Lutte contre les attaques DDoS à tous les niveaux

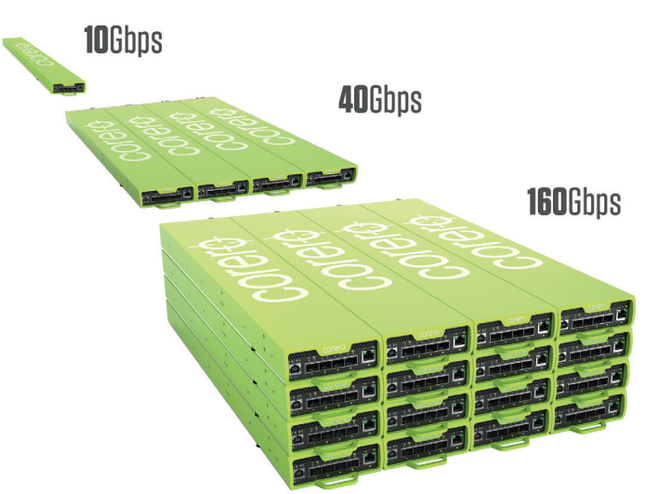
DDoS-Threat-Defense-Systems (TDS) de Corero

Les attaques «Distributed Denial of Service» (DDoS) font partie des menaces actuelles les plus importantes contre les infrastructures et applications informatiques. L'utilisation des DDoS-Threat-Defense-Systems (TDS) ultra-performants de Corero est recommandée pour identifier et lutter efficacement contre ces attaques.

L'objectif des attaques DoS et DDoS est de paralyser les applications et serveurs et de perturber les systèmes tels que les pare-feux, Load-Balancer, serveurs web et serveurs d'applications, bases de données et solutions de stockage en les empêchant d'exécuter leurs tâches («Denial of Service»). Les pirates utilisent pour cela les attaques bien connues basées sur le volume. Par ailleurs, ils lancent également de plus en plus d'attaques intelligentes multivecteurs ainsi que des attaques ciblant les applications.

Dans la première variante mentionnée, on utilise par exemple un réseau de zombies pour transmettre un nombre si important de demandes HTTP sans protocole d'authentification au système attaqué que ce dernier n'est plus en mesure de fournir des contenus en raison de la surcharge générée. Les formes d'attaques de type SYN-Flood ou Smurf font partie de cette catégorie.

Les attaques intelligentes à plusieurs niveaux sont de plus en plus fréquentes. Ces attaques «lentes» et «moins performantes» nécessitent des ressources plus modestes et se donnent souvent beaucoup de temps pour infecter les systèmes attaqués. C'est pourquoi elles sont généralement difficiles à identifier comme des menaces, étant donné que le volume de trafic du réseau n'est pas en nette augmentation. Parmi les formes intelligentes d'attaques, on compte notamment les attaques Reflecting-DDoS, les Application Layer DDoS, l'utilisation ciblée des vulnérabilités du serveur, les Pre-Attack Recon Scans (acquisition de connaissances approfondies sur l'infrastructure à attaquer) et les Advanced Evasion Techniques (combinaison de techniques d'évasion connues avec de nouvelles méthodes de camouflage pour introduire des codes malveillants dans le réseau cible souhaité).



Les DDoS-Threat-Defense-Systems totalement évolutifs de Corero protègent de la même manière les applications et les infrastructures.

Protection efficace contre les cyber-attaques

Grâce à l'intégration d'une «First Line of Defense» à la périphérie extérieure de l'infrastructure du réseau client ou du réseau du fournisseur de services, les TDS de Corero garantissent une disponibilité maximale et une performance illimitée de tous les services et infrastructures situés en aval.

- Solutions «First Line of Defense» ultra-performantes pour fournisseurs de services, hébergeurs, centres de données et entreprises
- Identification et lutte contre une large palette d'attaques (attaques High-Volume ou «Reflective and amplified Spoof Attacks») au niveau du réseau et attaques DDoS «intelligentes» et «lentes» au niveau des applications (Layer 3 à 7)
- Lutte efficace contre les attaques DDoS tout en autorisant les accès légitimes (Business Continuity ou préservation des services attaqués)
- Plateforme TDS dédiée avec CPUs Multicore à accélération matérielle
- Temps de latence réduits au minimum et très haut débits de 10 Gbps à 1 Tbps par rack
- Solution modulaire et évolutive par pas de 1 et 10 Gbps
- SDN- et Cloud-ready
- Approvisionnement automatique
- Système de reporting centralisé

First Line of Defense

Afin d'identifier et de lutter contre les attaques DOS et DDoS à tous les niveaux, du niveau des applications au niveau DNS et HTTP et jusqu'au niveau du protocole (Layer 3 à 7), le spécialiste de la sécurité des réseaux Corero présente les DDoS-Threat-Defense-Systems (TDS) ultra-performants. Ces systèmes rendent de précieux services aux entreprises (on-premise) ainsi qu'aux fournisseurs de services et hébergeurs. Ils bloquent les adresses IP dangereuses et les trafics de données indésirables provenant de zones géographiques définies, limitent le nombre de demandes et de connexions, stoppent les abus et violations de protocole et empêchent les AETs (Advanced Evasion Techniques). Ils bloquent également les accès non autorisés (Intrusion Prevention), repoussent les Buffer Overflows et Exploits et bloquent l'injection de codes exécutables (Code Injection). En bref: ils constituent un dispositif de sécurité unique pour lutter contre les attaques DDoS les plus variées.

BOLL
IT Security Distribution

BOLL ENGINEERING SA

En Budron H15, 1052 Le Mont s. Lausanne
Tél 021 533 01 60, contact@boll.ch,
www.boll.ch