Web Acceleration & DoS Protection

Verbetert prestaties, beveiliging en beschikbaarheid van webapplicaties

Web Acceleration & DoS Protection (WADP) is door Claranet ontwikkeld voor organisaties met bedrijfskritische webapplicaties. De dienst verbetert de prestaties, beveiliging en beschikbaarheid van webapplicaties indien de achterliggende server of platform een hoge load heeft doordat het druk bezocht is, of aangevallen wordt middels een DDoS-aanval. WADP wordt geleverd vanuit de Europese Claranet datacenters en vereist geen additionele hardware of software.

Extra capaciteit = acceleratie

Worden er veel websitebezoekers verwacht in verband met een kortingsactie, marketingprogramma of seizoensinvloeden waardoor de kans bestaat dat de website traag wordt of zelfs onbereikbaar is? WADP biedt extra capaciteit zonder dat de server een upgrade nodig heeft. WADP staat op de grens tussen het Claranet-netwerk en het internet en dus vóór de website waardoor het verkeer tussen webserver en de bezoekers geoptimaliseerd wordt. Hierdoor kan de website veel sneller laden én worden servers minder zwaar belast.

Europese knooppunten

Claranet maakt voor WADP gebruik van meerdere knooppunten die zijn verdeeld over de Europese Claranet datacentra in Nederland, Duitsland, Frankrijk, Spanje, Portugal en het Verenigd Koninkrijk. Alle statische en dynamische herbruikbare content wordt transparant opgeslagen in de caching-systemen die in deze datacentra staan opgesteld. Hiermee zorgt WADP er niet alleen voor dat bedrijfskritische web-applicaties 24x7 optimaal bereikbaar blijven maar daarnaast ook versneld worden.

Content van de web-applicaties kan sneller rechtstreeks vanuit de cache worden geladen dan wanneer het vanaf de webservers wordt geleverd. Hierdoor wordt de laadtijd van de pagina of applicatie verminderd wat de gebruikerservaring verbetert. Bovendien zorgt WADP ervoor dat de inspanning die is gedaan om een hoge ranking te krijgen bij de verschillende zoekmachines wordt behouden.

"Web Acceleration & DoS Protection is voor ons een prima oplossing. We hebben een enorme stijging gehad in het aantal mensen die onze online nieuwsbrief willen ontvangen. Na het versturen van de e-mails naar onze klanten zagen we dat ons hostingplatform het moeilijk begon te krijgen. Laadtijden werden langer met een directe impact op de bezoekers. Het is bekend dat mensen online snel afhaken als een webpagina niet snel geladen wordt. Met Web Acceleration & DoS Protection wordt het overgrote deel van de content door Claranet uit de cache geleverd, en dat is zelfs nog sneller dan het elke keer uit de server te moeten ophalen. We zien nu het aantal lezers van onze nieuwsbrief verder stijgen, zonder dat het hostingplatform in de problemen komt"

Maarten Verhappen - Hoofd IT - Van Cranenbroek

claranet

Meer informatie :
claranet.nl - twitter.com/claranet_nl
Voor het maken van een afspraak :
040 - 239 3300 - verkoop@claranet.nl

Wat is een DDoS-aanval?

Het doel van een Distributed-Denial-of-Service-aanval, kortweg: een DDoS-aanval of DoS, is het onbruikbaar maken van een service, zoals een applicatie, website of een webwinkel. Bij een succesvolle DDoS-aanval wordt het netwerk, systeem of applicatie overbelast waardoor ze gedurende de aanval niet meer bereikbaar zijn voor legitieme bezoekers, de potentiële klanten.

Hoe werkt een DDoS-aanval?

Bij een DDoS-aanval maakt een groot aantal computers, vaak enkele duizenden vanaf veel verschillende locaties ter wereld, verbinding met één enkele server (of platform). De server is het doelwit: de daders proberen deze server traag te maken of in het ergste geval onbereikbaar te maken. Een dergelijke aanval veroorzaakt men door een server te overspoelen met webverkeer. Om dit voor elkaar te krijgen zet men vaak botnets in. Botnets is vaak een verzameling van gehackte apparatuur, zoals PC's, TV's en andere devices. Deze zijn geïnfecteerd met software die ongemerkt geïnstalleerd is door een computervirus of malware, waardoor ze door hackers kunnen worden bestuurd en ingezet worden om veel verkeer te genereren.

Wat is het doel van een DDoS-aanval?

Het doel van een DDoS-aanval, en daarmee het platleggen van een of meerdere servers, kan veelzijdig zijn: afpersing, omdat de hacker er toe in staat is, competitie tussen hackers onderling, politieke of persoonlijke doeleinden en meer. DDoS-aanvallen worden tegenwoordig veelvuldig aangeboden op de zwarte markt van het internet waarbij ook veel Do-It-Yourself-tools te koop zijn of een aanval besteld kan worden voor een paar euro per minuut. Het wordt zo steeds makkelijker om een grote DDoS-aanval uit te voeren.

Wat is het gevolg van een DDoS-aanval?

Het gevolg van een DDoS-aanval is dat de webapplicatie of server onbereikbaar is. Afhankelijk van de duur van de aanval, een typische aanval duurt 2 tot 48 uur, zijn de gevolgen legio voor de aangevallen partij:

- Ontevreden of weglopende bezoekers;
- Financiele schade doordat een webwinkel uit de lucht is;
- Kosten voor het herstellen van de schade;
- Negatieve publiciteit, reputatieschade en wantrouwen van het grote publiek.

Waarom is een DDoS-aanval moeilijk te bestrijden?

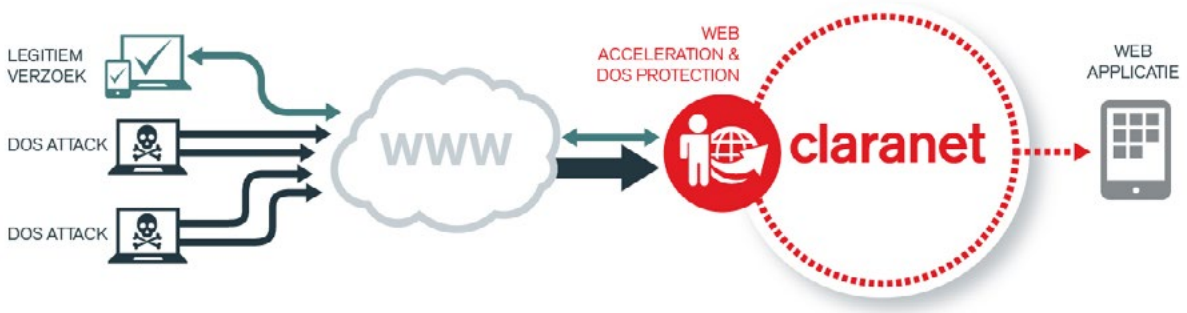
Een aanval kan op elke legitieme vorm van internetverkeer lijken. Omdat het internet duizenden legitieme toepassingen kent, is het moeilijk om legitiem verkeer te scheiden van besmet verkeer. Een DDoS-verdediging moet dan ook duizenden verschillende aanvallen kunnen afslaan die ook nog eens vanuit verschillende locaties met verschillende protocollen worden gestuurd. Aanvallers veranderen bovendien continu tactieken en methoden. Het vereist niet alleen een hoog niveau van deskundigheid om dergelijke dreigingen te kunnen afwenden, er is ook nog een forse capaciteit van het netwerk voor nodig om het ongewenste verkeer het hoofd te kunnen bieden.

Bescherming

WADP maakt gebruik van een reeks van voorzieningen die worden gecombineerd met de capaciteit van het Claranet netwerk om de meerderheid van de netwerk- en applicatie-aanvallen af te slaan voordat deze invloed hebben op de systemen en diensten van de klant. Claranet gebruikt meerdere technologieën om verkeer te filteren bij het entreepunt van het netwerk van Claranet. WADP heeft de mogelijkheid om grote hoeveelheden verkeer te verwerken om latency (vertraging) te verminderen en de prestaties van applicaties te verbeteren. Dit resulteert in een sterk verbeterde beschikbaarheid en capaciteit zonder dat het oorspronkelijke platform een upgrade nodig heeft. Zelfs als de originele webservers down zijn (de klant heeft een incident op het web-platform, problemen met het netwerk, is bezig met een migratie, etc.) kan Claranet de statische en dynamische herbruikbare content gedurende vier uur blijven leveren.

Garanties en voordelen:

Verbetering van de gebruikerservaring van de webapplicaties
Vermindering latency en verhoging van de snelheid en prestaties van de webapplicatie
Levering statische en dynamische herbruikbare inhoud als de webservers down zijn
Vermindering van (de gevolgen van) DDoS-aanvallen
Europese geografische spreiding op knooppunten met 99,99% beschikbaarheid.
Geen additionele installatie van hardware of software nodig
Eigen 24x7 support met proactieve monitoring



claranet

Meer informatie:
claranet.nl - twitter.com/claranet_nl
Voor het maken van een afspraak:
040 - 239 3300 - verkoop@claranet.nl