DDoS-bescherming

Een DDoS-aanval (Distributed Denial of Service) is een cyberaanval waarbij een grote hoeveelheid verkeer, meestal afkomstig van meerdere geïnfecteerde computers of apparaten, gericht wordt op een specifieke website, server of online dienst. Het doel van een DDoS-aanval is om de normale werking van het doelwit te verstoren of zelfs volledig te laten crashen. Ook veel verkeer naar een (willekeurig) IP-adres van een instelling, zelfs als dit niet in gebruik is, kan voor overlast zorgen tot een volledige volle aansluiting.

Instellingen hebben regelmatig te maken met DDoS-aanvallen. SURFcert is voortdurend actief om de overlast van deze aanvallen te minimaliseren, zodat instellingen beter beschermd zijn.

> **Lig je onder aanval?**
>
> Neem dan contact op met SURFcert dat 24/7 bereikbaar is op: +31 6 22 92 35 64

SURFcert helpt bij het voorkomen en onschadelijk maken van aanvallen

SURFcert helpt instellingen bij het analyseren en neutraliseren van diverse soorten DDoS-aanvallen. Om de impact van aanvallen op voorhand zo veel mogelijk te minimaliseren, bieden we de volgende anti-DDoS-middelen aan:

- **DDoS filter**
- **DDoS auto-mitigatie**

Instellingen hebben de mogelijkheid om deze anti-DDoS-middelen zelf aan en/of uit te zetten via het netwerkdashboard van SURF. **SURFcert raadt aan om het DDoS filter en de DDoS auto-mitigatie standaard actief te houden!** Alleen in bijzondere gevallen kan de auto-mitigatie voor false-positives zorgen. Denk bijvoorbeeld aan het gebruik van grootschalige netwerk performance testen (bijv. PerfSonar).

Hieronder staat beschreven wat het DDoS filter en DDoS auto-mitigatie precies inhouden en hoe ze ingezet kunnen worden.

DDoS-filter

Het DDoS-filter omvat doelgerichte netwerkfilters in het SURF-netwerk die bescherming bieden tegen de meest voorkomende DDoS-aanvallen. Met behulp van deze filters wordt een maximum throughput ingesteld op een aantal protocollen die vaak worden misbruikt bij DDoS-aanvallen. Het gaat hier om ongeveer 10 verschillende protocollen en enkel om UDP verkeer.

Hoe werkt het DDoS filter?

1. **Mitigatie:** Een filter staat standaard ingeschakeld op de netwerkaansluiting, waarbij de throughput van kwaadaardig verkeer wordt beperkt, terwijl ander legitiem verkeer ongehinderd door kan gaan.
    a. Het filter bevat bijvoorbeeld een regel die het inkomend DNS-verkeer (UDP source poort 53) beperkt tot 50 Mbps. Normaal meer dan voldoende voor dat protocol. In een aantal gevallen is er bovendien ook nog een uitzondering gemaakt voor "vertrouwde" bronnen. Zoals bijvoorbeeld de resolvers van SURF.

Om het DDoS filter aan of uit te zetten, heb je één van de volgende rollen nodig in het SURF-netwerkdashboard (zie ook de wiki van SURF Netwerkdashboard):

- Infraverantwoordelijke
- Beveiligingsverantwoordelijke

Zodra je de juiste rol hebt ga je naar het SURF netwerkdashboard

1. Klik op de **'SURFcert'-tegel** en ga daarna naar het **'DDoS-bescherming' tabblad**.
2. Activeer/deactiveer vervolgens het DDoS filter voor de gewenste netwerkaansluitingen onder de sectie **'DDoS filter'**.

Het aan- of uitzetten geeft geen onderbrekingen op de verbinding en kan dus op elk moment gebeuren.

DDoS auto-mitigatie

Voor de meer geavanceerde DDoS-aanvallen maakt SURFcert gebruik van een auto-mitigatie oplossing. Deze oplossing maakt gebruik van real-time DDoS-detectie en mitigatie om aanvallen te identificeren en ze onmiddellijk te blokkeren voordat ze het netwerk kunnen verstoren. Het doel is om de impact van DDoS-aanvallen te minimaliseren en ervoor te zorgen dat netwerken en applicaties beschikbaar blijven voor legitieme gebruikers. We gebruiken dit ook om het netwerk van SURF zelf te beschermen tegen (grootschalige) DDoS-aanvallen.

Hoe werkt DDoS auto-mitigatie?

1. **Detectie:** Het systeem analyseert al het netwerkverkeer dat het netwerk van SURF binnenkomt en identificeert verdachte patronen die kunnen duiden op een DDoS-aanval.
2. **Analyse:** Zodra een potentieel gevaarlijke activiteit is gedetecteerd, analyseert het systeem de aard en omvang van de aanval om de juiste tegenmaatregelen te nemen.
3. **Mitigatie:** Het systeem past vervolgens automatisch verkeersfilters toe om het kwaadaardige verkeer te isoleren en te blokkeren, terwijl het legitieme verkeer ongehinderd door kan gaan.
4. **Real-time respons:** Het hele proces van detectie en mitigatie gebeurt in real-time, waardoor de reactie op DDoS-aanvallen onmiddellijk is.

Om DDoS auto-mitigatie aan of uit te zetten, heb je één van de volgende rollen nodig in het SURF-netwerkdashboard (zie ook de wiki van SURF Netwerkdashboard):

- Infraverantwoordelijke
- Beveiligingsverantwoordelijke

Zodra je de juiste rol hebt ga je naar het SURF netwerkdashboard

1. Klik op de **'SURFcert'-tegel** en ga daarna naar het **'DDoS-bescherming' tabblad**.
2. Activeer/deactiveer vervolgens de DDoS auto-mitigatie voor de gewenste IP-reeksen onder de sectie **'DDoS auto-mitigatie'**

Het aan- of uitzetten geeft geen onderbrekingen op de verbinding en kan dus op elk moment gebeuren.

Wat gebeurt er als een instelling onder een DDoS-aanval komt te liggen?

SURFcert houdt voortdurend het SURF-netwerk in de gaten om DDoS-aanvallen te detecteren. In verreweg de meeste gevallen worden aanvallen automatisch gedetecteerd en afgevangen als de instelling gebruik maakt van het DDoS-filter en de DDoS auto-mitigatie oplossing. SURFcert volgt de volgende stappen wanneer een aanval is gedetecteerd:

1. SURFcert analyseert de aanval en controleert of de DDoS wordt afgevangen door het DDoS filter of de auto-mitigatie oplossing.
2. Indien een DDoS-aanval langdurig is (langer dan 10 minuten) en van grote omvang (meer dan 30% van de aansluitingscapaciteit) is, neemt SURFcert contact op met de instelling.
    a. Hierbij wordt aangegeven of het DDoS-filter en de DDoS auto-mitigatie actief zijn en of deze de aanval hebben gemitigeerd.
3. Samen met de instelling wordt er eventueel gekeken naar een oplossing als het DDoS-filter en de DDoS auto-mitigatie geen oplossing bieden.

Applicatie laag DDoS-aanvallen

Applicatie laag DDoS-aanvallen zijn een vorm van DDoS-aanvallen die zich richten op de applicatielaag van een netwerk. In tegenstelling tot traditionele DDoS-aanvallen die zich richten op het overweldigen van netwerkbandbreedte of serverbronnen, richten applicatie DDoS-aanvallen zich op het uitbuiten van kwetsbaarheden in applicaties of diensten om ze te overbelasten.

Hier zijn enkele kenmerken van applicatie DDoS-aanvallen:

- Focus op applicaties: Deze aanvallen zijn gericht op specifieke applicaties, zoals webapplicaties, API's, DNS-servers, e-commerce platforms, en andere diensten die toegankelijk zijn via internet.
- Complexiteit: Applicatie DDoS-aanvallen kunnen complexer zijn dan traditionele DDoS-aanvallen omdat ze vaak misbruik maken van de logica van de applicatie om de verwerkingscapaciteit te overweldigen.
- Lage bandbreedte vereist: In tegenstelling tot volumetrische DDoS-aanvallen hebben applicatie DDoS-aanvallen niet altijd enorme bandbreedte nodig om een impact te hebben.
- Doelgericht: Applicatie DDoS-aanvallen kunnen zich op specifieke functies of onderdelen van een applicatie richten om de prestaties ervan te verstoren. Bijvoorbeeld, ze kunnen zich richten op het uitvoeren van intensieve databasequeries, formulieren of authenticatieverzoeken.
- Lastiger te detecteren: Omdat applicatie DDoS-aanvallen lijken op legitiem verkeer, kunnen ze moeilijker te detecteren zijn in vergelijking met andere DDoS-aanvallen.

Om bescherming te bieden tegen applicatie DDoS-aanvallen, moeten instellingen applicatiefirewalls en andere geavanceerde beveiligingsmechanismen implementeren die verdacht verkeer kunnen herkennen en filteren. SURFcert biedt namelijk geen automatische bescherming tegen alle soorten DDoS-aanvallen, maar we kunnen wel advies geven over hoe hiermee om te gaan.

Wat kun je zelf doen?

Maak gebruik van het DDoS-filter en DDoS auto-mitigatie

Zorg ervoor dat je het DDoS-filter en de DDoS auto-mitigatie inschakelt via het netwerkdashboard!

Mocht je hierbij hulp nodig hebben of meer informatie willen over het DDoS-filter en de DDoS auto-mitigatie, neem dan contact met ons op via cert@surfcert.nl of telefonisch, zodat we je verder kunnen helpen.

Spoor de daders op!

Het technisch analyseren en onschadelijk maken van aanvallen is een deel van de oplossing. **Het is ook essentieel om de daders op te sporen**, wat helpt bij het voorkomen van toekomstige aanvallen, vooral als deze hun oorsprong vinden vanuit je eigen netwerk. Probeer daarom de veroorzakers te identificeren en, indien mogelijk, ter verantwoording te roepen, eventueel met hulp van externe experts.

Eventueel kan er aangifte worden gedaan van een DDoS-aanval bij de politie. Als je dit overweegt, is het raadzaam om eerst een afspraak te maken.

DDoS-Booters/Stressers: Hoe eenvoudig een DDoS-aanval kan worden gelanceerd

DDoS-booters, ook wel bekend als stressers of booter-services, zijn online diensten die iemand in staat stelt om op gemakkelijke wijze Distributed Denial of Service (DDoS) aanvallen uit te voeren. Met slechts een paar muisklikken kunnen individuen, soms zelfs zonder enige technische kennis, korte maar krachtige DDoS-aanvallen bestellen tegen een doelwit naar keuze. Het enige wat ze meestal nodig hebben, is een online betaling en soms een anoniem e-mailadres.

In de meeste gevallen kan er (zonder te betalen) een korte test van 5 minuten besteld worden met een zogenaamde loopback-aanval. Bij een loopback-aanval wordt het DDoS-aanvalverkeer teruggestuurd naar het eigen IP-adres van de gebruiker. Dit kan worden gebruikt om de effectiviteit van de booter-service te testen, om te zien hoeveel verkeer deze kan genereren.

SURFcert constateert regelmatig dergelijke loopback-aanvallen binnen het SURF netwerk. Wees je er daarom van bewust dat eindgebruikers binnen je eigen netwerk dit op een eenvoudige manier kunnen uitvoeren.

Zijn er kosten verbonden aan het gebruik van DDoS-bescherming?

Je betaalt niets extra voor de (D)DoS-bescherming van SURFcert. Dit maakt namelijk onderdeel uit van de reguliere dienstverlening van SURFcert en valt daarmee binnen de basisvergoeding voor Infrastructuur.