axians

JUNIPER NETWORKS
ELITE PARTNER

Whitepaper

DDos Protection mit Juniper Networks TDD

Warum ergibt eine erneute Betrachtung von DDoS Sinn?

Die Analyse von Bandbreite in den Core Netzwerken zeigt deutlich, dass zukünftig zunehmend Bandbreite zum Transport der Daten im Core benötigt wird. Dieser Anstieg begründet sich daraus, dass immer mehr Geräte eine höhere Bandbreite zum Internet bekommen (Broadband Internet Access) und neue Access-Technologien, wie 5G, Anwendung finden. Zudem nutzen immer mehr Geräte aus der IoT-Welt das Internet zum Bereitstellen ihrer Dienste.

Doch was bedeutet das für den Schutz des Provider Core Netzwerkes? Die Anzahl von unbewusst gekaperten Geräten wird signifikant zunehmen und auch die Gesamtbandbreite steigt. Wo es zurzeit noch wenige volumenlastige DDoS-Angriffe gibt, wird es zukünftig weitaus häufiger Volumenattacken geben, die an die Grenzen des Provider Core Netzwerkes kommen.

Unbegrenzte Next-Generation DDoS Protection

Verhindern Sie aktiv DDoS-Attacken, die Ihr Netzwerk bedrohen und vorhandene Ressourcen einschränken, indem Sie bereits am Edge und im Access-Layer auf eine Lösung zurückgreifen, welche nicht den marktüblichen Beschränkungen unterliegt.

Einschränkungen „klassischer" DDoS-Applikationen

Heutzutage filtern im DDoS-Angriffsfall sogenannte „Scrubbing Center" den Angriffsverkehr aus dem gesamten Datenverkehr des attackierten Hosts oder Netzwerkes heraus. Scrubbing Center sind typischerweise im Core Netzwerk platziert und haben dadurch erhebliche Nachteile:

- **Endliche Ressourcen:** Erhöht sich die Bandbreite am Edge des Core Netzwerkes zu anderen „Automen Systemen" (AS), Peerings oder Upstream-Providern, so steigt automatisch die Angriffsfläche. Daher müsste man das Scrubbing Center ebenfalls erweitern, um sich vor höheren Volumenattacken zu schützen. Das ist jedoch nur bedingt möglich und mit hohen Investitionen verbunden.
- **Flutung des Kernnetzes:** Mit dem Heranziehen des bösartigen Datenverkehrs zu den Scrubbing Centers verstopft das Core Netzwerk mit Daten. Hierbei kann es zu maximalen Auslastungen von physikalischen Links kommen, wodurch andere Datendienste in Mitleidenschaft gezogen werden.

Die Lösung von Juniper und Corero

Mit der Next-Generation DDoS Mitigation Lösung von Juniper Networks und Corero Network Security beseitigen Sie alle Nachteile – und profitieren jetzt und in Zukunft von folgenden Benefits:

Schutz direkt am Edge: Wird ein DDoS-Angriff durch die Corero Lösung entdeckt, werden binnen Sekunden Firewall-Filter auf den involvierten Core Routern von Juniper installiert und automatisch nach Beenden des Angriffs wieder gelöscht. Die ehemaligen Scrubbing Center befinden sich dadurch dezentral direkt auf den Core Routern.

Keine endlichen Ressourcen: DDoS-Angriffe werden nun direkt am Übergang zum Edge verworfen und können keine physikalischen Links innerhalb des Provider Core Netzwerkes fluten. Da es kein zentrales Scrubbing Center gibt, kann es auch keinen Mitigation-Engpass geben. Allenfalls ist die Corero Lösung in der Anzahl von zu überwachenden MX Core Routern limitiert und kann durch einfaches paralleles Aufbauen neue MX Core Router bedienen.

DDoS Protection im Access-Netzwerk: Auch durch das Mitigieren direkt auf den Access Core Router kann das eigene Provider Core Netzwerk problemlos vor DDoS-Angriffen durch gekaperte Kundengeräte geschützt werden.

DDoS Protection im Rechenzentrum: Unbewusst gekaperte Hosts im Datacenter, die von dort aus einen DDoS-Angriff mit sehr hohen Bandbreiten starten können, werden durch die Juniper TDD Lösung direkt an dem Übergang zum Provider Core Netzwerk gestoppt. Der Angriff selbst kommt daher nicht mehr aus dem Datacenter heraus.

Haben wir Ihr Interesse geweckt? Wir freuen uns über Ihre Kontaktaufnahme!

KONTAKT
info-networks-solutions@axians.de

axians.de

VINCI ENERGIES