Tjenestebeskrivelse DDoS Protection

Versjon 1.5
1.1.2025

GlobalConnect

Innhold

1. Innledning

Internett fra GlobalConnect kan bestilles med ulike tilleggstjenester.

Denne tjenestebeskrivelsen gir en beskrivelse av tjenestene for DDoS-beskyttelse fra GlobalConnect, et sett med tilleggstjenester for Internett.

DDoS-beskyttelse leveres ved hjelp av en DDoS-beskyttelsesplattform som er distribuert og integrert i GlobalConnects kjernenettverk.

Hvilke leveranser av internett- og tilleggstjenester som er spesifikt avtalt mellom GlobalConnect og Kunden fremgår av kontrakten mellom dem.

1.1. Distributed Denial of Service

DDoS-angrep (Distributed Denial of Service) er ondsinnede forsøk på å forstyrre tilgjengeligheten til et nettverk, en tjeneste eller et nettsted ved å overvelde det med en flood av trafikk.

Multivektor-DDoS-angrep er angrep som bruker en kombinasjon av angrepsvektorer eller teknikker for å kompromittere et målnettverk eller en applikasjon. Multivektorangrep er ofte mer sofistikerte og vanskeligere å oppdage enn angrep med én vektor.

GlobalConnect bruker ulike teknikker for å mitigere effekten av DDoS-angrep ved å filtrere kjente angrepssignaturer og utføre traffic scrubbing og/eller blackhole routing. Hvilke teknikker som benyttes avtales med Kunden.

Mange bedrifter og organisasjoner har løsninger for cybersikkerhet for å inspisere trafikken i sin digitale infrastruktur. Brannmurer og andre Stateful-enheter som VPN-gatewayer, IDS/IDP og lastbalanseringsenheter ble aldri utviklet for å stoppe DDoS-angrep. De er derfor mottakelige for dem.

Et typisk DDoS-angrep bruker mange infiserte datamaskiner, et såkalt Botnet, til å utføre et målrettet angrep mot en bedrift eller organisasjon.

DDoS-beskyttelse erstatter ikke en brannmur eller andre løsninger for cybersikkerhet. GlobalConnect kan som ISP stoppe DDoS-beskyttelsen før den når kundens infrastruktur, og beskytte brannmuren og andre kritiske tjenester for å sikre tilgjengeligheten til tjenesten.

1.2. Typer angrep

Generelt finnes det tre typer DDoS-angrep.

1.2.1 Volumetrisk angrep (lag 3 og 4)

Volumetriske angrep er det vanligste angrepet. Målet er å mette båndbredden til offeret.

Et volumetrisk angrep måles i bits per sekund (bps).

1.2.2 State-exhaustion-angrep (lag 3 og 4)

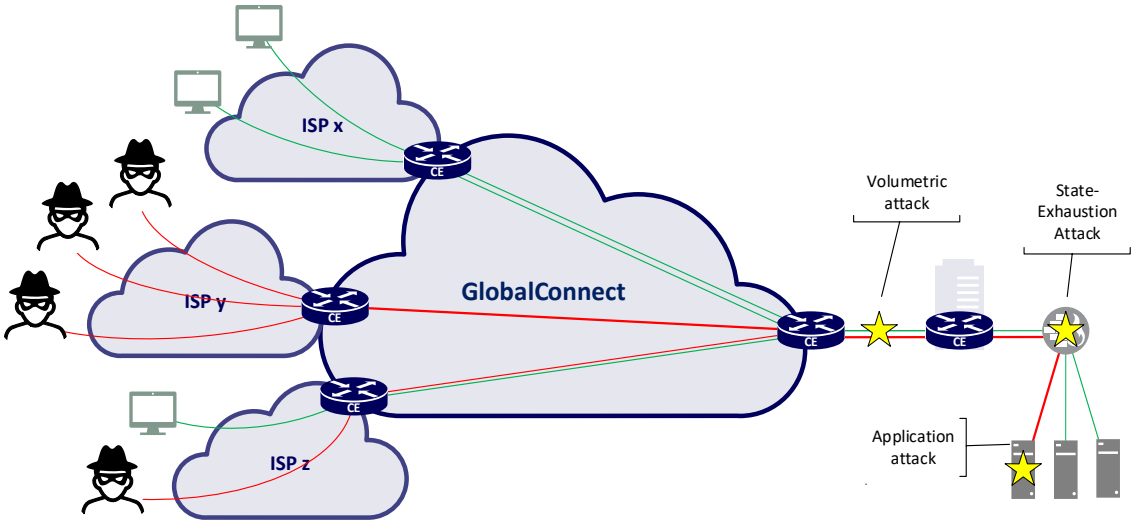
State-exhaustion-angrep overbelaster tilstandstabeller for forbindelser. Disse finnes i mange infrastrukturelementer som lastbalanseringsenheter og brannmurer, og også i selve applikasjonsserverne. Selv høykapasitetsenheter som er i stand til å opprettholde tilstanden til millioner av forbindelser, kan bli tatt ned av disse angrepene.

Et State-exhaustion-angrep måles i pakker per sekund (pps).

1.2.3 Application Layer-angrep (Layer-7)

Inkluderer low-and-slow-angrep. Målet med disse angrepene er å få webserveren til å krasje.

Application Layer-angrep måles i forespørsler per sekund (rps).



Figur 1: Typiske angrepspunkter for et DDoS-angrep

2. GlobalConnect DDoS-beskyttelse Tjeneste

GlobalConnects DDoS-beskyttelsestjeneste gir beskyttelse mot volumetriske angrep, state-exhaustion-angrep og applikasjonsangrep på internettforbindelser levert av GlobalConnect.

Plattformen for DDoS-beskyttelse er implementert i kjernen av GlobalConnects backbone og overvåkes 24/7.

Hvis en trafikkstrøm klassifiseres som et DDoS-angrep, iverksetter plattformen for DDoS-beskyttelse filtrering (mitigering) av den innkommende trafikken.

De enkelte variantene av tjenesten DDoS-beskyttelse tilbyr:

a) ulike nivåer av sensitivitet i forhold til når et angrep oppdages,
b) ulike reaksjonstider fra deteksjon til mitigering, samt
c) forskjeller i hva som kan mitigeres.

GlobalConnect tilbyr 4 varianter av tjenesten DDoS-beskyttelse, som gir ulik beskyttelse og ulike opsjoner for individuell tilpasning i henhold til punktene a - c ovenfor.

De fire variantene er

1. DDoS protection Base
2. Adaptive DDoS protection Standard
3. Adaptive DDoS protection Business
4. Adaptive DDoS protection Advanced

DDoS protection Base er et generisk filter som leveres som standard for alle kunder med forbindelse til internett fra GlobalConnect. For DDoS-beskyttelse Base er det ingen definert kapasitet per tjeneste, i stedet beskyttes tjenestene i et felles Managed Object som best-effort.

Adaptive DDoS protection gir dedikert beskyttelse, inkludert rapporter og alarmer, og består av våre varianter Standard, Business og Advanced. De adaptive variantene av DDoS-beskyttelse tilbyr et bredt spekter av beskyttelse i flere lag.

Ved bestilling av en Tjeneste for Adaptive DDoS protection bør Kunden velge en DDoS-beskyttelseskapasitet som minst tilsvarer kapasiteten på internettforbindelsen.

Et DDoS-angrep kan endre karakter over tid. Selv om alle varianter gir omfattende beskyttelse mot DDoS-angrep, kan GlobalConnect ikke garantere at DDoS-beskyttelsestjenesten kan stoppe dem alle til enhver tid.

GlobalConnect overvåker kontinuerlig plattformen for DDoS-beskyttelse for å identifisere om det er behov for å innføre nye tiltak og terskler for å beskytte mot nye former og typer angrep. GlobalConnect utfører monitorering per destinasjons-IP.

Kunder kan be om en oppgradering til en høyere variant av DDoS-beskyttelse for økt dekning.

2.1. Varianter av DDoS-beskyttelse - oversikt

DDoS-beskyttelse fra GlobalConnect er tilgjengelig i fire varianter: Base, Standard, Business eller Advanced. Alle variantene leveres som abonnementsbaserte tjenester.

		Adaptive DDoS protection		
Funksjoner for mitigering	Base	Standard	Business	Advanced
Mitigering av volumetriske angrep	Ja	Ja	Ja	Ja
Mitigering av state-exhaustion-angrep	Nei	Nei	Ja	Ja
Mitigering av applikasjonsangrep, Layer 7	Nei	Nei	Nei	På forespørsel
Mitigering av lekket ddos-angrep	Nei	Nei	På forespørsel	På forespørsel
Flowspec mitigering (signaturfiltrering)	Ja	Ja	Ja	Ja
Traffic Blackhole (NULL-routing)	Nei	Nei	Nei	På forespørsel
Inline-filter (multi-vector scrubbing)	Nei	Nei	Ja	Ja
Mitigering av DNS	Nei	Nei	Ja	Ja
UDP mitigering	Nei	Nei	Ja	Ja
Allowlist (Whitelist)	Nei	Nei	Nei	Ja
Geo-blokkering under angrep	Nei	Nei	Nei	Ja
Mitigering	Automatisk	Automatisk	Automatisk eller manuell	Automatisk eller manuell
Utgående mitigering	Nei	Nei	Nei	Nei
Profil for mitigering	Standard	Standard	Standard	Kan tilpasses
Funksjoner for deteksjon og tjenester				
Varsling ved high alert til kunder	Nei	Ja	Ja	Ja
Kunderapporter	Nei	Ukentlig	Ukentlig	Ukentlig
Rapporter om hendelser	Nei	På forespørsel**	På forespørsel**	På forespørsel
Brukertilgang	Nei	Nei	Nei	Nei
Økt forsinkelse under mitigering	Nei	Nei	Ja*	Ja*
Managed Objects (antall profiler)	Delte	1	1	4 inkludert

Trafikkterskelpolicy	Forhåndsdefinert	Forhåndsdefinert	Kan tilpasses	Kan tilpasses
Fast flood-deteksjon	Nei	Nei	Ja (opsjon)	Ja (opsjon)
Carpet bombing identifikasjon	Nei	Nei	Nei	Ja
Tid til å oppdage	< 300 sekunder	< 300 sekunder	< 180 sekunder	< 120 sekunder
På tide å starte automatisk mitigering	< 420 sekunder	< 420 sekunder	< 300 sekunder	< 240 sekunder
Tid til varsel om høy beredskap	N/A	< 300 sekunder	< 180 sekunder	< 120 sekunder
Service Level Agreement (SLA)	Tilgangsbasert	Subnet eller tilgangsbasert	Subnet eller tilgangsbasert	Subnet eller tilgangsbasert
Støtte for IPv4 og IPv6	Ja (IPv4)	Ja (IPv4)	Ja (støtte for IPv4 eller IPv6)	Ja (støtte for IPv4 og IPv6)

* Avhengig av angrepstype og geografisk lokasjon
** Med forbehold om engangsavgift
På forespørsel betyr at kunden må kontakte GlobalConnect for å starte en mitigering av den spesifikke funksjonen
Tilpassbar betyr at funksjonen kan tilpasses i henhold til kundens krav
Ja (opsjon) betyr at funksjonen er aktiv som standard, men at kunden kan velge den bort

2.2. Varianter av DDoS-beskyttelse - Liste over angrepstyper

De ulike produktene er satt opp for å oppdage og mitigere følgende angrepstyper:

Angrepstyper av mitigering	Base	Standard	Business	Advanced
Chargen Forsterkning	√	√	√	√
CLDAP forsterkning	√	√	√	√
IP/ICMP Fragmentering	√	√	√	√
L2TP forsterkning	√	√	√	√
memcached Forsterkning	√	√	√	√
MS SQL RS forsterkning	√	√	√	√
NetBIOS forsterkning	√	√	√	√
NTP forsterkning	√	√	√	√
RIPv1 forsterkning (kun IPv4)	√	√	√	√
rpcbind Forsterkning	√	√	√	√
SNMP forsterkning	√	√	√	√
SSDP Forsterkning	√	√	√	√
State-exhaustion-angrep	Nei	Nei	√	√
DNS forsterkning	Nei	Nei	√	√
UDP flood	Nei	Nei	√	√
GlobalConnect Intelligence Feed	√	√	√	√

Følgende avsnitt inneholder ytterligere detaljer om de fire variantene av DDoS-beskyttelse.

2.3. Variant: DDoS protection Base

DDoS protection Base er et standard og generisk DDoS-beskyttelsesfilter som leveres i hele GlobalConnects kjerne-IP-nettverk. DDoS-beskyttelse Base er en helautomatisk filtreringstjeneste som bruker kjente DDoS-signaturer fra ulike kilder og leverandører.

2.3.1 Begrensninger for DDoS protection Base:

- Alle tjenester er beskyttet i et delt managed object som best-effort.
- Ingen tilpasning er mulig for DDoS-beskyttelse Base.
- Base-varianten støtter ikke rapportering og varsling.

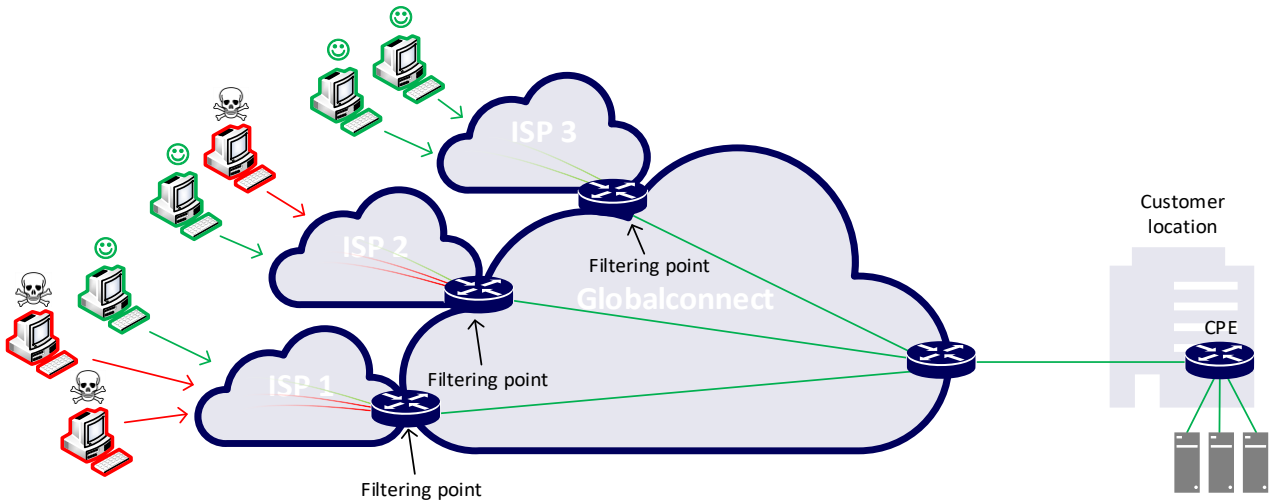
2.4. Variant: Adaptive DDoS protection Standard

Adaptive DDoS protection Standard tilbyr kundespesifikk monitorering av trafikk på GlobalConnects backbone. Hvis et angrep oppdages, setter GlobalConnect i gang filtrering på stamnettutstyret etter en kort forsinkelse. Adaptive DDoS protection Standard bruker et universelt filter, men er implementert på kundens IP-subnet, noe som gir kunden individuell rapportering og varsling under angrep.

- Standard-tjenesten gir automatisk filtrering av de vanligste og mest kjente volumetriske DDoS-angrepene.
- Angrep oppdages basert på terskler i en profil for mitigering. Hvis trafikken overskrider tersklene, starter systemet automatisk filtrering.
- Standard-tjenesten beskytter automatisk mot frittstående volumetriske angrep.
- Standard-tjenesten oppdateres kontinuerlig med informasjon om kjente globale trusler og angrepsmønstre. Denne informasjonen brukes til å sette opp automatisk deteksjon og mitigering.
- Ved flere, sekvensielle angrep oppdager og filtrerer systemet hvert enkelt angrep. Derfor kan det oppstå flere korte avbrudd mens systemet oppdager og starter filtreringen.

2.4.1 Begrensninger for Adaptive DDoS protection Standard:

- Én forhåndsdefinert profil for mitigering er i bruk og er ikke tilpasset til kundens miljø. Dette betyr at alle terskler og verdier settes universelt av GlobalConnect.
- DDoS-beskyttelse Standard er en automatisk tjeneste, noe som betyr at GlobalConnect ikke kan garantere at alle varianter av de angitte angrepene kan mitigeres.
- Standardtjenesten støtter bare beskyttelse for IPv4.
- Standardvarianten er "one-size-fits-all". Følgelig kan ikke angrep hvis volum faller under den universelle terskelen mitigeres.



Figur 2: Illustrasjon av DDoS-beskyttelse Base & Standard

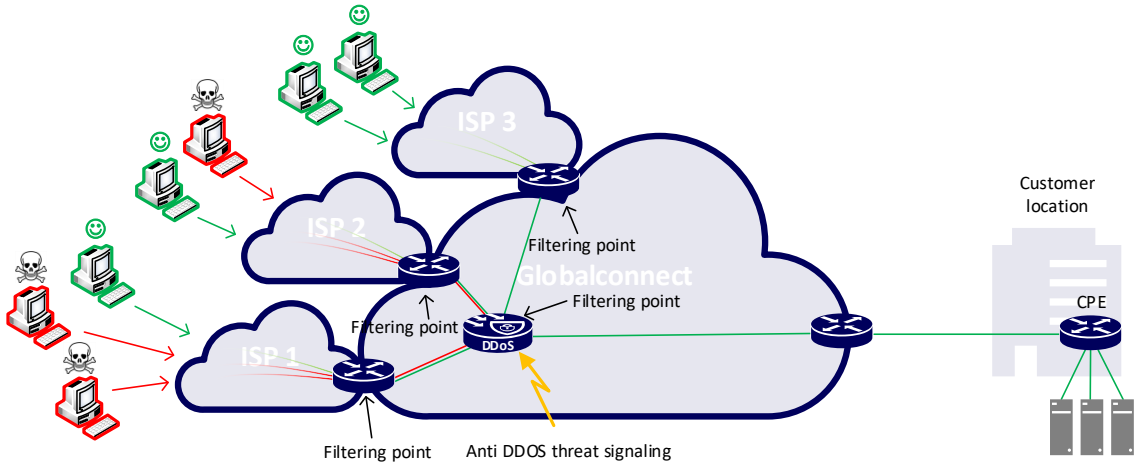
2.5. Variant: Adaptive DDoS protection Business

Adaptive DDoS protection Business inneholder alle funksjonene som er inkludert i Adaptive DDoS protection Standard, supplert med et ekstra beskyttelseslag og tilbyr følgende funksjoner:

- Adaptive DDoS protection Business gir automatisk beskyttelse mot State-exhaustion-angrep.
- Business-varianten beskytter også mot avanserte multivektorangrep, inkludert avanserte UDP-angrep.
- Ved angrep som ikke kan mitigeres av standardfilteret, videresendes kundens trafikk til GlobalConnects eget scrubbingsenter for DDoS-beskyttelse, som utfører ytterligere scrubbing av trafikken.
- Kunder som utsettes for sitt første angrep, kan oppleve en kort forsinkelse fra angrepet starter til trafikken omdirigeres til scrubbingsenteret.
- Hvis et pågående angrep endrer karakter, vil GlobalConnect fortsette å sende trafikken gjennom filteret for DDoS-beskyttelse. Dette sikrer at nye angrepsvektorer som startes, filtreres bort svært raskt.
- Med Adaptive DDoS protection Business er det mulig å tilpasse visse terskler for mitigering av angrep.
- Standardinnstillingen for DDoS-beskyttelse inkluderer automatisk mitigering for kontinuerlig beskyttelse. For Business-varianten kan manuell mitigering konfigureres for spesifikke subnett eller IP-adresser. Med manuell mitigering aktiveres filtreringen når kunden kontakter GlobalConnect.

2.5.1 Begrensninger for Adaptive DDoS protection Business

- Bare ett Managed Object er tilgjengelig for Adaptive DDoS protection Business.
- Beskyttelse for både IPv4- og IPv6-oppsett krever separate Managed Objects, noe som ikke støttes i Business-tjenesten.
- Profiler for mitigering kan ikke tilpasses for spesifikke kunder.



Figur 3: Illustrasjon av DDoS-beskyttelse Business

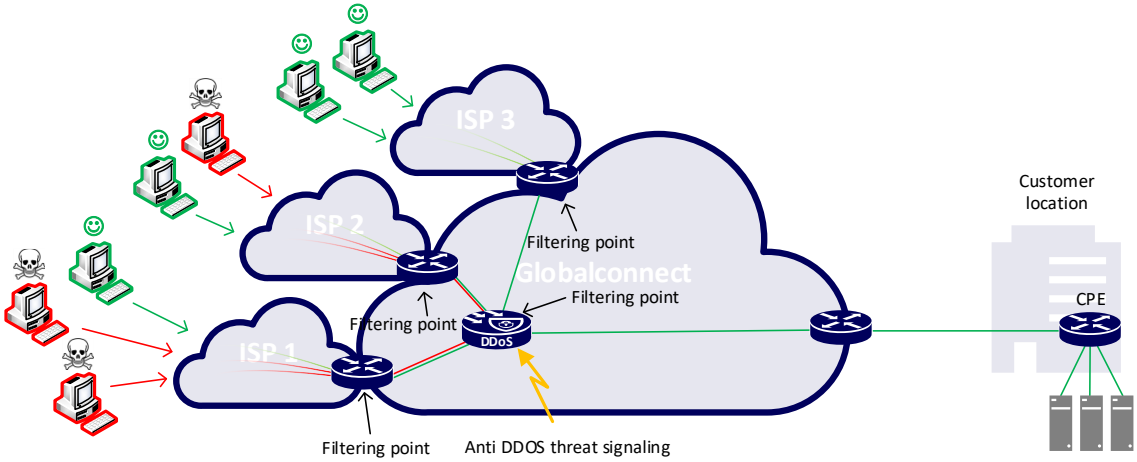
2.6. Variant: Adaptive DDoS protection Advanced

Adaptive DDoS protection Advanced inneholder alle funksjonene fra Standard- og Business-tjenestene, og tilbyr følgende funksjoner:

- Med Adaptive DDoS protection Advanced kan kunden be om hjelp til å mitigere application layer-angrep.
- Med Advanced-varianten er systemet satt opp til å oppdage og mitigering mot angrep raskere enn i de andre variantene.
- Adaptive DDoS protection Advanced gir mulighet til å tilpasse både filterregler og terskler for mitigering av angrep.
- Fire administrerte objekter er inkludert i varianten Adaptive DDoS protection Advanced. Dette gir ytterligere granularitet. Disse kan tilpasses i henhold til kundens krav ved levering. Hvilke objekter som skal beskyttes, defineres i samråd med kunden under installasjonen.

2.6.1 Opsjoner for Adaptive DDoS protection Advanced

- Flere Managed Objects kan bestilles (maksimalt 50 MO-er).
- Kunder kan kontakte GlobalConnect for å be om blackholing av trafikk på forbindelser som er beskyttet av DDoS-beskyttelse Advanced.
- Kunder kan be om endring av deteksjonsprofilen.
- Hvis kunden bruker eget utstyr for DDoS-beskyttelse, gir GlobalConnect opsjon på å integrere dette, forutsatt at det er kompatibelt med vårt sentralsystem.



Figur 4: Illustrasjon av DDoS-beskyttelse Advanced

3. Service Level Agreement (SLA)

Tjenesten er tilgjengelig med ulike tjenestenivåer. De garanterer ulike nivåer av tilgjengelighet og servicetid.

DDoS-beskyttelse kan leveres på følgende måter:

Option 1. Som en tilleggstjeneste til en enkelt Access-tjeneste
Tilgjengelig for: Base, Standard, Business, Advanced
Option 2. Som en aksessuavhengig tjeneste som dekker flere aksessuavhengige tjenester, der spesifiserte IP-subnett er beskyttet
Tilgjengelig for: Standard, Business, Advanced

For opsjon 1 arver DDoS-beskyttelsen SLA-nivået til aksesslinjen.

For opsjon 2 må SLA-nivået for DDoS-beskyttelse spesifiseres separat.

Definisjonen av GlobalConnects tjenestenivåer er spesifisert i "GlobalConnect Service Level Agreement - SLA". Tjenesten er begrenset til Bronze, Silver og Silver24. Som standard leveres tjenesten med tjenestenivået Bronze.

3.1. Definisjon av feil

Forringelse av tjenesten med hensyn til garantert kapasitet eller dens kvalitet kvalifiserer som "Degradert tjeneste" og tjenesteavbrudd eller alvorlig forringelse kvalifiserer som "Tjeneste nede", som brukt i "GlobalConnect Service Level Agreement - SLA". Eventuelle feil håndteres i henhold til GlobalConnects hendelseshåndteringsprosess.

- Tjeneste nede: Tjenesten klassifiseres som "tjeneste nede" hvis den ikke oppfyller tjenestens spesifikasjoner.
- Degradert tjeneste: Tjenesten klassifiseres som "degradert" hvis den bare delvis oppfyller tjenestens spesifikasjoner.

3.2. Tilgjengelig tjeneste

Tilgjengeligheten måles månedlig.

4. Begrensninger

Kunder som er sammenkoblet til mer enn én internettleverandør ("Multi-homed"-kunder), vil kun få beskyttelse på forbindelser levert gjennom GlobalConnect for tjenester som er beskrevet i dokumentet.

DDoS-angripere er hele tiden på jakt etter uoppdagede svakheter som kan brukes til å starte et DDoS-angrep. GlobalConnects DDoS-beskyttelse oppdateres kontinuerlig med informasjon om kjente angrepsformer og -metoder, men tjenesten vil ikke nødvendigvis oppdage og mitigere alle såkalte Zero Day-trusler.

DDoS-beskyttelse gjelder bare for IPv4- og IPv6-adresser som leveres av GlobalConnect.

5. Ordliste

Begrep	Definisjon
Adaptive DDoS protection	Ved å tilby en rekke ulike beskyttelser mot ulike typer angrep, leverer GC en adaptiv løsning for DDoS-beskyttelse
Applikasjonsangrep	Application Layer-angrep retter seg mot et aspekt av en applikasjon eller tjeneste på Layer-7
Traffic Blackhole (NULL-routing)	Traffic Blackhole (NULL-routing) kan være en effektiv kortsiktig løsning for å mitigere virkningen av DDoS-angrep. Det er imidlertid viktig å merke seg at all trafikk til den aktuelle IP-adressen forkastes, uansett om den er legitim eller ikke. Traffic Blackhole kan utføres ved hjelp av automatisk eller manuell mitigering
Carpet bombing	"Carpet bombing" i DDoS-angrep er når angriperen sprer trafikken over mange IP-adresser i et nettverk i stedet for å ramme bare ett mål. Dette gjør angrepet vanskeligere å oppdage og forårsaker mer omfattende forstyrrelser i hele nettverket.
Chargen Forsterkning	Systemer som kjører den eldre nettverkstestfunksjonen Chargen (Legacy Character Generator), kan misbrukes til å starte DDoS-angrep med refleksjon/forsterkning. De fleste Chargen-reflektorer/-forsterkere er IoT-enheter som ofte har slike tjenester som kan misbrukes, kjørende som standard.
CLDAP forsterkning	Usikrede tjenester for Connectionless Lightweight Directory Access Protocol (CLDAP) kan utnyttes til å utføre DDoS-angrep med refleksjon/forsterkning. De fleste CLDAP-reflektorer/-forsterkere som kan misbrukes, er Microsoft Windows-servere som uvettig har blitt eksponert mot internett. CLDAP DDoS-refleksjonsangrepet har en forsterkning på opptil 70 ganger. En av de mest effektive UDP-protokollene for misbruk.
Oppdagelse	• Oppdagelse av avvikende trafikk i sanntid (trafikk som avviker fra akseptabel bruk) • Trafikk som overstiger normale nivåer

	• Trafikk som overstiger en konfigurert terskel
DNS forsterkning	Domain Name System (DNS) er en database som lagrer domenenavn på internett og oversetter dem videre til IP-adresser. Et DDoS-angrep med refleksjon/forsterkning av DNS er et vanlig DDoS-angrep i to trinn der angriperen manipulerer åpne DNS-servere.
Mitigering av DNS	En metode for å forhindre eller mitigere virkningen av angrep med forsterkning av DNS (Domain Name System)
Fast flood-deteksjon	Utløser et vertsvarsel raskere enn alvorlighetsgraden når avviksfrekvensen er for stor
Flowspec mitigering	BGP Flowspec (protokoll) brukes til å pushe en Access Control List til grenseruteren. Dette er en effektiv 1. forsvarslinje for å beskytte mot kjente DDoS-angrep
Geo-blokkering under angrep	Geo-blokkering vil blokkere bestemte regioner/land fra å få tilgang til tjenester på din(e) lokasjon(er) under et angrep
IP/ICMP Fragmentering	IP/ICMP-fragmenteringsangrep bombarderer destinasjonen med fragmenterte pakker, noe som fører til at den bruker minne på å sette sammen alle fragmentene på nytt og overvelder nettverket.
Høy beredskap	Et varsel har en høy alvorlighetsgrad hvis følgende betingelser er oppfylt: • Trafikken holder seg over utløsningshastigheten lenger enn forsinkelseperioden for start av vertsdeteksjon. • Trafikken går over den høye alvorlighetsgraden. • Trafikken holder seg over den høye alvorlighetsgraden i hele varigheten av alvorlighetsgraden.
Inline-filter	Ad hoc-filter som er konfigurert spesielt for en mitigering
L2TP	L2TP (Layer 2 Tunnelling Protocol) er en tunnelprotokoll som brukes til å støtte virtuelle private nettverk (VPN)

Forsinkelse	Forsinkelse er tiden det tar for data å passere fra ett punkt i et nettverk til et annet
Lekket ddos-angrep	Et "lekket ddos-angrep" refererer til et angrep som faller under den generelle terskelen som er satt for DDoS-deteksjon, men som overskrider kapasiteten til en kunde med lav båndbredde. Dette er et angrep som er for lite til å starte den automatiske mitigeringen
Managed Objects	For å beskytte/spore en kunde eller en tjeneste opprettes et Managed Object. Managed Objects er knyttet til et sett med IP-adresser
memcached Forsterkning	memcached er et system for hurtigbufring av databaser i minnet som brukes til å forbedre ytelsen til tjenester som er rettet mot internett. Feilkonfigurerte memcached-servere brukes til å utføre angrep med store mengder UDP-refleksjon/forsterkning
Mitigering	DDoS mitigering bruker et sett med teknikker og verktøy for å motstå eller mitigere virkningen av DDoS-angrep
MS SQL RS angrep	Misbrukbare, internett-eksponerte Microsoft SQL Server-noder som kjører SQL Server Reporting Service, kan utnyttes til å utføre angrep med refleksjon/forsterkning.
NetBIOS forsterkning	Network Basic Input/Output System (NetBIOS) tilbyr tjenester knyttet til sesjonslaget i OSI-modellen som gjør det mulig for applikasjoner på separate datamaskiner å kommunisere over et lokalt nettverk. En angriper kan få offerets maskin til å avvise all NetBIOS-nettverkstrafikk, noe som resulterer i en "denial of service".
NTP forsterkning	Network Time Protocol (NTP) forsterkning er en type DDoS-angrep der angriperen utnytter offentlig tilgjengelige NTP-servere til å overvelde målet med User Datagram Protocol (UDP)-trafikk.
Utgående mitigering	Mitigering av trafikk som sendes fra kunden
RIPv1 forsterkning (kun IPv4)	Noder som eksponerer den utdaterte rutingprotokollen RIPv1 mot internett, kan misbrukes til å utføre refleksjons-/forsterkningsangrep.

Rpcbind forsterkning	Feilkonfigurerte tjenester som eksponerer rpcbind/portmapper-tjenesten mot internett, kan utnyttes til å utføre angrep med refleksjon/forsterkning.
SNMP forsterkning	Rutere, lag-3-switcher, Wi-Fi-aksesspunkter, servere og andre internett-tilkoblede enheter som kjører SNMPv2-administrasjonsprotokollen, og som er feilkonfigurert slik at de er eksponert mot internett med standard påloggingsinformasjon, kan utnyttes til å utføre refleksjons-/forsterkningsangrep.
UDP flood	En UDP flood er en form for volumetrisk DoS-angrep der angriperen overvelder tilfeldige porter på målverten med IP-pakker som inneholder UDP-pakker (User Datagram Protocol).
SSDP	Rutere for bredbåndsaksess i forbrukerklassen som eksponerer Simple Service Discovery Protocol (SSDP) mot internett, kan utnyttes til å utføre angrep med refleksjon/forsterkning av SSDP.
State-exhaustion-angrep	State-exhaustion-angrep bruker tilstandstabellene for forbindelser som finnes i mange infrastrukturkomponenter, for eksempel lastbalanseringsenheter, brannmurer og applikasjonsservere. Selv høykapasitetsenheter som kan opprettholde tilstanden til millioner av forbindelser, kan bli tatt ned av disse angrepene
UDP mitigering	En måte å forhindre et UDP-angrep på, der en angriper overbelaster tilfeldige porter på offeret med IP-pakker som inneholder UDP-pakker (User Datagram Protocol)
Volumetrisk angrep	Volumetriske angrep er utformet for å overvelde et mål med en flood av trafikk, slik at det blir utilgjengelig for brukerne. Volumetriske angrep bruker opp båndbredden enten innad i målnettverket/tjenesten, eller mellom målnettverket/tjenesten og resten av internett. Disse angrepene handler ganske enkelt om å forårsake overbelastning.
Allowlist (Whitelist)	Whitelist tillater en bestemt entitet å passere, selv om regelsettet har bestemt seg for å handle mot den
Zero Day-trusler	Begrepet "Zero Day" refererer vanligvis til en tidligere ukjent sårbarhet i et IT- eller

	datakommunikasjonssystem. Sårbarheten er ukjent både for organisasjonene som bruker systemet, og for leverandøren av systemet. Uten raske og effektive mottiltak kan angripere utnytte denne sikkerhetsbristen til å infisere eller på annen måte skade et system.