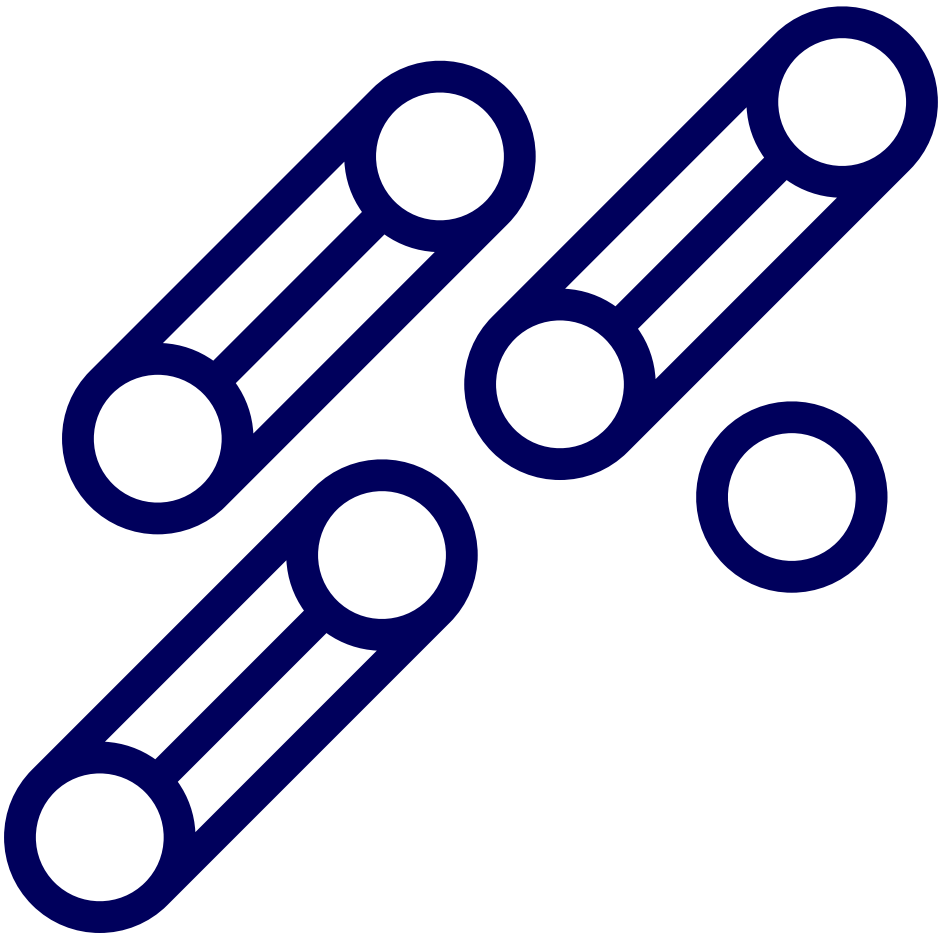


# Tjenestebeskrivelse

## DDoS beskyttelse for bedrifter

28.6.2019

# Innhold

# 1 Introduksjon

DDoS angrep er et økende problem og påfører virksomheter store økonomiske tap og negativt omdømme. Et DDoS angrep rettes typisk mot servere, tjenester eller applikasjon i en bedrift, og har til hensikt å hindre eller betydelig redusere tilgang til tjenester i virksomheten.

DDoS er i dag #1 trusselen mot tilgjengelighet og sikkerhet for bedriften og de reelle virkningene går langt utover de økonomiske kostnadene

| | |
|---|---|
| Distraksjon | IT-personell knyttes opp mot å løse DDoS angrepet |
| Interferens | Stort og økende antall henvendelser til kundeservice |
| Belastning | Ekstra arbeid med å håndtere transaksjoner manuelt |
| Utilgjengelighet | Effektiviteten synker vesentlig blant ansatte |
| Kostnad | Økt utbetaling for brudd på tjenestekvalitet (SLA) |
| Berøvelse | Nåværende og fremtidige tap for virksomheten |
| Rykte | Negativt omdømme |

Internett som markedskanal er ofte kritisk for virksomheten og tilgjengeligheten er vesentlig. Med dagens trusselbilde gir effektiv DDoS beskyttelse en stor verdiøkning til selve Internett aksessen.

# 2 GlobalConnect DDoS beskyttelse

GlobalConnect kan tilby DDoS beskyttelse og «vaske» trafikken mot Kunde ved et DDoS angrep. DDoS beskyttelsen med tilhørende SLA bestilles som en Internett tilleggstjeneste.

GlobalConnect kan i eget kjernenett monitorere lag 3 og 4[1] trafikk fra andre ISP-nettverk (se skisse under) og rapportere unormalt trafikkmønster til kunde. Et DDoS angrep gjenkjennes typisk med:

- Misbruk av protokoller og sårbarheter
- Trafikken overstiger forventet historisk volum
- Kjente signaturer på et DDoS angrep
- Trafikk fra Botnet
- Mye trafikk fra spesifikke land

## 2.1 Varianter

Konsekvensen med utilgjengelige tjenester oppleves forskjellig. Noen tjenester er mer kritiske enn andre med tanke på tilgjengelighet og den daglige drift. For å understøtte ulike behov tilbyr GlobalConnect følgende varianter:

1. DDoS beskyttelse med automatisk null-routing eller såkalt blackhole av host som er under angrep.
2. DDoS beskyttelse med manuell mitigering(vask) av fiendtlig trafikk før den når angrepsmålet.
3. DDoS beskyttelse med automatisk mitigering(vask) av fiendtlig trafikk før den når angrepsmålet.
4. DDoS beskyttelse med mitigering(vask) av fiendtlig trafikk. På forespørsel.

Variant 1-3 er abonnementstjenester med kundespesifikt regelsett og avtale. Variant 4 tilbys virksomheter som ønsker beredskap ved spesielle anledninger eller hjelp med å fjerne volumetrisk DDoS angrep som går utover tilgjengeligheten.

For overnevnte varianter defineres et “Managed Object” (MO). Hvert enkelt MO konfigureres til å beskytte spesifikke IP-adresser eller subnet. For DDoS beskyttelse av et IPv4 og et IPv6 subnet må 2 Managed Objects defineres. Eksempelet under illustrerer hvordan 4 forskjellige objekter kan behandles med tanke på mitigering av trafikken.

| MO | IP adresse / Subnet Mask | Beskrivelse | Mitigering (eksempler) |
|---|---|---|---|
| **1** | 192.0.2.0/24 | E-commerce systemer | Scrubbing (vask av trafikk) |
| **2** | 195.0.2.0/28 | Mail systemer | Scrubbing (vask av trafikk) |
| **3** | 198.0.2.0/28 | IPv4, Web systemer | Automatisk null-routing |
| **4** | fd12:3456:789a:1::/64 | IPv6 subnet, Web systemer | Automatisk null-routing |

DDoS angrep mot en tjeneste kan forandre seg fra gang til gang og regelsett må tilpasses for effektivt å kunne stoppe angrepet. Kunde kan være tjent med definere sine tjenester inn i ulike MO og benytte en blanding av manuell og automatisk mitigering. Ønskes manuell og automatisk mitigering bestilles mitigering av 2.stk MO.

[1] Referanse til OSI-modellen

## 2.2 Produkter

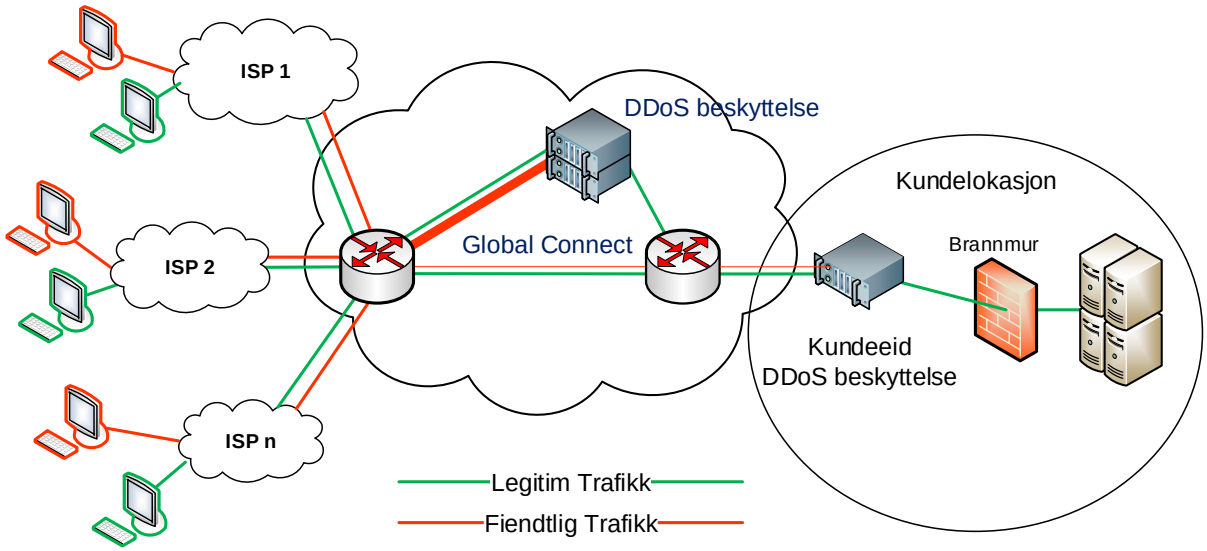
| Grunntjeneste | |
|---|---|
| **DDoS beskyttelse** | Analyse, rapportering og varsling om antatt angrep, deretter vask av infisert etter avtale med Kunde.<br>1 stk. Managed Object(MO) inkludert |
| **Automatisk null-ruting av angrepet host** | Analyse, rapportering og varsling om antatt angrep, deretter automatisk null-routing av angrepet Host.<br>1 stk. Managed Object(MO) inkludert |
| **DDoS beskyttelse for en 24 timer periode. Tjeneste kan etableres på forespørsel** | Mitigering av DDoS angrep.<br>1 stk. Managed Object(MO) inkludert |
| **Tilleggstjenester** | |
| **Extra Managed Object** | Ønskes beskyttelse av flere objekter (MO) som IPv4, IPv6 og/eller ulike mitigeringsprofiler bestilles dette produkt som tillegg til grunntjeneste. |
| **Service Level Agreement(SLA)** | |
| **Servicetid Basis** | Basis tjeneste |
| **Servicetid Utvidet** | Se kapittel 3 |
| **Servicetid Kontinuerlig** | Se kapittel 3 |
| **Servicegaranti 1** | Se kapittel 3 |
| **Servicegaranti 2** | Se kapittel 3 |
| **Servicegaranti 3** | Se kapittel 3 |

## 2.3 Stopp angrepet på rett sted

DDoS angrep utføres i ulike varianter og typiske er

- Volumetrisk angrep
  - Store mengder uønsket trafikk beslaglegger kapasiteten i Kundens nett
  - 75 % av DDoS angrepene er Volumetriske
- «Utmattelse» angrep
  - Hyppige kall sendes mot nettelementer som last-balansere, brannmurer og applikasjons-servere, inntil interne tabeller fylles opp
  - 12 % av DDoS angrepene er Volumetriske
- Applikasjons angrep (L7 angrep)
  - Er rettet mot spesifikke deler av en applikasjon. Hacker utnytter kjente sårbarheter og sender mange forespørsler inntil applikasjonen er utilgjengelig for andres bruk.
  - L7 angrep er ofte vanskelig å detektere når angriper oppfører seg som en legitim bruker.
  - Mail og VoIP applikasjoner er ofte utsatt for angrep
  - 13 % av DDoS angrepene er rettet mot applikasjoner

DDoS beskyttelsen fra GlobalConnect vil effektivt stoppe volumetriske og utmattelse -angrep og opprettholde tjenester hos Kunde under angrep.




Figur 1

DDoS angrep rettet mot applikasjoner og servere internt i Kundens lokalnett kan stoppes med en kundeplassert løsning (Figur 1), denne leveres ikke av GlobalConnect. En kundeplassert løsning kan dessverre ikke beskytte mot volumetriske angrep som fyller opp aksessforbindelsen mot Internett.

Etter DDoS mitigering[2] er igangsatt i vår nettsentriske plattform vil vi se ingress trafikk på lag 7, og er i stand til å vaske trafikk basert på IP headere og payload.

En effektiv DDoS beskyttelse forutsetter en nær dialog med Kunde. GlobalConnect bistår gjerne med informasjon om løsninger for å sikre høyest grad av tilgjengelighet og sikkerhet for virksomheten.

[2] Fjerning av identifisert DDoS trafikk

## 2.4 Deteksjon av trusler

Vi ser enkle og sofistikerte DDoS angrep og det er viktig å kunne agere på ulike angrepsmønstre for å kunne gi en god DDoS-beskyttelse. GlobalConnect benytter «state of the art» teknologi med kontinuerlig vedlikehold og oppdatering av plattform, en nødvendighet for å kunne gi en så god beskyttelse som mulig.

Kort oppsummert detekteres:

- Misbruk av protokoller
  - Reflekterende angrep som forsterkes gjennom misbruk av DNS og NTP
  - Flom av TCP SYN, ICMP, UDP pakker og IP Fragmentering
- Trafikkprofil
  - Legitim trafikk som overstiger forventet mønster f.eks. http flood attacks
- Fingeravtrykk
  - Kjente signaturer på angrep, Botnet deteksjon, Sikkerhets oppdateringer
- Geografi
  - Detektere og stoppe angrep fra spesifikke land

## 2.5 Monitorering

Ved hjelp av en analyse plattform monitorers infrastruktur vha. SNMP og Netflow trafikk for å kunne iverksette beskyttelse av Kunde som er under DDoS angrep. Vi vil understreke at Monitorering av datafeltet i IP-pakkene IKKE gjennomføres.

Røde alarmer indikerer en unormal hendelse og NOC/SOC i GlobalConnect vil umiddelbart undersøke hendelsen og sjekke:

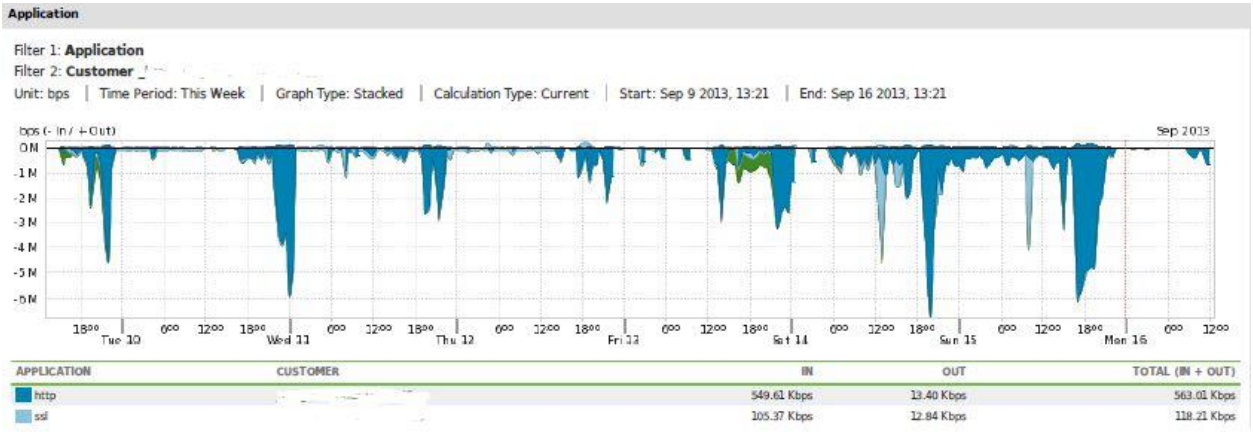
- Er det avtalt null-routing eller mitigering av trafikken.
- GlobalConnect driftspersonell kontakter Kunde innenfor tidsramme avtalt i SLA.
- Det vil ikke gjøres inngrep i trafikken uten Kundens samtykke (regulert av kundespesifikk driftsavtale). Det er kun kontaktpersoner hos Kunde som er nevnt i driftsdokumentasjonen som kan ta denne avgjørelsen.
- GlobalConnect driftspersonell iverksetter tiltak med DDoS beskyttelse etter samtykke fra Kunde
- GlobalConnect driftspersonell holder løpende dialog med Kunde og blir enig om å avslutte mitigering innenfor tidsramme avtalt i SLA

Hvis ønskelig kan det avtales automatisk mitigering av trafikken til Kunde etter minimum 1 uke i drift. Sikkerhetsplattformen sammenligner trafikkmønsteret med historikk og den første uken vil det normalt rapporteres «falske-positiver» som indikerer DDoS angrep uten at det nødvendigvis er det.

Avhengig av angrepets natur vil det ta 5-10 minutter før mitigering av trafikken utføres. Plattformen vil analysere trafikken grundig for å sikre filtrering av infisert trafikk. I starten av et DDoS angrep vil Kunde kunne oppleve degradering av kapasitet i aksessforbindelsen. Når vask av trafikk pågår vil Kunde ikke merke degradering av ytelsen.

## 2.6 Rapporter

GlobalConnect vil ukentlig sende rapport til en e-post adresse avtalt med Kunde. Rapporten vil vise inn- og utgående trafikk fordelt på applikasjon(protokoll). Rapporten vil også vise unormal aktivitet som er identifisert som DDoS angrep rettet mot Kunde.




Under et pågående DDoS angrep vil GlobalConnect oversende rapporter hyppigere med teknisk informasjon om hendelsens forløp og natur.


## 2.7 Implementasjon

Ved bestilling av tjenesten avtales samarbeidsform mellom GlobalConnect og Kunde. GlobalConnect vil oversende et driftsskjema (DDoS mitigering agreement and information matrix) som partene fyller ut. Driftsskjema inneholder informasjon om:

- Produktene som er bestilt(kapasitet og tjenestekvalitet)
- Informasjon om kritiske ressurser i kundens nett(servere og nettverk)
- Kontaktinformasjon hos GlobalConnect og Kunde. Kontaktperson hos Kunde må være autorisert bestiller (f.eks. IT-sikkerhetsansvarlig) som på vegne av bedriften kan godkjenne nødvendige tiltak.

# 3 Tjenestekvalitet (SLA)

Tjenestekvalitet (SLA) er detaljert beskrevet i eget dokument. Dette kapittel gir kun en kort oppsummering av dekningsperiode og servicegaranti for DDoS tjenesten.

Tjenestekvaliteten som tilbys er en kombinasjon dekningsperiode(servicetid) og ytelser(servicegaranti) spesifisert for tjenesten.

Avtale om tjenestekvalitet for DDoS tjenesten er uavhengig av SLA avtalen tegnet for de fysiske/logiske aksesser levert til Kunde. Ved leveranse av en Internett aksess med DDoS beskyttelse spesifiseres to SLA avtaler, 1 for aksess og 1 for DDoS beskyttelsen.

## 3.1 Servicetid

Servicetiden spesifiserer dekningsperioden for feilmelding, feilhåndtering og feilretting.

| Tjeneste | Type feil som rettes | Servicetid |
|---|---|---|
| **Basis** | Alle | Virkedager kl. 08:00 – 17:00 |
| **Utvidet** | Alle | Virkedager kl. 07:00-23:00<br>Lørdager kl. 07:00-23:00 |
| **Kontinuerlig** | Alle | 24/7/365 |

## 3.2 Servicegaranti

Servicegaranti spesifiserer responstid og tilbakemelding for DDoS tjenesten. Uten tegning av en spesifikk avtale gjelder Ingen Servicegaranti for DDoS tjenesten. Ønskes høyere Servicegaranti bestilles dette som en tilleggstjeneste.

DDoS tjenesten leveres med følgende Servicegarantier:

| DDoS tjenesten | Servicegaranti 1 | Servicegaranti 2 | Servicegaranti 3 |
|---|---|---|---|
| **Responstid etter sak er åpnet** | 2 timer | 1 time | 30 minutter |
| **Tilbakemelding etter sak påbegynt** | 2 timer | 1 time | 15 minutter |
| **Igangsette DDoS Mitigering etter bekreftelse** | 1 time | 30 minutter | 10 minutter |
| **Max. økt forsinkelse under trafikk mitigering** | 3 ms | 3 ms | 3 ms |
| **Beredskap etter DDoS angrep er avsluttet** | 1 time | 8 timer | 24 timer |