DYNAMX - TECHNISCHE OMSCHRIJVING DIENST XELION VOIP TELEFONIE

1. Xelion Managed VoIP – Cloud telefonie

Managed VoIP is een telefonieoplossing (ook wel bekend onder de naam Cloudtelefonie), die wordt geleverd als een dienst, in tegenstelling tot een conventionele telefonieoplossing waarbij een telefooncentrale op de klantlocatie staat. De telefooncentrale wordt namelijk in onze datacenters gehost. Er hoeft dus geen investering te worden gedaan in een centrale, uw klant betaald een bedrag per maand per gebruiker. In het premium product is het mogelijk mobiele aansluitingen deel te laten uitmaken van de bedrijfstelefooncentrale. In tegenstelling tot andere leveranciers die dit bieden is het bij deze oplossing niet nodig een mobiel abonnement af te sluiten, de bestaande mobiele abonnementen kunnen hiervoor worden gebruikt zolang het gebruikte toestel een smartphone is met als besturingssysteem IOS of Android.

Essentieel voor het functioneren van deze dienst is een goed functionerende internetverbinding tussen het toestel en de VoIP cloud server in het datacenter. Hierbij dient de router en/of firewall op een juiste wijze ingesteld te zijn. Ervaring leert dat niet alle producten hierin kunnen voorzien. In dat geval zal een firewall vervangen moeten worden voor een ander en passend product.

2. Xelion Managed VoIP Premium – Netwerk en firewall

Voor een goede werking van uw Managed VoIP account dient u alle verkeer van en naar de IP reeks(en) van de cloud voip server toe te staan in uw firewall:

In het kort:

- SIP ALG / SIP helper uitschakelen in de router en/of modem
- Geen poort forwardings voor SIP of RTP instellen in de router en/of modem
- Poort forwardings voor management afschermen d.m.v. een firewall

Bellen over IP en veiligheid:

Goed, we gaan bellen over IP oftewel gebruik maken van (Managed) VoIP. Even aansluiten en klaar zou je denken. Toch zijn er een aantal zaken die aandacht nodig hebben voordat we onbezorgd en veilig kunnen bellen over onze internet verbinding.

We gaan kijken naar de veiligheid, niemand wil geconfronteerd worden met onverwachte hoge telefoon rekening als het gevolg van een hack van de PaBX of misbruik van een IP toestel. Ook moet men de ICT kosten om een probleem te onderzoeken en op te lossen niet onderschatten.

Verder gaan we kijken naar de juiste firewall en NAT instellingen. Veel vage VoIP problemen komen voort uit ongeschikte apparatuur of onjuist ingestelde apparatuur, zoals bijvoorbeeld een modem / router of firewall.

NAT:

Een VoIP gesprek kan soms uren duren. NAT is hier niet altijd goed op ingesteld. Zogenaamde NAT helpers of een SIP ALG doet soms meer kwaad dan goed. Die schakelen we dan ook - indien mogelijk - als eerste uit.

Managed VoIP achter een router / modem / firewall:

Plaatsen we onze VoIP apparatuur achter een modem / router of firewall dan krijgen we vaak te maken met NAPT. In ons kenniscentrum hebben we een handleidingen gemaakt van door ons geteste en gecertificeerde apparatuur. We bevelen het aan om deze apparatuur in te zetten en deze in te stellen volgens de richtlijnen in het kenniscentrum. Enerzijds voorkomt dit de meest voorkomende VoIP problemen en anderzijds kunnen we nieuw inzichten of updates centraal doorgeven. Uit de praktijk blijkt dus dat niet alle routers even goed werken in combinatie met VoIP. Om er zeker van te zijn dat u een juiste netwerk setup hanteert, kunt u altijd contact met ons opnemen zodat wij u kunnen adviseren over een geschikt producten welke door ons gecertificeerd is.

Meest voorkomende vormen van misbruik:

Hieronder meer over de meest voorkomende vormen van VoIP hacks of telefonie fraude. Meestal probeert men toegang te krijgen tot een IP toestel of een PaBX om geld te verdienen. Men doet dit door zoveel mogelijk gesprekken op te zetten naar dure betaalnummers (premium rate numbers). Iedere call levert de eigenaar van het nummer (via een omweg altijd de hacker zelf) geld op. Een minder voorkomende vorm van telefonie fraude is het frustreren of plat leggen van telefonie verkeer, dan wel afluisteren van telefonieverkeer. De reden hiervoor mag je zelf bedenken...

De meest voorkomende vormen van misbruik zijn:

- de webinterface van de PaBX of het VoIP toestel is via internet voor iedereen bereikbaar. Ondanks username en wachtwoord weet men toch toegang te krijgen tot de PaBX / VoIP toestel. Veelal weet men ook alle accountgegevens te bemachtigen
- men heeft de accountgegevens in handen gekregen en zet vanaf een andere locatie gesprekken op met deze account
- een persoon binnen het netwerk zet zonder toestemming gesprekken op naar dure betaalnummers
- een virus of worm zoekt contact met de PaBX binnen het netwerk en functioneert als proxy naar de hacker toe
- ipv6 is nog actief in het netwerk of op de PaBX. Men denkt NAPT en firewall goed te hebben ingericht maar er zijn geen maatregelen genomen voor ipv6

Welke maatregelen nemen wij tegen fraude:

- naast gebruik te maken van een sterke username en password filteren we ook op IP adres
- inlogpogingen met een onbekende username of password worden tijdelijk geblokkeerd
- per account worden beperkingen opgelegd voor het uitgaande belverkeer, een zogenaamde threshold. Indien men buitensporig meer belverkeer genereert dan gemiddeld dan wordt een account uitgaand geblokkeerd
- verkeer naar premium rate numbers en bestemmingen die vaak worden gebruikt voor fraude kunnen worden geblokkeerd
- we maken klanten en resellers bewust van de risico's en geven trainingen aan technisch personeel

3. Xelion Managed VoIP – Autoprovisioning

Managed VoIP Premium maakt voor het autoprovisionen van IP telefoons gebruik van het TFTP protocol.

Protocol	Provisioning URL
TFTP	tftp://xelion-01.ictprovider.nl

Voordat een toestel zijn configuratie op kan halen via autoprovisioning zal het IP adres waar het toestel vandaan komt gewhitelist moeten worden in de Xelion firewall. Dit kan worden gedaan via de ViPro portal.
Navigeer naar de betreffende Managed VoIP order en klik op het tabblad “Details”. Vul bij het veld “IP whitelist” het publieke IP adres in waar het IP toestel zijn provision verzoek vandaan verstuurd.

Let op: van sommige routers / modems is bekend dat zij TFTP verkeer niet goed kunnen NAT-en naar het interne netwerk. In die gevallen zal het probleem moeten worden opgelost in de router / modem of zullen de toestellen handmatig geconfigureerd moeten worden.

4. Fair Use

Fair Use bepalingen bij onbeperkt bellen

Klant is ermee bekend dat de capaciteit van het netwerk niet onbeperkt is, waardoor overmatig gebruik door de klant van onbeperkt bellen overbelasting van het netwerk en hinder bij andere gebruikers tot gevolg kan hebben. De klant mag daarom niet dusdanig overmatig gebruik maken van, of verkeer genereren op het netwerk, dat dit andere gebruikers van het netwerk hindert of het netwerk overbelast. Als zich een dergelijke situatie voordoet, informeren wij u over uw overtreding van deze bepaling en maakt u hieraan onmiddellijk een einde. Indien u niet aan deze verplichting voldoet, kunnen wij maatregelen nemen, zonder ingebrekestelling. Deze maatregelen kunnen onder meer bestaan uit het, al dan niet tijdelijk, met onmiddellijke ingang beperken van de toegang tot, dan wel het opschorten, beperken of beëindigen van de levering van onbeperkt bellen, het abonnement onbeperkt bellen beëindigen en met terugwerkende kracht de additioneel gemaakte gesprekskosten tegen de reguliere tarieven in rekening te brengen.

De klant zal geen excessief gebruikmaken van onbeperkt bellen. Van excessief gebruik is sprake als de klant over een langere periode beduidend meer dan gemiddeld gebruik maakt van onbeperkt bellen, bijvoorbeeld, maar niet uitsluitend, door het open laten staan van de telefoonverbinding en/of het voeren van grote aantallen kort durende telefoongesprekken binnen een kort tijdsbestek als gevolg waarvan het netwerk of andere systemen dan wel derden hinder ondervinden. Als zich een dergelijke situatie voordoet, informeren wij u over uw overtreding van deze bepaling en maakt u hieraan onmiddellijk een einde. Indien niet aan deze verplichting voldoet, kunnen

wij maatregelen nemen, zonder ingebrekestelling. Deze maatregelen kunnen onder meer bestaan uit het, al dan niet tijdelijk, met onmiddellijke ingang beperken van de toegang tot, dan wel het opschorten, beperken of beëindigen van de levering van onbeperkt bellen, het abonnement onbeperkt bellen beëindigen en met terugwerkende kracht de additioneel gemaakte gesprekskosten tegen de reguliere tarieven in rekening te brengen.

De beoordeling of er sprake is van overlast, excessief gebruik of misbruik is geheel aan ons. Bij die beoordeling zullen wij de gemiddelde klant als uitgangspunt nemen.

5. Xelion Gespreksopname

De premium Managed VoIP oplossing van ViPro kent de mogelijkheid om gesprekken op te nemen.

Standaard is deze functionaliteit uitgeschakeld, maar deze kan desgewenst worden geactiveerd; dit kan tijdens het orderproces in de toetsing of naderhand door dit te vragen via het opmerkingenveld in de ordertool.

De volgende opties zijn beschikbaar:

1. Standaard staat gespreksopname uit
2. Retentie* 30 dagen gratis
3. Retentie* 90 dagen voor een vast bedrag per user per maand
4. Retentie* 365 dagen voor een vast bedrag per user per maand

Voor de betaalde opties bestaat tevens de mogelijkheid een export te ontvangen. Bij deze export ontvangt u zowel de opnames als een overzicht van de gesprekken in een spreadsheet voorzien van gespreks-ID's zodat u de opnames makkelijk terug kunt vinden. De kosten voor deze export worden op basis van regie in rekening gebracht.

Wanneer u gespreksopname bij uw klant wil inzetten, hou er dan wel rekening mee dat de gekozen oplossing voor alle accounts wordt toegepast. Het is dus niet mogelijk voor bepaalde accounts gespreksopname aan te zetten.

* Retentie betreft het aantal dagen dat een opname bewaard blijft.

Let op:

In het kader van wetgeving op het gebied van privacy bestaan er regels voor het opnemen van gesprekken. Generiek kan gesteld worden dat, wanneer een gesprek wordt opgenomen, alle betrokken partijen hier vooraf van op de hoogte dienen te zijn.