Backbone DDoS Protection

Reaktiver Schutz gegen Volumenangriffe au Internetverbindungen und Bandbreite, direkt im Telekom Backbone

Verhindern Sie DDoS Attacken, bevor sie ihre Organisation lähmen

DDoS Attacken haben ein neues Level erreicht. Während die Angriffe in Frequenz, Dauer und Diversität zunehmen, kann kein Unternehmen allein diesen großvolumigen DDoS Attacken begegnen.

Darum sind Organisationen auf externe Unterstützung angewiesen, um DDoS Attacken auf ihr eigenes Netzwerk abzuwehren. Wir schützen unsere Kunden direkt in unserem Backbonenetz vor DDoS Attacken. Der Verkehr muss nicht über Netzwerke Dritter umgeleitet werden. Das macht unser Produkt auf dem Markt einzigartig.

Um die Verkehrsmengen der Attacken einzudämmen, haben wir unsere hochmoderne IP Transit Security Plattform eingeführt, die für alle Telekom IP Transit Kunden verfügbar ist. Sie schützt gegen volumenbasierte DoS und DDoS Attacken oder Verkehrs spitzen durch Flash Crowds (z. B. Black).

Schlüsselmerkmale:

- Ein Expertenteam gewährleistet 24/7 die sichere Übertragung der Kundeninhalte
- Der Verkehr wird exklusiv im Telekom Netzwerk verarbeitet! Kein drittes Netzwerk ist involviert.
- Flexible und kombinierbare vier Säulen Strategie gegen DDoS Attacken (Verkehrsbereinigung, Filterung, Durchsatzratenbegrenzung und Blackholing
- Fixe monatliche Rate, keine versteckten Kosten
- Größtmögliche Sicherheit und Zuverlässigkeit durch kontinuierliche IP Verkehrsanalyse
- Auch für Multihomed-Kunden verfügbar

Die Telekom setzt auf eine 4 Säulen Strategie:

- **Mitigation Device (Reinigung des Verkehrs):** Filterung und Zurückweisung des Angriffsverkehrs durch ein Mitigation Device. Umleitung von bestimmten Adressen oder des gesamten IP Adressbereiches des Kunden, sowie Aktivierung automatischer Filterung.
- **Filterung:** Mithilfe von Edge Router Filterlisten trennt unser Filtersystem Angriffsverkehr von regulärem Verkehr. Filterlisten werden manuell auf den Routern konfiguriert und nach Beendigung einer Attacke deaktiviert.
- **Durchsatzratenbegrenzung:** Bandbreitenbeschränkung für einen bestimmten Service. Im Fall einer Attacke ist der betroffene Service nur in einem eingeschränkten Maß erreichbar. Dabei wird nur ein Teil der IP Pakete zur Zieladresse geroutet.
- **Blackholing:** Der gesamte Datenverkehr zu einer IP Adresse oder einem IP Adressbereich wird verworfen. Die IP Adresse oder der IP Adressbereich ist nicht länger im Internet erreichbar. Blackholing wird nur als letztmögliche Lösung eingesetzt.

Vorteile:

- 60 Tbps globale Interconnection-Kapazität
- Partnerschaft mit Netscout Arbor, dem weltweit führenden Anbieter von DDoS Defense Lösungen
- Alle großen Netzwerke sind mit unserem Backbone verbunden
- Einfache Einführung –keine Konfiguration seitens des Kunden und keine Hardwareeinrichtung notwendig
- Keine Latenz durch um routen des Verkehrs während einer Attacke
- Keine Notwendigkeit von GRE Tunneln
- Vorbeugung von BGP Abrissen
- Keine besonderen Prefixe oder Routenregistrierungen nötig, kein Prefix-Splitting

T Systems Let's power higher performance

Solution Package for Backbone DDoS Protection

Wann hilft es mir?	Eindämmung von DDoS-Angriffen direkt im Telekom Backbone
Welche Services sind inkludiert?	▪ Reaktiver DDoS DDoS-Schutz ▪ Schutz gegen Volumenangriffe
Welcher Support wird geboten?	▪ Service: Montag – Sonntag, 24/7 ▪ Reaktionszeit : 30 Minuten
Wieviel kostet es?	▪ Einmalige Einrichtung : ▪ Monatlich ab 2.500€ (< 1 Gbits) ▪ 36 Monate Vertragslaufzeit Produkt nur erhältlich für Telekom IP transit Kunden. Alle Preise zzgl. gesetzlicher Mehrwertsteuer.

Passen Sie den DDoS DDoS-Schutz durch zusätzliche Module an ihre Anforderungen an (Preise auf Anfrage)

Cloud Web DDoS Protection:
Aus der Cloud für lokale und gehostete Systeme
- Automatischer Schutz
- Gegen Komplex -und Volumenattacken

Border Gateway Protocol Cloud DDoS Protection:
Aus der Cloud für den Internet Access
- Gegen Komplex -und Volumenattacken
- Schutz vor DDoS Attacken über verschiedene Provider
- Für den Internet Access und Bandbreite

On Premise DDoS Protection:
Am Kundenstandort für die lokale Infrastruktur
- Automatischer Schutz gegen Komplexattacken
- Gekoppelt mit Backbone DDoS Protection automatische Mitigation von Volumenattacken über **Cloud Signaling**
- Für Systeme und Applikationen

Was ist Cloud Signaling: Die beste Lösung für höchsten und umfassenden

Mit Cloud Signaling bieten wir unseren Kunden einen Zusatzservice zur Kombination von On Premise DDoS Protection mit Backbone DDoS Protection.

Um Cloud Signaling nutzen zu können, muss gleichzeitig ein Vertrag über On Premise DDoS Protection und Backbone DDoS

Kontakt
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Deutschland
Tel: 0800 33 09030
E-Mail: info@t-systems.com
Internet: www.t-systems.com

Veröffentlicht durch
T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main
Deutschland