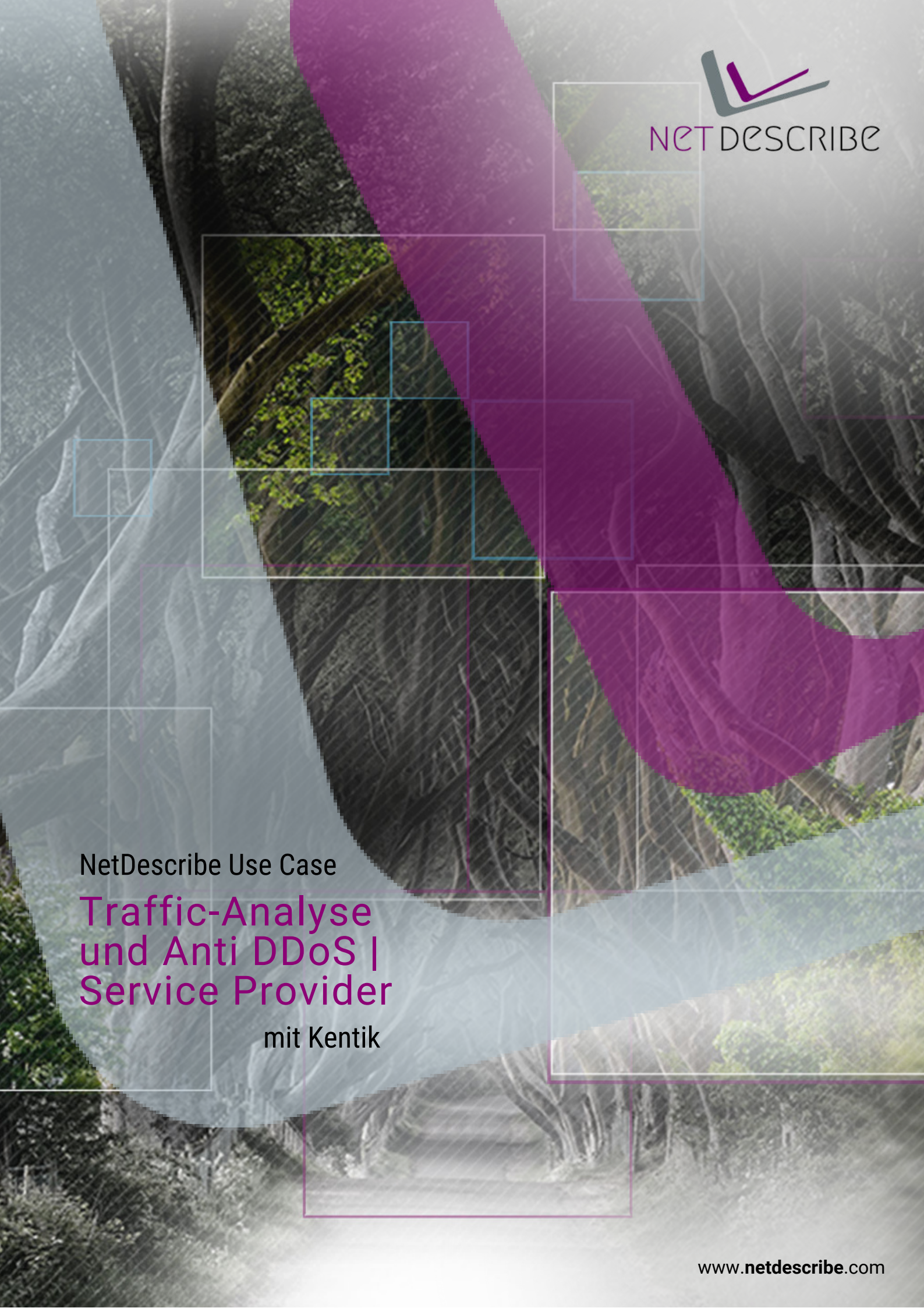


NetDescribe

NetDescribe Use Case

Traffic-Analyse und Anti DDoS | Service Provider

mit Kentik

1. Die Ausgangssituation

Mit dem Einsatz von Cloud Computing haben sich Netzwerke verändert. Hybride Netzwerke, eine Mischung aus Cloud- und On-Premises-Technologien oder Multi-Cloud-Netzwerke, sind bei vielen Unternehmen in Betrieb.

Die Verfügbarkeit der Applikationen und der Erfolg der Services hängt entscheidend von der Überwachung dieser hybriden Netzwerk-Infrastruktur ab. Eine schlechte User Experience geht zu Lasten der Kundenzufriedenheit.

Hinzu kommen Distributed Denial of Service-Angriffe. Die Programme, die dafür genutzt werden, sind mittlerweile sehr ausgefeilt und die Angreifer nur schwer zu ermitteln. Es gibt viele Möglichkeiten für Attacken durch Bugs und/oder Schwachstellen von Programmen, Betriebssystemen oder falschen Implementierungen von Protokollen. Andere Angriffe überlasten schlicht das ganze System mit zu vielen Anfragen.

Welche Möglichkeiten gibt es, sich gegen DDoS-Attacken zu schützen?

Ziel ist es, alle DDoS-Angriffe auf Netzwerkebene mit einem Null-Sekunden-SLA sofort an der Edge abzuwehren. Das bedeutet, dass Angreifer, die DDoS-Angriffe auf Netzwerkebene starten, kaum eine Chance haben.

Die Schlüssel dazu: Visibilität und das Schließen von Informationslücken!

Ein zwischengeschalteter Schutz gegen DDoS-Angriffe analysiert den Traffic. Anti-DDoS-Dienste können dabei helfen, das Netzwerk zu schützen sowie Ausfallzeiten und die damit verbundenen Kosten zu vermeiden.

2. Der Use Case

In diesem Fall geht es um einen regionalen Anbieter von Telekommunikationsdiensleistungen in Norddeutschland, der ein komplettes Multimediapaket mit Telefonie, schnellem Internet und Kabelfernsehen anbietet.

Das Ziel des Unternehmens war die Beschaffung einer SaaS-Lösung für die technische Analyse von IP-Traffic durch die Verwendung von aufgezeichneten Metadaten durch NetFlow v9 und IPFIX.
Außerdem sollte die Software die Fähigkeit haben, aktuelle DDoS-Angriffe zu erkennen und automatisiert zu bekämpfen, indem sie BGP Blackholing und BGP FlowSpec verwendet.

Die Lösung von NetDescribe

Mit Kentik Network Observability, einer skalierbaren Netzwerkanalyse Lösung, die leicht zu implementieren und einfach zu bedienen ist, können Sie jedes Netzwerk planen, betreiben und reparieren. Die proaktive Überwachung von hybriden und Multi-Cloud Netzwerken zeigt im Detail Anomalien Ihres Datenverkehrs. So kann Ihr Net-Ops Team rechtzeitig reagieren und Gegenmaßnahmen ergreifen.

Die Eckdaten des Use-Cases

Verarbeitung von ca. 7000 FPS (Flows Per Second) bei einer Sampling-Rate von 1:3000.

Einbindung folgender Geräte zur Analyse des Datenverkehrs:
Cisco Router NCS 5500 Serie
Cisco Router IOS-XRv 9000-CC
PowerDNS und Bind9 Nameserver

Die Anforderungsanalyse

Anforderungen an Traffic-Analyse

Analyse des Traffics mit folgenden Filtermöglichkeiten:

- Quell und Ziel IP-Adresse
- Quell und Ziel IP-Präfix
- IP-Version
- UDP, TCP und ICMP Protokoll
- Quell und Ziel Portnummer
- Quell und Ziel ASN
- ASN Path
- BGP Communities für Quell und Ziel IP-Präfix
- IP-Präfix
- Eingehendes Netzwerkgerät
- Eingehende Netzwerk-Schnittstelle
- Speicherung der Daten für 1 Kalenderjahr und der Möglichkeit diese Abzurufen
- Zuordnung von Traffic einzelner Endkunden-Dienste (OTT Services) z.B. Amazon Prime Video, Youtube, Playstation, Xbox Live, Netflix, Microsoft Teams, Telegram, WhatsApp etc.)
- Zuordnung von Traffic zu CDN-Betreibern (OTT Provider) z.B. Amazon, Google, Facebook, Apple
- Kategorisierung des OTT-Traffics zu weiteren allgemeinen (Kategorien z.B. Video, Spiele, Web, Kommunikation und Sozial)

Anforderungen an Anti DDoS

Erkennung folgender bekannter DDoS-Angriffsmuster:

- Amplification and Reflection
- ICMP Flood
- Invalid Protocol Flood
- UDP Fragment
- UDP Flood
- TCP-Synfloods
- Non-Reflective DNS Floods
- Total Volumetric

Versand von Meldungen eines erkannten DDoS-Angriffes über:

- E-Mail
- Syslog
- Webhook (http-get) im JSON-Format

Automatische Abwehr des Angriffs mit:

- BGP Blackholing (Hostroute) zzgl. BGP Community
- BGP Blackholing als Netzwerkroute in Netzgröße /24 (IPv4) und /48 (IPv6) zzgl. BGP Community
- BGP FlowSpec mit Filteroptionen auf Quelle und Ziel (IP, Protokoll, Portnummer) und Option zum Traffic verwerfen als auch ein Traffic Rate-Limit zu konfigurieren

net•work ob•serv'a•bil'i•ty (n)

The ability to answer any question about your network.

Die gesamte technologieübergreifende Netzwerkinfrastruktur anzeigen | Daten sammeln | Daten mit Kontextinformationen anreichern | umfassende Einblicke erhalten | jegliche Frage stellen und Daten filtern | passgenaue Maßnahmen ergreifen

Die Anforderungsanalyse

Anforderungen an Verbindungskosten

- Erfassung von monatlichen IP-Transit Kosten mit 95%th-percentile und Flatrate-Modell
- „Kosten pro Mbit“ – Berechnung anhand von Transit und Peering Kosten
- Kostenübersicht (Fix-/Variable Kosten) über einzelne IP Transit und Peering Verbindungen

Anforderungen an die grafische Darstellung

(Webinterface/ grafische Oberfläche)

- Absicherung des Zugangs mit einer 2-fach Authentifizierung (Yubico oder TOTP)
- Auslesbarkeit der erfassten Daten der Trafficanalyse mit einer HTTPS-API im JSON Format
- Zeitdarstellungen in lokaler Zeit des Anwenders und UTC+00:00
- Umstellung der Farben in einen sogenannten „Dark“-Theme Modus
- Frei definierbare Farben für die Darstellung der Graphen

Anforderungen an das Monitoring

Monitoring der Erreichbarkeit von IP-Services (IP+Port) auf Layer-3 Ebene zzgl. Speicherung folgender Informationen:

- Latenz in ms
- Jitter in ms
- Packet Loss in Prozent
- Traceroute Informationen
- Funktionstest von DNS-Servern zur Namensauflösung von Layer-3 bis Layer-8 zzgl. Speicherung der Antworten
- Möglichkeiten Tests innerhalb des Netzwerkes Ihres Unternehmens, als auch von externen Standorten aus zu starten
- Versand von Meldungen bei fehlgeschlagenen Tests über:
  - E-Mail
  - Syslog
  - Webhook (http-get) im JSON Format

Eine hybride IT-Infrastruktur fordert ein hybrides Netzwerk

Eine hybride Infrastruktur oder hybride Cloud ist ein IT-Infrastruktur-Design, das aus einer Mischung aus lokalen Rechenzentren, privaten Clouds und/oder öffentlichen Clouds besteht.

Das hybride Netzwerk verbindet all diese Bestandteile über Technologie-Grenzen hinweg.

Was ist die Kentik Intelligence Platform?

Komplexe Multi-Cloud- und Rechenzentrumsnetzwerke werden auf einen Blick sichtbar. Dies ermöglicht die proaktive Überwachung der Leistung, um eine optimale Performance von Applikationen oder Services zu gewährleisten. Fehlgeleiteter Datenverkehr oder suboptimale Netzwerkkonfigurationen können gefunden und behoben werden. Kostenfaktoren des Netzwerks können im Auge behalten werden.

Mit Kentik können auch DDoS-Angriffe präzise erkannt und automatisiert unschädlich gemacht werden. Kontinuierlicher DDoS-Schutz bedeutet Schadensbegrenzung für Ihr Unternehmen. Hosts, die von Botnets kompromittiert wurden, werden aufgespürt. Angriffe, Sicherheitsverletzungen und Bedrohungen werden in Echtzeit und anhand historischer Daten analysiert. Incident-Response-Tools werden integriert, um Warnungen zu senden und Workflows zu initiieren.

"Das Netzwerk kennt die ganze Wahrheit"
Mikhail Elchin, Kentik-Experte bei NetDescribe

Die Kentik-Features auf einen Blick

CORE
Analyse des gesamten Netzwerkverkehrs. Kapazitätsplanung. Visualisierung von Telemetriedaten. Spontane Insights. Einrichten von Workflows.

EDGE
Volle Visibilität des Netzwerks. Verwaltung von Transits und Interconnections. Entdecken von Peers. Organisation des Datenverkehrs und Kostenoptimierung.

SYNTHETICS
Management der Netzwerk- und Application-Experience. Automatische Konfiguration auf Basis des Datenverkehrs, der Tests und der Analyse in Echtzeit.

CLOUD
Einblicke in alle Clouds und Hybride Infrastrukturen. Migrationsplanung. Sicherheitsüberprüfungen. Performanceverbesserung und Cloud-Kosten Optimierung.

PROTECT
Frühzeitiges Erkennen und Minimieren von DDoS-Angriffen. Erkennung von Botnets. Bedrohungsanalyse. Verhinderung von Route-Leaks und BGP-Hijacking.

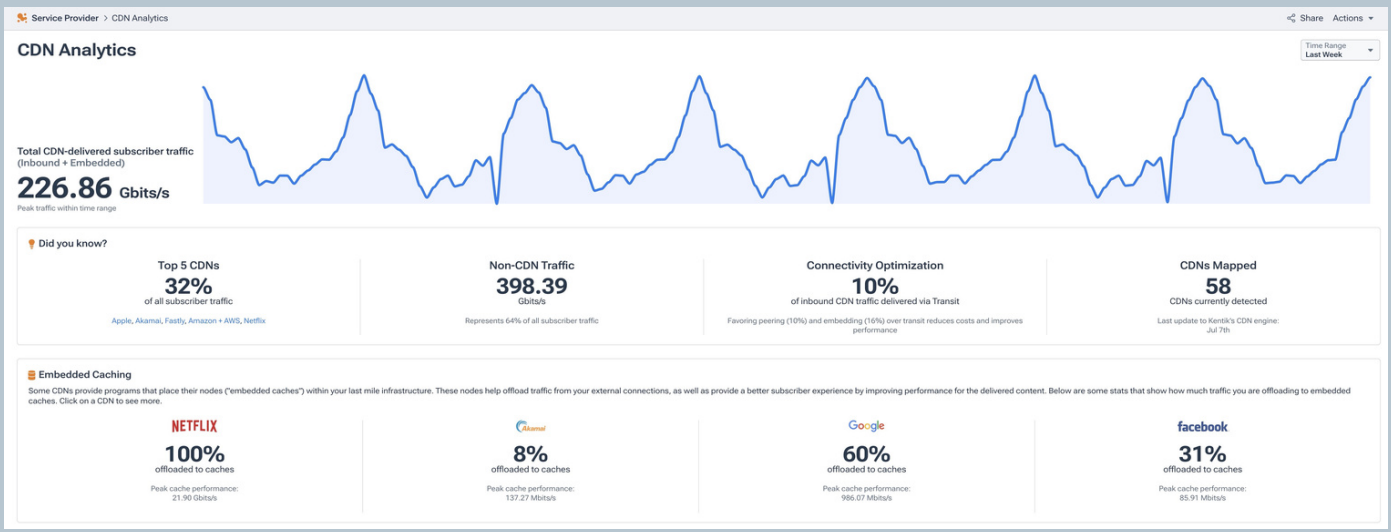
SERVICE PROVIDER ANALYTICS
Analyse von Abonnenten-Trends. Verfolgen der digitalen Lieferkette. Entdecken neuer Absatzmöglichkeiten und Kostenverwaltung.

Was bietet die Kentik Intelligence Platform?

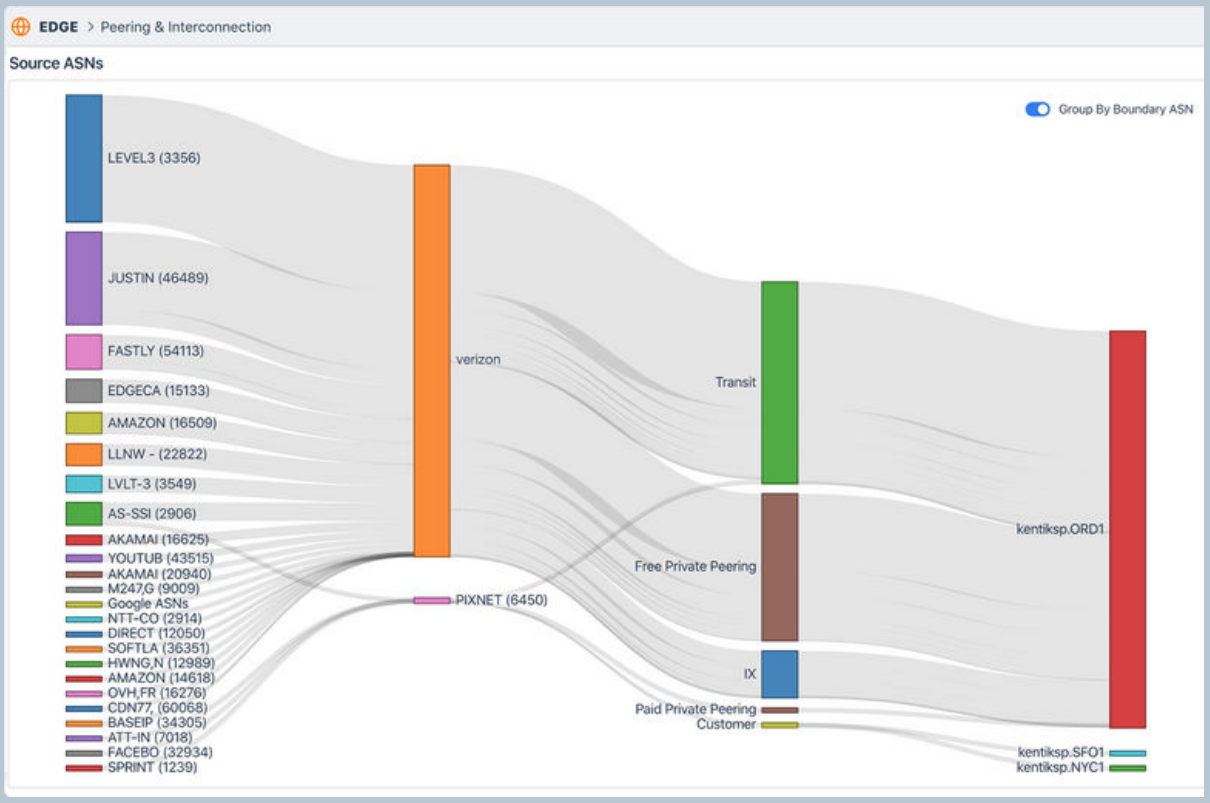
Kentik ermöglicht detaillierte Einblicke in die Aktivitäten der Applikationen/ Services im gesamten Netzwerk über die reine Datenbeobachtung hinaus, um die Gründe für die Netz- und Anwendungsleistung zu verstehen.

Hier einige der Möglichkeiten:

Content Delivery Netzwerk Analyse*

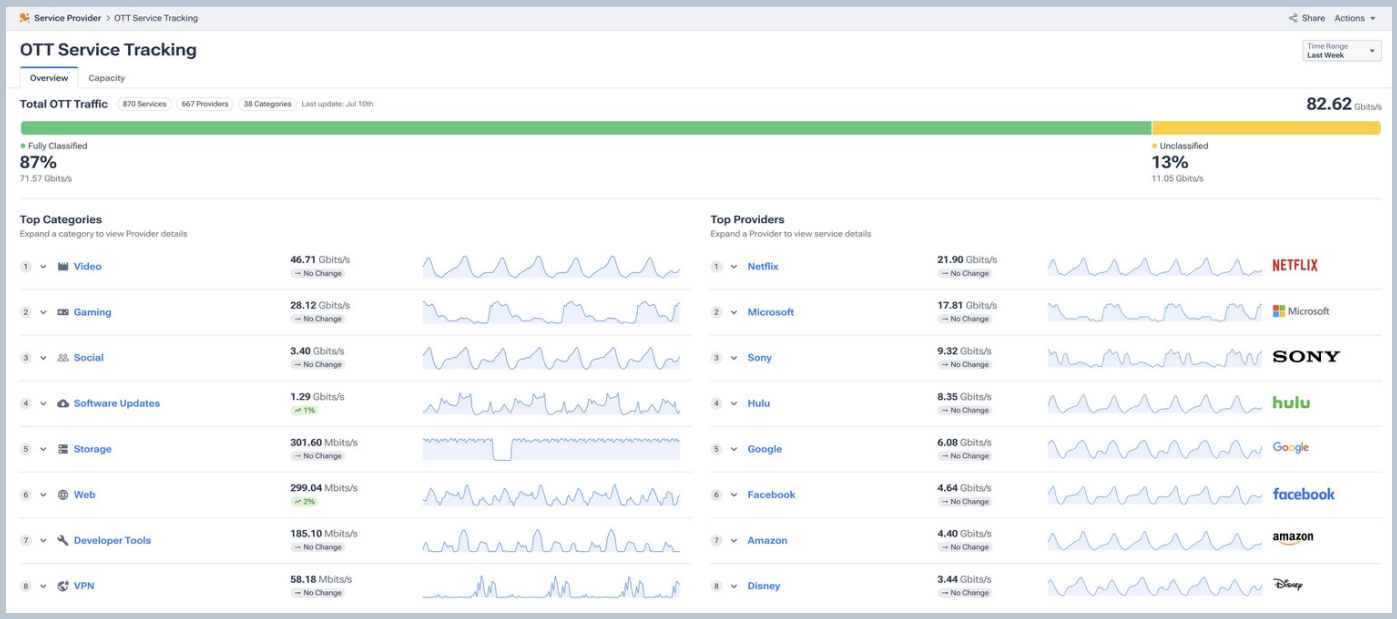


Analyse von Peering and Interconnection*

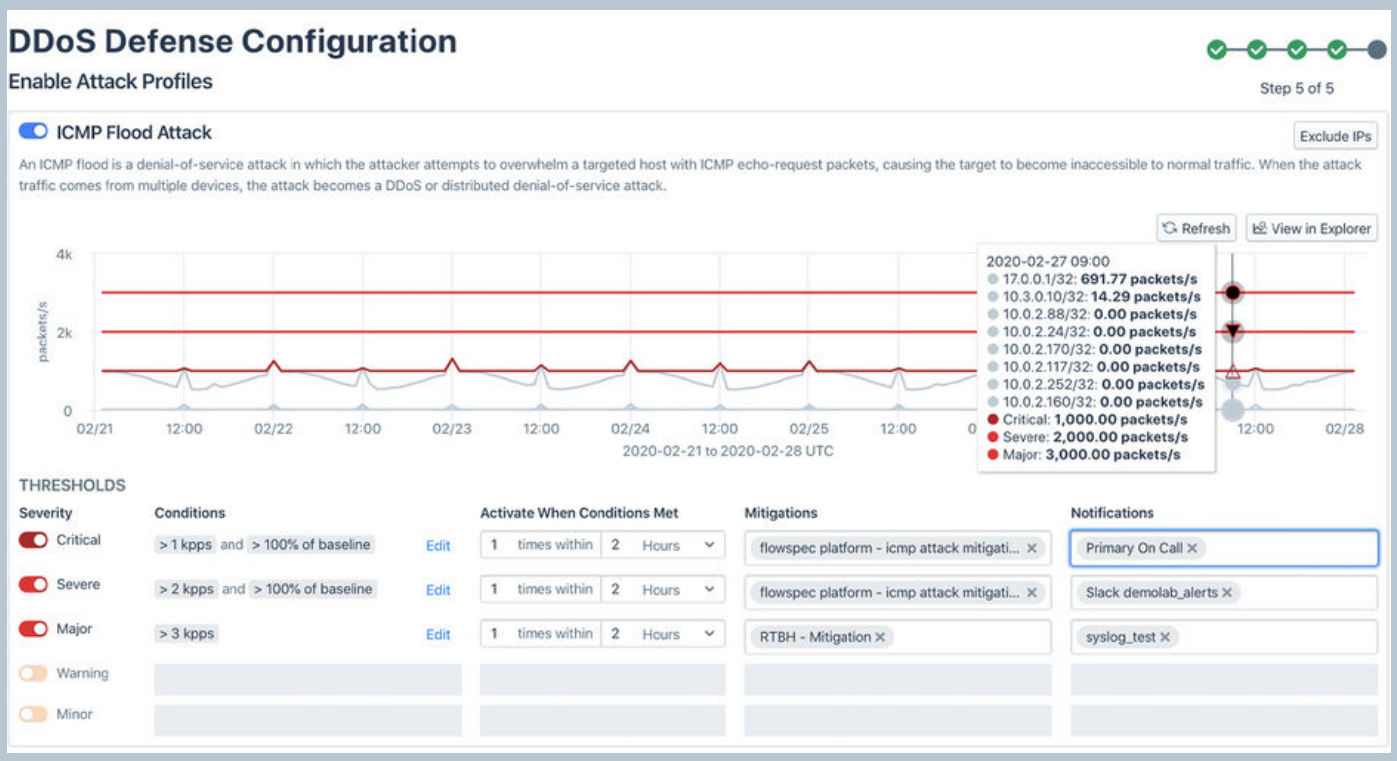


*Quelle aller hier gezeigten Screenshots: www.kentik.com

OTT Service Tracking*



Verteidigung gegen DDoS*



*Quelle aller hier gezeigten Screenshots: www.kentik.com

Was bietet Kentik Observability für Service Provider

Optionen:

Echtzeit-Netzwerküberwachung mit detaillierten Einblicken in den Datenverkehr auf verschiedenen Ebenen, einschließlich Protokoll, Anwendung, Gerät und Benutzer.

→ Netzwerkprobleme schnell erkennen und beheben, Leistung optimieren und Servicequalität gewährleisten

Netzwerkanalyse: Daten können über einen bestimmten Zeitraum gesammelt, analysiert und visualisiert werden, um Erkenntnisse über den Datenverkehr, die Bandbreitennutzung, die Ursachen von Latenzzeiten und andere Leistungsmetriken zu gewinnen.

→ Engpässe identifizieren, Netzwerkprobleme diagnostizieren und Kapazitätsplanung verbessern

Sicherheitsüberwachung durch Identifikation verdächtigen Datenverkehrs, Angriffe erkennen sowie proaktiv und zielgerichtet reagieren.

→ Ressourcenschonung und Kosteneinsparung

Kapazitätsplanung: Analyse des Netzwerkverkehrs und der Bandbreitennutzung. Erkennen von Trends, Prognose der Nachfrage und damit Skalierbarkeit der Netzwerkressourcen.

→ Optimale Leistung und Kundenzufriedenheit

Kunden-Reporting durch Berichtserstellung mit Visualisierung wichtiger Netzwerkleistungsdaten.

→ Transparente Kommunikation und bei Bedarf Anpassungen oder Optimierungen

Was bietet Kentik Observability für Service Provider im DDoS

Funktionen und Ansätze:

Echtzeit-Detection von DDoS-Angriffen. Kontinuierliche Überwachung des Netzwerkverkehrs zur Erkennung von Anomalien und verdächtigen Mustern.

→ Frühzeitige Erkennung und Reaktion

Angriffserkennung und Analyse: Identifikation verschiedener Arten von DDoS-Angriffen, wie z. B. volumetrische Angriffe (z. B. UDP Floods, ICMP Floods), Angriffe auf Anwendungsebene (z. B. HTTP Floods) und Protokollanomalien.

→ Einleitung passgenauer Gegenmaßnahmen

Traffic Engineering und Blackholing: Umleitung des Netzwerkverkehrs und Blockade spezifischer Verkehrsströme (z. B. von einer verdächtigen Quelle).

→ Aufrechterhaltung der Verfügbarkeit für legitimen Verkehr

Automatisierte Maßnahmen zur DDoS-Minderung und -Eindämmung. Dies kann die Umleitung des Verkehrs, die Aktivierung von Firewalls oder andere Maßnahmen umfassen. Es können DDoS Lösungen der unterschiedlichen Hersteller automatisiert angebunden werden. Bereits in Kentik implementiert sind A10, Radware und Cloudflare Magic Transit.

→ Blockierung des schädlichen Verkehrs zum Schutz der Netzwerkressourcen

Echtzeit-Berichterstattung und Alarmierung über DDoS-Angriffe, die betroffenen Ressourcen und die Auswirkungen auf das Netzwerk.

→ Schnelle Reaktion und Minderung von DDoS-Angriffen