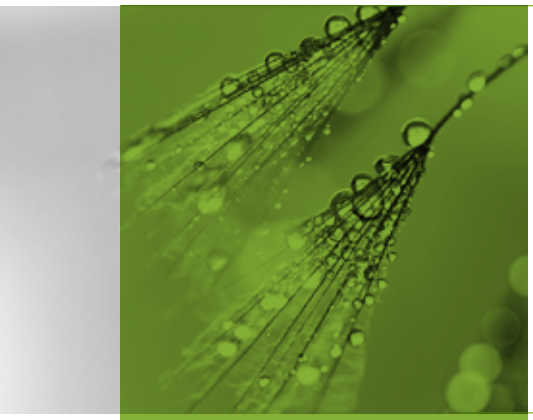

JUNIPER NETWORKS UND CORERO: EIN MODERNER ANSATZ FÜR SKALIERBAREN DDOS-SCHUTZ

Kosteneffiziente Erkennung und Abwehr volumetrischer DDoS-Angriffe

Die Herausforderung

DDoS-Angriffe stellen eine erhebliche Bedrohung für moderne Unternehmen dar. Bislang wird der Datenverkehr bei einem solchen Angriff über externe Datencenter umgeleitet und dort gefiltert. Die Angriffserkennung und die Umleitung müssen allerdings oft manuell erfolgen. Da das Ausmaß, die Häufigkeit und die Komplexität von DDoS-Angriffen immer weiter steigen, ist dieser Ansatz nicht mehr zeitgemäß.

Die Lösung

Juniper und Corero haben einen völlig neuen Ansatz entwickelt, um DDoS-Angriffe in Echtzeit zu erkennen und ihre Auswirkungen zu begrenzen. Dieser Ansatz nutzt die ständig aktivierte Paketüberwachung, automatisierte maschinelle Analysen und infrastrukturbasierte Kontrollmaßnahmen am Netzwerkrand, um auch Angriffe mit extrem großem Volumen unschädlich zu machen.

Die Vorteile

- *Kosteneffizienterer Schutz vor DDoS-Angriffen durch das Herausfiltern des schädlichen Datenverkehrs am Netzwerkrand*
- *Automatisierte Reaktion zur Abwehr von DDoS-Angriffen innerhalb von Sekunden*
- *Bessere Transparenz durch ständig aktivierte Paketüberwachung, die vor, bei und nach einem Angriff detaillierte, praktisch nutzbare Einblicke liefert*
- *Ausweitung der Überwachungskapazität auf Dutzende von Terabits pro Sekunde*

Distributed Denial of Service oder DDoS-Angriffe sind so alt wie das Internet. Hacker nutzen sie in Protestaktionen, um „nur aus Spaß“ Unheil zu stiften, Konkurrenten gezielt zu schädigen oder sich für empfundenes Unrecht zu rächen. Bei einem DDoS-Angriff wird eine Website, ein Netzwerk oder eine Cloud-Umgebung mit einer riesigen Anzahl von Netzwerkmeldungen überflutet, sodass die dort bereitgestellten Services und Unternehmensnetzwerke für legitime Nutzer nicht oder nur mit großer Verzögerung verfügbar sind oder sogar ganz zusammenbrechen. Angesichts der nahezu vollständigen Abhängigkeit vieler Unternehmen von Netzwerk- und Serviceanbietern kann das verheerend sein. Schätzungen zufolge belief der durchschnittliche Schaden sich im Jahr 2017 auf über 2,5 Millionen US-Dollar pro DDoS-Angriff.[1]

Die Herausforderung

Inzwischen gibt es Hacker, die spezielle Dienste für DDoS-Angriffe anbieten, teilweise für unter 100 US-Dollar.

Infolgedessen können nun auch technisch wenig versierte Kriminelle ohne Programmiererfahrung DDoS-Angriffe starten. Viele dieser DDoS-Dienste missbrauchen das Internet der Dinge, denn die riesige Anzahl der oft kaum geschützten vernetzten Geräte ist geradezu perfekt für DDoS-Angriffe geeignet. Wir möchten hier beispielsweise an das IoT-Botnetz Mirai aus dem Jahr 2016 erinnern, das fast 100.000 gekaperte Geräte in aller Welt umfasste. Von diesem Botnetz aus wurde ein DDoS-Angriff auf den DNS-Anbieter Dyn gestartet, der ein Spitzenvolumen von 1,2 Terabit pro Sekunde (Tbit/s) erreichte, den Service zeitweise völlig lahmlegte und für über vier Stunden erheblich störte. Und das war nur der Anfang. Seitdem sind mit JenX, Hajime, Satori und Reaper neuere und ausgefeiltere Varianten derselben Angriffsmethode aufgetaucht.

Das zunehmende Angebot an Services für DDoS-Angriffe und die Milliarden nicht oder nur unzureichend geschützter Geräte im Internet der Dinge haben erheblich zum Anstieg der DDoS-Angriffe beigetragen. Dem aktuellen Bericht DDoS Trends and Analysis von Corero zufolge mussten Unternehmen im dritten Quartal 2017 durchschnittlich 237 DDoS-Angriffe pro Monat (also acht pro Tag) abwehren. Das entspricht einem Anstieg von 35 Prozent gegenüber dem vorhergehenden Quartal. Mit dem Übergang zu 5G wird die verfügbare Netzwerkbandbreite steigen, sodass Hacker noch mehr Spielraum haben, um Unternehmensnetzwerke von gekaperten vernetzten Geräten aus zu überfluten.

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

Angesichts der steigenden Anzahl, Größe und Komplexität von DDoS-Angriffen sind herkömmliche Gegenmaßnahmen wie die manuelle Umleitung des Netzwerkverkehrs über externe Datencenter, in denen die DDoS-Pakete erkannt und herausgefiltert werden, sowohl zu langsam als auch zu teuer. Durch die Umleitung steigt die Latenzzeit und da die Kosten für die Filterung vom Volumen des umgeleiteten Netzwerkverkehrs abhängig sind, können sie bei groß angelegten Angriffen schnell ausufern. Zudem sind zur Erkennung des Angriffs und zur Umleitung des Datenverkehrs eine manuelle Analyse und andere Administratoreingriffe erforderlich, die die Latenz und die Kosten zusätzlich in die Höhe treiben. Zwischen der Erkennung eines Angriffs und der Einleitung der erforderlichen Gegenmaßnahmen verstreichen mitunter bis zu 30 Minuten. Das ist eindeutig zu viel, denn ein DDoS-Angriff kann eine Website in wenigen Minuten lahmlegen.

Die moderne Geschäftswelt schläft nicht und Ausfälle aller Art sind ein riesiges Problem für nahezu jedes Unternehmen. Deshalb sollten Verantwortliche in Unternehmen und insbesondere bei Serviceanbietern ihre aktuelle Strategie für den DDoS-Schutz dringend überdenken und neue Methoden in Erwägung ziehen, die schnelleren, effektiveren und kostengünstigeren Schutz bieten. Das IP-Netzwerk sollte ein integraler Bestandteil einer modernen Lösung sein und groß angelegte Angriffe schon am Netzwerkrand abschwächen. Telemetrie, maschinelle Analysen und programmierbare Netzwerke sollten anspruchsvollere Komponenten für die intelligente, automatisierte und anpassbare Erkennung und Abwehr von Angriffen beisteuern.

Die Lösung von Juniper Networks und Corero

Juniper Networks und Corero Network Security haben gemeinsam eine Lösung entwickelt, die Netzwerke vor DDoS-Angriffen schützt und automatisch repariert. Diese Lösung zeichnet sich durch die schnelle Erkennung von Angriffen, eine präzise Entscheidungsfindung, automatisierte Gegenmaßnahmen an strategischen Punkten im Netzwerk und die kontinuierliche Überwachung des Netzwerkverkehrs aus (siehe Abbildung 1).

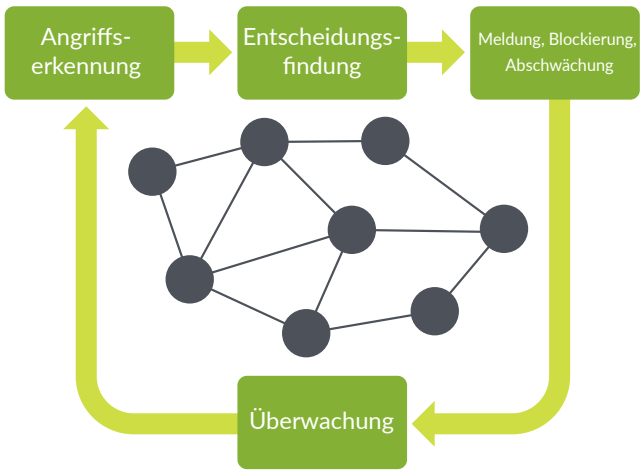

Abbildung 1: Selbstheilendes Netzwerk

Zu den Best Practices für den wirksamen Schutz vor DDoS-Angriffen gehört, Angriffe so nah an der Quelle wie möglich zu stoppen, typischerweise am Netzwerkrand. Deshalb werden Abwehrmaßnahmen oft an Peering-Punkten des Serviceanbieters sowie an der Netzwerk-peripherie des Datencenter- und des Abonnentennetzwerks installiert.

Die gemeinschaftlich von Juniper Networks und Corero Network Security entwickelte Lösung für den DDoS-Schutz ist sehr effektiv, automatisiert und kostengünstiger für Netzwerkverkehrsvolumen im Terabit-Bereich skalierbar als jede andere derzeit verfügbare Lösung für den Schutz vor DDoS-Angriffen. Die Lösung sollte am Netzwerkrand installiert werden, wo ihre Methoden für die Erkennung und Abschwächung von DDoS-Angriffen besonders wirksam sind (siehe Abbildung 2):

- Die universelle 5G-Routing-Plattform der MX-Serie von Juniper Networks® wird am Netzwerkrand eingesetzt, um den eingehenden Netzwerkverkehr nach Anzeichen für einen solchen Angriff zu durchsuchen. Dazu wird ein Datenspiegel erstellt, auf dem Stichproben (sowohl Header als auch Paketinhalte) für die Analyse entnommen werden. Diese Analysen können in Abhängigkeit vom Ausmaß der Bedrohung dynamisch skaliert werden.
- Die Router der MX-Serie leiten die Stichproben an den Corero SmartWall Threat Defense Director (TDD) weiter, der jedes empfangene Paket inspiziert und mithilfe einer regelbasierten, maschinellen Analyse schnell und zuverlässig ermittelt, ob es Teil eines DDoS-Angriffs ist.
- TDD deckt Angriffe binnen Sekunden auf und generiert automatisch flexible Firewall-Filter für die Router der MX-Serie, mit denen die schädlichen Datenpakete aus dem Datenstrom entfernt werden können.
- Anschließend nutzt TDD das Network Configuration Protocol (NETCONF), um diese Filter automatisch auf den Routern der MX-Serie zu installieren, damit die schädlichen Pakete an dem Netzwerkzugangspunkt herausgefiltert werden können, der ihrem Ursprungsort am nächsten liegt. Ebenso wichtig ist, dass der legitime Datenverkehr ungehindert und ohne Leistungseinbußen weitergeleitet wird.
- Statistische Werte über den weitergeleiteten und den blockierten Netzwerkverkehr werden mithilfe der Streaming-Telemetrie-Funktionen der Router an Corero SmartWall TDD weitergeleitet.
- SmartWall TDD SecureWatch Analytics bietet einen umfassenden Überblick über den Netzwerkverkehr vor, bei und nach jedem Angriff. Diese auf Splunk basierende Anwendung generiert auch Angriffsberichte und andere detaillierte, praxistaugliche Informationen über die Wirksamkeit der DDoS-Abwehr für die Betriebsteams.

Dieser Prozess läuft während des gesamten Angriffszyklus weiter, bis die Stichproben von den Netzwerkzugangspunkten keine schädlichen Datenpakete mehr enthalten. Dann entfernt SmartWall TDD seine automatisch generierten, flexiblen Filter von den Routern der MX-Serie und kehrt zum normalen Betrieb zurück. Die Router senden weiterhin Stichproben und Streaming-Telemetrie-Daten an Corero TDD. Diese werden analysiert, um sicherzugehen, dass der Angriff wirklich vorbei ist und um nach Hinweisen auf den nächsten Angriff Ausschau zu halten.

Alle Abläufe sind automatisiert, sodass der Geschäftsbetrieb umfassend geschützt ist und das Betriebsteam jederzeit alles im Blick hat.

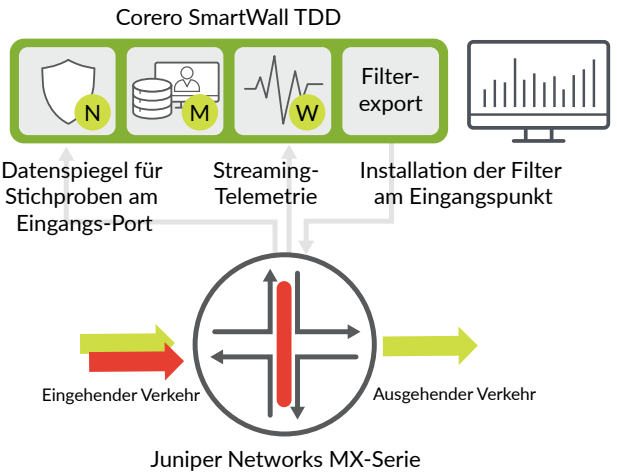

Abbildung 2: Gemeinsame DDoS-Schutzlösung von Juniper und Corero

Funktionen und Vorteile

Die von Juniper und Corero entwickelte Lösung vereint die Vorteile der Verkehrsanalyse auf Paketebene mit infrastrukturbasierten Maßnahmen für die Durchsetzung und ist dadurch in der Lage, DDoS-Angriffe mit Volumen im zweistelligen Terabit-Bereich automatisch abzuschwächen – und gleichzeitig die Kosten erheblich zu reduzieren.

Kostengünstigere Abschwächung von DDoS-Angriffen

Durch die Nutzung der Filterfunktionen der Universellen 5G-Routing-Plattform der MX-Serie können schädliche Datenpakete dezentralisiert – und bereits am Netzwerkrand – entfernt werden. Dadurch entfällt die Umleitung des gesamten Datenverkehrs über ein externes Datencenter samt der damit einhergehenden Latenz und Kosten. Für Serviceanbieter und Unternehmen bedeutet das, dass sie sich zu erschwinglichen Kosten und ohne teure Kapazitätserweiterung wirksam vor DDoS-Angriffen schützen können. Und da über 95 Prozent der Maßnahmen vollständig automatisiert sind, entsteht auch keine zusätzliche Belastung für das Betriebspersonal oder die Analysten. Die Gesamtbetriebskosten sind daher erheblich niedriger als für Lösungen, die auf konventionellen Ansätzen mit vielen manuellen Arbeitsschritten beruhen.

Schnellere Reaktion und bessere Customer Experience

Mit dem automatisierten Ansatz können DDoS-Angriffe in Sekundenschnelle erkannt und blockiert werden. Das ist eine erhebliche Verbesserung gegenüber dem oben beschriebenen her-kömmlichen Ansatz, der zu einem großen Teil auf manuellen Schritten basiert und mehr als 30 Minuten in Anspruch nehmen kann. Ebenso wichtig wie diese schnelle Reaktion ist, dass nur die schädlichen Datenpakete blockiert werden. Die Lösung von Juniper und Corero lässt legitimen Datenverkehr ungehindert passieren, sodass die Geschäftsabläufe der Kunden selbst am Höhepunkt eines Angriffs nicht beeinträchtigt werden.

Bessere Transparenz, effizientere Ressourcennutzung und wirksamere Abwehr

Die Lösung von Juniper und Corero unterstützt die kontinuierliche Überwachung des Datenverkehrs auf Paketebene. Diese paketbasierte Analyse ist effizienter als herkömmliche, flussbasierte Erkennungsmaßnahmen und gibt dem Betriebspersonal zudem einen besseren Überblick über den Datenverkehr – nicht nur über die Header, sondern auch über die Paketinhalte. Darüber hinaus beanspruchen die Erstellung der Datenspiegel und die Stichprobenentnahme weniger Router-Ressourcen als das IPFIX-Protokoll (IP Flow Information Export), da die Router keine großen Datenmengen aggregieren und verarbeiten müssen. Ein dritter Vorteil ist, dass die vorhandene Infrastruktur nicht ersetzt werden muss. Die Lösung von Juniper und Corero kann nahtlos mit den bereits vorhandenen Lösungen zu einer mehrschichtigen DDoS-Abwehrstruktur verbunden werden, in der die IP-Router am Netzwerkrand groß angelegte Angriffe abschwächen, während zentralisierte Filtermechanismen die verbleibenden, ausgefeilteren Angriffe auf der Anwendungsebene erkennen und blockieren.

Skalierbarkeit bis in den zweistelligen Terabit-Bereich

Corero SmartWall TDD ist bis zu 40 Tbit/s Durchsatz skalierbar, ohne dass der DDoS-Datenverkehr im Netzwerk umgeleitet werden muss. In Kombination mit der Universellen 5G-Routing-Plattform der MX-Serie, die bis zu 80 Tbit/s Kapazität für die Weiterleitung von Paketen bietet, ist die Skalierbarkeit dieser Lösung höher als die aller anderen alleinstehenden, derzeit am Markt verfügbaren DDoS-Abwehrsysteme.

Die Lösung im Detail

Corero SmartWall Threat Defense Director

Corero SmartWall TDD stellt einen Durchbruch in der Abwehr volumetrischer DDoS-Angriffe in Echtzeit dar und zeichnet sich durch die folgenden Merkmale aus:

- Die Überwachung des Datenverkehrs und die Abschwächung von Angriffen ist bis in den zweistelligen Terabit-Bereich skalierbar.
- Die Analyse findet auf Paketebene statt, um DDoS-Angriffe zuverlässig zu erkennen.
- Maschinelle Analysen ermöglichen die automatische Filterung und eine intelligente Abschwächung von Angriffen.
- Die Reaktion erfolgt in Echtzeit, sodass bis zur Abschwächung eines Angriffs meist nur Sekunden vergehen.
- Eine geschlossene Feedback-Schleife verhindert, dass legitime Datenpakete blockiert werden.
- Logdateien können einen Rückblick auf Zeitabschnitte von Sekunden, Minuten, Tagen, Wochen, Monaten oder Jahren bieten.
- Forensische Daten geben Aufschluss über Stichproben, erlaubten und blockierten Netzwerkverkehr.
- Analysen, Berichte, Warnmeldungen und Analysen basieren auf Splunk.
- Offene APIs unterstützen die Verknüpfung mit automatisierten Gegenmaßnahmen und SecOps.
- Für den Informationsaustausch zur Angriffsabwehr können BGP, NETCONF, REST (Representational State Transfer), JSON (JavaScript Object Notation) und die Cloud verwendet werden.

Universelle 5G-Routing-Plattform der MX-Serie von Juniper Networks

Die MX-Serie enthält ein ganzes Portfolio robuster, SDN-fähiger Router mit den folgenden Features:

- Konkurrenzlose Kapazität, Dichte, Sicherheit und Leistung
- Branchenweit erste Sicherheitsmaßnahmen auf der Data Plane für Sicherheit ohne Abstriche beim Durchsatz
- Progressive Unterstützung für zukünftige Innovationen durch unbegrenzte Programmierbarkeit
- Beschleunigte Servicebereitstellung durch Automatisierung
- Multiservice-Netzwerk und Node-Slicing-Funktionen für um bis zu 40 Prozent niedrigere Gesamtbetriebskosten
- Geringeres Ausfallrisiko durch Junos® Continuity und einheitliche Software-Upgrades bei laufendem Betrieb (Unified ISSU)
- Hervorragende Netzwerk- und Serviceverfügbarkeit mit zahlreichen Resilienzfunktionen
- Deep Packet Inspection (DPI) zur anwendungsabhängigen Bewertung des Datenverkehrs
- Junos Telemetry Interface (JTI) für das Streaming von Daten zu einzelnen Komponenten an Überwachungs- und Analysetools
- Platz- und energiesparend

Fazit – Ein moderner Ansatz für skalierbaren, kostengünstigen DDoS-Schutz in Echtzeit

In unserer von Multiclouds, dem Internet der Dinge und 5G geprägten Zeit ändert die Bedrohungslage sich ständig. Insbesondere nehmen das Ausmaß, die Häufigkeit und die Komplexität von DDoS-Angriffen weiter zu, sodass sowohl Serviceanbieter als auch Unternehmen gezwungen sind, ihre vorhandenen Schutzmaßnahmen durch Lösungen zu ergänzen, die schnelleren, wirksameren und kostengünstigeren Schutz bieten.

Das IP-Netzwerk sollte ein integraler Bestandteil einer modernen Lösung sein und groß angelegte Angriffe schon am Netzwerkrand abschwächen. Telemetrie, auf maschinellem Lernen basierende Analysen und programmierbare Netzwerke sollten anspruchsvollere Komponenten für die intelligente, automatisierte und anpassbare Erkennung und Abwehr von Angriffen beisteuern.

Die gemeinsam von Juniper und Corero entwickelte Lösung vereint die Vorteile der Verkehrsanalyse auf Paketebene mit infrastrukturbasierten Maßnahmen für die Durchsetzung und ist dadurch in der Lage, DDoS-Angriffe mit Volumen im zweistelligen Terabit-Bereich automatisch abzuschwächen – und gleichzeitig die Kosten erheblich zu reduzieren.

Nächste Schritte

Wenn Sie mehr darüber erfahren möchten, wie Juniper Networks und Corero Sie beim Schutz Ihres Unternehmensnetzwerks vor DDoS-Angriffen unterstützen können, wenden Sie sich an Ihren Vertriebspartner bei Juniper oder Corero.

Über Corero

Corero Network Security ist ein führender Anbieter leistungsstarker Lösungen für die Abwehr von DDoS-Angriffen in Echtzeit. Die preisgekrönte Technologie von Corero schützt die Infrastrukturen von Service- und Hostinganbietern sowie die Online-Präsenz von Unternehmen durch die automatische Erkennung und Abschwächung von DDoS-Bedrohungen und bietet gleichzeitig umfassende Netzwerktransparenz, Analysen und Berichte. Die preisgekrönten Lösungen von Corero bieten kostengünstigen, skalierbaren Schutz vor DDoS-Angriffen, selbst in den komplexesten Umgebungen, und machen so kostengünstigere Betriebsmodelle möglich. Weitere Informationen finden Sie unter www.corero.com.

Über Juniper Networks

Juniper Networks vereinfacht mit seinen Produkten, Lösungen und Services die Netzwerke, die unsere Welt umspannen. Durch kontinuierliche Innovation überwinden wir die Einschränkungen und die Komplexität, mit der Netzwerkadministratoren in der Cloud-Ära zu kämpfen haben, und unterstützen unsere Kunden und Partner bei der Überwindung ihrer größten Herausforderungen. Wir bei Juniper Networks sind überzeugt, dass Netzwerke ein Medium für den weltweiten Wissensaustausch und den die Welt verändernden Fortschritt der Menschheit sind. Deshalb haben wir uns das Ziel gesetzt, bahnbrechende Lösungen für automatisierte, skalierbare und sichere Netzwerke zu entwickeln, die mit dem Tempo unserer schnelllebigen Geschäftswelt Schritt halten.

Hauptsitz
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Telefon: 888.JUNIPER
(+1 888 586 4737)
oder +1 408 745 2000
Fax: +1 408 745 2100
www.juniper.net/de/de/

Hauptniederlassung für die Regionen APAC und EMEA
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Niederlande
Telefon: +31 0207 125 700
Fax: +31 0207 125 701