HPE aruba networking

Lösungsüberblick



Abschwächen von DDoS-Angriffen mit Single-Vendor SASE

HPE

Angesichts der zunehmenden Komplexität und Häufigkeit von Cyberbedrohungen stehen Unternehmen zunehmend unter dem Druck, innovative Lösungen zum Schutz ihrer Netzwerke einzuführen. Distributed-Denial-of-Service-Angriffe (DDoS) zählen nach wie vor zu den schädlichsten Formen von Cyberangriffen und verursachen erhebliche Ausfallzeiten, finanzielle Verluste und Reputationsschäden.

Die Auswirkungen dieser Angriffe nehmen zu – laut einem Bericht von Gcore 2024[1], nahmen DDoS-Angriffe im ersten Halbjahr 2024 um 46 % im Vergleich zum gleichen Zeitraum im Jahr 2023 zu, wobei allein im zweiten Quartal 2024 alarmierende 445.000 Angriffe registriert wurden.

Um diesen sich entwickelnden Bedrohungen entgegenzuwirken, bietet die HPE Aruba Networking SASE Lösung eine leistungsstarke, mehrschichtige Verteidigung, die sicheres SD-WAN mit Adaptive-DDoS-Schutz integriert. Dieser erweiterte Schutz wird durch andere wichtige Sicherheitsfunktionen wie Systeme zur Angriffserkennung und -prävention (IDS/IPS) und rollenbasierte Segmentierung ergänzt. Darüber hinaus integriert HPE Aruba Networking Zero Trust Network Access (ZTNA) in seine Secure Access Service Edge (SASE)-Lösung, was die Angriffsfläche erheblich reduziert, indem sichergestellt wird, dass keine Netzwerk-Services nicht autorisierten Benutzern zugänglich gemacht werden. Durch die Durchsetzung strenger Zugriffskontrollen trägt ZTNA nicht nur dazu bei, das Risiko von DDoS-Angriffen zu minimieren, sondern bietet auch eine wichtige Schutzebene gegen unbefugten Zugriff und verbessert so die allgemeine Sicherheitslage des Unternehmens.

Dieser umfassende Ansatz trägt dazu bei, sicherzustellen, dass Unternehmen für die wachsende Bedrohungslandschaft mit widerstandsfähigen und anpassungsfähigen Lösungen gerüstet sind, die ihre Organisationen sowohl vor herkömmlichen als auch vor komplexen DDoS-Angriffen schützen.

Was ist ein DDoS-Angriff?

Bevor wir uns damit befassen, wie HPE Aruba Networking zur Abwehr von DDoS-Angriffen beiträgt, ist es wichtig zu verstehen, was ein DDoS-Angriff ist.

Ein DDoS-Angriff ist ein böswilliger Versuch, ein Netzwerk, einen Service oder eine Anwendung durch Überflutung mit Datenverkehr aus mehreren Quellen zu überlasten. Das Ziel eines solchen Angriffs besteht darin, die normale Funktionsweise des angegriffenen Service zu stören und zu verhindern, dass legitime Benutzer darauf zugreifen können. DDoS-Angriffe lassen sich in drei Kategorien einteilen: volumenbasierte, protokollbasierte und Angriffe auf Anwendungsebene.

[1] „DDoS Attack Trends for Q1–Q2 2024: Insights from Gcore Radar Report“, Gcore, 14. August 2024

Beispiele für volumenbasierte Angriffe sind:

— **ICMP-Flood:** Angreifer verwenden das Internet Control Message Protocol (ICMP), um eine riesige Anzahl von Ping-Anfragen zu senden und so die Bandbreite des Netzwerks zu überlasten.

— **UDP-Flood:** Angreifer überfluten das Ziel mit User Datagram Protocol (UDP)-Paketen und belegen Ressourcen, indem sie den Server zwingen, jedes Paket zu verarbeiten und darauf zu antworten.

Beispiele für protokollbasierte Angriffe sind:

— **SYN-Flood:** Angreifer nutzen den TCP-Handshake-Prozess aus, indem sie mehrere Verbindungsanforderungen senden, diese jedoch nie abschließen und so Serverressourcen belegen.

— **IP-Spoofing:** Angreifer verschleiern ihre IP-Adressen, indem sie Datenverkehr senden, der legitim erscheint. Dadurch wird es schwierig, bösartigen Datenverkehr zu blockieren.

Ein Beispiel für Angriffe auf Anwendungsebene ist:

— **HTTP-Flood:** Bei einer HTTP-Flood werden zahlreiche HTTP-GET- oder POST-Anfragen an einen Webserver gesendet und damit die Verarbeitungskapazität und Bandbreite des Servers erschöpft.

Diese Angriffe können dazu führen, dass ein Netzwerk erheblich überlastet wird, Anwendungen verlangsamt werden oder sogar vollständig ausfallen und alles von Web-Services bis hin zu internen Unternehmensanwendungen beeinträchtigen.

Herausforderungen bei der herkömmlichen DDoS-Abwehr

Im herkömmlichen Modell war der DDoS-Schutz weitgehend reaktiv. Dafür mussten Administratoren Denial-of-Service-Schwellenwerte (DoS) manuell festlegen, um bösartigen Datenverkehr zu erkennen und einzudämmen. Bei diesem Ansatz ergaben sich mehrere Einschränkungen:

— **Manuelle Konfiguration:** Administratoren mussten die geeigneten Schwellenwerte für die Erkennung von DoS-Angriffen anhand von Netzwerkverkehrsmustern abschätzen. Diese Methode war fehleranfällig und führte häufig dazu, dass die Schwellenwerte entweder unter- oder überschätzt wurden.

— **Häufige Aktualisierungen:** Die Netzwerkverkehrsmuster ändern sich ständig, sodass die Schwellenwerte häufig angepasst werden müssen. Werden die Schwellenwerte nicht aktualisiert, kann dies zur Folge haben, dass Angriffe nicht entdeckt oder legitime Datenströme blockiert werden.

— **Unflexible Antwort:** Herkömmliche DDoS-Abwehrmechanismen betrachteten häufig alle Datenverkehrsspitzen als potenziell bösartig. Dieser Ansatz könnte den legitimen Datenverkehr während Spitzenzeiten (z. B. bei Anmeldespitzen oder regelmäßigen Backups) blockieren und so zu Serviceunterbrechungen führen.

Angesichts dieser Herausforderungen bestand ein klarer Bedarf an einer dynamischeren, automatisierten Lösung, um DDoS-Bedrohungen wirksam zu begegnen.

Adaptive DDoS: Ein neuer Ansatz zur DDoS-Abwehr basierend auf maschinellem Lernen (ML)

EdgeConnect SD-WAN, Teil von HPE Aruba Networking SASE, bietet dank der integrierten Firewall der nächsten Generation eine hochmoderne Adaptive-DDoS-Schutzlösung, die die Einschränkungen herkömmlicher DDoS-Abwehrmaßnahmen überwindet. Durch die Nutzung von ML und erweiterter Verkehrsanalyse bietet Adaptive DDoS kontinuierlichen Schutz und trägt dazu bei, dass sich das Netzwerk in Echtzeit an geänderte Verkehrsmuster anpasst.

Administratoren können das Netzwerk während eines DoS-Angriffs verwalten, indem sie sowohl Mindest- als auch Höchstschwellenwerte festlegen. Der Mindestschwellenwert ermöglicht eine frühzeitige Erkennung potenzieller Probleme, während der Höchstschwellenwert dazu beiträgt, sicherzustellen, dass legitimer Datenverkehr nicht zu früh unterbrochen wird. Das gibt Administratoren mehr Kontrolle und trägt dazu bei, sicherzustellen, dass der Datenverkehr nur dann blockiert wird, wenn dies unbedingt erforderlich ist.

Adaptive DDoS legt diese Schwellenwerte mithilfe von zwei Hauptfunktionen fest: Auto-Rate-Limiting, womit der minimale Schwellenwert automatisch mit maschinellem Lernen (ML) auf Basis der Netzwerkbedingungen angepasst wird, und Smart Burst, womit der maximale Schwellenwert optimiert wird, um Verkehrsspitzen zu bewältigen (Abbildung 1).

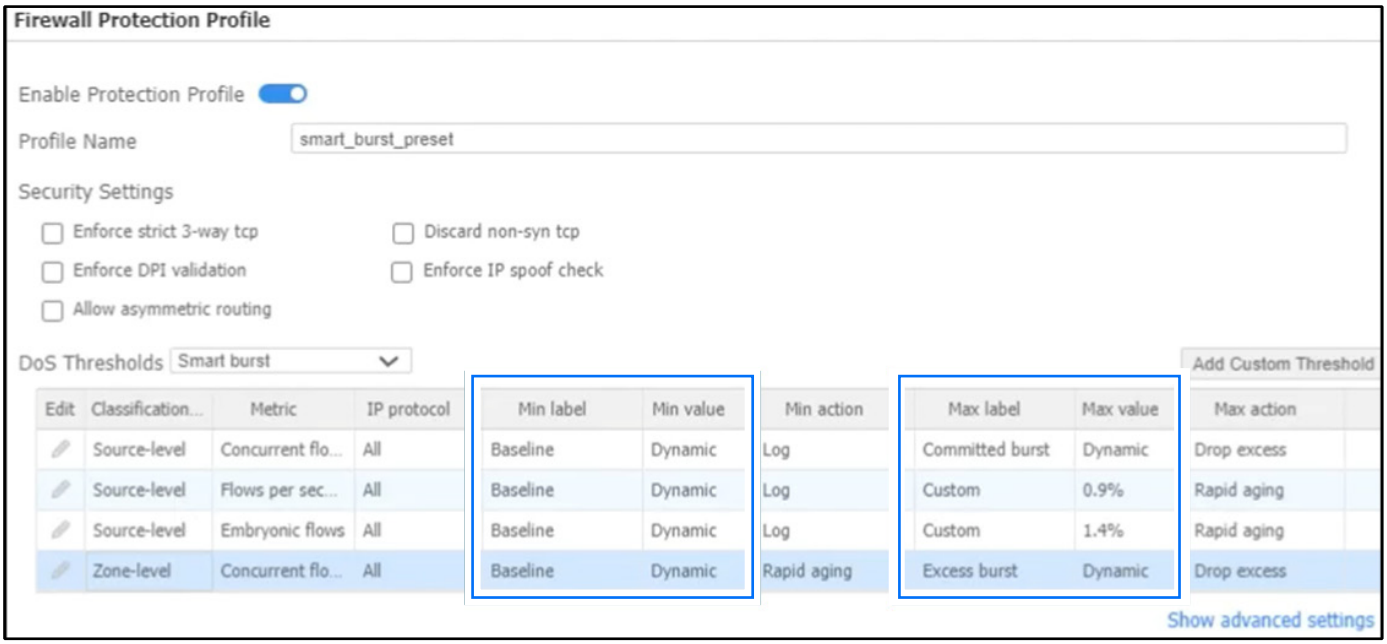


Abbildung 1. Minimale und maximale Adaptive-DDoS-Schwellenwertdefinition durch Nutzung von ML-basiertem Auto-Rate-Limiting und Smart Burst

Auto-Rate-Limiting

Diese Funktion verwendet ML und berechnet damit dynamisch eine Basislinie für normale Netzwerkverkehrsmuster. Basierend auf Netzwerkstatistiken und -mustern passt Auto-Rate-Limiting den minimalen DoS-Schwellenwert kontinuierlich an, der als Grundlage für die Erkennung von Anomalien dient.

Wenn sich die Netzwerkbedingungen ändern (wenn beispielsweise neue Services bereitgestellt werden, das Datenverkehrsaufkommen steigt oder wenn sich Spitzenzeiten verschieben), wird diese Basislinie durch Auto-Rate-Limiting aktualisiert, um den neuen Normalwert widerzuspiegeln. Dadurch werden Fehlalarme minimiert und potenzielle DDoS-Bedrohungen frühzeitig erkannt.

Durch den Wegfall der manuellen Schwellenwertkonfiguration wird die Belastung der Administratoren verringert und sichergestellt, dass das Netzwerk ohne ständige Neukonfiguration stets geschützt ist.

Smart Burst

DDoS-Angriffe haben oft zum Ziel, vorübergehende Spitzen im Netzwerkverkehr auszunutzen. Allerdings sind nicht alle Verkehrsspitzen böswillig. Beispielsweise können legitime Aktivitäten wie Benutzeranmeldungen oder Datensicherungen zu einem erheblichen, vorübergehenden Anstieg des Datenverkehrs führen.

Smart Burst wurde entwickelt, um diesen **guten** Datenverkehr zu bewältigen und gleichzeitig sicherzustellen, dass **schlechter** (d. h. bösartiger) Datenverkehr nicht die Bandbreite des Netzwerks in Anspruch nimmt. Es weist ungenutzte Flusskapazitäten zwischen den Firewall-Zonen automatisch auf der Grundlage der aktuellen Verkehrsbedingungen zu.

Smart Burst verfügt über vier Betriebsmodi:

Baseline Plus: Fügt dem Basisschwellenwert einen Puffer hinzu, sodass legitime Verkehrsspitzen berücksichtigt werden können, ohne dass sie vorzeitig als Angriffe gekennzeichnet werden

Festgelegter Burst: Verteilt zusätzliche Datenflusskapazität proportional auf die Firewall-Zonen und hilft so dabei, die Bandbreitennutzung optimal zu nutzen

Zusatz-Burst: Teilt ungenutzte Flusskapazitäten zonenübergreifend auf und bietet so zusätzlichen Schutz bei plötzlichen Verkehrsspitzen

Benutzerdefiniert: Administratoren können eigene Schwellenwerte und Verkehrsregeln für bestimmte Netzwerksegmente definieren

Durch die Integration von ML und Verkehrsanalyse in seine DDoS-Abwehrmechanismen bietet die Adaptive-DDoS-Funktion von HPE Aruba Networking automatisierten, intelligenten und dynamischen Schutz, der in Echtzeit an das Netzwerkverhalten angepasst wird. Dies hilft dabei, eine bessere Kontrolle über den DDoS-Schutz sicherzustellen, ohne dass ständige manuelle Eingriffe erforderlich sind.

Firewall-Schutzprofile und DDoS-Kontrolle

Dank der Firewall-Schutzprofile (Abbildung 2) im sicheren SD-WAN von HPE Aruba Networking können IT-Administratoren den DDoS-Schutz durchsetzen. Sie können:

— **einen strikten Drei-Wege-Handshake durchsetzen:** Dadurch wird sichergestellt, dass alle Verbindungen zustandsbehaftet sind, sodass protokollbasierte Angriffe, wie z. B. SYN-Flood-Angriffe, effektiv bewältigt werden können.

— **Mindest- und Höchstschwellenwerte festlegen:** Administratoren können Schwellenwerte auf der Grundlage von Datenverkehrsparametern festlegen, einschließlich Datenflussrate, gleichzeitige Datenflüsse und embryonale Datenflüsse (d. h. halboffene TCP-Verbindungen). Der minimale Schwellenwert hilft, frühe Anzeichen eines Angriffs zu erkennen, der maximale Schwellenwert sorgt dafür, dass legitimer Datenverkehr nicht zu früh unterbrochen wird.

— **Bekannte Angreifer-Blockliste:** Das System kann eine Liste bekannter Angreifer-IP-Adressen verwalten und während eines Angriffs automatisch den Datenverkehr aus diesen Quellen blockieren.

— Indem Administratoren die Möglichkeit haben, verschiedene Firewall-Schutzprofile an Firewall-Zonen zu binden, ermöglicht die HPE Aruba Networking Lösung eine detaillierte Kontrolle über die DDoS-Schutzstufen. Diese Flexibilität hilft dabei, sicherzustellen, dass jedes Segment des Netzwerks je nach seiner Sensibilität oder Funktion das angemessene Schutzniveau erhält.

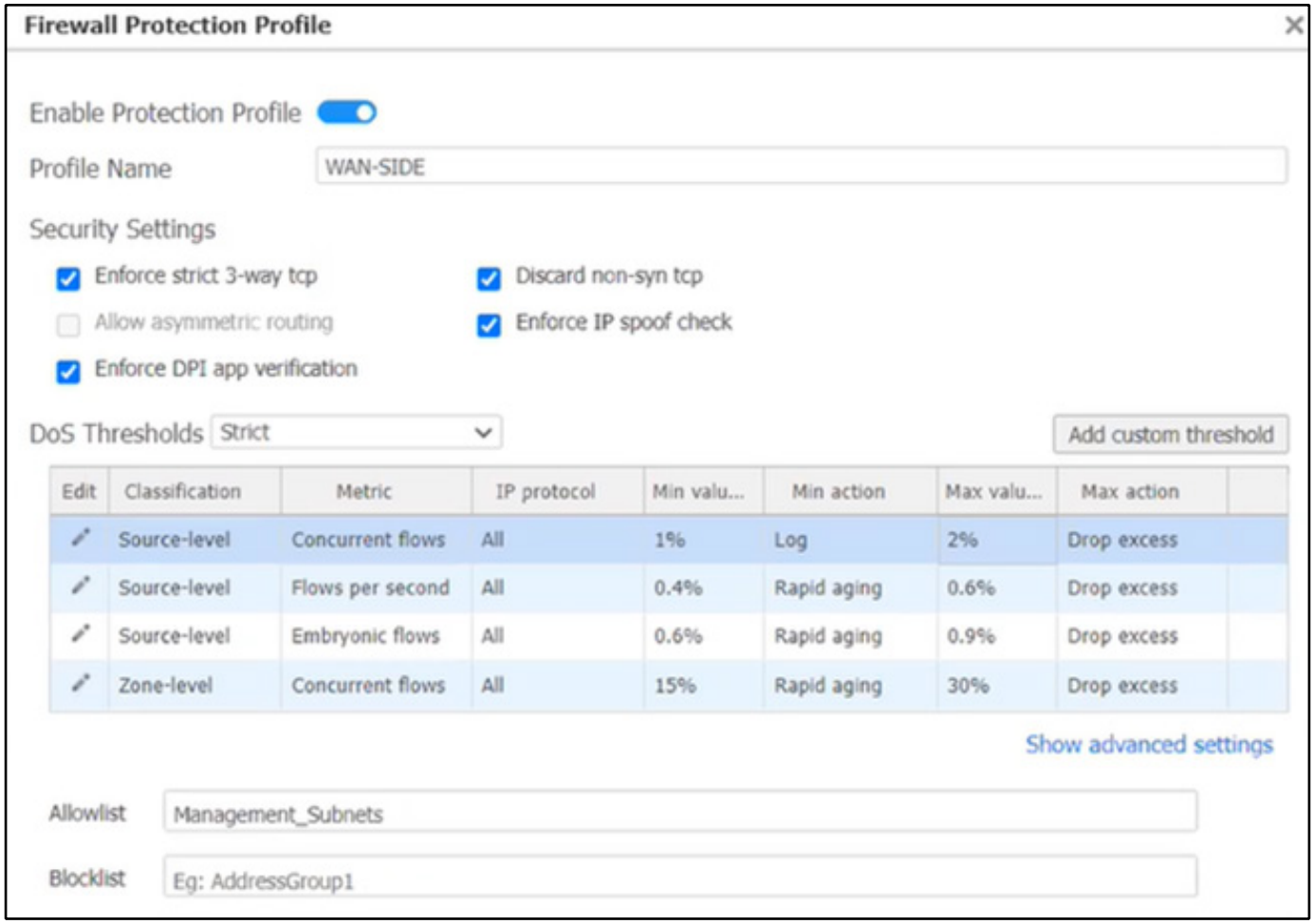


Abbildung 2. EdgeConnect SD-WAN Firewall-Schutzprofil

DDoS-Analytik: Transparenz und Berichterstellung

Als Ergänzung zur Adaptive-DDoS-Funktionalität umfasst das sichere SD-WAN von HPE Aruba Networking umfassende DDoS-Analysen. Diese Berichte bieten wertvolle Einblicke in die Leistung und Sicherheitslage des Netzwerks und ermöglichen Administratoren, potenzielle Bedrohungen in Echtzeit zu verfolgen und darauf zu reagieren (Abbildung 3).

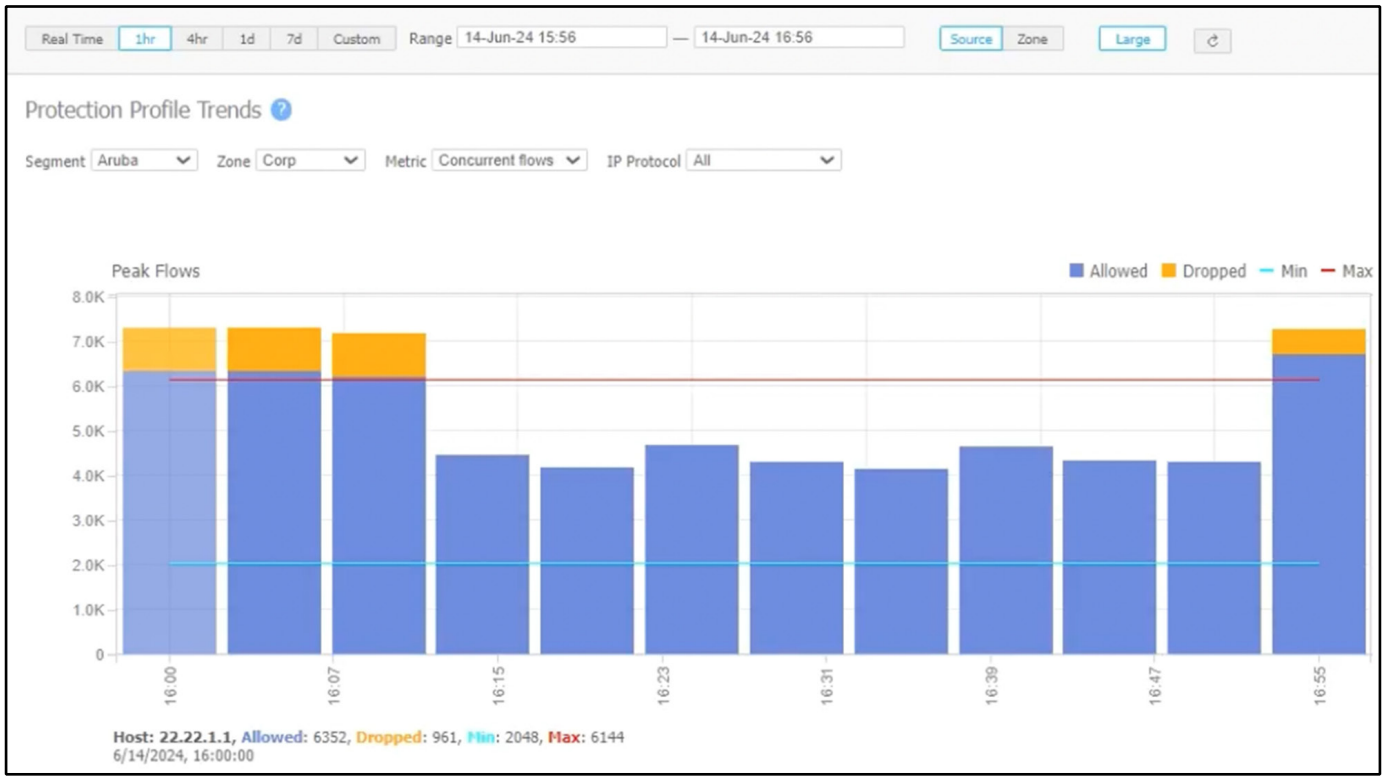


Abbildung 3. Anzahl der zulässigen und gelöschten Flows für jedes Fünf-Minuten-Zeitintervall pro Firewall-Zone in EdgeConnect SD-WAN

Die Berichte beinhalten Folgendes:

- **Schwellenwertverletzungen:** Benachrichtigt Administratoren, wenn der Datenverkehr voreingestellte oder dynamisch konfigurierte Schwellenwerte überschreitet
- **Durchflussunterbrechungen:** Liefert Details über unterbrochene Datenströme und hilft Administratoren bei der Identifikation und Beseitigung potenzieller Angriffsquellen
- **Abgelehnte Hosts und Pakete:** Verfolgt IP-Adressen und Pakete, die aufgrund bekannten böswilligen Verhaltens blockiert wurden
- **Top-Talker:** Identifiziert die Geräte oder Benutzer, die den meisten Datenverkehr erzeugen, und hilft so dabei, potenzielle Quellen für anormalen Datenverkehr zu ermitteln
- **Alarmbenachrichtigungen:** Benachrichtigt Administratoren automatisch bei Überschreiten von Schwellenwerten und ermöglicht so eine rechtzeitige Reaktion auf DoS-Angriffe

Dank dieser detaillierten Transparenz in den Bereichen Verkehrsmuster und Sicherheitsvorfällen können Netzwerkteams fundierte Entscheidungen treffen und so die Wirksamkeit der DDoS-Schutzstrategie insgesamt verbessern.

DDoS-Abwehr mit ZTNA ergänzen

Durch Hinzufügen von ZTNA, Teil von HPE Aruba Networking SASE, können Unternehmen eine mehrschichtige Verteidigung gegen DDoS-Angriffe bereitstellen. Die Fähigkeit von ZTNA, Services vor dem Internet zu verbergen, Anwendungsverkehr zu segmentieren und den Zugriff auf ausschließlich verifizierte Benutzer und Geräte zu beschränken, stärkt die allgemeine DDoS-Schutzstrategie erheblich (Abbildung 4). In Kombination mit dem Adaptive-DDoS-Schutz von EdgeConnect SD-WAN erhalten Unternehmen eine umfassende Lösung zum Schutz ihrer Netzwerke vor DDoS-Angriffen.

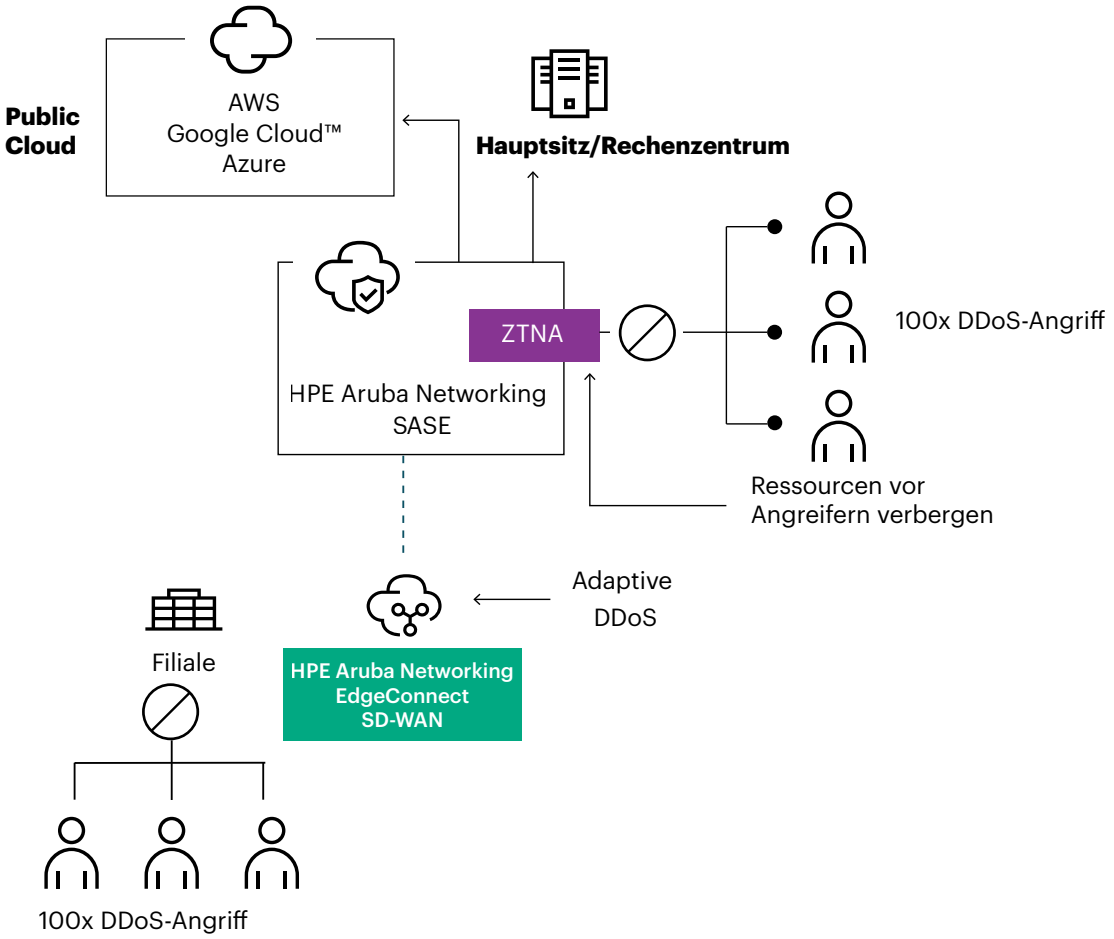


Abbildung 4. Zweischichtiger DDoS-Schutz durch EdgeConnect SD-WAN Adaptive DDoS gepaart mit HPE Aruba Networking ZTNA

HPE Aruba Networking ZTNA funktioniert nach dem Prinzip „Vertraue nie, überprüfe immer". Wenn interne Services vor dem Internet verborgen bleiben, werden die üblichen Einstiegspunkte für DDoS-Angriffe eliminiert. Nur authentifizierte und autorisierte Geräte können auf bestimmte Services zugreifen. Dadurch wird sichergestellt, dass Angreifer von außen diese Services nicht direkt für DDoS-Angriffe angreifen können.

Darüber hinaus erlaubt ZTNA keine seitliche Bewegung. Da ZTNA strenge Zugriffskontrollrichtlinien durchsetzt, können Benutzer nicht seitwärts zu anderen Ressourcen wechseln. Jede Verbindung wird individuell hergestellt, sodass autorisierte Benutzer nur mit autorisierten Ressourcen verbunden werden. Dadurch wird die gesamte Angriffsfläche verringert und sichergestellt, dass die Auswirkungen begrenzt bleiben und sich nicht auf das restliche Netzwerk ausbreiten, selbst wenn ein Gerät kompromittiert wird.

Außerdem gewährt ZTNA im Gegensatz zu VPN keinen umfassenden Zugriff auf interne Ressourcen. Dies macht ZTNA zu einer attraktiven Alternative für Unternehmen, die VPN ersetzen möchten, die durch die Offenlegung einer breiten Palette von Netzwerkressourcen als Leuchtturm für böswillige Akteure fungieren können.

Durch die kontinuierliche Überprüfung der Benutzer- und Geräteidentität vor der Gewährung des Zugriffs trägt HPE Aruba Networking ZTNA dazu bei, sicherzustellen, dass nur legitimer Datenverkehr an die autorisierte Anwendung fließen kann, während Benutzer vom Unternehmensnetzwerk ferngehalten werden. Dadurch wird es weniger wahrscheinlich, dass bösartiger Datenverkehr die Netzwerkressourcen überlastet, und das Risiko von DDoS-Angriffen wird weiter verringert. ZTNA verringert effektiv die Anzahl der Geräte und Services, die angegriffen werden können, und macht groß angelegte Angriffe weniger durchführbar.

Dank der dynamischen kontextbasierten Richtlinien von ZTNA können Netzwerk- und Sicherheitsadministratoren unterschiedliche Zugriffsebenen basierend auf Benutzerrollen, Gerätestatus und Standort festlegen. Diese detaillierte Kontrolle schützt das Netzwerk zusätzlich, indem sie dazu beiträgt, dass nur authentifizierter und vertrauenswürdiger Datenverkehr mit kritischen Ressourcen interagieren kann. Dadurch wird das Risiko verringert, dass bösartiger Datenverkehr durchkommt und bei DDoS-Versuchen Bandbreite belegt (Abbildung 5).

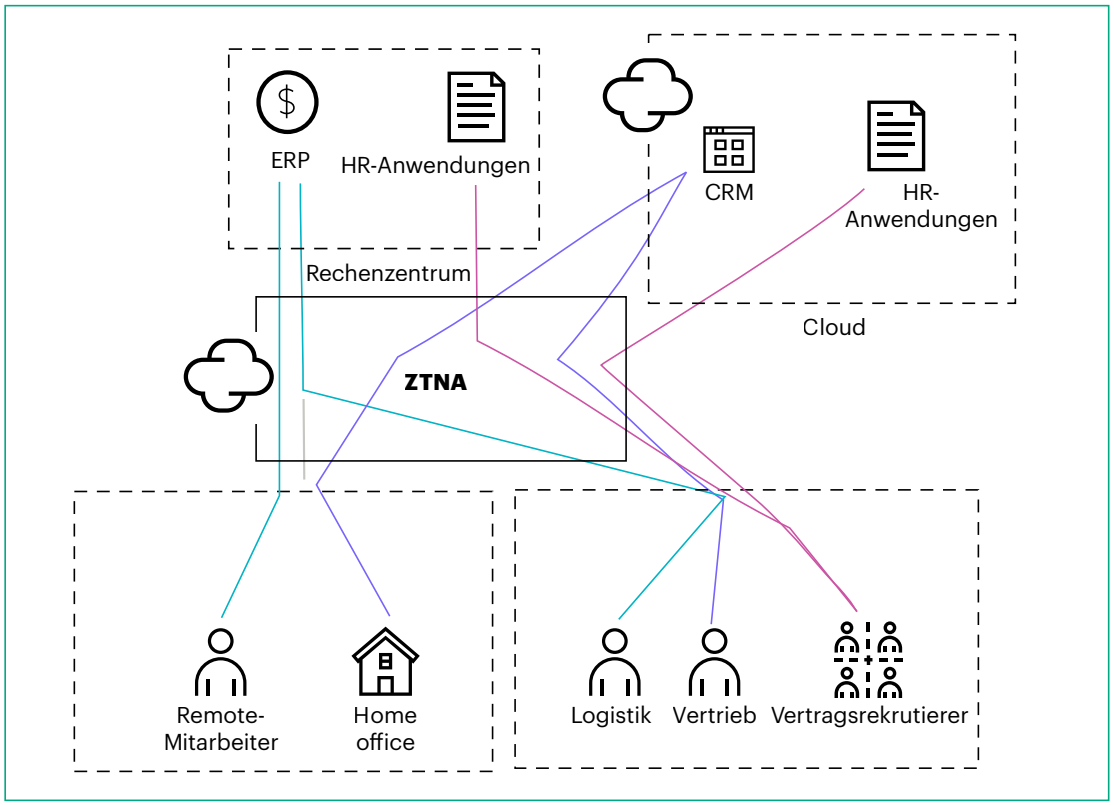


Abbildung 5. Strikte Durchsetzung der Zugriffsrichtlinien mit ZTNA

HPE Aruba Networking ZTNA unterstützt sowohl Remote- als auch lokale Benutzer mit der lokalen Edge-Funktion. Dadurch wird sichergestellt, dass der lokale Datenverkehr lokal bleibt, und Hairpin-Routing in die Cloud vermieden wird. Mit dem lokalen Edge erzwingt ZTNA für Benutzer vor Ort dieselben Zugriffskontrollrichtlinien wie für Remote-Benutzer. Dadurch können Unternehmen eine einzige, einheitliche Richtlinie für alle Benutzer verwalten. Dieser Ansatz hilft dabei, die Komplexität zu minimieren und potenzielle Sicherheitslücken zu verringern, die häufig durch die Verwaltung separater Richtlinien für unterschiedliche Benutzertypen entstehen. So wird die Sicherheit optimiert und gleichzeitig ein konsistenter Schutz gewährleistet.

Umfassende Netzwerksicherheit über DDoS hinaus

Während Adaptive DDoS dynamischen und automatisierten Schutz vor DDoS-Angriffen bietet, bietet HPE Aruba Networking SASE einen ganzheitlichen Sicherheitsrahmen, der weitere wichtige Funktionen umfasst.

So ermöglicht die integrierte Firewall der nächsten Generation von EdgeConnect SD-WAN zum Beispiel eine durchgängige Netzwerksegmentierung über LAN, WAN und sogar bis in die Cloud. Die Sicherheitsrichtlinien werden für jede Zone einzeln definiert und schränken die Konnektivität mit anderen Zonen gemäß den vordefinierten Sicherheitsrichtlinien ein. EdgeConnect SD-WAN kann auch in HPE Aruba Networking ClearPass integriert werden, um Identitäten und rollenbasierte Kontexte für Benutzer und Geräte bereitzustellen und so eine feinkörnige Segmentierung zu ermöglichen. So wird sichergestellt, dass Benutzer und Geräte (einschließlich IoT) nur Ziele erreichen, die mit ihrer Rolle im Netzwerk übereinstimmen.

EdgeConnect SD-WAN umfasst ein regelbasiertes IDS/IPS, das den Netzwerkverkehr überwacht und bekannte Angriffsmuster erkennt. Dieses signaturbasierte System kann so konfiguriert werden, dass es entweder im Inline-Modus für mehr Sicherheit oder im Out-of-Band-Modus zur Priorisierung der Leistung betrieben wird. In Kombination mit DDoS-Schutz stellt IDS/IPS sicher, dass das Netzwerk vor einer breiten Palette von Bedrohungen geschützt bleibt, nicht nur vor DDoS-Angriffen.

Darüber hinaus bietet die Integration mit Splunk ein umfassendes Dashboard zur Anzeige von IDS-/IPS-Ereignissen, sodass Administratoren Sicherheitsereignisdaten effizient filtern, sortieren und analysieren können (Abbildung 6).

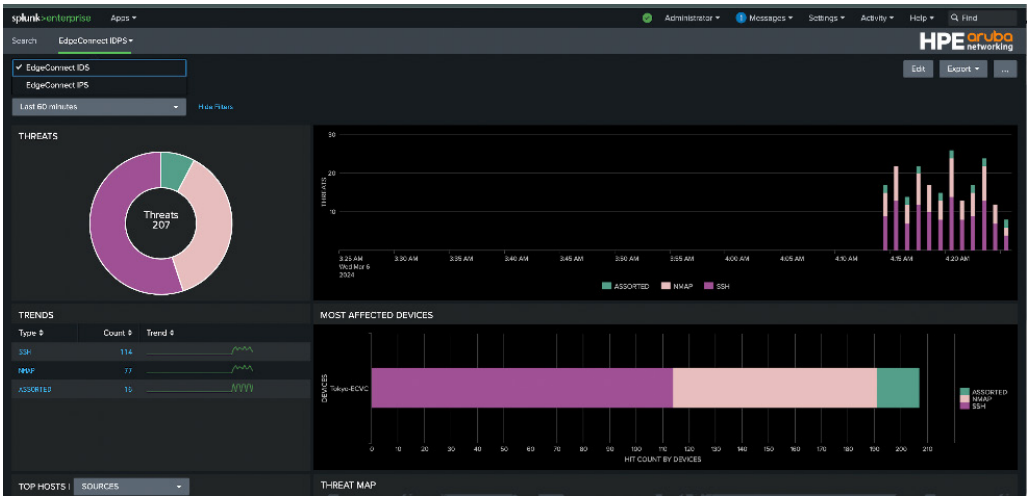


Abbildung 6. Eine Ansicht von IDS-/IPS-Ereignissen in Splunk, die von HPE Aruba Networking SD-WAN stammen

Organisationen können ihre Sicherheitslage verbessern, indem sie weitere Security Service Edge (SSE)-Funktionen wie HPE Aruba Networking Secure Web Gateway (SWG) und Cloud Access Security Broker (CASB) hinzufügen, um eine Single-Vendor SASE-Lösung aufzubauen (Abbildung 7).

SWG ist eine Sicherheitslösung, die Benutzer vor webbasierten Bedrohungen schützt, indem sie den Internetverkehr in Echtzeit überwacht und filtert. Dabei werden Sicherheitsrichtlinien durchgesetzt, um den Zugriff auf bösartige Websites zu blockieren, verhindert das Herunterladen von Malware und filtert unangemessene oder schädliche Inhalte heraus. Darüber hinaus lässt sich EdgeConnect SD-WAN in unsere SWG integrieren, um alle Netzwerkgeräte, einschließlich nicht verwalteter Geräte (z. B. Gäste und IoT-Geräte), zu schützen, ohne dass auf jedem Gerät einzelne Agenten erforderlich sind. Diese Funktion ist besonders nützlich für Organisationen mit einer großen Anzahl von IoT-Geräten, die möglicherweise keine herkömmlichen Sicherheitsagenten unterstützen, aber dennoch Schutz vor webbasierten Bedrohungen benötigen.

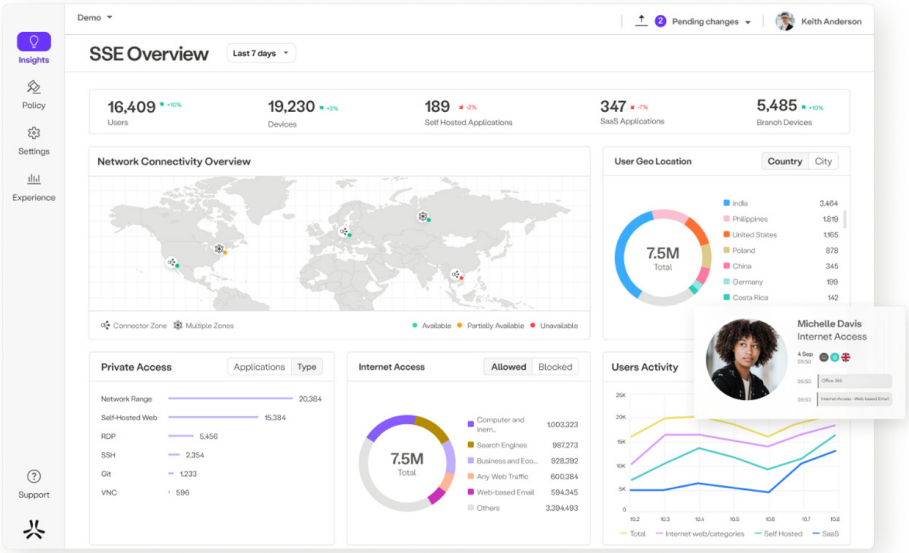


Abbildung 7. Eine Ansicht des HPE Aruba Networking SSE Dashboards zur Überwachung des Zugriffs auf private Anwendungen, SaaS und das Internet

CASB fungiert als Kontrollpunkt zwischen Cloud-Service-Benutzern und SaaS-Anwendungen und trägt zur sicheren Nutzung cloudbasierter Ressourcen bei. CASB bietet Einblick in die Cloud-Nutzung im gesamten Unternehmen, setzt Sicherheitsrichtlinien durch und schützt vertrauliche Daten durch die Überwachung des Zugriffs und des Verhaltens in Cloud-Anwendungen. CASB trägt durch Verschlüsselung, Datenverlustprävention und Zugriffskontrollen dazu bei, Datenlecks zu verhindern. CASB bietet detaillierte Kontrollen über die Interaktion der Benutzer mit Cloud-Services und trägt damit zur Sicherung vertraulicher Daten und zur Gewährleistung der Einhaltung gesetzlicher Anforderungen bei und ermöglicht zugleich eine sichere Cloud-Einführung.

Fazit

HPE Aruba Networking EdgeConnect SD-WAN, erweitert mit Adaptive-DDoS-Schutz und HPE Aruba Networking ZTNA, bietet eine robuste, mehrschichtige Verteidigung gegen DDoS-Angriffe. Der Adaptive-DDoS-Schutz passt Schwellenwerte mithilfe von maschinellem Lernen dynamisch an. So werden Unterbrechungen verhindert und gleichzeitig ein reibungsloser Fluss legitimer Daten gewährleistet. ZTNA reduziert die Angriffsfläche, indem es strenge Zugriffskontrollen durchsetzt und die unbefugte Offenlegung von Netzwerkressourcen verhindert. Darüber hinaus können Unternehmen ihre Sicherheitslage durch die Integration von SWG und CASB weiter stärken und so eine vollständige SASE-Architektur bilden. SWG bietet Schutz vor webbasierten Bedrohungen, CASB stellt den Cloud-Zugriff sicher. Beide Komponenten sorgen für eine umfassende Abdeckung aller Zugangspunkte und tragen dazu bei, eine widerstandsfähige, sichere Netzwerkumgebung gegen DDoS-Angriffe und andere Cyberbedrohungen zu gewährleisten. (Abbildung 8)

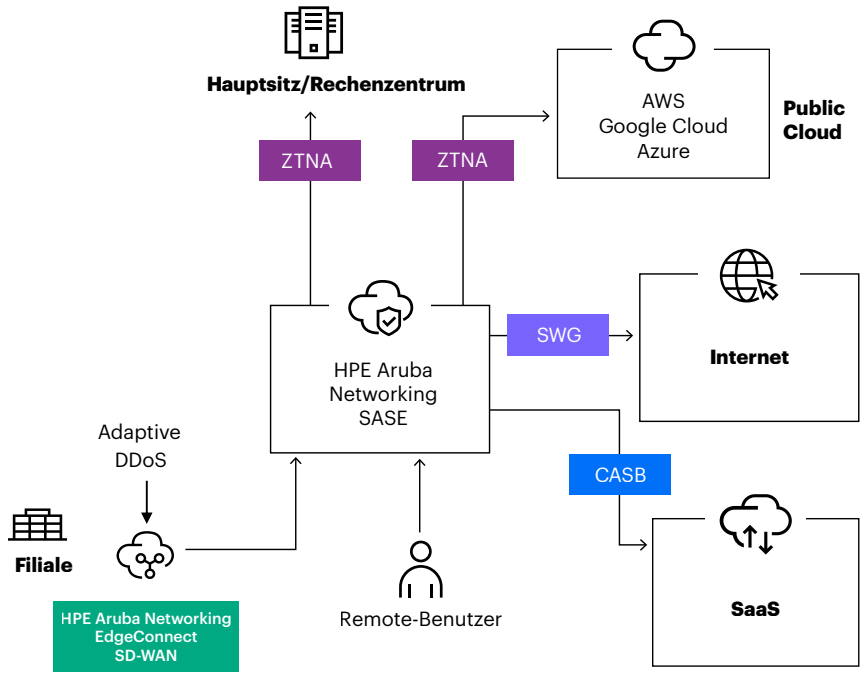


Abbildung 8. Verbesserter DDoS-Schutz und sicherer Zugriff auf private Anwendungen, SaaS und Internet mit HPE Aruba Networking SASE

Weitere Informationen finden Sie unter

HPE Aruba Networking SD-WAN

HPE Aruba Networking SSE

HPE Aruba Networking SASE

HPE.com besuchen

Jetzt chatten

© Copyright 2025 Hewlett Packard Enterprise Development LP. Die hier enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern. Neben der gesetzlichen Gewährleistung gilt für Produkte und Services von Hewlett Packard Enterprise (HPE) ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Services explizit genannt wird. Aus dem vorliegenden Dokument sind keine weiterreichenden Garantieansprüche abzuleiten. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument.

Google Cloud ist eine eingetragene Marke von Google Inc. Azure ist eine eingetragene Marke oder Marke der Microsoft Corporation in den USA und/oder anderen Ländern. Alle genannten Marken von Dritten sind Eigentum der jeweiligen Unternehmen.

a50011705DEE, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com