DDoS-beskyttelse

Tjenestebeskrivelse

18-11-2022

GlobalConnect

Innhold

1. Introduksjon 3
2. Spesifikasjon 5
2.1. Tjeneste varianter 5
2.1.1 Tjeneste - sammenligning 6
2.1.2 Angrepstyper - sammenligning 7
2.2. DDoS beskyttelse - Standard 8
2.2.1 Tilleggsprodukter DDoS beskyttelse Standard 8
2.2.2 Begrensinger DDoS beskyttelse Standard 8
2.3. DDoS beskyttelse – Business 9
2.3.1 Tilleggstjenester DDoS beskyttelse Business 9
2.3.2 Begrensinger DDoS beskyttelse Business 9
2.4. DDoS beskyttelse – Advanced 10
2.4.1 Tilleggsprodukter DDoS beskyttelse Advanced 10
2.4.2 Begrensinger DDoS beskyttelse Advanced 11
3. Rapporter 12
4. Implementasjon 12
5. Tjenestekvalitet (SLA) 13
5.1. Servicetid 13
5.2. Servicegaranti 13
6. Generelle begrensninger 14

1. Introduksjon

Virksomheter har aldri vært mer digitale enn i dag og vi kommuniserer med kunder og brukere via Internett. Kommunikasjonen skjer digitalt gjennom portaler, netthandel, samhandlingsplattformer med mer.

Når et selskap utsettes for et angrep får det ofte store konsekvenser med inntektstap, negativt signal til omverden om dårlig sikkerhet, tap av omdømme og tap av kunder.

Derfor har mange virksomheter søkelys på sikkerhet og investert bl.a. i brannmur teknologi for å beskytte selskapets digitale infrastruktur.

En type angrep som virksomheten kan utsettes for er Distributed Denial of Service (DDoS), et såkalt tjenestenektangrep. Under et typisk DDoS angrep benytter kriminelle seg av et større antall infiserte maskiner på internett og foretar et målrettet angrep mot virksomheten. DDoS angrep er svært utbredt og dessverre lett tilgjengelig fra kriminelle aktører på Internett.

I motsetning til angrep som en brannmur beskytter mot, er ikke formålet med et DDoS angrep å trenge seg igjennom et IT-sikkerhetsforsvar. Formålet med et DDoS angrep er å gjøre tjenester utilgjengelig for omverdenen, med å sende store trafikk mengder mot infrastruktur eller hyppige kall mot nettelementer og servere

DDoS beskyttelse erstatter ikke en brannmur eller andre sikkerhetsløsninger, men er et supplement for å beskytte brannmuren selv, kritiske nettelementer og servere mot spesifikke angrepstyper fra Internett.

Generelt kan vi dele DDoS inn i 3 kategorier

Volumetrisk angrep

Mest vanlig er Volumetrisk angrep har til hensikt å fylle opp forbindelsen med angreps trafikk, så det ikke er ledig kapasitet igjen som kan benyttes av legitim trafikk

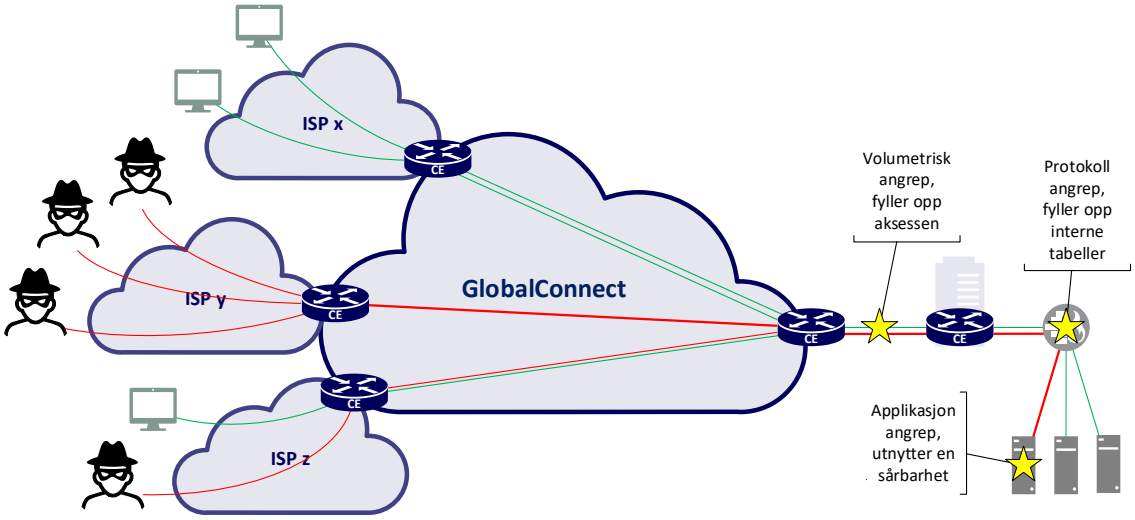
Protokoll angrep

Hyppige kall med lag 3 og 4 trafikk sendes mot elementer som last-balansere, brann-murer og applikasjons-servere og fyller opp interne tabeller. Enhetene vil «utmattes» og ikke være i stand til å prosessere legitim trafikk

Applikasjons angrep

Rettes mot spesifikke deler av en applikasjon og utnytter kjente sårbarheter (ofte mangel på patching). Det sendes typisk mange eller «lange» forespørsler som gjør ap-plikasjon utilgjengelig for legitim trafikk

Skissen under viser typiske steder som DDoS angrep rettes mot



Figur 1: Typiske steder som DDoS angrep rettes mot

GlobalConnect kan tilby en aktiv DDoS beskyttelse som stopper angrep før det når kundens infrastruktur, en forutsetning for å hindre utilgjengelighet grunnet et Volumetrisk angrep

Vi benytter markedsledende teknologi i kjernenettet som overvåkes og vedlikeholdes døgnet rundt. Med et eget dedikert sikkerhets-team samarbeider vi tett med kunden for å sikre tilgjengelighet på den digitale infrastruktur

2. Spesifikasjon

DDoS beskyttelsen iverksetter mitigering (filtrering) av trafikk etter deteksjon av et angrep. Tjeneste variantene beskrevet i dette kapittel har forskjellig følsomhet med tanke på mitigering av et angrep og hvilken type angrep som vil stoppes før det når kundens infrastruktur

Enkle angrep med kjente signaturer vil filtreres i våre grense-routerne og avanserte angrep vil stoppes i vår DDoS beskyttelse plattform. Med spesifikke regler filtreres angrepstrafikk vekk fra nyttetrafikken før den når Kundens infrastruktur.

2.1. Tjeneste varianter

GlobalConnect tilbyr 3 varianter av DDoS beskyttelse (Standard, Business og Advanced), der ulike mitigerings-profiler spesifiseres basert IP-subnet

1. **Standard**
    a) Automatisk filtrering av kjente «signaturer» på angrep

2. **Business**
    a) Automatisk filtrering av kjente «signaturer» på angrep
    b) Automatisk null-routing av angrepet host, ivaretar tilgjengelighet for øvrige tjenester

3. **Advanced**
    a) Automatisk filtrering av kjente «signaturer» på angrep
    b) Automatisk og/eller manuell vask av angrep, ivaretar tilgjengelig for alle tjenester også den som er under angrep
    c) Kundetilpasset filtreringsprofiler, støtter flere objekter

2.1.1 Tjeneste - sammenligning

	Standard	Business	Advanced
IPv4 og IPv6 Support	Ja	Ja	Ja
Beskyttelse mot Volumetrisk angrep	Ja[1]	Ja	Ja
Beskyttelse mot Protokoll angrep	Nei	Nei	Ja
Beskyttelse mot Applikasjon angrep	Nei	Nei	Ja
Automatisk mitigering	Ja	Ja	Ja
Manuell mitigering	Nei	Nei	Ja
Detekteringsmetode	Sampling av trafikk	Sampling av trafikk	Sampling av trafikk
Start mitigering av angrep	5-10 minutter	5-10 minutter	1 – 5 minutter
Antall profiler inkludert i tjeneste	1	1	2
Max antall profiler som kan leveres på tjenesten	1	1	8
Endring av detekteringsprofiler inkludert i tjeneste	Nei	2 stk. per måned	3 stk. per måned
Økt forsinkelse med DDoS beskyttelsen i normal drift	Nei	Nei	Nei
Økt forsinkelse med DDoS beskyttelsen under angrep	Nei	Nei	1-5 ms
Forespørsel om manuell mitigering inkludert i tjeneste	Nei	Nei	3 stk. per måned.
Påbegynt konfigurasjon av manuell mitigering	Nei	Nei	Spesifisert i SLA
Varsling til kunde pr. e-mail (start/stop av mitigering)	Ja	Ja	Ja
Månedsapportering pr. e-mail (angrepstype, størrelse)	Nei	Ja	Ja
Tilleggstjeneste; Forespørsel om manuell blackholing av bestemt kunde IP adresse	Ja	Ja	Ja

[1] Av kjente signaturer

2.1.2 Angrepstyper - sammenligning

De forskjellige tjenester vil detektere og mitigere angrepstyper som

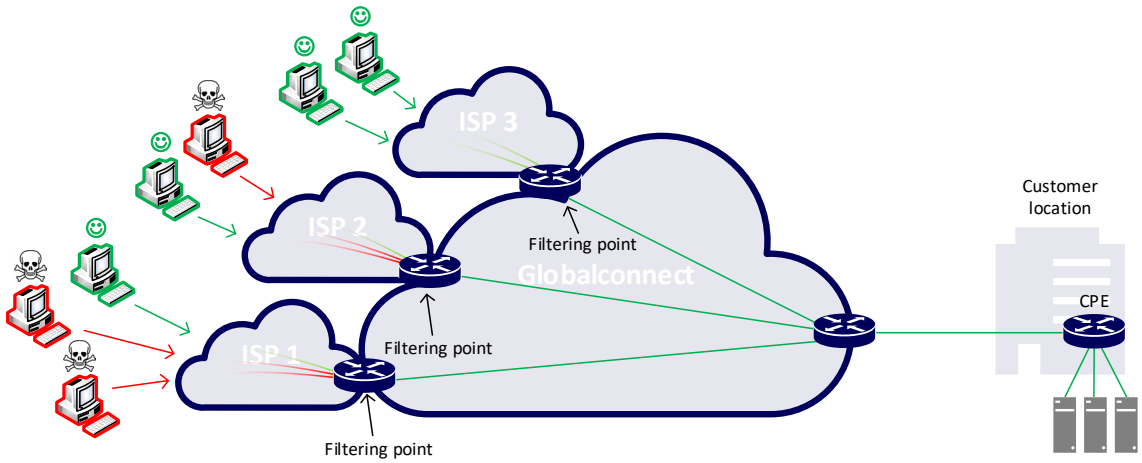
Angrepstyper	Standard	Business	Advanced
chargen Amplification	Ja	Ja	Ja
CLDAP Amplification	Ja	Ja	Ja
IP Fragmentation	Ja	Ja	Ja
L2TP Amplification	Ja	Ja	Ja
mDNS Amplification	Ja	Ja	Ja
memcached Amplification	Ja	Ja	Ja
MS SQL RS Amplification	Ja	Ja	Ja
NetBIOS Amplification	Ja	Ja	Ja
NTP Amplification	Ja	Ja	Ja
RIPv1 Amplification (IPv4 only)	Ja	Ja	Ja
rpcbind Amplification	Ja	Ja	Ja
SNMP Amplification	Ja	Ja	Ja
SSDP Amplification	Ja	Ja	Ja
State exhaustion attacks	Nei	Ja	Ja
DNS Amplification	Nei	Nei	Ja
General UDP	Nei	Nei	Ja
Applikasjons angrep	Nei	Nei	Manuell mitigering

I de neste kapitler beskrives variantene av DDoS beskyttelse i mer detalj

2.2. DDoS beskyttelse - Standard

Standard tjenesten vil automatisk rense trafikken og stopper DDoS angrep med kjente signaturer.

- Standard tjenesten; bestilles som tilleggstjeneste per enkel aksess
- Trafikken mitigeres basert et pre-definert regelsett uten individuell tilpasning for Kunde
- Plattformen analyserer metadata (lag 3 og 4) som sendes til kundens nettverk og starter en filtreringsregel på grense routere som fjerner kjente angrep.
- Deler av trafikken(samples) analyseres og det vil være en viss forsinkelse fra et angrep detekteres til mitigering av trafikken iverksettes.
- Ved flere etterfølgende angrep detekteres og filtreres hvert enkelt angrep. Det kan forekomme korte avbrytelser mens systemet detekterer og starter filtreringsregler. Det skal ikke forekomme lange avbrytelser.



Figur 2: Illustrasjon av DDoS beskyttelse Standard

2.2.1 Tilleggsprodukter DDoS beskyttelse Standard

- Ved henvendelse til GlobalConnect kan Kunde forespørre om manuell null-routing (Blackhole) av bestemt IP adresse hos segselv

2.2.2 Begrensinger DDoS beskyttelse Standard

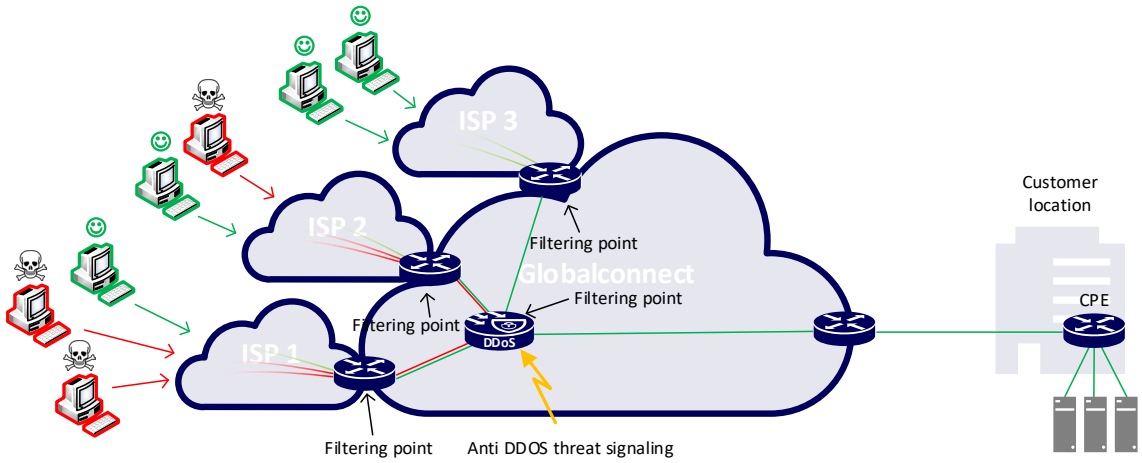
- DDoS beskyttelse – Standard leveres uten SLA (automatisert tjeneste)
- Analysering av trafikk på aksess med 62 offentlige IP-adresser maksimalt (/26 nett)

2.3. DDoS beskyttelse – Business

Denne tjenesten vil stoppe volumetriske angrep med automatisk null-routing (blackhole) av den spesifikke IP-adressen som angripes. Dette for å hindre utilgjengelighet for øvrige brukere og tjenester i virksomheten.

Standard tjenesten er også inkludert som del av denne tjeneste og stopper kjente DDoS signaturer automatisk.

- Business tjenesten; er aksessuavhengig og beskytter spesifisert(e) IP-prefix forvaltet av Kunde
- Tjenesten utfører automatisk filtrering av de mest kjente og utbredte volumetriske DDoS angrep.
- Tjenesten utfører automatisk null-routing av angrepet Host som er del av IP-nettet (spesifisert subnet) som beskyttes
- Plattformen analyserer metadata (lag 3 og 4) som sendes til kundens nettverk.
- Dersom trafikken overstiger definerte terskelverdier, vil systemet starte en filtreringsregel på grense routere og eller utføre automatisk null-routing av angrepet Host.
- Analysen er basert på ”samples” (deler av trafikken), det vil være en viss forsinkelse fra et angrep detekteres til mitigering av trafikken iverksettes.
- Alle filtre og verdier er satt opp statisk og konfigureres av GlobalConnect. Hele Kundens IP-nett spesifisert av Kunden vil inngå i DDoS beskyttelsen



Figur 3: Illustrasjon av DDoS beskyttelse - Business

2.3.1 Tilleggstjenester DDoS beskyttelse Business

- Ved henvendelse til GlobalConnect kan Kunde forespørre om manuell null-routing (Blackhole) av bestemt IP adresse hos segselv

2.3.2 Begrensinger DDoS beskyttelse Business

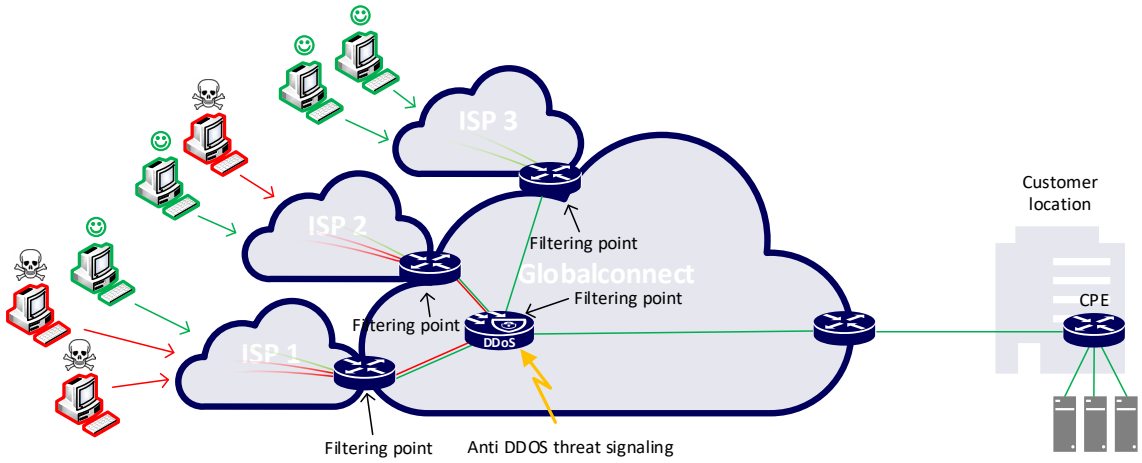
- Max. 1 detektering og mitigering-profil per DDoS beskyttelse Business
- DDoS beskyttelse – Business leveres uten SLA (automatisert tjeneste)

2.4. DDoS beskyttelse – Advanced

Denne tjenesten vil stoppe volumetriske angrep og vaske trafikken mot den spesifikke IP-adressen som angripes. Dette for å hindre utilgjengelighet for øvrige brukere og tjenester i virksomheten.

Standard tjenesten er også inkludert som del av denne tjeneste og stopper kjente DDoS signaturer automatisk.

- Advanced tjenesten; er aksessuavhengig og beskytter spesifisert(e) IP-prefix forvaltet av Kunde
- Advanced tjenesten vil detektere og mitigere angrep raskere enn Standard og Business -tjenestene
- Advanced tjenesten utfører automatisk filtrering(vask) av de mest utbredte og kente volumetriske DDoS angrep.
- Etter avtale med Kunden kan Advanced tjenesten mitigere avanserte angrep mot spesifikke applikasjoner
- Hvis et angrep endrer karakter eller forsvinner i en kortere periode, vil GlobalConnect fortsatt sende trafikken gjennom "vaskeriet" i en periode. Dette for hurtig å kunne vaske angrepstrafikk dersom angrep gjenopptas
- DDoS beskyttelse Advanced tilpasses Kundens behov og flere mitigerings-profiler kan opprettes. Under installasjon defineres grupper av tjenester som skal beskyttes. Eksempelvis IP-adresser for server-farm 1, Mail server, klient-nett, gjeste-nett osv.



Figur 4: Illustrasjon av DDoS beskyttelse Advanced

2.4.1 Tilleggsprodukter DDoS beskyttelse Advanced

- Ulike nivåer av tjenestekvalitet (SLA) er beskrevet i kapittel 3 og kan bestilles som tilleggstjeneste
- Oppsett av flere detektering og mitigerings-profiler ut over de 4 som er inkludert i produktet.

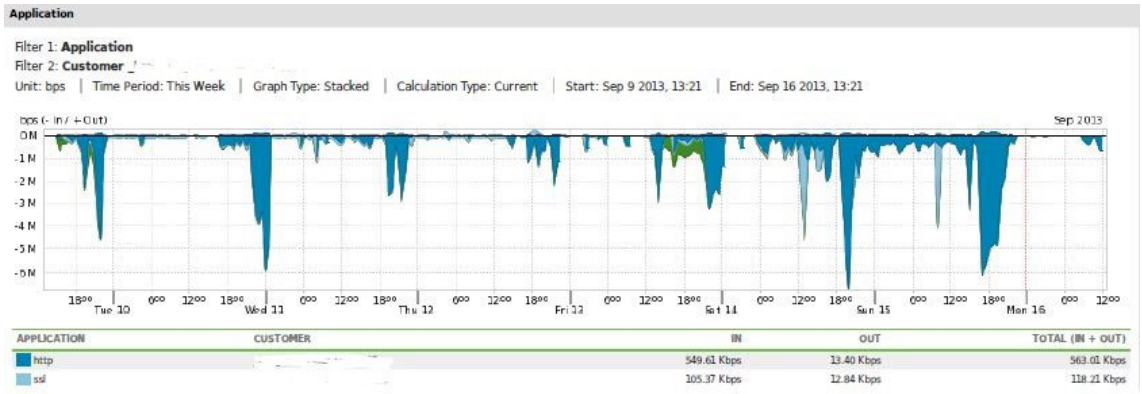
- Ved henvendelse til GlobalConnect kan Kunde be om oppsett av Automatisk null-routing (Blackholing) av trafikk på forbindelser som er beskyttet av Advanced tjenesten
- Kunde kan be om manuell mitigering ut over 3 stk. per måned som er inkludert i Advanced tjenesten
- Endring av mitigerings-profiler ut over 3 stk. per måned som er inkludert i Advanced tjenesten

2.4.2 Begrensinger DDoS beskyttelse Advanced

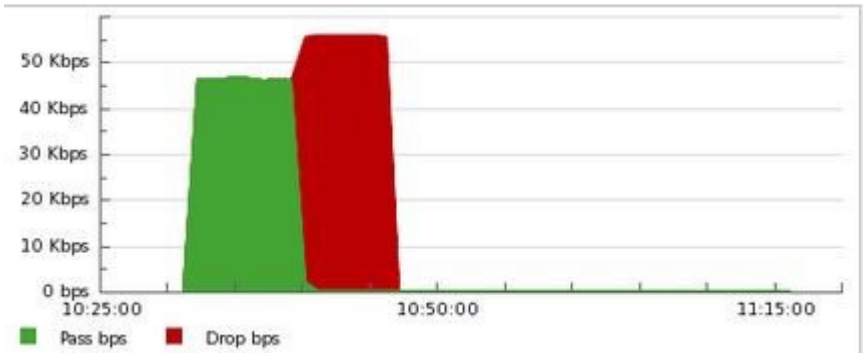
- Max. 8 detektering og mitigerings-profiler per DDoS beskyttelse Advanced

3. Rapporter

GlobalConnect sender rapporter til en e-post adresse avtalt med Kunde. Rapporten vil vise inn- og utgående trafikk fordelt på applikasjon(protokoll). Rapporten viser også 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.



4. Implementasjon

Ved bestilling av tjenesten avtales samarbeidsform mellom GlobalConnect og Kunde. GlobalConnect oversender et driftsskjema som partene fyller ut sammen

5. 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.

5.1. Servicetid

Servicetiden spesifiserer dekningsperioden for feilmelding, feilhåndtering og feilretting.

Tjeneste	Type feil som rettes	Servicetid
Standard	Alle	Virkedager kl. 08:00 – 17:00
Utvidet	Alle	Virkedager kl. 07:00-23:00 Lørdager kl. 07:00-23:00
Kontinuerlig	Alle	24/7/365

5.2. 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	Garanti 1	Garanti 2	Garanti 3
Responstid etter sak er åpnet	2 timer	1 time	30 min.
Tilbakemelding etter sak påbegynt	2 timer	1 time	15 min.
Igangsette DDoS Mitigering	1 time	30 min.	10 min.
Max. økt forsinkelse under trafikk mitigering	5 ms	5 ms	5 ms
Beredskap etter DDoS angrep er avsluttet	1 time	8 timer	24 timer

6. Generelle begrensninger

Kunder som har tilkoblinger fra mer enn én internettleverandør (ISP), vil kun oppnå DDoS beskyttelsen beskrevet i dette dokumentet på forbindelser levert av GlobalConnect.

Kriminelle utvikler stadig nye angrepsmetoder og leter etter nye sårbarheter som kan utnyttes i et DDoS angrep. GlobalConnect oppdaterer plattformen fortløpende med informasjon om nye metoder og sårbarheter, men systemet vil ikke nødvendigvis kunne detektere og mitigere alle såkalte 0-dags sårbarheter.

DDoS angrep endres stadig og nye varianter og angrepsmetoder dukker opp. Selv med markedsledende teknologi og en aktiv driftet tjeneste, kan vi ikke garantere at tjenesten til enhver tid vil stoppe alle angrep. Vårt dedikert sikkerhets-team vil være tilgjengelig å bistå med endringer av mitigerings-profiler ved behov.