



Die wirksame DDoS-Protection

Distributed Denial of Service (DDoS) Attacken gehören mittlerweile zu den häufigsten Cyberattacken in einem Rechenzentrum. Als Rechenzentrumsbetreiber bieten wir Ihnen mit unserem DDoS Protection Service die Möglichkeit, Ihre Applikationen und Systeme wirkungsvoll und effektiv vor Angriffen zu schützen.

Unser System filtert dabei automatisiert unerwünschten Traffic, so dass lediglich die gewünschten Daten Ihre Systeme erreichen. Wir schaffen für Sie maximale Flexibilität in der Filterung und hohe Transparenz in der Überwachung von DDoS-Attacken. Entscheiden Sie dabei selbst, wie und wann Sie bei Angriffen reagieren wollen oder überlassen Sie die Arbeit dem vollautomatisch handelnden System.

Im automatischen Modus erkennt unser System Anomalien in Ihrem Traffic schon beim Übergang vom Internet in unser Backbone. Anschließend leitet das intelligente Regelwerk des Systems den Traffic an unsere redundanten Filtersysteme weiter. Die Filterung ist für Sie transparent und nicht spürbar.

Der umgeleitete Traffic wird von unserem System mitigiert („gewaschen“) und anschließend an die Zielsysteme geroutet. Für Sie bedeutet das: keine Änderungen oder Einstellungen im System.

Durch den modularen Aufbau unseres DDoS Protection Service können wir individuell auf Ihre Umgebung eingehen und spezielle Anforderungen, wie zum Beispiel Schwellwerte, anpassen. Unsere Spezialisten beraten Sie sehr gerne.

IHRE DDoS APPLIANCE VON QSC

SICHER.
INNOVATIV.
AN IHRER SEITE.

QSC AG

IHRE VORTEILE:

- Bedarfsgerechter DDoS Protection Schutz durch verschiedene Service Pakete „Basic“, „Advanced“, „Advanced Plus“
- Keine Konfiguration oder Änderung in Ihrer Netzwerk-Umgebung notwendig
- Individuelle Parametrisierung der Schwellwerte möglich (nur im Service Paket „Advanced Plus“ möglich)
- Überwachung an allen relevanten Übergabepunkten des QSC-Netzwerkes
- Hohe Verfügbarkeit durch redundant angebundene Systeme
- Modulare, skalierbare Infrastruktur-Plattform
- Filterung direkt im QSC-Backbone ohne Traffic Weiterleitung an 3rd Party Provider
- Umfassender DDoS-Schutz für Netzwerkprotokolle (UDP / TCP, SMTP, FTP, SSH, VoIP, etc.)
- Schutz vor massiven Attacken via BGP-Re-Routing

UNSERE PAKETE AUF EINEM BLICK:

BASIC

- Live Analyse des gesamten Datenverkehrs auf DDoS-Angriffe
- Überwachung an allen Übergabepunkten in das QSC-Backbone, 365 Tage 24/7h
- Erkennung und Reaktion in weniger als 10 Minuten
- Schutz vor Uplink-Überlastung durch Deaktivierung der betroffenen IP-Adresse

Hinweis: Dieser Service ist nur bei einem Gbit/s Anschluss oder entsprechendem Angriffsvolumen voll funktionsfähig.

ADVANCED

- Filterung einer DDoS-Attacke bis zu 15 Gbit/s
- Whitelisting für wiederkehrende Verbindungen
- Konfigurationsaufwand zur Ersteinrichtung inklusive

- Live Analyse des gesamten Datenverkehrs auf DDoS-Angriffe
- Überwachung an allen Übergabepunkten in das QSC-Backbone, 365 Tage 24/7h
- Erkennung und Reaktion in weniger als 10 Minuten
- Schutz vor Uplink-Überlastung durch Deaktivierung der betroffenen IP-Adresse

Hinweis: Dieser Service ist nur bei einem Gbit/s Anschluss oder entsprechendem Angriffsvolumen voll funktionsfähig.

ADVANCED PLUS

- Filterung einer DDoS-Attacke bis zu 30 Gbit/s
- Es können individuelle Schwellwerte festgelegt und konfiguriert werden

- Whitelisting für wiederkehrende Verbindungen
- Konfigurationsaufwand zur Ersteinrichtung inklusive

- Live Analyse des gesamten Datenverkehrs auf DDoS-Angriffe
- Überwachung an allen Übergabepunkten in das QSC-Backbone, 365 Tage 24/7h
- Erkennung und Reaktion in weniger als 10 Minuten
- Schutz vor Uplink-Überlastung durch Deaktivierung der betroffenen IP-Adresse

Hinweis: Dieser Service ist nur bei einem Gbit/s Anschluss oder entsprechendem Angriffsvolumen voll funktionsfähig.

OPTIONALE LEISTUNGEN

- Automatisiertes monatliches Reporting
- Dedizierte Sensoren im internen Kundennetzwerk

Weitere Informationen erhalten Sie unter www.qsc.de/colocation oder kontaktieren Sie uns unter vertrieb.nue@qsc.de