Koldingweg 19-1
9723 HL Groningen

Postbus 5236
9700 GE Groningen

T (050) 820 00 00
F (050) 820 00 08
E callvoip@callvoip.nl
W www.callvoiptelefonie.nl

VoIP Troubleshooting Guide

v261116MT

In deze handleiding vindt u een aantal vragen en antwoorden met betrekking tot het optimaal laten werken van uw Simmpl telefoonverbinding. Om via internet te kunnen bellen is een werkende internetverbinding noodzakelijk. Ook als uw internetverbinding verder goed werkt, kan het zo zijn dat uw router bepaalde poorten blokkeert, die voor VoIP-verkeer noodzakelijk zijn. In dit document vindt u enkele suggesties.
Niet alle netwerk-apparatuur is goed instelbaar voor VoIP. Mocht blijken dat uw huidige apparatuur niet of onvoldoende presteren om VoIP te kunnen gebruiken, dan adviseren wij u graag over alternatieven.

Deze informatie wordt u aangeboden door:

CallvoipTelefonie
Koldingweg 19-1
9723 HL GRONINGEN

T: 050 – 820 00 00
F: 050 – 820 00 08

@: callvoip@callvoip.nl
W: www.callvoiptelefonie.nl

ING BANK 5041280
IBAN NL66INGB0005041280
BIC INGBNL2A
KVK 02066541
BTW NL1041.63.252.B01

Inhoud

Algemene troubleshooting vragenlijst

Als u problemen ondervindt met de ingebruikname van uw Simmpl VoIP-accounts zullen wij u altijd vragen enkele eerste checks uit te voeren. Deze checks dienen om te bepalen waar zich het probleem bevindt.

1. **Mijn VoIP-apparaat (telefoon, fritzbox) registreert niet**
   U heeft een VoIP-apparaat, u heeft uw Callvoip klantgegevensformulier bij de hand en u bent op de Simmpl telefooncentrale ingelogd. Wat u ook doet, de VoIP-account registreert niet; het VoIP-apparaat blijft zeggen [**not registered**].
   Enkele suggesties:
   - heeft u een werkende internetverbinding?
   - probeert u toch eens uit te bellen; hoort u een (fout-)melding of bepaalde toon?

   Als dit niet het geval is, ga dan door met de onderstaande punten.

2. **Heeft u de juiste gegevens in de juiste velden ingevuld?**
   Voor een aantal merken en modellen toestellen is **provisioning** mogelijk (Yealink, Gigaset, etc.). Als provisioning beschikbaar is, maakt u dan daarvan gebruik om te beschikken over de geadviseerde instellingen.

   Voor alle overige toestellen:
   Voor het registreren van een VoIP-account in een verder VoIP-toegankelijk netwerk heeft u doorgaans slechts drie gegevens nodig:
   - uw SIP gebruikersnaam → deze vindt u op de Simmpl telefooncentrale
   - uw SIP-wachtwoord → deze vindt u op de Simmpl telefooncentrale
   - het SIP-serveradres: **pbx.callvoip.nl**
   - vermeld de sip-server ook in het veld proxyserver

3. **Is het VoIP-apparaat goed geconfigureerd?**
   Een eerste check is om te controleren of u het VoIP-apparaat (FRITZ!Box, IP-telefoon, etc.) goed heeft geconfigureerd. Zie ook punt 2. Zie bijvoorbeeld de handleidingen op de Simmpl supportpagina: www.simmpl.nl/support.
   U kunt op de Simmpl telefooncentrale inloggen en zien of u het toestel daar geregistreerd staat.

4. **Is het VoIP-apparaat defect?**
   Er bestaat een (zeer) kleine kans dat uw VoIP-apparaat (FRITZ!Box, IP-telefoon, etc.) defect is. Of een apparaat defect is kunt u bv. vaststellen als alle lampjes van het product uit zijn (voeding defect), als u niet meer kunt inloggen en als het apparaat bv. elders (in een ander netwerk) ook niet werkt.

5. Controleer in ieder geval:
   - of het product is voorzien van een recente / de laatste firmware
   - of het helpt indien u het productreset naar fabrieksinstellingen

   Bij IP DECT systemen is het ook mogelijk dat een handset het contact met de basis heeft verloren. Probeer de handset dan opnieuw op de basis aan te melden. Als dit niet lukt en er brandt geen lampje op de basis, dan is mogelijk de voeding van het basisstation defect.

   Als het apparaat wel werkt en aan is, maar de VoIP-account niet registreert, dan is het niet waarschijnlijk dat het apparaat defect is, maar het ligt aan de wijze waarop het apparaat op uw netwerk is aangesloten en/of aan de signalen die de router(s) in het netwerk wel of niet doorlaten.
   Probeert u dan eens:
   - het apparaat op een andere plaats in het netwerk aan te sluiten
   - bij voorkeur zo DICHT mogelijk achter uw ADSL- of kabelmodem

6. **Ligt het probleem in uw netwerk?**
   Als u heeft geverifieerd dat uw VoIP-apparatuur goed is geconfigureerd, u een werkende internetverbinding heeft, de apparatuur niet defect is, maar toch nog niet werkt met uw Simmpl-account, test dan of het apparaat in een andere plaats in uw netwerk wel goed functioneert. Zet de IP telefoon bv. rechtstreeks achter uw modem/router en vermijd zo switches en bekabeling die mogelijk een probleem opleveren. Blijft het probleem, probeer dan om de IP telefoon of VoIP-adapter mee te nemen naar een andere locatie (ander netwerk, bv. thuis of juist op kantoor). Functioneert het apparaat daar wel, dan weet u dat het probleem zich ergens in uw netwerk voordoet.

   In 75% van de gevallen worden problemen veroorzaakt door de netwerkrouter. De modem-routers van het merk/type Experiabox (SpeedTouch/Siemens, meegeleverd door KPN), ZyXEL (meegeleverd door Telfort) en de standaard kabelmodems (ZIGGO, UPC) leveren vaak problemen op. Problemen hebben vaak een adhoc karakter: het ene gesprek is er geen probleem, een volgend gesprek wel. Dit is ook verklaarbaar. Telefonie loopt over wisselende poorten; sommige zijn opene en andere staan dicht. Zo kan het geruime tijd goed gaan en ineens na het herstarten van uw telefoon helemaal mis zijn. Het oplossen hiervan is in veel gevallen erg lastig.
   Omdat uw uren en die van uw systeembeheerder kostbaar zijn, raden wij aan om met ons te overleggen wat voor ander apparaat in uw situatie goed zal werken en het ongehoorzame apparaat te vervangen.
   Ons advies is in de meeste gevallen: vervanging van uw apparaat door een FRITZ!Box of DrayTek. Wij adviseren u graag verder.

7. **Mijn VoIP-account was geregistreerd maar is dat inééns niet meer!**
   Door uiteenlopende redenen kan een VoIP-apparaat zijn registratie met de Simmpl telefooncentrale verliezen. Redenen zijn bijvoorbeeld: een korte hic-up van de internetverbinding, onderhoud van de internetprovider (bv. op DNS-vlak), een korte stroomstoring/-piek, een probleem met één van uw netwerkapparaten (router, switch, computer), onderhoud van de telefooncentrale.
   Een eerste advies dat vaak ook doeltreffend is in deze situatie, is het uit- en aanschakelen van uw VoIP-apparatuur en evt. van uw modem, router, switch, IP-telefoon. Wacht ca. 15 seconden tussen het uit- en weer aandoen.
   Bv: heeft u een FRITZ!Box, en is deze inééns zijn registratie kwijt, dan wil een herstart van de FRITZ! in veel gevallen het probleem oplossen.

8. **Audioprobleem: als mijn nummer wordt gebeld hoort de beller niets en uiteindelijk mijn voicemail**
   Deze situatie wordt veroorzaakt doordat het grootste deel van de registratie van uw account goed verloopt, maar het transport van de gespreksgegevens binnen uw netwerk niet. Als u op de Simmpl Telefooncentrale inlogt en u gaat naar het apparaatoverzicht, dan ziet u een bolletje achter het toestelaccount staan. Dit betekent dat de telefooncentrale denkt dat alles in orde is en stuurt een inkomend gesprek gedurende een aantal seconden naar uw apparaat. Pas bij geen gehoor gaat het gesprek naar de voicemail. Dat verklaart de stilte voordat het gesprek doorschakelt naar voicemail of naar een follow-me regel (bv. mobiel).
   Het signaal van het inkomende gesprek komt bij uw netwerk aan, maar (een deel van het signaal) staat daar voor een dichte deur. Dit veroorzaakt dat er geen telefoon overgaat, dat de beller geen overgangstoon hoort. Soms gebeurt dit ook wel, en vallen andere onderdelen van de signaalstroom weg (zie ook volgende punt).
   De oorzaak is uw netwerkrouter. De oplossing moet dan ook hier worden gezocht. Pas de configuratie aan zodat de router de signalen wel goed routeert.
   → suggesties en tips: zie de hierna volgende punten.

9. **Audioprobleem: ik hoor mijn gesprekspartner niet of andersom**
   Bij audioproblemen kunt u de volgende vuistregel in gedachten houden:
   * Als er één kant is die niet hoort dan ligt de oorzaak vaak bij de router.
   * Als er twee kanten zijn die elkaar niet horen, dan kan het ook het toestel zijn.

   Bij een zogenaamde **single-way-audio** situatie hoort u uw gesprekspartner niet en deze u wel, of andersom. Veelal zult u uw gesprekspartner niet horen: uw firewall blokkeert het inkomende VoIP-signaal dat van buiten naar binnen gaat. Dit betekent doorgaans dat uw router moeite heeft om het audiosignaal binnen uw netwerk te transporteren. Dat is nl. een ingewikkelde klus waarvoor een reeks poorten wordt gebruikt (doorgaans UDP: 10000 – 60000).
   Zie de hierna volgende punten voor algemene instructies t.a.v. het instellen van uw firewall. Het is helaas niet mogelijk om een punt-voor-punt instructie voor elk merk en type router te geven, maar wij kunnen u vaak wel alternatieve apparatuur adviseren die uw probleem gaat oplossen.

   Enkele suggesties:
   Het is een goed streven om ervoor te zorgen dat uw firewall niet achter een kabel- of DSL-router wordt geplaatst. Is dit niet te voorkomen, stel in deze eerste router dan een DMZ in die naar de firewall erachter verwijst. Is ook dat niet mogelijk, kijk dan of u het modem als bridge kunt instellen en laat de firewall erachter via de WAN-kant de verbinding opbouwen. Het IP-adres komt dan rechtstreeks in de firewall-router en niet in de eerste router (feitelijk passeert u de eerste router).
   Sommige modem-routers kunt u configureren als bridge (IP Spoofing).
   Behoudt u een single-audio-probleem of komen inkomende gesprekken niet door, dan is dit een blokkade van de firewall of de natting van de router.

   Suggestie 1:
   stel in dat verkeer afkomstig van de Simmpl telefoooncentrale (185.19.236.x) altijd wordt doorgelaten

   Suggestie 2:
   plaats uw IP-telefoon of de tweede router in uw netwerk in DMZ zodat alle verkeer van buitenaf hiernaar wordt doorgelaten en NIETS wordt geblokkeerd

Suggestie 3:
als uw router kennelijk zelf niet zo goed is in het maken van de juiste NAT-routeringen, maak dan in de NAT-tabel van de router een regel aan waardoor de achterliggende VoIP-apparatuur op een aantal vaste poorten naar buiten gaat. Deze poorten kunt u middels een andere NAT-regel ook weer openstellen voor inkomend verkeer.

Heeft u een Cisco router? Probeert u dan eens de volgende configuratie:
no ip nat service sip udp port 5060

Een **FRITZ!Box** aan het begin van uw netwerk is doorgaans een uitstekende basis voor VoIP. Heeft u ook nog een geavanceerde firewall, dan kan de volgende opstelling u van past komen: gebruik de FRITZ! als modem-router en sluit hierop uw telefoons aan (analoog, ISDN-apparatuur en IP Phones).
Via menu [Internet] > [Port Forwarding] kunt u de instelling [Exposed Host] kiezen en alle netwerkverkeer doorsturen naar het IP-adres van uw firewall.

Single-way-audioproblemen bij ZyXEL modem-routers kunnen in diverse gevallen worden opgelost op de volgende manier:
- Ga naar menu [**Netwerk**] > [**NAT**] > kies tab [**ALG**]
- Vink hier [**Enable SIP ALG]** uit en sla op.
- Test u nu of het probleem zich nog steeds voordoet.

Bij het gebruik van de X-Lite softphone kunt u single-way audioproblemen proberen op te lossen als volgt:
- bel met X-Lite het nummer ***7469 > er wordt een aparte settingspagina geopend
- zoek parameter [honor] en stel deze in van [0] naar [1]
- test nu of het probleem zich nog steeds voordoet.

10. Welke poortinstellingen zijn nodig om VoIP door de NAT-router/Firewall te laten komen?

De NAT-router / firewall moet in beginsel de poorten 1**0000-60000 (UDP)** toelaten om een symmetrische verbinding (= audio in twee richtingen) met de Simmpl telefooncentrale mogelijk te maken.
Hieronder een overzicht van poorten en ranges die doorgaans door VoIP worden gebruikt. Deze ranges dienen bereikbaar te zijn voor verkeer van en naar de telefonie-servers, zowel van binnenaf (vanaf IP Phones op het lokale netwerk) als van buitenaf (inkomend verkeer). De telefonieservers bevinden zich op domein **pbx.callvoip.nl**, netwerk 185.19.236.0/22. De router dient het verkeer goed te routeren.

UDP **van** alle poorten in bereik: 185.19.236.0 - 185.19.239.255
UDP **naar** alle poorten in bereik: 185.19.236.0 - 185.19.239.255
Poort 80 TCP naar 185.19.236.0 - 185.19.239.255 (webinterface en provisioning)
Poort 443 TCP naar 185.19.236.0 - 185.19.239.255 (webinterface en provisioning)

5060	UDP → SIP (signaleringspoort → maakt registratie mogelijk)
10000- 60000	UDP → RTP (audioverkeer > belangrijk als u audioproblemen heeft)

Belangrijk advies: probeer in de firewallconfiguratie alle UDP-poorten toe te staan in het bereik van de Simmpl telefooncentrale. Ga terughoudend om met het wijzigen van de firewall-settings omdat dit invloed kan hebben op alle gebruikers.
In een lokaal netwerk kan een heel stel IP-telefoons aanwezig zijn.

De IP-telefoon registreert SIP-accounts op basis van de standaardpoort 5060. De netwerkrouter koppelt poort 5060 (registratie) voor een specifieke account aan een

pseudopoort in de range 10000 t/m 60000. Zo weet de netwerkrouter welk signaal voor welke telefoon is bedoeld.

Als uw account geregistreerd is op uw apparatuur kunt u deze terugzien op de telefooncentrale. Hiertoe kunt u inloggen op de klantlogin, kiest u in het menu onderdeel [Accounts], klikt u op [Show accounts]. Indien geregistreerd ziet u een blauw bolletje achter de betreffende account staan. Klik op de account door, en u ziet bij User Agent ook het merk en type apparaat vermeld staan.

Indien het u of uw systeembeheerder niet lukt om uw netwerkrouter tot orde te roepen en de routering succesvol uit te voeren, overweegt u dan de aanschaf van een router die deze mogelijkheden wel biedt. Dit kan een stuk goedkoper zijn dan doorzoeken en het probleem oplossen. Denk aan de uren van uw systeembeheerder en de frustratie van uw personeel.

Handige links:
http://www.pc-library.com/ports/
http://www.chebucto.ns.ca/~rakerman/port-table.html

Callvoip adviseert het gebruik van:
DrayTek-(modem-)routers: http://www.tijdhof.com/index.php?manufacturers_id=23
FRITZ!Box modem-routers: http://www.fritzshop.nl/

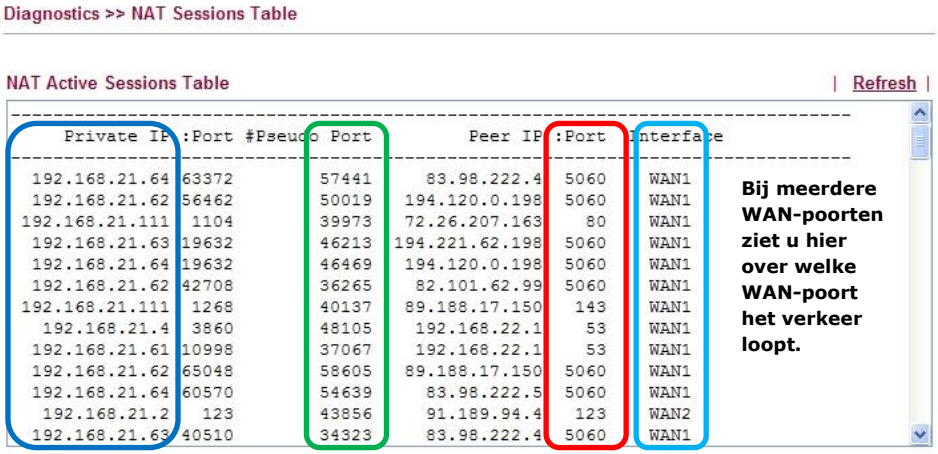
11. **Modem, router, firewall, server: hoe bouw ik het netwerk op?**
    Het is zaak om uw VoIP-verkeer door zo weinig mogelijk zaken te laten belemmeren om daarmee uw gesprekskwaliteit te kunnen optimaliseren.
    Zet uw VoIP-apparatuur daarom bij voorkeur zo DICHT mogelijk achter het kabel/ADSLodem met evt. een eenvoudige switch die de routering niet verstoort, en bij voorkeur **niet** achter een zware firewall en **niet** achter uw Windows Small Business Server of andere server met routingfunctie.
    Voor de duidelijkheid: VoIP achter uw server is wel mogelijk, maar toch vaak merkbaar in termen van kwaliteit. Het goed krijgen van deze configuratie stelt meer eisen aan de vaardigheden van uw netwerkbeheerder en dit zal u in ieder geval extra werk opleveren….

    Enige achtergrond: een normale FireWall die zogezegd VoIP-aware of VoIP-compatible is, zal automatisch de juiste poorten laten openen een open houden op basis van keep-alive sessies. Daarvoor hoeft u als het goed is NIETS te doen.
    Als dit in een bepaalde situatie niet het geval is, zult u het apparaat even moeten helpen het gedrag aan te passen aan wat er vereist is voor VoIP. VoIP op meerdere telefoons in één netwerk is vergelijkbaar met het internetverkeer van meerdere computers in één netwerk. Als u op een computer een bepaalde website raadpleegt en daar overheen navigeert, dan is dat vergelijkbaar met een VoIP-telefoongesprek. Een verschil tussen telefoneren via internet en surfen is, dat het spraakgeluid natuurlijk zonder of met zo weinig mogelijk vertraging moet binnen komen (= realtime karakter) en dat het hier gaat om audiosignalen die door het netwerk heen moeten.

    Omdat VoIP dynamisch is en dus op basis van de sessie willekeurig poorten gebruikt, is het een nachtmerrie voor ingewikkelder FireWalls. Omdat daarnaast het RTP-verkeer nogal wat eisen stelt met betrekking tot de vertraging (zo klein mogelijk), is het gebruik van een FireWall die al het verkeer via een zogenaamde "proxy" laat verlopen af te raden. Het telt immers allemaal bij elkaar op en voor je het weet is er in het gesprekspad veel vertraging, tot duidelijk merkbaar aan toe.

Deze hele combinatie aan eisen heeft ervoor gezorgd dat sommige fabrikanten ertoe zijn over gegaan om speciale VoIP-Firewall's te bouwen. Deze wordt dus parallel gezet met een bestaande FireWall, gebruikt eigen adressen en maakt dan vaak nog gebruik van een apart VLAN op het netwerk om telefoon- en dataverkeer gescheiden te houden. In deze hele combinatie wordt VoIP- en dataverkeer dus zo gescheiden mogelijk behandeld om voor beiden te kunnen voldoen aan de eisen die eraan gesteld kunnen worden. Ook kan er een tweede WAN-poort zijn om twee internetverbindingen te kunnen gebruiken.

De simpele benadering is: UDP open voor de wereld
Hiermee zou het voor iedere User Agent (VoIP-apparaat) achter de firewall dus mogelijk moete zijn om met de buitenwereld te communiceren. Poort 5060 laat verkeer door, via poort-mappings weet de router welke User Agent welke sessie met de buitenwereld heeft en elke user agent voert zijn eigen gesprek.
Er zijn netwerk-beheerders die dit niet willen wegens mogelijke beveiligingslekken. Dit risico is minimaal omdat er weinig tot geen lekken op UDP zijn - het wordt niet gebruikt voor normaal internetverkeer.



IP-adres v/d User-agent i/h netwerk **De pseudo-poort (soms getoond in centrale)** **Poort 5060 toont VoIP-verkeer**

Er is een alternatief: normaal gesproken werkt een User Agent op poort 5060. Via NAT wordt alles keurig geregeld, zodat de zogenaamde poort-mappings ervoor zorgen dat iedere User Agent kan communiceren met de buitenwereld. In de lastigere gevallen moet er dus per User Agent een set poorten gereserveerd worden om de FireWall open te houden voor het SIP-verkeer.

Bijvoorbeeld:
5060 voor telefoon 1
5062 voor telefoon 2
5064 voor telefoon 3
etc.

Merk op dat dit in **even** getallen gaat! Poorten vanaf **10000 tot 60000** worden dan open gezet voor de wereld, teneinde het dynamische RTP-verkeer toe te laten.

TIP: diverse producten bieden de instelling [use random port]. Als deze optie wordt geboden, zet deze dan aan. Dit is o.a. het geval bij GrandStream IP Phones en Siemens IP DECT toestellen.

12. **Mijn account is wel geregistreerd maar de verbinding valt na een enige tijd (aantal seconden of minuten) weg**
    Ook dit kan een symptoom zijn van uw router of telefonie-apparatuur die niet helemaal goed is ingesteld of is afgestemd op andere apparatuur in het netwerk (bv. VoIP-apparatuur tov router). Uw VoIP-apparaat (IP Phone, ATA, Gateway, PBX) houdt zich niet aan de regels voor het openhouden van een sessie (= gesprek) binnen NAT, of de NAT-router/firewall heeft last van misdragingen.

    Veel routers/firewalls kennen een timer die na x tijd afloopt en waarbij een geopende poort weer gesloten wordt. Als deze poort dus 5060 is – waarop de communicatie met de Simmpl Telefooncentrale plaatsvindt, dan is uw apparatuur van buiten af niet meer bereikbaar.
    Heel vaak is er sprake van **session timers** in de VoIP-apparatuur die keurig poort 5060 openhouden mits de timerwaarde wordt ingesteld **binnen de helft van de timer van de NAT-router/firewall**.

    Advies: zorg ervoor dat de **session refresh timer** (er zijn verschillende termen in omloop) van uw VoIP-apparaat onder de helft van de **time-out** van de router wordt ingesteld (of zet hem gewoon heel laag) en stel de **session re-register** in op ca. 20-30 minuten. Dan blijft alles bereikbaar. Ook al wordt er 1 pakket verloren, het 2e pakket valt dan nog binnen de timer. Als u meerdere soorten VoIP-apparaten heeft, waarbij één apparaat het wel goed doet, en de andere niet, zoek dan hier de oorzaak.

    N.B.: in de praktijk is middels tools als **Ethereal** en **Wireshark** aangetoond dat niet ieder apparaat ook werkelijk doet wat er geconfigureerd kan worden. De fabrikant van de apparatuur is er op aan te spreken dat het apparaat zich houdt aan de standaarden en samenwerkt met apparatuur die zich ook aan de standaarden houdt. Dit is slechts een schrale troost. Wij adviseren u graag met welke apparatuur wij goede ervaringen hebben.

13. **Waar vind ik handige netwerktools om te zien wat er gebeurt?**
    Op de Simmpl Supportpagina (www.simmpl.nl/support) vindt u een overzicht van handige tips, tools en (online) programma's om te zien wat de stand van zaken is. Zo vind tu een overzicht van de SIP statuscodering, een online tool MyVoipSpeed om te beoordelen of uw netwerk geschikt is voor VoIP-verkeer (let op: dit is een momentopname!), online poortscanners, een apparaat waarmee u het MAC-adres van een apparaat in uw netwerk kunt opzoeken, etc.

    Ook zeer handig is http://www.wireshark.org/ (versies voor Windows, Linux'en, MacOS X etc.). Let op dat voor het monitoren van verkeer op een netwerk wel een hub of switch met monitor-poort vereist is.

14. **Mijn account is wel geregistreerd maar de verbinding is erg slecht**
    CODEC - Controleert u of uw apparatuur met een bepaalde CODEC (codering - decodering) uw apparatuur werkt. De Simmpl telefooncentrale werkt met de ISDN-codecs G.711a-law en G.711u-law. Dit biedt de hoge kwaliteit die u gewend bent. Pas uw codecs aan en kijk of de spraakkwaliteit nu verbetert.

15. BANDBREEDTE - Vervolgens kunt u controleren of u voldoende bandbreedte tot uw beschikking heeft. Voor deze check bestaan er on-line tools: Wij adviseren u de volgende tools:

- speedtest.ziggo.nl | www.speedtest.nl | www.speedtest.net
Hier kunt u uitvinden hoeveel uploadsnelheid u heeft. Voor elk VoIP-gesprek heeft u als vuistregel ca. 100kB up- en downloadsnelheid nodig.

- http://myvoipspeed.visualware.com/
Een uitgebreide test van uw bandbreedte en de kwaliteit die u qua VoIP zou moeten kunnen behalen. Deze test eindigt met een conclusie en enkele tips.

QUALITY OF SERVICE - Indien u wel genoeg bandbreedte heeft, maar u houdt een slechte gesprekskwaliteit, dan is het mogelijk dat uw router de beschikbare bandbreedte niet effectief in uw netwerk verspreidt. Stel dat andere gebruikers in het netwerk zo nu en dan teveel bandbreedte gebruiken, dan kan dit een slechte gesprekskwaliteit opleveren.

De term **Quality of Service (QoS)** heeft betrekking op een intelligente routerfeature, waarmee uw router in staat is voorrang te geven aan bepaalde informatiestromen in het netwerk. Doorgaans is VoIP één van de informatiestromen in het netwerk die voorrang krijgen boven andere soorten netwerkverkeer. De andere netwerkgebruikers merken hier doorgaans nauwelijks tot niets van, de VoIP-bellers daarentegen wel! Een intelligente router met QoS biedt u de garantie dat VoIP voorrang krijgt, en daarmee een optimale gesprekskwaliteit.

Wij adviseren u een professionele netwerkrouter, bijvoorbeeld één van de DrayTek-producten, of een all-in-one VoIP-apparaat (bv. FRITZ!Box) dat zelf de verdeling van bandbreedte doet, dat weet dat er VoIP-verkeer is en dat daarmee rekening houdt (QoS).
Als u een FRITZ!Box in routermode gebruikt, bijvoorbeeld achter een kabelmodem, let dan op de instelling voor uploadsnelheid en downloadsnelheid bij de Account Information > deze staan default erg laag ingesteld.

16. **Hoe kan een SIP-verzoek door een Stateful Firewall heenkomen?**
Een stateful firewall accepteert alleen requests van binnenuit, hoe kan een inkomend gesprek dan überhaupt worden gedetecteerd?
De SIP-User Agent (uw VoIP-apparaat) zet een sessie op met de Simmpl Telefooncentrale. Dat werkt via een proxy. Alle gesprekken lopen ook via die proxy, zodat een STUN-server en waslijsten open poorten niet nodig zijn.
M.a.w.: het VoIP-apparaat heeft op poort 5060 een sessie open met de Simmpl telefooncentrale. Een braaf VoIP-apparaat stuurt iedere x seconden (bv. 20-60 seconden) een refresh/keepalive-signaaltje naar de telefooncentrale die daarop ook braaf een antwoord geeft. De gemiddelde Firewall met Stateful Packet Inspection sluit een poort/sessie pas na inactiviteit tussen de 1 en 15 minuten, afhankelijk van hoe dit ingesteld is.

17. **Heb ik iets aan STUN?**
    Een STUN-service kan een antwoord zijn, maar daar hoeft u in principe niet mee te werken. STUN is een 'lapmiddel' om een pad terug door een router te krijgen. Met STUN dienen er ook vaak ook nog in de configuratie van de router diverse poorten te worden geopend (herkomst ANY) naar het interne adres van het VoIP-apparaat. Dat is geen gaatje maken maar een gat in uw netwerk waar u kwetsbaar bent voor bv. een DoS attack.

18. **Kan DID / DDI ook met Callvoip?**
    DID of DDI staat voor Direct Inward Dialing is in feite het gebruik van een nummer van één account dat wordt meegezonden als ID met een of meer andere accounts. Binnen een blok van nummers op één klantenaccount is het mogelijk om het nummer van een andere account mee te zenden als CLI (Caller Line Identification).
    U kunt op de Simmpl telefooncentrale zelf instellen welk nummer met uw gebruikersaccounts wordt meegestuurd. Dat doet u bij de instellingen van de gebruiker.

19. **Ik wil niet dat er een nummer wordt meegezonden - toestellen mogen niet van buitenaf direct te bellen zijn**
    U kunt toestelaccounts aanmaken; deze hebben altijd een intern nummer zodat ze door collega's kunnen worden gebeld. Als u het account niet opneemt in uw belplan voor één of meer nummers, dan kan het nummer niet worden gebeld van buitenaf.

20. **Wat betekenen de termen Attended en Unattended transfer?**
    Attended Transfer of **warm** doorverbinden is het doorverbinden met ruggespraak. U heeft iemand aan de lijn, zet dit gesprek in de wacht en belt naar een ander nummer. U kondigt het gesprek aan en verbindt hem dan door. Niet alle apparatuur ondersteunt de functie attended transfer vlekkeloos – er moeten er als het ware twee gesprekken (call-legs) aan elkaar worden geknoopt. Niet alleen de IP Phones maar ook de router in het netwerk (en soms de switches) kunnen van invloed zijn op de mogelijkheid om door te verbinden. Wij hebben goede ervaringen met vrijwel alle soorten gangbare IP-toestellen met speciale aanbeveling voor de IP-toestellen van het merk Tiptel / Yealink. Ook de meeste FRITZ!Boxen ondersteunen extern doorverbinden (warm/koud) door een gesprekspartner in de wacht te zetten, een tweede te bellen en dan [R4] te kiezen (raadpleegt u de handleiding van de FRITZ!Box voor de exacte codes voor uw type box). Beide gesprekspartners worden met elkaar doorverbonden.

    Unattended Transfer of **koud** doorverbinden is doorverbinden zonder ruggespraak: het gesprek wordt direct doorgeschoven naar degene waarnaar u doorverbindt. Dit is een technisch vrij een eenvoudige functie die werkt met de SIP-functie REFER.

21. **Kan ik de voicemail-files ook ontvangen in een ander formaat dan .mp3?**
    Nee, dit is helaas niet mogelijk. Voor veel gebruikers is het mp3 formaat echter het meest geschikt door haar brede inzetbaarheid en het feit dat het kleine bestanden zijn.

22. **Ben ik ook bandbreedte kwijt voor intern bellen?**
Ja, het bandbreedte-verbruik geldt voor zowel interne als externe toestellen. Bandbreedte is tegenwoordig de basis van al uw werkzaamheden. Dit zal dus niet snel een probleem hoeven opleveren.

23. **Loop ik ook een veiligheidsrisico als ik VoIP gebruik?**
Het grote voordeel van VoIP is dat het niet is gebonden aan een vaste locatie. Bij onze dienst is het gebruik van een account ook niet gebonden aan een bepaalde IP-adres. Uw VoIP-account kan dus overal ter wereld op elke internetverbinding worden gebruikt. Dit betekent dat uw VoIP-accountgegevens een open portemonnee zijn. Bescherm deze gegevens daarom goed!
Wij doen ons best om u hierbij te helpen: alleen op het Callvoip Klantgegevensformulier worden uw inloggegevens vermeld. De toegang tot de telefooncentrale sluit automatisch na 6 uur.

Mocht het toch gebeuren dat er onverhoopt misbruik van uw VoIP-account wordt gemaakt, ook dan zal de schade beperkt blijven. De Simmpl telefooncentrale monitort uw gebruik en er worden voor alle klanten limieten ingesteld. Als 80% van deze limiet wordt bereikt ontvangt u daarvan een bericht. Als 100% van de limiet wordt bereikt wordt uw account automatisch gesloten.
Beseft u dat zowel de alerts als het aanlopen tegen een ingestelde limiet slechts gebeuren als er reeds schade is geleden. Zonder deze mechanismen was de schade ongetwijfeld hoger uitgekomen. Tref uw voorbereidingen om deze vervelende situatie te voorkomen.

U kunt ook zelf iets doen.
- hou uw Callvoip klantgegevensformulier veilig en buiten bereik van onbevoegden
- meld ons diefstal van toestellen
- wijzig uw SIP passwords en toegangsrechten bij vertrek van een medewerker
- bescherm uw apparatuur en netwerk goed

24. Belangrijk - kwetsbaarheid van OpenSource PBX-systemen
Gebruikt u een eigen telefooncentrale (Asterisk, Elastics, FreePBX, etc.) met daarop één of meer Simmpl-accounts als trunk? Weest u dan alert op een sterk toenemende trend met hack- en inbraakpogingen op OpenSource PBX-centrales zoals Asterisk. Deze trend is niet beperkt tot onze klanten, maar doet zich wereldwijd voor als randeffect van het wereldwijd toenemende gebruik van Voice over IP.

De hack begint doorgaans met het doen van belpogingen vanuit 'het Internet'. Als dat door de asterisk als 'mogelijk relevante' invite in processing wordt genomen kan e.e.a. gaan rollen. Het begint met het zetten van access-lists op de asterisk server. De meeste Linux servers hebben iptables aan boord, waarmee je een verdraaid sterke firewall kunt bouwen. Het komt erop neer dat een asterisk server van niemand een Invite toestaat, behalve van de Simmpl-centrale. Dan heb je het OS van de asterisk server aangepakt, de volgende stap is iets vergelijkbaars doen in het asterisk dialplan, waarbij alleen maar calls afkomstig van de trunk (= de Simmpl SIP server) verder het dialplan in mogen. Extension 's' als ingang gebruiken naar het dialplan is gevaarlijk.
Dit vereist toch wel wat kennis van zowel Linux als asterisk.
Ontbreekt deze kennis, dan is het aan te raden gebruik te gaan maken van een firewall, zoals bijvoorbeeld Astaro appliances.
Test uw firewall met bijvoorbeeld de firewall tester op www.grc.com (Shields Up).

Het meest opvallende symptoom is dat er onverwacht veel verkeer wordt gestuurd naar regio's als Noord-Korea, Somalië, Letland, Litouwen, Cuba, Eritrea en overige

minder courante bestemmingen. Vaak is de misbruik terug te voeren tot het niet beheersen van algemene systeem beveiligingsprincipes. In sommige gevallen een gat in het dialplan, en in een enkel geval een hack in de webserver ‘die ernaast staat’ waardoor toestellen aan de binnenkant zijn gekraakt vanwege zwakke wachtwoorden.
Wij brengen hierbij graag dringend onder uw aandacht dat Open Source PBX'en van huis uit kwetsbaar zijn, en dat speciale aandacht moet worden geschonken aan de beveiliging op netwerk-, (operating)systeem en dial-plan niveau.
Waarschuwingssystemen en andersoortige vangnetten moeten evenwel gezien worden als last resort: als die functies worden geactiveerd, is er aan de voorkant al teveel verkeerd gegaan.
Wij raden u met klem aan om extra aandacht te besteden aan de beveiliging van uw netwerken en systemen, maar ook te bezien hoe deze omgevingen in te richten zijn ter zake van rapportage en alarmering naar uw systeem beheerder.

Deze informatie wordt u aangeboden door:

CallvoipTelefonie.nl

CallvoipTelefonie
Koldingweg 19-1
9723 HL GRONINGEN

T: 050 – 820 00 00
F: 050 – 820 00 08

@: callvoip@callvoip.nl
W: www.callvoiptelefonie.nl