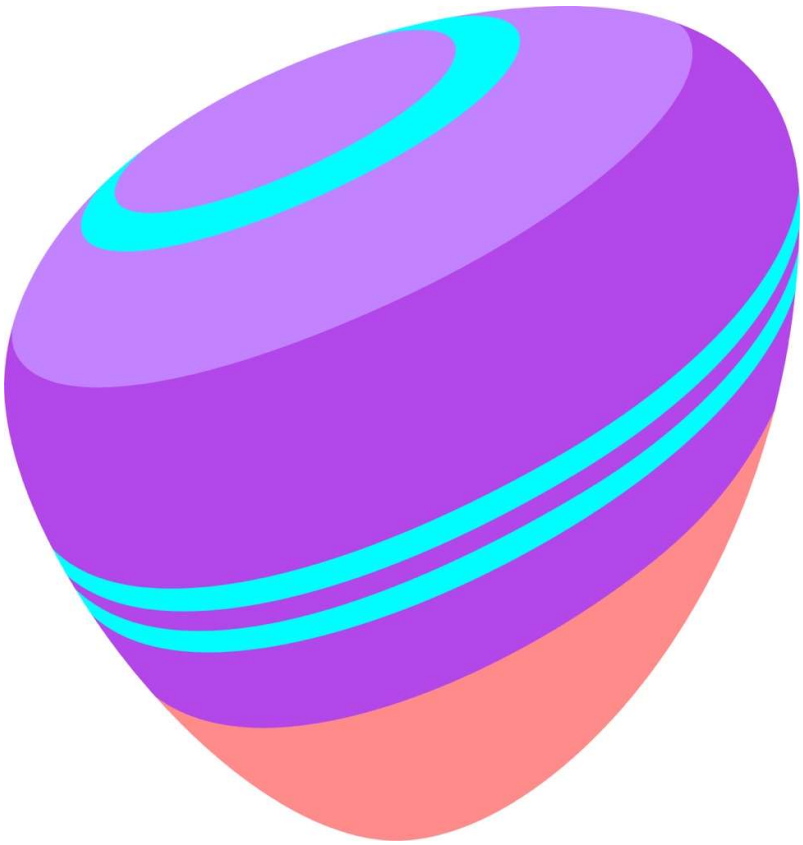
TELIA DDOS PROTECTION

Tjenestebeskrivelse



INNHOLD

1. Telia DDoS Protection 3
1.1 Grunnfunksjon 3
1.2 Definisjoner 3
1.3 Pakker 5
1.3.1 DDoS Protection Standard 5
1.3.2 DDoS Protection Small 5
1.3.3 Funksjonsoversikt 5
1.4 Tilleggsfunksjoner 6
1.5 Teknisk beskrivelse 6
1.6 Kundegrensesnitt 8
1.7 Servicedesk 8
1.8 Overvåkning 8

2. Levering 8
2.1 Oppstartsmøte 8
2.2 Bestilling 8
2.3 Levering 9
2.4 Leveringstid 9

3. Øvrig 9

1 Telia DDoS Protection

1.1 Grunnfunksjon

Telia DDoS Protection er en avansert nettverksbasert beskyttelse mot datasabotasje i form av koordinerte overbelastningsangrep over Internett, som ellers enkelt fyller opp og slår ut en forbindelse. Med Telia DDoS Protection får kunden rask tilgang til kvalifisert hjelp for å avverge eller begrense virkningen av et angrep slik at legitim trafikk kan komme frem og normal drift kan fortsette. Tjenesten består av en rekke funksjoner som er inkludert i standardtjenesten og kan suppleres med en rekke valgfrie funksjoner. Tjenesten inkluderer automatisk periodisk rapportering.

DDoS Protection støtter både automatisk detektering, aktivering og deaktivering av identifisert volumetrisk overbelastningsangrep samt mulighet for manuell aktivering. Se eventuelle begrensninger nedenfor.

DDoS Protection er en "Best Effort"-tjeneste, men Telia tilstreber at plattformen og konfigurasjonen for DDoS-beskyttelse er operativ og driftsavdelingen er best mulig tilpasset for å oppdage og håndtere volumetriske angrep, slik at kundens virksomhet i størst mulig grad kan fortsette som vanlig.

Telias tjeneste er basert på plattformer fra markedsledende leverandører. Dette, sammen med Telias kraftige globale nettverk samt ekspertise og erfaring, sikrer at vi kan tilby markedets beste nettverksbaserte beskyttelse mot overbelastningsangrep også kjent som tjenestenektangrep.

1.2 Definisjoner

Definisjoner	
Automitigering	Volumetriske angrep oppdages automatisk og vasking startes når tersklene for et DDoS-angrep mot en offentlig IP-adresse/vertsmaskin, konfigurert i en hvilken som helst beskyttelsesgruppe, er overskredet i en viss periode. Automitigering er alltid det raskeste og mest effektive alternativet for beskyttelse ved angrep.
DDoS	Distributed Denial of Service (ofte referert til som "tjenestenektangrep")

IP-lokasjonsfilter	Ved mitigering/vasking har vi i tjenesten mulighet til å filtrere ut eller tillate kildetrafikk basert på IP-adressers geografiske tilhørighet/opprinnelse. I kompliserte angrepsscenarier er det derfor alltid mulighet for å eksempelvis bare tillate trafikk fra Norden/Europa til et spesifikt beskyttelsesobjekt (MO) eller å blokkere trafikk fra et geografisk område, for eksempel et kontinent eller et enkeltland. Dette støttes for IP-adresser/vertsmaskiner definert i en hvilken som helst beskyttelsesgruppe.
Beskyttelsesobjekt/-gruppe	De offentlige vertsmaskinene og nettverkene som kunden definerer i den grunnleggende profilen samt eventuelle vertsmaskiner som er definert i en av de mer spesifikke profiler som er konfigurert i DDoS-beskyttelsen.
Managed Object (MO)	Et Managed Object (administrert objekt) er en forhåndsdefinert mitigeringsprofil. Eksempler på valgbare profiler er blant annet Felles, HTTP/HTTPS, SIP, DNS og SMTP. I et Managed Object samles de vertsmaskinene og nettverkene som kunden velger, og som er knyttet til deres forhåndsdefinerte profil. Til sammen danner disse vertsmaskinene et beskyttelsesobjekt
Hvitelisting	Betyr at kunden kan definere et antall eksterne kilder/IP-adresser som sikre og som aldri skal vaskes.
Kontroll-ID	Brukes til å sikre en godkjent identitet for å utføre endringsordrer og kontakte Telias prioriterte telefonnumre for support av DDoS-Protection.

1.3 Pakker

Telia DDoS Protection tilbys i to kundebehovsbaserte pakker: Standard og Small.

1.3.1 DDoS Protection Standard

- Passer selskaper og organisasjoner som har krav til høye båndbredder på internett, flere Managed Objects (MO) og mange vertsmaskiner som skal beskyttes og som ønsker mulighet for utvidet rapportering og personlig rådgivning i forbindelse med angrep.
- Mulighet for mer personlig hjelp ved å justere beskyttelsen og manuelt kontrollere mottiltak, er også tilgjengelig.
- I forbindelse med start og stopp av vask, kontakter Telias support alltid kunden for å sikre at alt fungerer som det skal.
- Både automatisk og manuell start av mitigering støttes.
- Mulighet for tilpassede mitigeringsprofiler.
- Ytterligere MO'er ut over de som er inkludert i basistjenesten, kan bestilles.

1.3.2 DDoS Protection Small

- Implementeres på samme plattform som standardpakken, men er tilpasset mindre kunder med lavere krav til internettkapasitet, antall administrerte objektsprofiler, antall beskyttede objekter og funksjonalitet.
- SMALL støtter bare automitigering, det vil si automatisk start/stopp av vasking ved angrep. Varsler ved start og stopp sendes automatisk via e-post, uten personlig tilbakemelding.
- Manuell aktivering av mitigering eller tilpasning av standardprofiler kan ikke velges.
- Flere administrerte objektsprofiler, i tillegg til de som er inkludert i basistjenesten, kan legges til.

1.3.3 Funksjonsoversikt

Oversikt over forskjellen på pakkene:

		Small	Standard
Tilgang	**Begrensning av høyeste båndbredde**	**300 Mbit/s**	**10 Gbit/s**
Grunnbeskyttelse	**Emergency Protection (Nødstilfeller)**	○	○
	Fellesprofil	●	●
	IP-lokasjonsfilter	○	●
	Hvitelisting	○	●
Utvidet beskyttelse	**Antall spesifikke profiler inkludert**	**2**	**5**
	Maks. ant. IP-adresser per profil	**5**	**-**
	Maks. ant. IP-adresser som vaskes samtidig	**10**	**32**

	Bruk av blandede (kundetilpassede) profiler	**N/A**	●
Kundekommunikasjon	**Telia ringer ved angrepshåndtering**	**N/A**	●
Rapportering	**Omfang**	**Begrenset**	**Full**
	Hyppighet	**Måned**	**Uke**

●= Grunnfunksjon inngår

o = Tilvalg

N/A = Ikke tilgjengelig

1.4 Tilleggsfunksjoner

Følgende alternativer tilbys for å imøtekomme kundens spesifikke behov for økt funksjonalitet i tjenesten.

Funksjon	Beskrivelse
Emergency Protection (Nødbeskyttelse)	For organisasjoner som ikke har DDoS-beskyttelse og blir utsatt for et overbelastningsangrep, kan Telia DDoS Emergency Protection raskt gi full beskyttelse til en permanent og tilpasset DDoS beskyttelse er implementert. Automitigering og en standardisert fellesprofil blir aktivert i løpet av 2 timer etter godkjent ordre. Funksjonen er aktiv (1) uke fra aktivering eller til full DDoS beskyttelse (Standard/Small) er levert.
Utvidelse, flere objektsprofiler (MO)	Flere objektsprofiler i tillegg til de som er inkludert i grunnfunksjonaliteten.

1.5 Teknisk beskrivelse

Som kunde av Telia DDoS Protection vil du motta full støtte fra den ekspertisen som Telia har innen sikkerhet, og dra nytte av vår kraftige og avanserte infrastruktur for å kunne identifisere, spore og bekjempe angrep.

Tjenesten inkluderer all nødvendig maskinvare, teknologi og funksjonalitet for å levere DDoS-beskyttelse til kunden. Telia eier plattformen og er ansvarlig for vedlikehold. Den er basert på standardiserte teknologier og har høye krav til sikkerhet og tilgjengelighet.

Funksjon	Beskrivelse
Detektering	Den grunnleggende beskyttelsen baseres på fellesprofilen som inngår som standard. Med automitigering og forhåndsdefinerte deteksjonsmaler oppnås en grunnleggende helautomatisk beskyttelse mot volumetriske angrep mot kundens offentlige IP-adresser og vertsmaskiner. For ytterligere å forbedre beskyttelsen og oppnå en enda mer treffsikker mitigering, kan man for eksempel velge spesifikke profiler som HTTP, SIP, SMTP, DNS-servere eller Client Filter (Brannmur, utside). Detektering kan konfigureres for både IPv4- og IPv6-trafikk.
Mitigering (Vasking)	Ved aktivering blir innkommende trafikk mot kundens angrepne IP-adresser/vertsmaskiner rutet om til å gå gjennom vår kraftige nettverksbaserte tjenesteplattform. Der vaskes trafikken før den rutes videre til kundens miljø. Ved behov finnes det mulighet for å begrense trafikken fra ulike land og antallet TCP-sesjoner. Mitigeringstid for "normal" mitigering inngår uten ekstra kostnad. Den grunnleggende konfigurasjonen er at plattformen automatisk aktiverer vasking (såkalt "automitigering") i forbindelse med et identifisert angrep. For volumetriske angrep starter dette vanligvis i løpet av 30–180 sekunder, avhengig av angrepstype og -mål. For kunder med Standard-pakken, er det også mulig å be om manuell mitigering når et mistenkt angrepet detekteres. Av sikkerhetsmessige årsaker krever dette en prosedyre som innebefatter tilbakeringing til autentisert person hos kunden før mitigering kan igangsettes og dette øker den garanterte responstiden til maksimalt 30 minutter innenfor avtalt servicetid. Mitigering kan konfigureres for både IPv4- og IPv6-trafik.
Hvitelisting	All innkommende trafikk fra en pålitelig/sikker ekstern IP-adresse overføres uten vask, uavhengige av angrep. Det vil si at innkommende trafikk fra disse kildene aldri blir mitigert, men følger normal trafikkvei.
Rapportering	Angrepsoppdateringer: Ved innledende/pågående/avsluttet angrep sender Telia statusinformasjon via e-post til forhåndsbestemte mottakere. Statistikkrapporter: Statistikkrapporter med informasjon om trafikkmønster distribueres via e-post til forhåndsbestemte mottakere.

	• DDoS Emergency: Ingen • DDoS Small: Månedlig i grunnversjon • DDoS Standard: Ukentlig i fullversjon

1.6 Kundegrensesnitt

Kunden har to kanaler for kontakt med Telia når det gjelder DDoS-tjenesten spesifikt. Begge kanalene sikrer identiteten gjennom separering fra Telias andre kanaler, og det stilles krav til kundespesifikk kontroll-ID.

Telefon: Dedikert telefonlinje for DDoS-Kunder.

Webskjema: Enkelt/raskt grensesnitt for endringsbestillinger

1.7 Servicedesk

Kunden kan kontakte Telia hele døgnet, syv dager i uken for feilmelding, via telefon eller webportalen.

Ved å kontakte Servicedesk via telefon, får man to valg:

(1) Feilmelding

(2) Fakturaspørsmål (hverdager 8–16)

Feil som medfører driftsproblemer håndteres i henhold til SLA.

1.8 Overvåkning

Telia er ansvarlig for installering og drift av løsningen. Overvåking skjer døgnet rundt, alle dager. Løsningen produseres i Telias sikkerhetsklassifiserte driftsmiljø.

Telia er ansvarlig for og oppdaterer plattformen/tjenesten kontinuerlig for å opprettholde høy funksjonalitet, tilgjengelighet og sikkerhet.

2 Levering

2.1 Oppstartsmøte

Før bestilling og levering starter, gjennomfører Telia et oppstartsmøte med kunden for å informere om tjenesten og fremfor alt hjelpe kunden med å optimalisere konfigurasjonen av DDoS-beskyttelsen fra starten av.

2.2 Bestilling

For å bestille Telia DDoS Protection fyller kunden ut et skjema som sendes til Telia.

Telia kontakter kunden for å verifisere konfigurasjonsgrunnlaget som brukes til å sette opp kundespesifikke detaljer.

Hvis en endringsbestilling sendes til Telia etter at bestillingen er godkjent, kan dette påvirke leveringstiden.

Telia DDoS Emergency Protection bestilles hos Servicedesk, alternativt Customer Management Center som må godkjenne kundekontoen og innhente detaljer om nettet som skal beskyttes.

2.3 Levering

Når all informasjon om løsningskonfigurasjonen er tilgjengelig og godkjent av kunden, starter selve installasjonen. Ved levering av Telia DDoS Protection inngår totalansvar for installasjon og konfigurasjon. Når levering er fullført og leveransegodkjenning er oppnådd, vil avtalen begynne å gjelde og kunden vil da ha tilgang til support for tjenesten og motta rapporter.

Hvis levering ikke er fullført på grunn av ufullstendig informasjon fra kunden, begynner avtalen likevel å gjelde senest to måneder etter mottatt ordre.

Når konfigurasjonen er fullført, sendes en bekreftelsesmelding til kundens utpekte kontaktperson med informasjon om tjenesten og kontroll-ID for kontakt med Telia.

2.4 Leveringstid

Leveringstid for kundens opprinnelige løsning og endringer bestilt gjennom selger, fremgår av ordrebekreftelsen etter at kunden har sendt en fullstendig ordre.

For Telia DDoS Emergency Protection aktiveres tjenesten normalt innen 2 timer etter den godkjente bestillingen.

3 Øvrig

For fullstendig informasjon om Telia DDoS Protection, se Funksjonsbeskrivelse og Tjenestespesifikasjon