QUANZA GROUP B.V.

DDOS-VERDEDIGING ALS MANAGED SERVICE

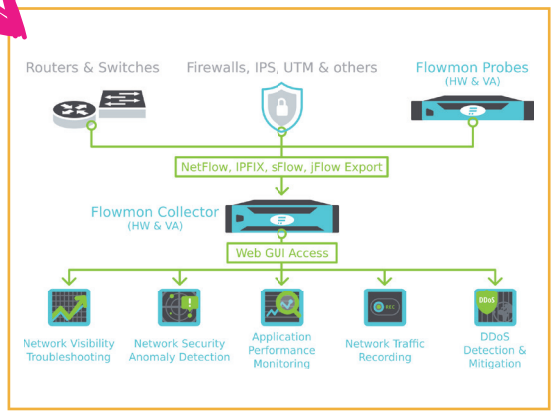
Cyberaanvallen blijven de komende jaren in aantal, complexiteit en intensiteit toenemen. Daardoor staan IT-securityverantwoordelijken dagelijks voor de uitdaging afwijkingen in het netwerkverkeer sneller te detecteren en aanvallen effectiever tegen te houden. Quanza levert bewezen effectieve cybersecurity-oplossingen als managed service, in samenwerking met Flowmon Networks, Juniper Networks en NaWas. Met als resultaat een flexibeler schaalbare verdedigingscapaciteit voor lagere operationele kosten.

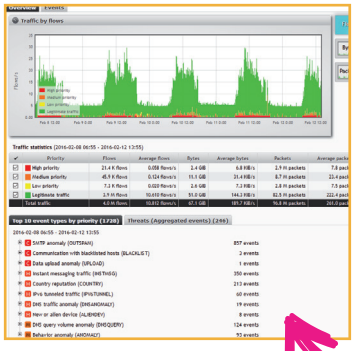
CYBERSECURITY-UITDAGINGEN

Cybercriminelen en hackers voeren aanvallen uit om de online services van organisaties te verstoren, informatie te stelen, of losgeld te incasseren. Welk motief een aanvaller ook heeft, de impact en gevolgen zijn vaak desastreus. Variërend van aanzienlijke imagoschade als gevolg van datalekken, tot grote financiële verliezen door niet beschikbare apparatuur, processen en informatie. Uit een onderzoek onder IT-securityverantwoordelijken door het Ponemon Institute blijkt een minuut downtime gemiddeld zo'n € 20.000,-- te kosten en de gemiddelde downtime 54 minuten. Vooral de intensiteit van DDoS-aanvallen neemt nog steeds gestaag toe, mede door het gebruik van slecht beveiligde IoT-apparatuur, tot een recente piek van ruim 1 Tbps (1000 Gbps). Ook andere aanvalstypes en hacktechnieken worden complexer en vaker toegepast. Behalve bedrijven en overheden zijn cloud providers regelmatig het doelwit, omdat zij de online services voor meerdere klanten hosten.

INTELLIGENTE EN VOLUMETRISCHE AANVALLEN

Criminelen gebruiken zowel intelligente als volumetrische aanvallen en combinaties van beide om bij organisaties binnen te dringen, of de serviceverlening te verstoren. Intelligente aanvallen richten zich op de bedrijfsapplicaties en -services, terwijl volumetrische aanvallen als doel hebben met brute kracht online services te verstoren. Voor de verdediging tegen elk aanvalstype is het belangrijk de volledige infrastructuur continu te monitoren op afwijkingen in de herkomst en gedrag van het verkeer. Verder moet de verdediging flexibel schaalbaar zijn en internationale standaarden ondersteunen voor het integreren van netwerkapparatuur. Omdat complete oplossingen van één leverancier moeilijk de beste securityfuncties voor alle verdedigingslinies kunnen bieden, adviseren en creëren wij altijd 'best-of-breed' maatwerkoplossingen. Een voorbeeld daarvan is de combinatie van Flowmon Networks Collector en DDoS Defender met de routers en het Software-Defined Secure Network van Juniper Networks.





NETWERKINZICHT EN AANVALSDETECTIE

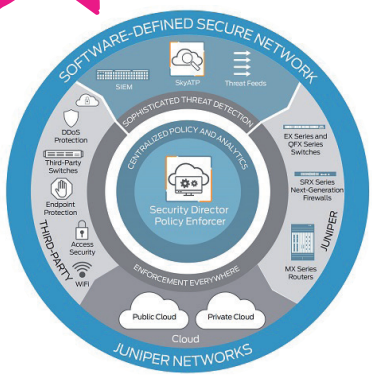
Cyberaanvallen zijn alleen snel tegen te houden als een organisatie real-time inzicht heeft in het gebruik van de totale netwerkinfrastructuur. Daarom analyseert Flowmon Network's Collector met DDoS Defender continu al het verkeer met geavanceerde telemetrie- en gedragsanalysefuncties (flowdetectie). Als gevolg daarvan is deze oplossing in staat om met een interval van slechts 30 seconden aanvallen te detecteren. Zodra verdacht verkeer het netwerk probeert te infiltreren, wordt die communicatie omgeleid naar een extern 'scrubbingcenter' totdat de betreffende aanval is afgeslagen. Verder alarmeert Flowmon Collector direct een verantwoordelijke beheerder, met belangrijke aanvalsinformatie zoals de getroffen subnetten, systemen en services. Om de detectie-effectiviteit van DDoS-aanvallen te vergroten zijn kritische segmenten, IP-apparatuur, subnetten en services indien gewenst extra te beschermen met complementaire securitytools.

OMLEIDEN EN OPSCHONEN

Juniper Networks is een wereldwijde leverancier van geautomatiseerde schaalbare netwerken. Voor het snel detecteren van cyberaanvallen moeten alle netwerkrouters en -switches flowinformatie exporteren. Bij Juniper Networks kan dat zowel via J-Flow als het gedetailleerdere ipfix-protocol. Na het omleiden van verdachte communicatie worden alleen de datapakketten die onderdeel uitmaken van een aanval tegengehouden en het legitieme verkeer na opschoning alsnog op de doelbestemmingen afgeleverd. Zonder dat applicatieservers, opslagsystemen en netwerkapparatuur geïnfecteerd of ontoegankelijk raken door overbelasting. De gezamenlijke oplossing van Flowmon Networks en Juniper Networks verdedigt de meest kritische hoge snelheid netwerkinfrastructuren op alle lagen effectief tegen elk type DDoS-aanval. Zelfs als de cybercriminelen tussentijds hun protocollen en vectoren veranderen.

CLOUDGEBASEERD COÖPERATIEF DDOS-SCRUBBINGCENTER

Een bekend voorbeeld waar de gecombineerde DDoS-oplossing van Flowmon Networks en Juniper Networks effectief wordt toegepast, is de Nationale Anti-DDoS wasstraat (NaWas) van de Stichting Nationale Beheersorganisatie Internet Providers (NBIP). Dat is een cloudgebaseerd coöperatief scrubbingcenter, waarin alleen het DDoS-verkeer er binnen enkele minuten wordt uitgefilterd. Gebouwd vanuit de visie dat een groep van deelnemers met dezelfde doelstelling sterker is dan de individuele organisaties. NaWas is al sinds 2014 operationeel en beschikt nog steeds over de grootste schaalbare capaciteit in Europa om zowel volumetrische als intelligente DDoS-aanvallen effectief tegen te houden. Quanza heeft deze oplossing in samenwerking met alle betrokken leveranciers ontworpen en geleverd en werkt sindsdien met NaWas samen voor het leveren van managed securityoplossingen tegen DDoS-aanvallen. Afhankelijk van de behoeften en wensen kan Quanza uiteraard ook een cloudgebaseerd extern scrubbingcenter voor individuele klanten realiseren op andere locaties.



MANAGED NETWERK- EN SECURITYOPLOSSINGEN

Quanza is al 17 jaar gespecialiseerd in het bedenken, bouwen, beveiligen en operationeel beheren van complete IT-infrastructuren voor Internet Service Providers, bedrijven en non-profit organisaties. Inclusief alle bijbehorende bekabeling, hardware, software en opslagcapaciteit. Op basis van alle eisen en wensen maken ervaren Quanzanen een design en de best passende oplossing op maat, die vaak tegen een vast bedrag per maand als managed service door klanten wordt gebruikt. 24/7 beheerd vanuit een eigen Network Operation Center (NOC) in Amsterdam, indien gewenst ook 24/7 bemand. Met onze managed securityservices zijn vaak interessante kostenbesparingen te realiseren in vergelijking met de 'on premise' of cloudoplossingen van andere leveranciers. Enkele bekende klanten van Quanza zijn de Amsterdam Internet Exchange, AVROTROS, Ingram Micro, KPN International, Qmusic en SURFnet.

SCHAALBAARHEID VERGROTEN EN OPEX VERLAGEN

Behalve de beste functionaliteit voor complementaire toepassingen bieden 'best-of-breed' oplossingen vaak een betere prestatie-/prijsverhouding in vergelijking met totaaloplossingen van één leverancier. Organisaties en serviceproviders die datacenters en bedrijfsnetwerken tegen DDoS-aanvallen willen beschermen met Flowmon Networks en Juniper Networks kunnen zowel hun schaalbaarheid vergroten als de operationele kosten (OPEX) verlagen. Als onafhankelijke netwerkintegrator helpen wij u graag bij het sneller detecteren en effectiever tegenhouden van alle typen cyberaanvallen met advies, ontwerp, levering, implementatie, integratie, operationeel beheer en technische ondersteuning. Daag onze Quanzanen gerust uit om de effectiviteit van Flowmon Networks en Juniper Networks' DDoS-beveiliging te bewijzen binnen uw organisatie, vanuit ons eigen NOC of de samenwerking met NaWas.

"DDoS-aanvallen zijn een serieus dagelijks probleem in de Benelux", zegt Pim van Stam van stichting NBIP. "NaWas is gebouwd vanuit de gedachte dat een groep deelnemers met dezelfde doelstelling sterker is dan elke individuele organisatie. NaWas is ook een alternatief voor ISP's, hostingproviders en andere geïnteresseerden, die niet zelf in staat zijn of voldoende kunnen investeren in effectieve DDoS-bescherming voor hun klanten."

Flowmon Networks en Juniper Networks

Flowmon Networks is de ontwikkelaar en leverancier van Flowmon, een veelgebruikte oplossing voor het monitoren van netwerkverkeer en gedragsanalyses, op basis van flowdetectie. Het bedrijf is door Gartner gepositioneerd als de enige Europese fabrikant in het segment voor Network Performance Monitoring & Diagnostics (NPM&D). Juniper Networks maakt veilige en gegarandeerde communicatie mogelijk via één IP-netwerk. Op basis van de netwerkoplossingen van het bedrijf kunnen klanten op elke schaal uiteenlopende services en applicaties ondersteunen. Providers, bedrijven, overheden en onderzoeks- en onderwijsinstellingen in de hele wereld vertrouwen op Juniper Networks om netwerken te bouwen, die zijn afgestemd op de behoeften van gebruikers, services en applicaties.

CONTACT

Quanza Group B.V. • Willem Fenengastraat 7 • 1096BL in Amsterdam
T +31 20 530 1600 • info@quanza.net • www.quanza.net • werkenbij.quanza.net