relie des paires de pare-feu redondants dans les centres de données afin de maintenir une sécurité totale pour tous les flux de trafic des centres de données redondants. Sa technologie brevetée de basculement en mode double synchronise automatiquement les configurations et les sessions de pare-feu entre les pare-feu des centres de données redondants, assure la sécurité des flux asymétriques entre les centres de données, permet une visibilité et une sécurité totales de tout le trafic de centre de données à centre de données sur les liaisons DCI, garantissant ainsi la continuité des activités du centre de données.

6. Des solutions virtuelles automatisées et compatibles

Les menaces et les réseaux étant devenus plus complexes, la défense de la surface d'attaque élargie est d'autant plus géométrique et exponentiellement plus complexe, en particulier lorsque l'environnement est virtualisé ou dans le nuage. Hillstone CloudHive est une solution de sécurité avancée conçue dès le départ pour répondre aux exigences du centre de données virtuel, multitenant et multi-cloud, et construite sur la plateforme technologique de base Hillstone. Grâce à une microsegmentation avancée et à une API d'orchestration cloud standard, CloudHive insère ses capacités de surveillance et de sécurité en profondeur et de manière transparente dans l'environnement virtuel. Il surveille et traite l'ensemble du trafic nord-sud et est-ouest afin de détecter, d'isoler et d'éliminer les logiciels malveillants, les violations de données potentielles et les autres problèmes de sécurité avant qu'ils ne se propagent dans les machines virtuelles, les locataires et les réseaux virtuels.

7. Améliorer les performances et l'efficacité des liaisons de l'entreprise

Les entreprises recherchent des solutions qui réduisent le nombre d'appareils sur le réseau. L'équilibrage de charge du serveur intégré est une solution complète qui permet de réduire le nombre d'appareils sur le réseau et de réduire les coûts pour l'organisation. Avec Hillstone Networks, aucun dispositif supplémentaire n'est nécessaire pour assurer l'équilibrage de la charge des liens multiples entrant dans l'organisation. Cela inclut le routage des applications afin d'en améliorer les performances. Hillstone prend essentiellement en charge l'algorithme de hachage pondéré, le round robin pondéré et la moindre connexion pondérée.

Hillstone propose un portefeuille de solutions de sécurité réseau à plusieurs niveaux qui se complètent mutuellement ainsi que d'autres offres de sécurité sur le marché, car la cybersécurité d'aujourd'hui implique une coopération entre les lignes de produits et les fournisseurs. Aujourd'hui, plus de 14 000 réseaux d'entreprises dans le monde s'appuient sur les solutions Hillstone, ce qui en fait un choix sûr pour votre entreprise. Qu'attendez-vous ?

Comment contacter Hillstone Networks

www.hillstoneNet.fr

EMAIL: inquiry@hillstoneNet.fr