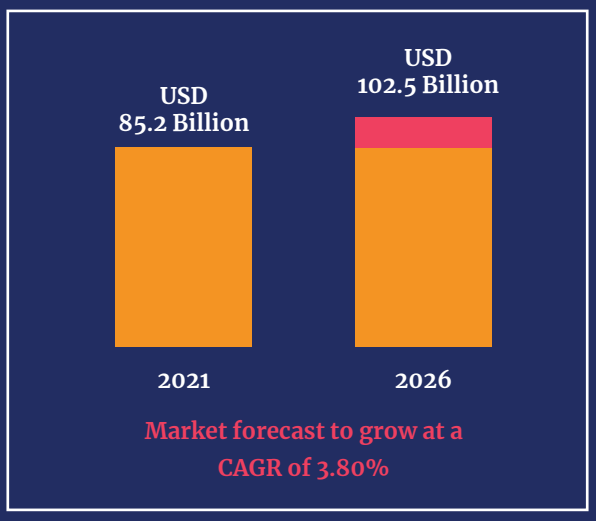
NBIP NaWas

VoIP beschermen tegen DDoS-aanvallen

Groeiende afhankelijkheid VoIP

De wereldmarkt voor VoIP-diensten is de afgelopen twintig jaar exponentieel gegroeid naar 85 miljard dollar in 2021 en blijft de komende vijf jaren doorgroeien naar ruim 100 miljard. Sinds de coronapandemie zijn veel meer mensen afhankelijk geworden van VoIP, voor alle online gesprekken en vergaderingen met collega's, businesspartners en klanten. Tegelijkertijd communiceren mensen thuis ook vaker via VoIP met familieleden en vrienden. Dat groeiend volume en een toenemende afhankelijkheid stelt VoIP-providers voor de uitdaging om de capaciteit en beschikbaarheid van hun services te verbeteren en storingen te voorkomen.

Global VolP Services Market



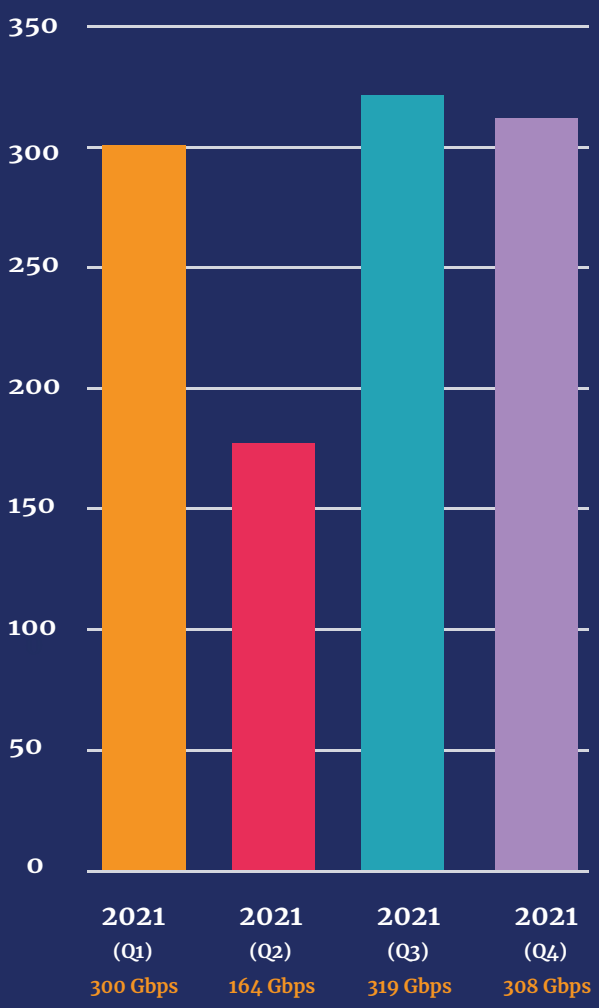
DDoS-aanvallen bedreigen VoIP

Net als alle andere Internet-services is VoIP kwetsbaar voor het toenemend aantal DDoS-aanvallen. In 2021 is alleen in Nederland al het aantal geregistreerde aanvallen gegroeid naar 2860 stuks, in vergelijking met 1610 in 2020. Ook de omvang groeide naar 319 Gbps versus 200 in 2020 en 124 Gbps in 2019, terwijl ze gemiddeld langer dan 4 uren duren. Als die DDoS-aanvallen VoIP-diensten verstoren, of hinderlijk vertragen, leidt dat zowel tot directe omzetderving als imagoschade voor een langere termijn. Momenteel wordt VoIP-verkeer minder aangevallen dan ander dataverkeer, maar de businessimpact van een VoIP-verstoring is altijd groot.

Aantal aanvallen:	Gemiddeld aantal aanvallen per dag:	Maximale grootte aanval:
700	7,6	308Gbps

bron: NBIP - Infographic - DDoS data - 2021 Q4 - NL.pdf

Maximale grootte aanval



DDoS-aanval op Britse infrastructuur

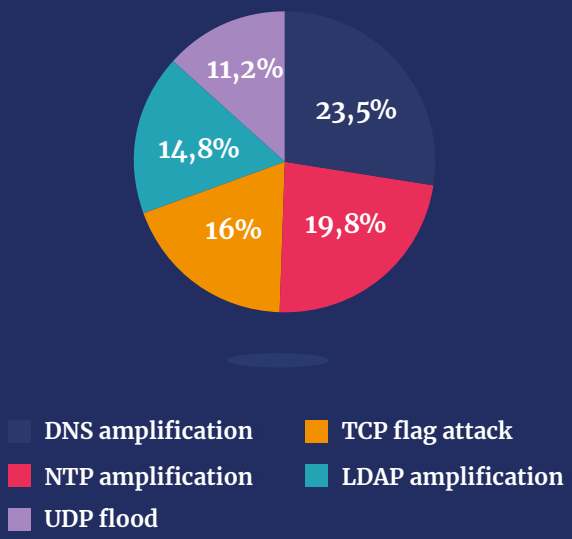
De DDoS-aanval op de Britse communicatie-infrastructuur in het najaar van 2021 was een doordringende wake-up call. Telecommanagers hebben er nachten wakker van gelegen om ervoor te zorgen dat hun werkgevers de volgende keer beter zijn voorbereid. Tijdens overleg tussen de Comms Council UK en de CCA is besloten nauwer te gaan samenwerken met de Britse regering, de National Cyber Security Centre, Ofcom en internationale agencies, om dit soort criminele activiteiten zo snel mogelijk een halt toe te roepen. Maar ook strategieën en oplossingen te bedenken die de schade beperken. NaWas kan daarbij uitkomst bieden.

VoIP-trends

Het gebruik van VoIP groeit snel vanwege de flexibel schaalbare capaciteit en eenvoud van integratie met andere IP-communicatietoepassingen. De komende jaren wordt de populariteit van VoIP verder gestuwd door het toenemend aantal glasvezelaansluitingen en de adoptie van 5G, waardoor zowel hogere snelheden als nog betere kwaliteit te garanderen zijn. Maar ook door nieuwe AI-toepassingen voor klantenservice, VoIP-support voor het snel groeiend aantal IoT-apparaten (zoals camera's) en het uitrangeren van analoge telefoonsystemen. Dat is een florissant perspectief voor alle VoIP-providers, met als keerzijde het toenemende securityrisico. Behalve het bedrijfskritische VoIP-verkeer zijn ook de achterliggende databases bijzonder waardevolle targets.

VoIP beschermen

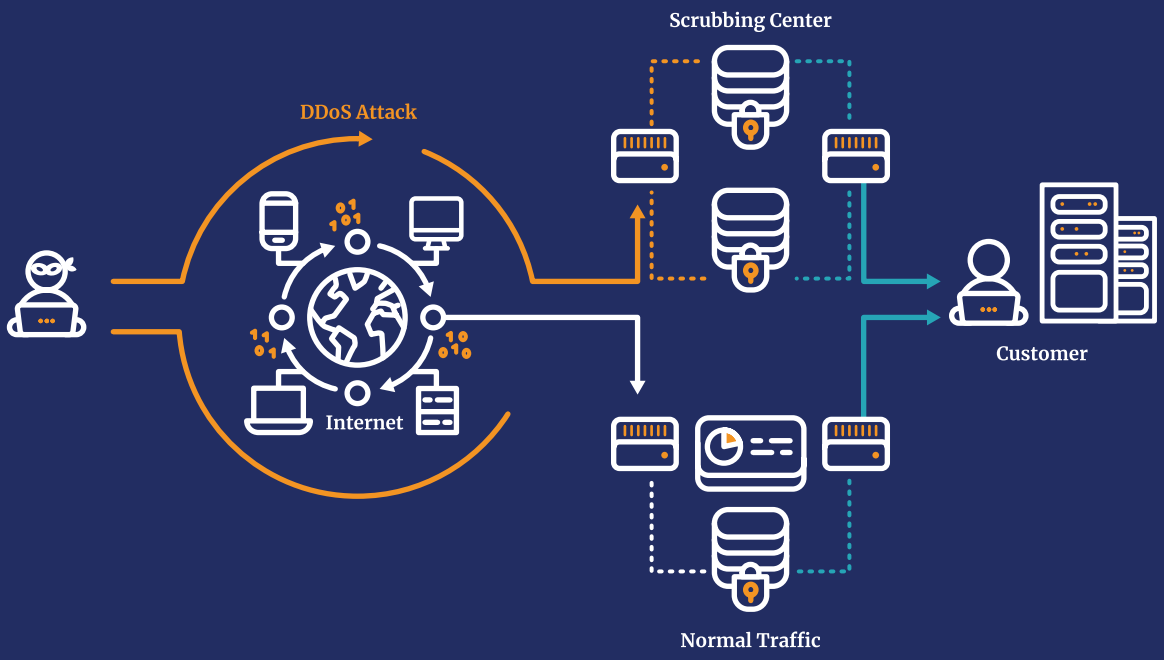
VoIP is meer UDP-verkeer dan TCP en gebruikt RTP voor de audio en SIP voor de benodigde handshaking. Natuurlijk verwerken ISP's en VoIP-providers al deze protocollen, omdat ze deel uitmaken van het totale IP-verkeer. VoIP-verkeer verschilt op enkele belangrijke punten van ander IP-verkeer, omdat het tijdkritisch (latency) en realtime is. Er mogen geen vertragingen optreden tijdens de gesprekken, waardoor VoIP bij een DDoS- aanval al snel wordt verstoord. Bij de mitigatie van een aanval moet hiermee terdege rekening worden gehouden. Een ander aspect dat meespeelt tijdens een verstoring van het VoIP-verkeer, zoals bij een DDoS- aanval, is dat gesprekken naar hulpdiensten ook verstoord kunnen worden. Dat is een extra reden om VoIP zo goed mogelijk te beschermen.



bron: NBIP - Infographic - DDoS data - 2021 Q4 - NL.pdf

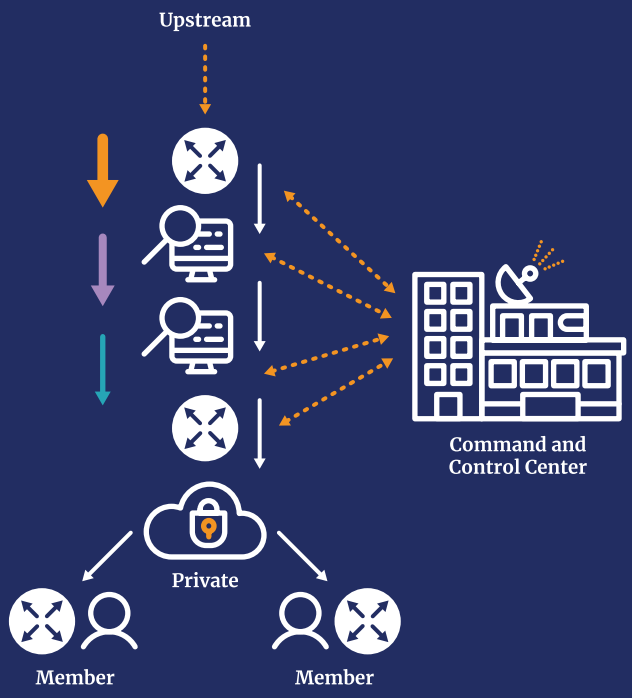
Krachten bundelen tegen DDoS-aanvallen

Net als ISP's moeten VoIP-providers de servicekwaliteit en -beschikbaarheid waarborgen en informatie van klanten beschermen. Dat kan door ieder voor zich te investeren in effectieve securityoplossingen en het onderhouden daarvan, of de krachten te bundelen via NaWas. NaWaS maakt deel uit van de non-profit organisatie Stichting NBIP, waarin al meer dan 200 ISP's zich sinds 2002 hebben verenigd voor de bescherming tegen cyberaanvallen. Een belangrijke service is het DDoS Scrubbing Center NaWas, dat ruim 6,5 miljoen domeinen en 1,5 miljoen websites beschermt met de modernste cloudgebaseerde securityoplossingen. Deze service is in veel landen in Europa en het VK beschikbaar.



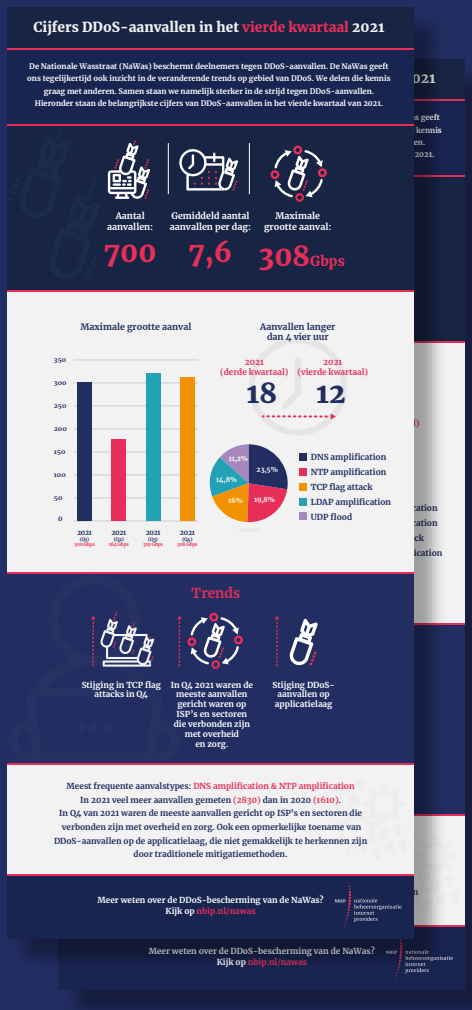
Hoe werkt NaWas?

NaWas beschermt VoIP-providers door een DDoS-aanval snel te detecteren, al het verdachte verkeer via de mitigatiestraat te wassen en daarna het schone IP-verkeer terug te leveren via een van de aangesloten Internet Exchanges. Daarvoor benut NaWas verschillende tier 1 Internet-transits en public peering op Internet Exchanges, een DDoS Scrubbing Center en failover-sites gecreëerd met securityoplossingen van verschillende leveranciers en privé- verbindingen met AMS-IX, NL-IX, Dcspine, Linx, MIX, Top-IX, Namex en NetIX. Verder benut NaWas baselines voor detectie aan de klantzijde en diverse mitigatiemethoden tijdens het omleiden en schoonwassen, om VoIP-verkeer zonder teveel latency effectief te beschermen. Nu steeds meer ISP's en VoIP-providers zich bij NaWas aansluiten neemt ook de synergie toe.



R&D en rapportages

Als non-profit organisatie voor ISP's en VoIP-providers investeren Stichting NBIP en NaWas ook in technieken voor wettelijk toegestane onderschepping en analyses van IP-verkeer. Maar ook tegen het verspreiden van onrechtmatige content via het Clean Networks Platform. De resultaten van deze investeringen, R&D en samenwerkingsinitiatieven worden regelmatig gerapporteerd en gedeeld met alle aangesloten ISP's en VoIP-providers, om samen te kunnen profiteren van de geleerde lessen en 'best practices'. Een voorbeeld daarvan is de update die wij elk kwartaal uitbrengen over alle geregistreerde DDoS-aanvallen.



Europese samenwerking

Steeds meer ISP's, VoIP-providers, leveranciers en overheden beseffen dat internationale samenwerking onmisbaar is om DDoS-aanvallen effectief te kunnen blijven tegenhouden. Daarom werkt NaWas nauw samen met een aantal Europese InternetExchanges, zoals LINX in het Verenigd Koninkrijk en MIX en NetIX in Italië. Dankzij deze marktontwikkeling in andere Europese landen blijft het aantal NaWas-partners gestaag groeien. Tenslotte werkt NaWas ook nog samen met de Nederlandse Anti-DDoS-Coalitie, om het bedrijfsleven, overheden en universiteiten meer van alle beschikbare kennis en opgedane ervaringen te laten profiteren.

Voordelen voor VoIP-providers

Net als alle aangesloten Internet Service Providers kan elke VoIP-provider via NaWas profiteren van:

- Bewezen effectieve bescherming tegen DDoS-aanvallen
- Reduceren risico's VoIP-verstoring en -vertraging
- Lagere CAPEX en OPEX voor DDoS-bescherming
- Gezamenlijke kennis en ervaring
- 24/7 support via onder andere een NOC
- Redundante setup voor multi-vendor mitigatie
- Ondersteuning bij inrichten en uitvoeren detectie, of Detectie-as-a-Service (Daas)

Ervaringen van VoIP-providers

"Speakup is als VoIP-provider regelmatig het doelwit geweest van DDoS-aanvallen", zegt Rick Sulman, CEO van Speakup. "Met NaWas van de NBIP hebben wij een effectieve oplossing om deze aanvallen te mitigeren. Het inregelen van de service op specifieke VoIP-eisen is samen met NaWas opgepakt en werkt nu uitstekend. Dankzij de samenwerking tussen Speakup en NaWas hebben beide partijen veel kennis opgedaan over het mitigeren van DDoS-aanvallen op VoIP-diensten. Wij zijn erg tevreden en hebben geen noemenswaardige onderbrekingen van onze dienstverlening meer gehad sinds de samenwerking met NaWas."

> *"Met NaWas van de NBIP hebben wij een effectieve oplossing om DDoS-aanvallen te mitigeren. Het inregelen van de service op specifieke VoIP-eisen is samen met NaWas opgepakt en werkt nu uitstekend."*
>
> *- Rick Sulman*
> *CEO van Speakup*