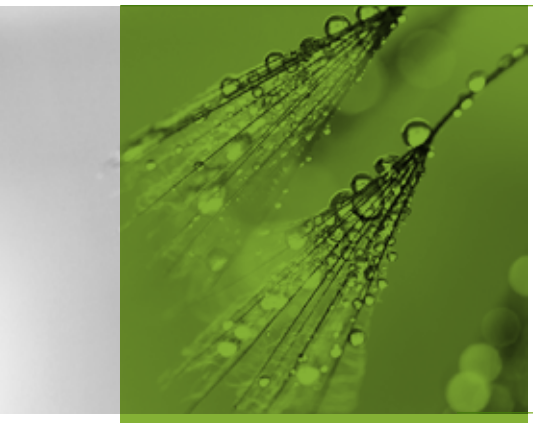

corero

JUNIPER NETWORKS ET CORERO : ENSEMBLE POUR UNE NOUVELLE PROTECTION ANTI-DDOS À GRANDE ÉCHELLE

Détectez et neutralisez les attaques DDoS volumétriques en temps réel et à moindre coût

Problématique

Omniprésentes dans le champ actuel des menaces, les attaques DDoS sont de plus en plus fréquentes, dévastatrices et sophistiquées. À tel point que les interventions manuelles et les centres de scrubbing hors-bande traditionnels ne suffisent plus à les contrer.

Solution

Juniper et Corero ont développé une solution révolutionnaire pour contrer les attaques DDoS. En alliant la surveillance continue des paquets de données à l'analyse machine automatique et aux contrôles sur l'infrastructure de toute la périphérie réseau, la solution opère une détection anti-DDoS à vitesse de ligne pour neutraliser les menaces en temps réel et à très grande échelle.

Avantages

- *Réduction des coûts de neutralisation des attaques DDoS en bloquant le trafic malveillant en périphérie du réseau*
- *Blocage automatique et quasi-instantané des attaques DDoS*
- *Visibilité accrue grâce à la surveillance continue des paquets de données, garante d'une Threat Intelligence exploitable avant, pendant et après l'attaque*
- *Augmentation de la capacité de protection à des dizaines de téraoctets par seconde*

Depuis la création d'Internet, les cybercriminels ont toujours eu recours à des attaques par déni de service distribué (DDoS) pour protester, perturber des activités, nuire à la concurrence ou encore se venger d'organisations qu'il jugent fautives. Ces attaques consistent à noyer les sites web, les réseaux et le cloud sous un énorme volume de trafic pour engendrer des pannes et des interruptions de services, bloquant de fait l'accès aux utilisateurs légitimes qui dépendent de ces services et réseaux pour accomplir leurs missions au quotidien. Selon les estimations, le coût moyen d'une attaque DDoS pour les entreprises s'élevait à plus de 2,5 millions de dollars en 2017[1].

La problématique

Aujourd'hui, pour moins de 100 $, n'importe qui peut lancer une attaque DDoS dévastatrice, sans la moindre expérience de codage.

En effet, les mercenaires du web, qui se vendent à qui veut bien payer leur prix, ont sérieusement baissé les barrières à l'entrée, tant financières que techniques. À l'heure où l'IoT (Internet des objets) connaît une croissance exponentielle, les cybercriminels passent de plus en plus par les objets connectés : peu sécurisés, ils offrent en effet une puissance de feu énorme une fois détournés. En 2016, le botnet Mirai a ainsi compromis près de 100 000 appareils connectés partout dans le monde. Des appareils qui ont ensuite été utilisés pour lancer une attaque DDoS à l'encontre de Dyn, un fournisseur de services DNS. Un pic de 1,2 téraoctets par seconde (To/s) a même été atteint, provoquant une interruption de service de plus de quatre heures. Mais Mirai ne marquait que le début des hostilités. Depuis, des variantes toujours plus sophistiquées et difficiles à contrecarrer sont apparues, telles que JenX, Hajime, Satori et Reaper.

Ensemble, la croissance des services DDoS à la demande et la prolifération de milliards d'appareils IoT non sécurisés ont donc conduit à une très forte hausse du nombre d'attaques DDoS. À en croire le dernier rapport Corero intitulé DDoS : tendances et analyses, les entreprises ont subi en moyenne 237 tentatives d'attaques DDoS par mois durant le premier trimestre de 2017, soit une augmentation de 35 % par rapport au trimestre précédent et l'équivalent de huit tentatives par jour. Sans compter que l'arrivée imminente de la 5G risque fortement d'aggraver le problème en augmentant la bande passante disponible. Les tuyaux étant plus gros, les cybermalfaiteurs vont pouvoir constituer des armées de zombies de plus en plus puissantes.

[1] https://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/

À mesure que les attaques DDoS gagnent en ampleur, en fréquence et en sophistication, les méthodes traditionnelles reposant sur les centres de scrubbing hors bande et les interventions manuelles s'avèrent aussi inefficaces que coûteuses. Dans le cas particulier des attaques volumétriques, la déviation du trafic suspect vers des centres de scrubbing pèse non seulement en termes de latence mais aussi de coût, ce dernier étant directement lié au volume de données à neutraliser. De plus, cette approche traditionnelle exige une analyse et une intervention humaines, ce qui ne fait qu'allonger la latence et alourdir les coûts de remédiation. Avec ces méthodes, pas moins de 30 minutes peuvent s'écouler entre la détection et la neutralisation, un délai inacceptable quand on sait qu'il ne faut souvent pas plus que quelques minutes pour paralyser un site web.

Dans un monde hyperconnecté où la moindre interruption de service se paie comptant, il est indispensable de revoir sa stratégie anti-DDoS et de mettre en place des défenses plus rapides, plus efficaces et plus économiques. Les réseaux IP doivent constituer la première ligne de défense contre les attaques volumétriques. La télémétrie, l'analyse machine et la programmabilité réseau interviennent ensuite pour favoriser l'élaboration d'un processus de détection et de neutralisation plus intelligent, plus automatisé et plus adaptable.

Protection anti-DDoS : la solution co-signée Juniper Networks et Corero

Juniper Networks et Corero Network Security ont uni leurs forces pour développer une protection anti-DDoS qui répare automatiquement le réseau grâce à une identification rapide, des décisions fiables, une surveillance continue et une neutralisation automatique sur les points stratégiques du réseau (Figure 1).

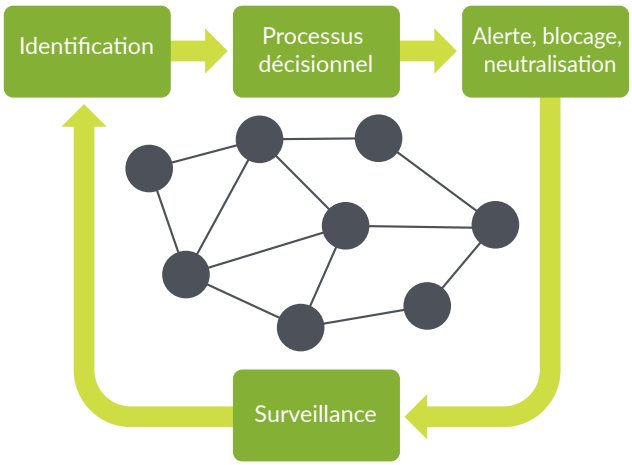

Figure 1 : Réparation automatique du réseau

Pour être la plus efficace possible, la protection anti-DDoS doit bloquer les attaques au plus près de la source, c'est-à-dire le plus souvent en périphérie du réseau. Les trois grands points de neutralisation se situent donc au niveau des points de peering avec les fournisseurs de services (SP, Service Providers), de la périphérie du datacenter et de la périphérie de l'abonné.

Impressionnante d'efficacité et d'automatisation, la solution anti-DDoS de Juniper Networks et Corero Network Security peut monter jusqu'à plusieurs téraoctets par seconde à un coût plus bas que toutes les solutions concurrentes. Déployée en périphérie du réseau, elle détecte et neutralise les attaques DDoS de la manière suivante (voir Figure 2) :

- Les plateformes de routage universelles 5G MX Series de Juniper Networks® sont déployées en périphérie du réseau pour surveiller le trafic entrant par le biais d'un échantillonnage en miroir (entête et payload inclus) capable de monter en charge dynamiquement pour s'adapter à la volumétrie de l'attaque.
- Les routeurs MX Series transfèrent les échantillons au SmartWall Threat Defense Director (TDD) de Corero qui inspecte chaque paquet de flux au moyen de règles et de machine learning. TDD détecte ainsi avec rapidité et précision les signes symptomatiques d'une attaque DDoS.
- En quelques secondes, TDD identifie l'attaque et génère automatiquement des filtres de correspondance sur les pare-feu pour neutraliser la menace à l'aide des routeurs MX Series.
- TDD configure automatiquement les routeurs MX Series via le Network Configuration Protocol (NETCONF) afin d'installer des filtres éphémères qui bloquent les paquets DDoS au point d'entrée le plus proche de la source du trafic perturbateur. De son côté, le trafic légitime peut poursuivre son chemin jusqu'à sa destination sans aucune perte de performance.
- Les routeurs MX Series opèrent une télémétrie en streaming puis transfèrent les statistiques des trafics autorisés et bloqués au Corero SmartWall TDD.
- Les analyses SmartWall TDD SecureWatch Analytics offrent une visibilité complète sur le trafic réseau avant, pendant et après l'attaque. Grâce à cette application sous Splunk, les équipes opérationnelles ont accès à des récapitulatifs d'attaques et autres informations indiquant l'efficacité du processus de neutralisation.

Ce processus se poursuit tout au long du cycle de l'attaque, jusqu'à ce que les échantillons indiquent que les points d'entrée ne sont plus menacés. Après quoi SmartWall TDD supprime les filtres des routeurs MX Series pour retourner à un mode opérationnel normal. Les routeurs MX Series continuent de transférer les échantillons et la télémétrie vers Corero TDD de façon à assurer un retour complet à la normale tout en surveillant le moindre signe d'une nouvelle attaque.

Ce modèle opérationnel 100 % automatisé protège intégralement les fonctions métiers opérationnelles tout en offrant une visibilité continue aux équipes Ops.

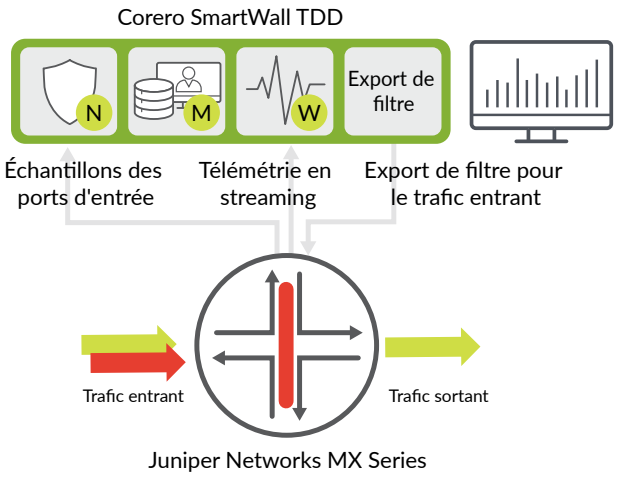

Figure 2 : Solution de protection anti-DDoS de Juniper et Corero

Fonctionnalités et avantages

La solution anti-DDoS de Juniper et Corero associe les avantages d'une inspection du trafic au niveau des paquets à la puissance d'un contrôle basé sur l'infrastructure. Résultat : une neutralisation automatique et temps réel des attaques DDoS à une échelle de dizaines de téraoctets à la seconde, le tout en réduisant les coûts. Du jamais vu.

Neutralisation des DDoS à moindre coût

Grâce aux fonctionnalités de filtrage des plateformes de routage universelles 5G MX Series, le trafic malveillant est bloqué en périphérie de manière distribuée. Au lieu de rediriger tout le trafic vers un centre de scrubbing centralisé – un système qui coûte cher et ajoute de la latence – cette approche permet aux entreprises et SP de réduire considérablement le coût de neutralisation des attaques DDoS sur de tels volumes de trafic, sans avoir à investir dans une augmentation de capacité. Par ailleurs, plus de 95 % du processus s'opère automatiquement, sans aucune intervention de la part d'un analyste ou opérateur. Cela a pour effet de réduire drastiquement le coût total de possession par rapport aux approches manuelles traditionnelles.

Réponse rapide et meilleure expérience client

L'automatisation permet d'identifier et bloquer les attaques DDoS en quelques secondes – une véritable prouesse par rapport aux méthodes traditionnelles qui peuvent prendre plus de 30 minutes. Mieux encore, la solution Juniper-Corero ne bloque que les paquets de l'attaque et laisse le trafic légitime suivre son cours. L'expérience client n'est donc pas impactée, même lorsque l'attaque est à son paroxysme.

Visibilité améliorée + ressources optimisées = neutralisation efficace

La solution anti-DDoS de Juniper Corero permet de surveiller le trafic au niveau des paquets. Comparée aux approches de détection traditionnelles basées sur les flux, l'inspection des paquets est plus efficace et offre aux opérateurs davantage de visibilité sur les données d'en-tête et de payloads. De plus, par rapport aux protocoles IPFIX (IP Flow Information Export), l'échantillonnage en miroir mobilise très peu les ressources du routeur, puisque le routeur n'a pas à agréger et traiter une forte volumétrie de données. Enfin, nul besoin de tout changer sur votre réseau. La solution fonctionne parfaitement avec vos outils dans un modèle de protection anti-DDoS multi-niveau où les routeurs de périphérie constituent la première ligne de défense. Ils dévient le trafic d'attaque volumétrique et font appel aux ressources de scrubbing centralisées pour gérer les attaques plus sophistiquées au niveau applicatif.

Capacité de traitement de dizaines de To/s

Corero SmartWall TDD peut neutraliser jusqu'à 40 To/s de trafic à vitesse de ligne, sans backhaul du trafic DDoS sur le réseau. Associée aux plateformes de routage universelles 5G MX Series et à leurs transferts de paquets pouvant atteindre 80 To/s, la solution affiche la plus forte évolutivité des systèmes anti-DDoS du marché.

Composants de la solution

Corero SmartWall Threat Defense Director

Corero SmartWall TDD est une révolution dans la protection anti-DDoS volumétrique en temps réel, comme en témoignent ses nombreux avantages :

- Capacité de surveillance et de neutralisation pouvant atteindre plusieurs dizaines de téraoctets par seconde
- Inspection au niveau des paquets pour une détection fiable des attaques DDoS volumétriques
- Filtrage automatique par analyse machine pour une neutralisation intelligente
- Réponse en temps réel, pour un délai de neutralisation de quelques secondes seulement
- Boucle de rétroaction pour éliminer les faux positifs
- Granularité des journaux à la seconde, minute, journée, semaine, mois, année
- Analyse forensique des échantillons de paquets issus du trafic bloqué et autorisé
- Analyses, reporting, alertes et automatisation signés Splunk
- API ouvertes pour permettre une réponse autonomique et faciliter le travail du SecOps
- Recours aux outils BGP, NETCONF, Representational State Transfer (REST), JavaScript Object Notation (JSON) et au cloud

Plateformes de routage universelles 5G MX Series de Juniper Networks

Les plateformes MX Series offrent tout un éventail de routeurs compatibles SDN et équipés de multiples fonctionnalités :

- Capacité, densité, sécurité et performances système sans précédent

- Pionnier de la sécurité inline des plans de données, sans compromis sur les performances
- Support progressif des innovations futures grâce à une programmabilité infinie
- Livraison accélérée des services grâce à l'automatisation
- Réseau multi-services et fonctionnalités de découpage de nœuds pouvant réduire le TCO de 40 %
- Réduction des risques d'interruption de service avec Junos® Continuity et la mise à niveau unifiée des logiciels intra-service (ISSU)
- Disponibilité hors pair du réseau et des services avec tout un ensemble d'outils de résilience
- Capacité à traiter le trafic par application via une inspection approfondie des paquets (DPI)
- Collecte de données au niveau des composants et envoi en streaming aux outils de surveillance et d'analyse via l'interface de télémétrie de Junos (JTI)
- Encombrement minimal et puissance maximale

Synthèse – Une protection anti-DDoS en temps réel, à grande échelle et à moindre coût

Multicloud, IoT et 5G oblige, les menaces de cybersécurité ne cessent de se muer en de nouvelles formes. C'est le cas des attaques DDoS qui se font de plus en plus fréquentes, sophistiquées et dévastatrices. Face à cette triste réalité, les entreprises et les fournisseurs de services doivent trouver des moyens plus rapides, plus efficaces et moins coûteux de renforcer leurs défenses.

Le réseau IP constitue en ce sens la première ligne de défense d'une solution moderne de neutralisation des attaques volumétriques. La télémétrie, le machine learning et la programmabilité réseau doivent permettre, quant à elles, l'élaboration d'un processus de détection et de neutralisation plus intelligent, plus automatisé et plus adaptable.

La solution de protection anti-DDoS de Juniper et Corero associe les avantages d'une inspection du trafic au niveau des paquets à la puissance d'un contrôle basé sur l'infrastructure. Résultat : une neutralisation automatique et temps réel des attaques DDoS à une échelle de dizaines de téraoctets à la seconde, le tout en réduisant les coûts. Du jamais vu.

Prochaines étapes

Pour découvrir comment Juniper Networks et Corero peuvent renforcer la résistance de votre réseau face aux attaques DDoS, contactez votre représentant Juniper ou Corero.

À propos de Corero

Corero Network Security est le leader des solutions anti-DDoS hautes performances et temps réel. Hébergeurs, fournisseurs de services, acteurs du numérique… tous font confiance à la technologie multi-primée de Corero pour bloquer les attaques DDoS contre leur environnement. L'approche Corero ? Une détection et neutralisation automatiques des attaques, doublée d'une visibilité réseau complète et de rapports et analyses détaillés. Cette technologie pionnière offre des capacités de protection à la fois évolutives et économiques pour lutter contre les attaques DDoS dans les environnements les plus complexes. Plus d'informations sur www.corero.com

À propos de Juniper Networks

Juniper Networks simplifie le réseau grâce à des produits, solutions et services qui connectent le monde. Nos capacités d'innovation nous permettent d'écarter les obstacles et de briser la complexité des réseaux à l'ère du cloud pour éliminer les difficultés que connaissent nos clients et partenaires au quotidien. Pour Juniper Networks, le réseau est un moyen de partager des connaissances et de favoriser un progrès au service de l'humain. Pour cela, nous inventons des méthodes de conception de réseaux automatisés, évolutifs et sécurisés, capables d'évoluer au rythme des entreprises.

Siège social et commercial
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089, États-Unis
Téléphone : +1 888 586 4737
ou +1 408 745 2000
Fax : +1 408 745 2100
https://www.juniper.net/fr/fr/

Siège EMEA et APAC
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Pays-Bas
Téléphone : +31 0 207 125 700
Fax : +31 0 207 125 701