

XPHONE CONNECT SOFTPHONE MOBILE

KONFIGURATION UND TROUBLESHOOTING

Inhaltsverzeichnis

1. Einleitung.....	3
Grundkonfiguration.....	3
Interaktives Ablaufdiagramm Softphone Mobile.....	4
2. Mobileapp mit XPhone Server verbinden.....	5
Installation der Mobile Web Anwendung im IIS.....	5
2.1.1 SSL Zertifikat.....	5
2.1.2 IIS auf XPhone Server.....	5
2.1.3 IIS in DMZ ausgelagert.....	5
Konfiguration XPhone Server.....	7
2.1.4 Externe URL für Mobile und WebAPI.....	7
2.1.5 Softphone Mobile für einen Standort aktivieren.....	7
Funktionsprüfung, Troubleshooting.....	8
2.1.6 WebApi Tester.....	8
2.1.7 SignalR auf LongPolling umstellen.....	8
2.1.8 Externe Erreichbarkeit.....	9
2.1.9 Verbindungstest in der Mobile App.....	9
2.1.10. Probleme beim Verbindungstest eingrenzen.....	10
2.1.11. Werden Telefonie-Devices angezeigt?.....	10
2.1.12. Firewall, Reverse-Proxy.....	10
3. Gespräche über Softphone Mobile führen.....	12
Konfiguration XPhone Server.....	12
3.1.1. STUN Server konfigurieren.....	12
3.1.2. Ports in der Firewall freigeben.....	13
3.1.3. Bei Bedarf: Konfiguration der ACL's (White und Blacklist).....	13
4.Netzwerkanalyse.....	14
Interaktives Ablaufdiagramm Netzwerkanalyse.....	15
Wireshark Analyse.....	16
4.1.1. Erstellen und Vorbereitung des Wireshark Traces.....	16
4.1.2. Analyse der Kandidaten-Aushandlung.....	17
4.1.3. Analyse der Bindings.....	18
5.Bekannte Fehlerbilder.....	20
Mobile App Anmeldung nicht möglich.....	20
Keine Geräte in der Mobile App verfügbar.....	20
Fehlende Binding Success Meldungen im Wireshark.....	20
Fehlende öffentliche oder private Kandidaten im Wireshark.....	22
IP Adressen der Pakete stimmen nicht überein.....	23
Geblockter Call (durch ACL) – 403 forbidden.....	23
Geblockte Kandidaten (durch ACL) – 488 Not acceptable here.....	24
6.Ticketerstellung.....	25

1. EINLEITUNG

Dieser Artikel richtet sich an Partner, Kunden und Netzwerk-Admins. Er soll sie bei der Inbetriebnahme von Softphone Mobile unterstützen.

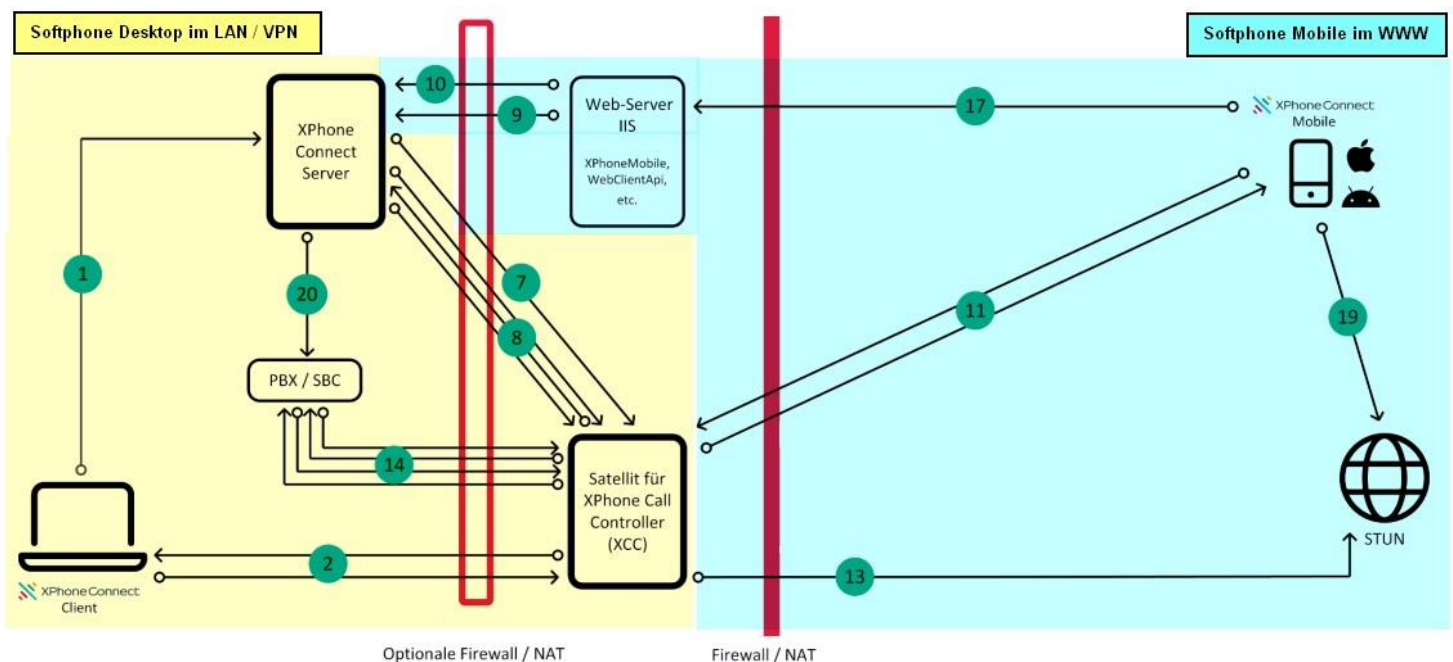
Mit dem Artikel soll interaktiv gearbeitet werden können. Wenn Sie in einem Diagramm / Text auf einen Link stoßen, zögern Sie nicht diesen als Absprungspunkt zur passenden Stelle zu nutzen. Am Ende eines Abschnitts werden Sie wieder zurück zum Diagramm geleitet.

Zur grafischen Veranschaulichung ist der Netzwerkbereich, der für Softphone Desktop relevant ist, gelb hinterlegt.

Für Softphone Mobile kommen Konfigurationen im blau hinterlegten Netzwerkbereich hinzu - das ist das Thema dieses Artikels.

Die gesamte Netzwerkübersicht findet sich hier:

<https://help.c4b.com/xphone-connect-9/doc/de/admin/start/sys-req/infstrctr.html#netzwerk>



GRUNDKONFIGURATION

Wir setzen an dieser Stelle voraus, dass bereits ein funktionierendes Softphone Desktop im LAN bzw. VPN für mindestens zwei XPhone User in Betrieb ist.

Das bedeutet (für den gelben Bereich):

- Ausgelagerter XCC in der DMZ. Dieser wird für Softphone Mobile bzw. Payload Separation beim Desktop Client empfohlen. Ist aber nicht zwingend.
- Erfolgreicher Softphone Testanruf mit dem XPhone Connect Desktop Client.
- Erfolgreiche Sprachverbindung zwischen zwei Softphone Desktop Clients.
- Erfolgreiche Sprachverbindung zwischen dem Softphone Desktop Client und einem externen Anrufer (ein- und ausgehend).

Anders formuliert: es müssen die Verbindungen (1), (2), (7), (8), (14) und (20) funktionieren.

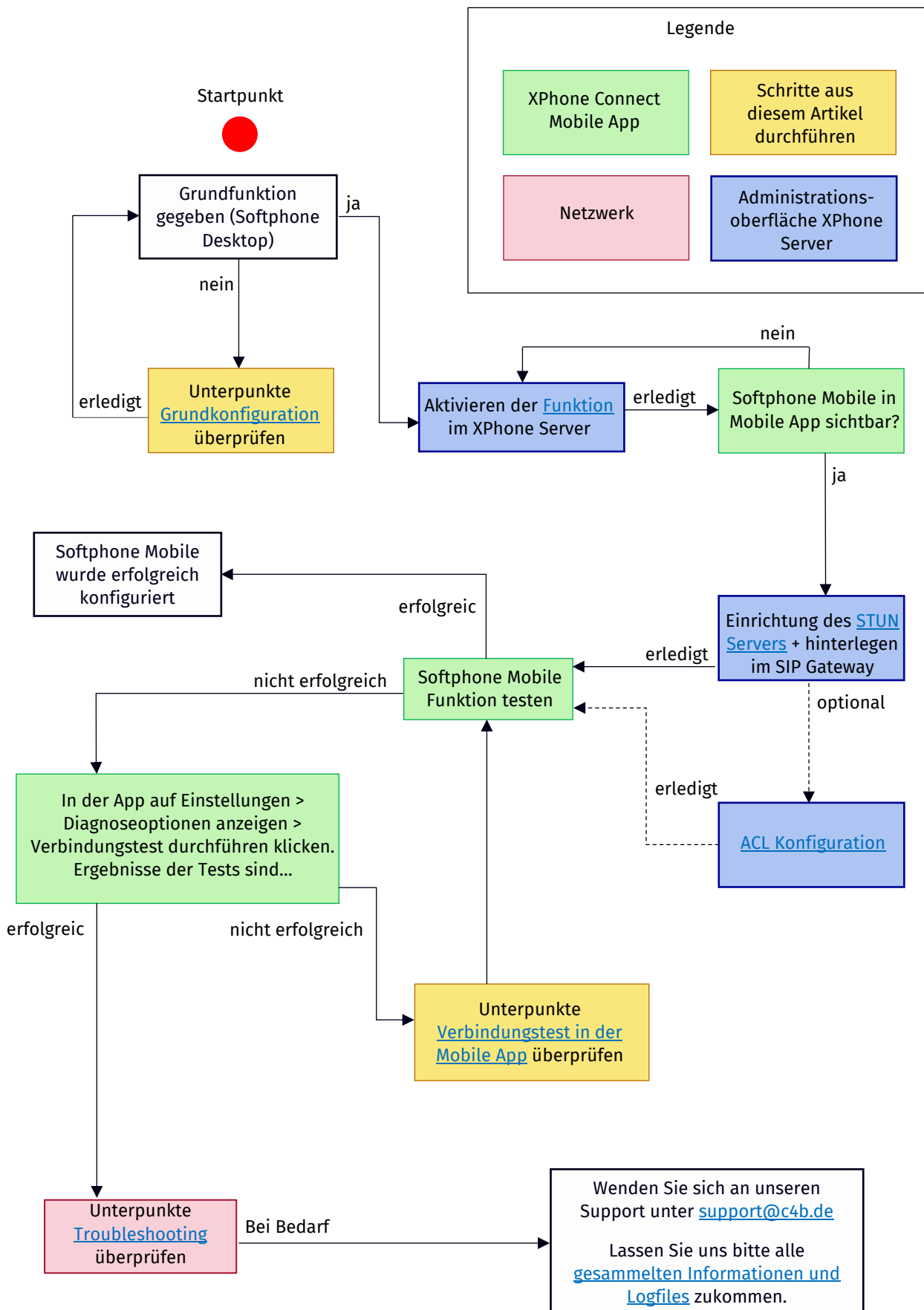
Wenn diese Voraussetzungen erfüllt sind, sind Sie bestens für die Inbetriebnahme von Softphone Mobile gerüstet!

Die Inbetriebnahme von Softphone Mobile gliedert sich in zwei Teile:

1. **Mobile App mit dem XPhone Server verbinden** (Steuerung und Signalisierung).
2. **Gespräche über Softphone Mobile führen** (Audio Übertragung per VoIP).

Wir haben die anstehenden Arbeitsabläufe zur leichteren Orientierung in diesem Schaubild visualisiert. Sie starten am roten Punkt!

INTERAKTIVES ABLAUFDIAGRAMM SOFTPHONE MOBILE



2. MOBILEAPP MIT XPHONE SERVER VERBINDEN

In diesem Kapitel geht es darum, die XPhone Connect Mobile App mit dem XPhone Server zu verbinden, so dass man sich in der App am XPhone Server anmelden kann, seine Geräteliste sowie sieht, und Zugriff auf seine Kontakte und sein Journal hat.

Im ersten Schaubild entspricht das den Verbindungen (9), (10) und (17).

INSTALLATION DER MOBILE WEB ANWENDUNG IM IIS

Die Mobile Web Anwendung läuft im Microsoft IIS. Zur Auswahl stehen

1. der IIS auf dem XPhone Server Rechner
2. ein ausgelagerter IIS, z.B. in der DMZ

Beide Varianten sind am Ende funktional identisch, unterscheiden sich aber in ihrer Netzwerk-Konfiguration.

2.1.1 SSL Zertifikat

Im Allgemeinen wird man auf eines dieser Netzwerkszenarien treffen. Ein wichtiger Unterschied besteht darin, wo das SSL Zertifikat für den gesicherten Zugriff installiert werden muss. Betrifft Verbindung (17).

Ohne Reverse Proxy

XPhone Mobile App > Externe Firewall / Port Forwarding / NAT > IIS > XPhone Server

In diesem Fall muss das SSL-Zertifikat auf dem IIS installiert werden, auf dem auch die Mobile Web Anwendung läuft.

Mit Reverse Proxy

XPhone Mobile App > Externe Firewall / Port Forwarding / NAT > Reverse Proxy > IIS > XPhone Server

In diesem Fall muss das SSL-Zertifikat auf dem Reverse Proxy installiert werden.

Soll die Verbindung zwischen Reverse Proxy und IIS ebenfalls verschlüsselt erfolgen, ist ein weiteres Zertifikat notwendig! Hier reicht dann i.d.R. ein selbst ausgestelltes Zertifikat.

Hinweis: Sogenannte Sub-sub-domains können Probleme bereiten da Android und IOS strikter arbeiten siehe:

<https://support.c4b.de/hc/de/articles/8809009914268-Warum-kann-ich-mich-in-der-Mobile-App-nicht-anmelden-> bzw. [bekannte Fehlerbilder](#).

2.1.2. IIS auf XPhone Server

Läuft der IIS auf dem XPhone Server Rechner, vereinfacht sich das Szenario wie folgt:

XPhone Mobile App > Externe Firewall / Port Forwarding / NAT (>Reverse Proxy) > IIS auf XPhone Server

Es müssen keine zusätzlichen Einstellungen im IIS vorgenommen werden.

2.1.3. IIS in DMZ ausgelagert

Läuft der IIS auf einem ausgelagerten Rechner in der DMZ:

XPhone Mobile App > Externe Firewall / Port Forwarding / NAT (>Reverse Proxy) > IIS in DMZ > XPhone Server müssen folgende Verbindungseinstellungen zwischen IIS und XPhone Server angepasst werden.

- Die beiden Ports 2230 und 2231 von der DMZ zum XPhone Server müssen freigegeben werden.
- Betrifft Verbindung (10): In der Datei "C:\Program Files\C4B\XPhone Connect Server\XPhoneMobile\web.config" muss der WCF-Endpoint von "localhost" auf den Hostnamen bzw. die IP-Adresse des XPhone Servers umgestellt werden.



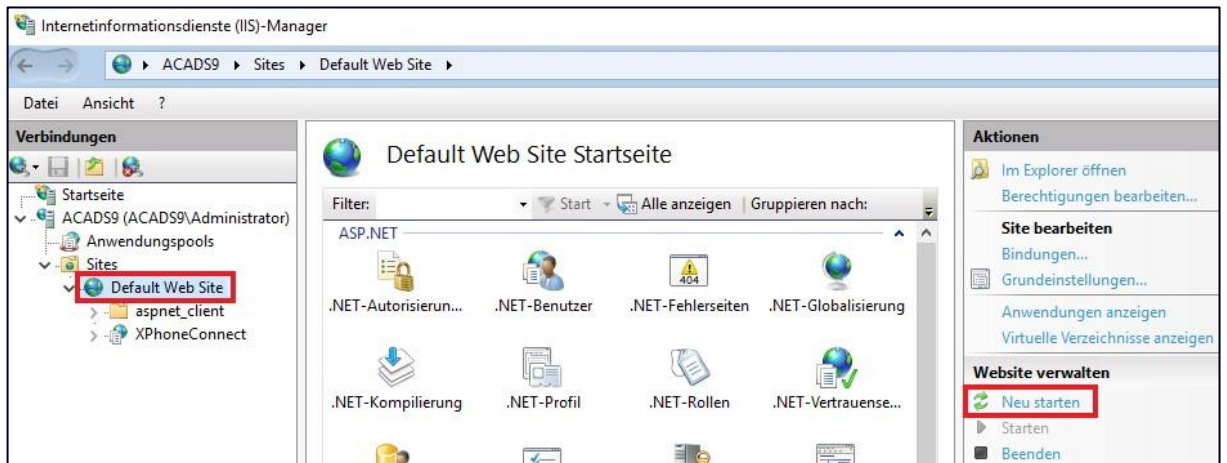
- Betrifft Verbindung (9): In der Datei "C:\Program Files\C4B\XPhone Connect Server\WebClientApi\appsettings.json" muss der GRPC-Endpoint auf den Hostnamen bzw. die IP-Adresse des XPhone Servers umgestellt werden.

```

{
  "AppSettings": {
    "Secret": "THIS IS USED TO SIGN AND VERIFY JWT TOKENS. VER",
    "JwtTokenLifetime_Comment": "6 minutes is minimum value",
    "JwtTokenLifetimeInMinutes": 30,
    "RefreshTokenLifetimeInHours": 96,
    "SignalRLongPolling": false,
    "XPhoneServerHost": "10.1.1.54",
    "XPhoneServerUnifiedPort": ""
  }
}

```

- Öffnen Sie anschließend die Konfigurationsoberfläche des IIS und starten Sie die Default Webseite neu.



Zurück zum [Ablaufdiagramm Softphone Mobile](#)

KONFIGURATION XPHONE SERVER

2.1.4. Externe URL für Mobile und WebAPI

Seit der V9 gibt es in den Allgemeinen Einstellungen des XPhone Connect Servers eine zweite URL beim Punkt Mobile App für die Client WebAPI. Diese muss eingetragen sein und von außen erreichbar sein (wie auch die URL für Mobile)



Da die meisten Kunden die Domain-Namen mit einem Zertifikat versehen, müssen Sie ggf. nur diesen für die Web-API URL anpassen (der Teil "/xphoneconnect/webclientapi" muss natürlich bestehen bleiben). Sind die expliziten Webseiten URLs mit einem Zertifikat ausgestattet, dann wird auch ein entsprechendes Zertifikat für die Web-API URL benötigt.

2.1.5. Softphone Mobile für einen Standort aktivieren

Öffnen Sie z.B. einen Standort, navigieren Sie in die Einstellungen > Telefonie und setzen Sie das folgende Häkchen:



Zurück zum [Ablaufdiagramm Softphone Mobile](#)

FUNKTIONSPRÜFUNG, TROUBLESHOOTING

2.1.6. WebApi Tester

Verwenden Sie das frei verfügbare Tool "WebApi Tester" zur Überprüfung Ihrer Installation und Konfiguration.

Das Tool ist über die öffentliche URL <https://wonderful-wave-0fef5e603.2.azurestaticapps.net/> erreichbar und in jedem gängigen Browser lauffähig. Es simuliert viele Funktionen der Mobile Web-Anwendung und bietet darüber hinaus ausführliche Logausgaben in der F12 Developer Konsole des Browsers.

Für welche Anwendungsfälle das Tool geeignet ist, sehen Sie in der Übersicht in der Hilfe-Seite des WebApi Testers:

<https://wonderful-wave-0fef5e603.2.azurestaticapps.net/help.html>

2.1.7. SignalR auf LongPolling umstellen

Manche Firewalls blockieren die Verwendung des WebSocket-Protokolls. Dann funktioniert die SignalR Kommunikation zwischen Mobile App und der Web-Anwendung im IIS nicht.

In solchen Fällen editiert man die Datei appsettings.json im Verzeichnis "C:\Program Files\C4B\XPhone Connect Server\WebClientApi" auf dem (ggf. ausgelagerten) IIS und ändert den Wert für "SignalRLongPolling" von false (=Default) auf true.

```
{
  "AppSettings": {
    "Secret": "THIS IS USED TO SIGN AND VERIFY JWT TOKENS. VERY SECRET STRING",
    "JwtTokenLifetime_Comment": "6 minutes is minimum value",
    "JwtTokenLifetimeInMinutes": 30,
    "RefreshTokenLifetimeInHours": 96,
    "SignalRLongPolling": false,
    "XPhoneServerHost": "",
    "XPhoneServerUnifiedPort": ""
  },
  "FeatureManagement": {
    "V9": false
  },
  "Logging": {
    "EventLog": {
      "LogLevel": {
        "Default": "Information",
        "Microsoft.AspNetCore": "Error",
        "Microsoft.Hosting": "Error",
        "Microsoft.AspNetCore.SignalR": "Error",
        "Microsoft.AspNetCore.Http.Connections": "Error"
      }
    }
  },
  "AllowedHosts": "*"
}
```

In besonderen Fällen kann es notwendig werden, detaillierte Debug-Informationen zu SignalR zu erhalten. In diesem Fall müssen die markierten Einträge in der Datei appsettings.json sowie das Log Level insgesamt auf "Debug" gestellt werden:

```
"Logging": {
  "EventLog": {
    "LogLevel": {
      "Default": "Debug",
      "Microsoft.AspNetCore": "Error",
      "Microsoft.Hosting": "Error",
      "Microsoft.AspNetCore.SignalR": "Debug",
      "Microsoft.AspNetCore.Http.Connections": "Debug"
    }
  }
}
```


2.1.8. Externe Erreichbarkeit

Ist die XPhone Connect Mobile Web-Anwendung aus dem Internet erreichbar?

Geben Sie dazu die in der XPhone Server Web-Admin konfigurierte Mobile-URL im Browser ein

("https://IHR-SERVER/xphoneconnect/mobile") oder verwenden Sie den Link "Mobile App" im WebApi-Tester. Erwartetes Ergebnis:

Schlägt dieser Test fehl, überprüfen Sie die externe Erreichbarkeit Ihres Webservers.

2.1.9. Verbindungstest in der Mobile App

Installieren Sie jetzt den aktuellen XPhone Connect Mobile Client auf Ihrem Smartphone und überprüfen Sie die Installation mit Hilfe des integrierten Verbindungstests (Einstellungen > Diagnoseoptionen > Verbindungstest durchführen).

Der Test prüft diese fünf aufeinander aufbauenden Funktionen. Im besten Fall sehen Sie dieses Ergebnis:

Check	Beschreibung
CONFIGURED WEB-API URL CHECK: Erfolgreich	prüft, ob die Mobile App die WebApi-URL vom XPhone Server erhalten kann. Das sollte in 99,9% der Fälle gut gehen. Wenn nicht, ist vermutlich schon die externe Erreichbarkeit nicht gegeben (siehe oben).
WEB-API HEALTH CHECK: Erfolgreich	prüft, ob die Mobile App das WebApi auf dem IIS erreichen kann. Bei einem Fehler könnte es an einem ungültigen Zertifikat oder einem Fehler in der Zertifikatskette liegen. Im WebApi-Tester ist ein einfacher SSL-Chain-Checker zu diesem Zweck verlinkt.
WEB-API AUTHENTICATION CHECK: Erfolgreich	prüft, ob sich der XPhone User am WebApi authentifizieren kann. Wenn das nicht gegeben ist, findet man die Ursache am einfachsten mit dem WebApi-Tester . Überprüfen Sie auch nochmal die Einstellungen auf dem IIS (web.config, appsettings.json), und insbesondere die Freigabe von Port 2231 in der Firewall.
SIGNALR HUB CHECK: Erfolgreich	prüft, ob der Event-Kanal vom XPhone Server in Richtung Mobile App funktioniert. Auch hier analysiert man die Probleme am einfachsten mit dem WebApi-Tester . (wenn Long Polling nicht aktiv ist, kann es sein, dass der Test im Tool funktioniert, jedoch nicht in der App, so war es bei meiner Umgebung bis ich den LongPolling Patch verwendet habe)
REINITIALIZE SOFTPHONE: Erfolgreich	prüft, ob das WebApi sauber mit dem XPhone TelefonieService kommuniziert. Wenn die ersten 4 Punkte funktionieren, ist Punkt 5 in 99,9% der Fälle auch gegeben.

Sollte einer der Tests fehlschlagen, befolgen Sie die folgenden Hinweise zur Fehlerbehebung.

2.1.10. Probleme beim Verbindungstest eingrenzen

Zur Eingrenzung von Verbindungsproblemen empfiehlt es sich, die Mobile App sowohl im Firmennetz (WLAN) als auch im öffentlichen Internet zu verbinden.

Klappt die Verbindung im Firmen-WLAN, ist die Ursache für die Problem in der Firewall bzw. im Netzwerk zu suchen.

2.1.11. Werden Telefonie-Devices angezeigt?

Der WebApi-Tester hat einen eigenen Befehl zur Anzeige der Telefonie-Devices. Wenn diese nicht angezeigt werden, könnte dieser KB-Artikel helfen:

<https://support.c4b.de/hc/de/articles/5664874337692>

2.1.12. Firewall, Reverse-Proxy

Freizugebende URLs

Folgende Pfade müssen im Reverse Proxy eingetragen und zugelassen werden (bitte Groß-/Kleinschreibung beachten):

<https://beispieldomain/XPhoneConnect/mobile>

<https://beispieldomain/XPhoneConnect/Mobile>

<https://beispieldomain/XPhoneConnect/webclientapi>

<https://beispieldomain/XPhoneConnect/doc>

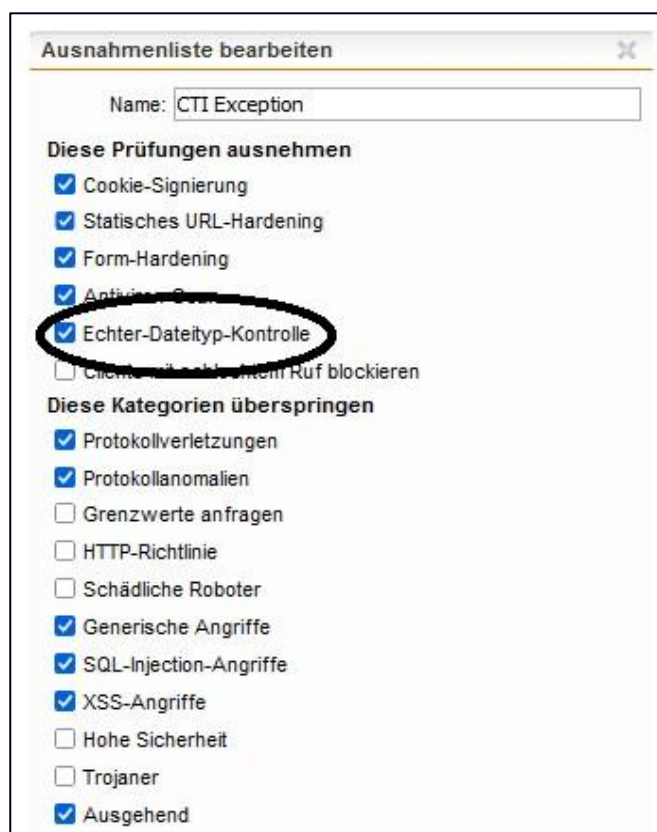
<https://beispieldomain/XPhoneConnect/WebMeeting> (Nur wenn Web-Meeting verwendet wird. Nicht für Softphone Mobile notwendig.)

Netscaler

Netscaler unterstützt Stand heute (02/2023) das WebSocket-Protokoll nicht. Daher sollte die SignalR Konfiguration auf LongPolling umgestellt werden. Siehe [SignalR auf LongPolling umstellen](#).

Sophos UTM

Sollte es Probleme in Verbindung mit Sophos UTM geben, prüfen Sie die folgenden beiden Einstellungen. Die Einstellung "Echter-Dateityp-Kontrolle" sollte aktiviert sein:



Ist ein Port-Forwarding von der Sophos direkt auf den XPhone Server eingerichtet, sollte die Einstellung "Cookie signing" abgeschaltet werden:

Warning: This firewall belongs to a Sophos Central firewall group. To prevent potential conflicts, use caution when making changes locally.

Edit protection policy

Feedback | [How-to guides](#) | [Log viewer](#) | [Help](#)

- Web servers
- Protection policies**
- Authentication policies
- Authentication templates
- General settings

Name *

Description

Pass Outlook Anywhere ☐ OFF

Mode *

Cookie signing ☐ OFF **Muss ausgeschaltet sein**

Static URL hardening ☐ OFF

Form hardening ☐ OFF

Antivirus ☒ ON

Mode

Direction

Block unscannable content ☐ OFF

Zurück zum [Ablaufdiagramm Softphone Mobile](#)

3. GESPRÄCHE ÜBER SOFTPHONE MOBILE FÜHREN

In diesem Kapitel geht es darum, die eigentliche Sprachübertragung ("Payload") zwischen dem Mobile Softphone und der Gegenstelle zuverlässig einzurichten.

Im ersten Schaubild entspricht das den Verbindungen (11), (13) und (19).

KONFIGURATION XPHONE SERVER

Für den Betrieb von Softphone Mobile muss ein STUN Server konfiguriert werden.

Wichtiger Hinweis:

Im weiteren Verlauf des Artikels wird öfter die Rede von "STUN" sein, dies hat bei uns zwei Bedeutungen, je nach Kontext.

- Der erste Anwendungsfall ist der "normale" STUN (auch classic STUN genannt), der verwendet wird um die öffentliche IP eines Gerätes zu erhalten.

Wenn wir den Begriff STUN im Zusammenhang mit dem Stichwort "Candidates" bzw. „Kandidaten“ (die angebotenen RTP-Endpunkte eines Geräts) verwenden, handelt es sich um diesen Classic STUN welcher im Standard über die Ports 3478 und 3479 läuft.

- Der zweite Anwendungsfall ist die Aushandlung der RTP Endpunkte zwischen Gerät und XCC, hier haben wir uns einen STUN-Mechanismus geliehen, damit sich diese Endpunkte finden (das sogenannte STUN-Binding Verfahren).

Sollte es also um UDP/RTP Ports, STUN-Binding Requests oder "fehlenden STUN Paketen von einem Device" gehen, handelt es sich um diese Art von STUN. (die Standard Portrange hierfür ist 30000-33000 UDP)

3.1.1. STUN Server konfigurieren

Ist ein STUN Server konfiguriert sowie im SIP-Gateway aktiviert, passiert folgendes:

- Der XCC fragt den STUN Server bei Erstaktivierung des STUN sowie bei jedem Neustart einmalig nach seiner öffentlichen IP-Adresse. Diese wird gecached, es gibt keine neuen STUN-Anfragen bei jedem einzelnen Anruf. Für bestimmte Softphone-Anrufe (genauer erklärt in Whitelist/Blacklist) wird dann die gespeicherte öffentliche IP-Adresse als Kandidat mit angeboten. Der Connect Client fragt bei jedem Call erst den STUN Server nach seiner öffentlichen IP-Adresse und liefert diese dann samt seiner lokale IP-Adresse als Kandidaten an den XCC.

Ist kein STUN Server konfiguriert oder nicht im SIP-Gateway aktiviert, passieren die oben genannten Schritte nicht. Es gibt keine anderen Kriterien, wann ein Request an einen STUN Server geschickt wird.

Um Softphone Mobile zu verwenden muss zwingend ein STUN Server konfiguriert werden. Wir empfehlen den Sipgate STUN Server, es kann aber auch jeder andere STUN verwendet werden. Gehen Sie wie folgt vor:

- Navigieren Sie zu Telefonie & Meetings > Netzwerk
- Klicken Sie beim STUN-Server auf "Hinzufügen..."
- Legen Sie den Namen, FQDN/IP und Port fest z.B.:

STUN Server hinzufügen
► Systemeinstellungen > Kommunikation > Netzwerk

STUN-Server aktivieren ☒

Name

FQDN/IP-Adresse
z.B: stun.sipgate.net

Port
STUN-Server default Port = 3478

- Klicken Sie auf Übernehmen und anschließend auf der Netzwerk-Seite auf Speichern
- Öffnen Sie das SIP-Gateway unter Telefonie & Meetings > Telefonie > SIP

- Setzen Sie das Häkchen bei "STUN Server verwenden" und Speichern Sie die Einstellung (**Achtung: Löst einen SIP-Gateway Neustart aus**)

SIP-Verbindung XCC <-> XPhone Connect Server (AnyDevice / Softphone)

Aktiviert ☒

IP-Adresse des XPhone Call Controllers Port

IP-Adresse des XPhone Connect Server Port

STUN Server verwenden ☒

LoopBack Adapter für SIP-Logging

Wichtig: Bei ausgelagertem XCC darf in beiden IP-Adress-Feldern keine 127.0.0.1 stehen, sondern die konkreten Adressen der Komponenten (XCC und Server).

3.1.2. Ports in der Firewall freigeben

Die Ports gemäß unserer Portliste müssen freigegeben sein: <https://help.c4b.com/xphone-connect-9/doc/de/admin/start/sys-req/infrstrctr.html#netzwerk> Zum Testen der Ports kann ebenfalls unser **WebApi-Tester** verwendet werden.

3.1.3. Bei Bedarf: Konfiguration der ACL's (White und Blacklist)

Achtung: Die ACL's sollten NUR verändert werden, wenn nach der gesamten restlichen Konfiguration etwas nicht funktioniert.

ACL steht für Access Control List und bietet zusätzliche Steuerungs- bzw. Konfigurationsmöglichkeiten für Payload.

Für die SIP Invites und Registrierung muss die Adresse des XPhone Servers (die Adresse die auch bei den SIP Gateways hinterlegt wird) explizit in der Whitelist freigegeben werden.

Im Regelfall gilt:

Whitelist-Einträge stechen Blacklist-Einträge. Whitelist-Einträge sollten definierter sein als Blacklist-Einträge, z.B.:

- Blacklist: 192.168.0.0/16
- Whitelist: 192.168.1.0/24

Somit wird nur das 192.168.1er Netz freigegeben, alle anderen 192.168er Netze sind geblockt. Es wird immer die White UND die Blacklist geprüft bis das erste "Allow" gefunden wurde.

Whitelist

Grundsatz: Der Block "Whitelist" blockiert alles, außer die konfigurierten Einträge.

Die 127.0.0.1/32 muss in der Whitelist gepflegt sein, wenn folgendes gegeben ist: XCC ist nicht ausgelagert und in der Loopback-Konfiguration wird mit 127.0.0.1 gearbeitet

Zusätzlich: Die im Screenshot markierte Adresse muss in der Whitelist gepflegt sein. Wenn man hier eine andere als die 127.0.0.1 verwendet, muss diese entsprechend eingetragen werden.

Blacklist

Grundsatz: Der Block "Blacklist" erlaubt alles, außer die konfigurierten Einträge.

ACL Konfiguration

Eine vom Default abweichende ACL Konfiguration macht dann Sinn, sobald mit STUN gearbeitet wird (i.d.R., wenn Softphone Mobile eingesetzt wird).

Lange Medienaushandlung bei Call-Annahme kann von schlecht konfigurierten ACL Einstellungen stammen. Hintergrund: Wenn zu viele ACL-Regeln hinterlegt sind, braucht es länger diese zu überprüfen und das kostet Zeit.

Kandidaten (SDP Session Description Protocol)

Der Freeswitch nimmt im Geradeausfall die erste, gültige Adresse für die Kandidatenaushandlung.

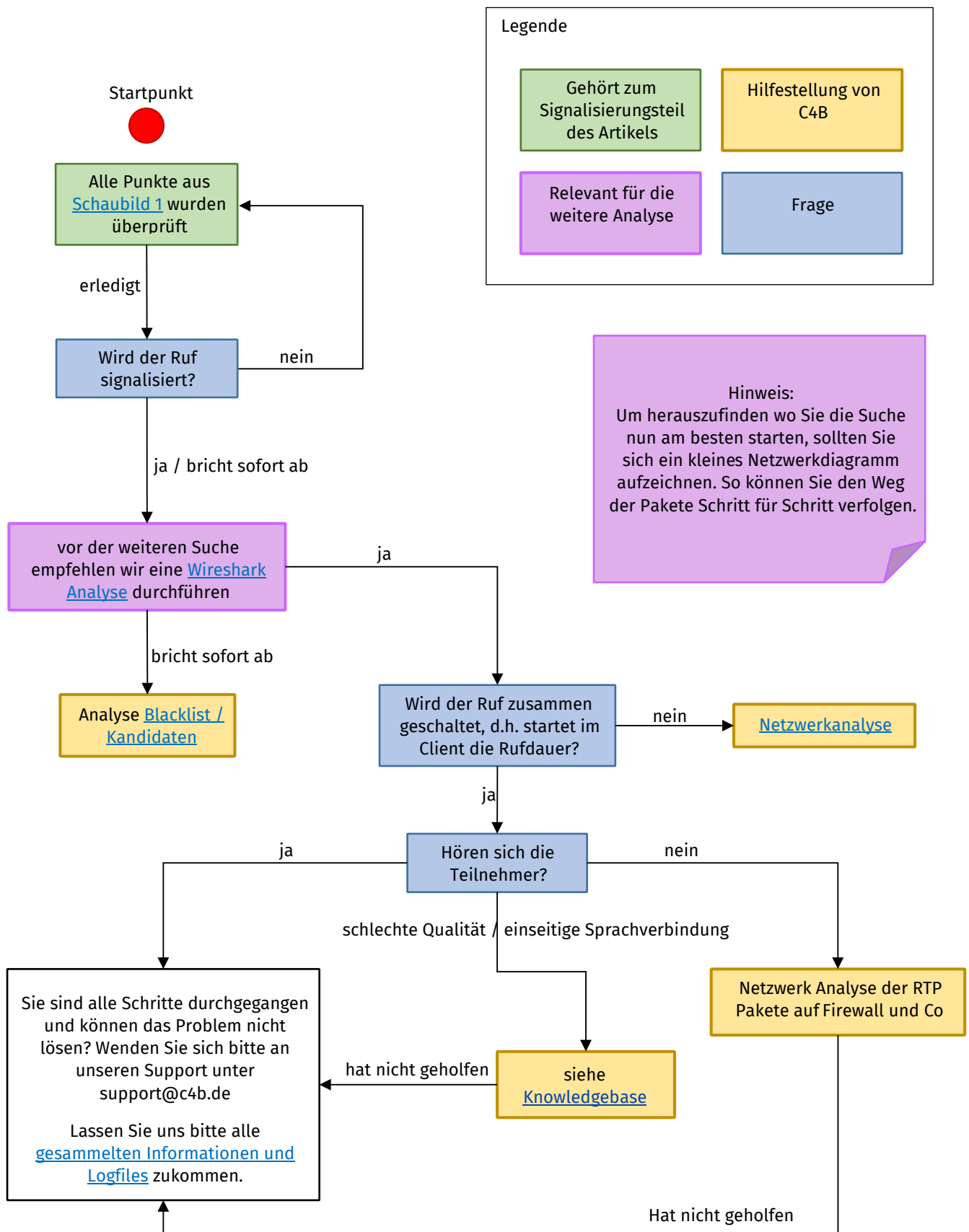
Zurück zum [Ablaufdiagramm Softphone Mobile](#)

4. NETZWERKANALYSE

Alle Punkte auf die unser erstes Schaubild verwiesen hat wurden überprüft und es klappt trotzdem nicht? Das deutet darauf hin, dass innerhalb des Kundennetzwerkes etwas schief geht. Um Ihnen bzw. dem Kunden auch an dieser Stelle unter die Arme greifen zu können haben wir diverse mögliche Ursachen aus Supportfällen gesammelt und aufbereitet. Da jede Kundenumgebung individuell ist, werden sicher einige Punkte fehlen. Sollten Sie mit den folgenden Ansätzen nicht weiterkommen oder Verbesserungsvorschläge / weitere Lösungsansätze für uns haben, melden Sie sich unter support@c4b.de.

Hier nun das zweite Schaubild für die genauere Analyse im Netzwerk. Starten Sie erneut beim roten Punkt.

INTERAKTIVES ABLAUFDIAGRAMM NETZWERKANALYSE



WIRESHARK ANALYSE

4.1.1. Erstellen und Vorbereitung des Wireshark Traces

Bevor man in die tiefere Analyse im Netzwerk geht, empfehlen wir ein Wireshark Trace vom XCC zu erstellen. Der XCC kann entweder lokal liegen oder als Satellit ausgelagert werden. Je nach Konstellation, gehen Sie gefolgt vor:

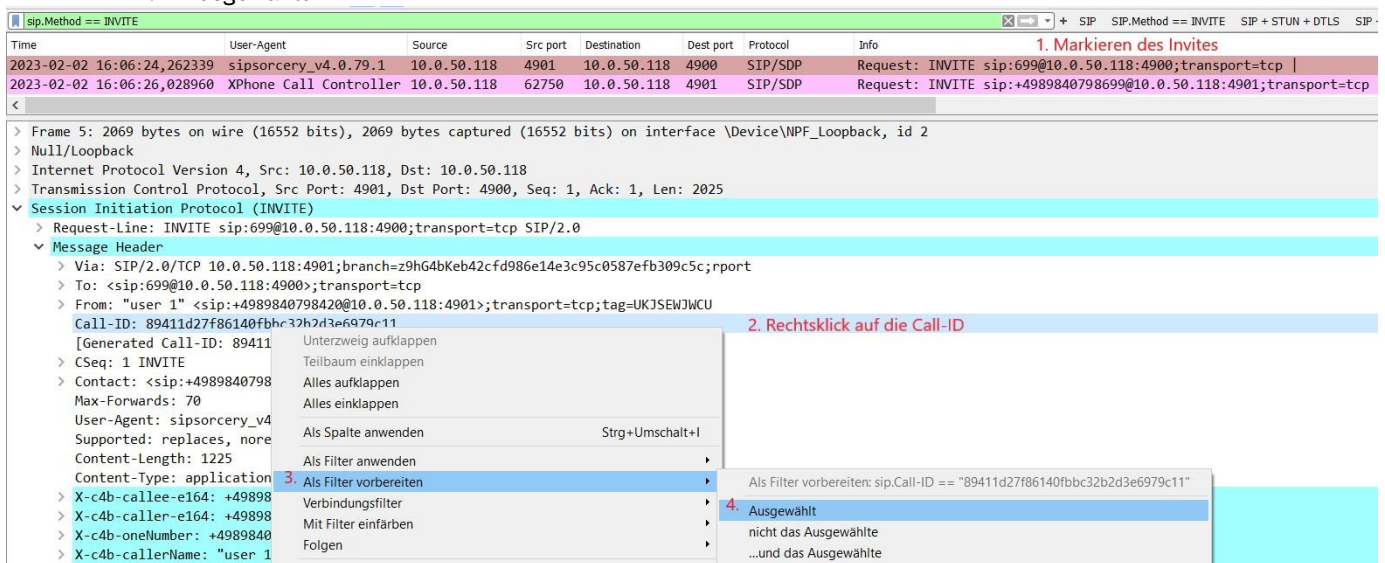
- Öffnen Sie das Programm Wireshark (falls das Programm noch nicht installiert ist finden Sie hier die aktuellste Version: <https://www.wireshark.org/#download>)
- Sie sehen hier nun die beiden Schnittstellen Ethernet und Npcap Loopback Adapter (ggf. heißen diese bei Ihnen etwas anders). Sollten Sie keine Schnittstelle sehen, versuchen Sie den Wireshark als Administrator zu starten oder den npcap-Treiber neu zu installieren.
- Markieren Sie dann die Ethernet-Schnittstelle und auch den Loopback Adapter mit gedrückter STRG-Taste an, um beide Schnittstellen zu markieren und drücken Sie anschließend im Eingabefeld Enter Hinweis:

Bei Verwendung eines Satelliten gehen Sie wie hier beschrieben vor:

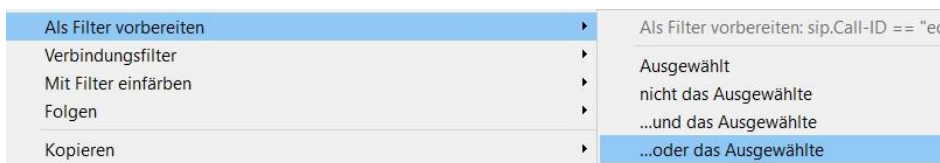
<https://support.c4b.de/hc/de/articles/5795413937308-Wie-erstelle-ich-einen-Wireshark-Trace-auf-dem-XCCSatelliten->

Im Folgenden wird die Analyse des Traces anhand eines Gutfalls gezeigt. So wie es auf den Screenshots aussieht (oder so ähnlich) sollte es bei Ihnen / dem Kunden auch aussehen.

- Geben Sie im Wireshark für eine bessere Übersicht nun erstmal den Anzeigefilter "**sip.Method == INVITE**" an und starten Sie nun einen Test Anruf.
- Suchen Sie sich nun den ersten Invite (=1. Call Leg) Ihres Anrufes und markieren Sie nun dessen Call-ID, diese ID bereiten Sie nun als Anzeigefilter vor, dies geht folgendermaßen:
 1. Markieren des Invites
 2. Rechtsklick auf die Call-ID
 3. Als Filter vorbereiten
 4. Ausgewählt



- Für die Call-ID des 2. Invites (=2. Call Leg) klicken Sie dann auf "...oder das Ausgewählte"



- Der Filter sieht dann wie folgt aus (Call-IDs sind nur exemplarisch):
(sip.Call-ID == "89411d27f86140fbbc32b2d3e6979c11") || (sip.Call-ID == "0135695c-1dae-123c-97a3-cb2054650f49")
- Fügen Sie nun noch "|| stun" zum Filter hinzu:
(sip.Call-ID == "89411d27f86140fbbc32b2d3e6979c11") || (sip.Call-ID == "0135695c-1dae-123c-97a3-cb2054650f49") || stun

- Drücken Sie nun Enter, werden Ihnen alle SIP Events zu den Call IDs, sowie alle STUN Meldungen des Traces angezeigt. (zur besseren Übersicht wurden für den Screenshot die beiden Call-Legs eingefärbt):

Time	User-Agent	Source	Src port	Destination	Dest port	Protocol	Info
2023-02-02 16:06:24,262339	sipsorcery_v4.0.79.1	10.0.50.118	4901	10.0.50.118	4900	SIP/SDP	Request: INVITE sip:699@10.0.50.118:4900;transport=tcp
2023-02-02 16:06:24,263545	XPhone Call Controller	10.0.50.118	4900	10.0.50.118	4901	SIP	Status: 100 Trying
2023-02-02 16:06:26,028960	XPhone Call Controller	10.0.50.118	62750	10.0.50.118	4901	SIP/SDP	Request: INVITE sip:+4989840798699@10.0.50.118:4901;transport=tcp
2023-02-02 16:06:26,011917		10.0.50.118	30012	192.168.178.28	65268	STUN	Binding Request user: 3a39ca0c:cHPTSDgupcMw88V0
2023-02-02 16:06:26,127829		93.228.1.1	65268	10.0.50.118	30012	STUN	Binding Request user: cHPTSDgupcMw88V0:3a39ca0c
2023-02-02 16:06:26,209483		10.0.50.118	30012	93.228.1.1	65268	STUN	Binding Success Response XOR-MAPPED-ADDRESS: 93.228.1.1:65268
2023-02-02 16:06:26,247820		192.168.178.28	65268	10.0.50.118	30012	STUN	Binding Request user: cHPTSDgupcMw88V0:3a39ca0c
2023-02-02 16:06:26,247885		10.0.50.118	30012	192.168.178.28	65268	STUN	Binding Success Response XOR-MAPPED-ADDRESS: 192.168.178.28:65268
2023-02-02 16:06:26,029203	XPhone Call Controller	10.0.50.118	4900	10.0.50.118	4901	SIP/SDP	Status: 183 Session Progress
2023-02-02 16:06:26,127829		10.0.50.118	4901	10.0.50.118	62750	SIP	Status: 100 Trying
2023-02-02 16:06:26,127970		10.0.50.118	4901	10.0.50.118	62750	SIP	Status: 180 Ringing
2023-02-02 16:06:27,041445		10.0.50.118	30012	93.228.1.1	65268	STUN	Binding Request user: 3a39ca0c:cHPTSDgupcMw88V0
2023-02-02 16:06:27,045080		93.228.1.1	65268	10.0.50.118	30012	STUN	Binding Success Response XOR-MAPPED-ADDRESS: 93.228.1.1:30012
2023-02-02 16:06:27,231016		93.228.1.1	65268	10.0.50.118	30012	STUN	Binding Request user: cHPTSDgupcMw88V0:3a39ca0c
2023-02-02 16:06:27,231083		10.0.50.118	30012	93.228.1.1	65268	STUN	Binding Success Response XOR-MAPPED-ADDRESS: 93.228.1.1:65268

4.1.2. Analyse der Kandidaten-Aushandlung

Im ersten Schritt prüft man, ob der XCC und auch der Client (also die Gegenstelle) private und/oder öffentliche Kandidaten austauschen.

Die für uns relevanten Kandidaten findet man im Message Body im SDP Header des INVITES vom Loopback Adapter (Default 127.0.0.1 sofern der XCC nicht ausgelagert ist, in unserem Fall die 10.0.50.118) und im Session Progress des gleichen Call Legs.

Time	User-Agent	Source	Src port	Destination	Dest port	Protocol	Info
2023-02-02 16:06:24,262339	sipsorcery_v4.0.79.1	10.0.50.118	4901	10.0.50.118	4900	SIP/SDP	Request: INVITE sip:699@10.0.50.118:4900;transport=tcp
<p>> Frame 5: 2069 bytes on wire (16552 bits), 2069 bytes captured (16552 bits) on interface \Device\NPF_{Loopback}, id 2</p> <p>> Null/Loopback</p> <p>> Internet Protocol Version 4, Src: 10.0.50.118, Dst: 10.0.50.118</p> <p>> Transmission Control Protocol, Src Port: 4901, Dst Port: 4900, Seq: 1, Ack: 1, Len: 2025</p> <p>> Session Initiation Protocol (INVITE)</p> <p>> Request-Line: INVITE sip:699@10.0.50.118:4900;transport=tcp SIP/2.0</p> <p>> Message Header</p> <p>> Message Body</p> <p>> Session Description Protocol</p> <p>Session Description Protocol Version (v): 0</p> <p>> Owner/Creator, Session Id (o): Icelink-3.14.3.12044 1298520866481146880 1 IN IP4 127.0.0.1</p> <p>Session Name (s): Frozen Mountain</p> <p>> Time Description, active time (t): 0 0</p> <p>> Session Attribute (a): group:BUNDLE audio</p> <p>> Media Description, name and address (m): audio 65268 UDP/TLS/RTP/SAVPF 96 9 0 8 97 98 99</p> <p>> Connection Information (c): IN IP4 93.228.130.114</p> <p>> Media Attribute (a): ice-ufraq:3a39ca0c</p> <p>> Media Attribute (a): ice-pwd:97842c82623c4396aeb8af51757cbf28</p> <p>> Media Attribute (a): mid:audio</p> <p>> Media Attribute (a): candidate:0bf81202d9fd5688b7c7804967e8e0f5 1 udp 2122294527 192.168.178.28 65268 typ host</p> <p>> Media Attribute (a): candidate:720fe172798f7cef93f7597fe02613c8 1 udp 1686086655 93.228.1.1 65268 typ srflx raddr 192.168.178.28 rport 65268</p>							

Was im Screenshot zu sehen ist, ist optimal. Es kommt ein RTP Endpunkt (Kandidat) mit einer öffentlichen und einer mit einer privaten IP Adresse.

Hinweis: Bei Owner / Creator sehen Sie den Begriff "Icelink". Das bedeutet in diesem SDP findet man die Kandidaten des Clients.

Zusatz: Falls der Candidate den Typ "srflx raddr" trägt, handelt es sich um eine IP Adresse die über STUN aufgelöst wurde (gelb markiert). Des Weiteren, stehe am Ende dieses Candidates auch über welche lokale IP Adresse der STUN Request abgesendet wurde:

> Media Attribute (a): candidate:0bf81202d9fd5688b7c7804967e8e0f5 1 udp 2122294527 192.168.178.28 65268 typ host
> Media Attribute (a): candidate:720fe172798f7cef93f7597fe02613c8 1 udp 1686086655 93.228.1.1 65268 typ srflx raddr 192.168.178.28 rport 65268

Bei einem Blick in das Session Progress sieht man ebenfalls beide Kandidaten:

Time	User-Agent	Source	Src port	Destination	Dest port	Protocol	Info
2023-02-02 16:06:26,029203	XPhone Call Controller	10.0.50.118	4900	10.0.50.118	4901	SIP/SDP	Status: 183 Session Progress
<							
> Frame 13: 1871 bytes on wire (14968 bits), 1871 bytes captured (14968 bits) on interface \Device\NPF_{Loopback}, id 2							
> Null/Loopback							
> Internet Protocol Version 4, Src: 10.0.50.118, Dst: 10.0.50.118							
> Transmission Control Protocol, Src Port: 4900, Dst Port: 4901, Seq: 359, Ack: 2026, Len: 1827							
> Session Initiation Protocol (183)							
> Status-Line: SIP/2.0 183 Session Progress							
> Message Header							
> Message Body							
> Session Description Protocol							
Session Description Protocol Version (v): 0							
> Owner/Creator, Session Id (o): FreeSWITCH 1675320373 1675320374 IN IP4 10.0.50.118							
Session Name (s): FreeSWITCH							
> Connection Information (c): IN IP4 10.0.50.118							
> Time Description, active time (t): 0 0							
> Session Attribute (a): msid-semantic: WMS Sv6a9cPDA7fn0h3vCY17JTSpcP7FaFhf							
> Media Description, name and address (m): audio 30012 UDP/TLS/RTP/SAVPF 96 97							
> Media Attribute (a): rtpmap:96 opus/48000/2							
> Media Attribute (a): fmp:96 useinbandfec=1; maxaveragebitrate=64000; maxplaybackrate=48000; sprop-maxcapture=48000; stereo=1							
> Media Attribute (a): rtpmap:97 telephone-event/48000							
> Media Attribute (a): ptime:20							
> Media Attribute (a): fingerprint:sha-256 32:69:55:38:8D:76:A5:68:C1:03:94:4A:5F:7A:99:75:21:8A:72:3F:33:74:CC:FC:1B:CC:75:B2:17:02:DD:B4							
> Media Attribute (a): setup:active							
> Media Attribute (a): rtcp-mux							
> Media Attribute (a): rtcp:30012 IN IP4 10.0.50.118							
> Media Attribute (a): ice-ufrag:cHPTSdgupcMw88V0							
> Media Attribute (a): ice-pwd:B2Xc1T1PX54EBraP750mfZT0							
> Media Attribute (a): candidate:3456002643 1 udp 2130706431 10.0.50.118 30012 typ host generation 0							
> Media Attribute (a): candidate:5177754415 1 udp 2130706431 93.228. 30012 typ host generation 0							

Hinweis: Bei Owner / Creator sehen Sie den Begriff "FreeSWITCH", das steht für die Kandidaten des Servers.

Liefern beide Gegenstellen (Client und Server) je eine öffentliche und eine private IP Adresse, kann man die Analyse der Kandidaten abschließen. Falls nicht, prüfen Sie die Unterpunkte bei unseren **bekannten Fehlerbildern**.

Tipp: Für die Fehleranalyse (auf Kundennetzwerkseite) eignet es sich den UDP Port des XCC-Candidates zu notieren, dieser kann später als Filter für die Firewall- oder Wireshark-Logs dienen. Filtert man z.B. ein Wireshark-Trace hiermit, kann man auf einem Blick die call-spezifische Aushandlung von STUN-Binding, DTLS und die schlussendliche Kommunikation über RTP sehen, in der Firewall lassen sich mit dem Filter ggf. geblockte/gedropte Pakete identifizieren.

4.1.3. Analyse der Bindings

Über Binding Requests wird versucht, die tatsächliche RTP Verbindung aufzubauen. Es wird initial ein Binding

Request vom XCC zu einem Kandidaten des Clients geschickt, damit die Netzwerkverbindung für diese eine Strecke "offen" ist (so etwas wie Pin-Hole-Punching). Dieser Binding Request wird jedoch nicht für die RTP Verbindung genutzt, selbst wenn er erfolgreich vom Client beantwortet werden sollte.

Der Client schickt danach ebenfalls Binding Requests von seinen Kandidaten zum XCC. Der XCC beantwortet dann die Binding Requests, nimmt jedoch für den Verbindungsaufbau den ersten beantworteten Binding Request her. Für weiteren Verbindungsaufbau wird dann DTLS ausgehandelt.

Binding Requests werden immer durchgeführt, unabhängig von einem konfigurierten STUN Server (Achtung, dieser ist dennoch Voraussetzung).

Binding Requests laufen über das STUN Protokoll.

Kehren wir zu unserem gefilterten Wireshark zurück:

Time	User-Agent	Source	Src port	Destination	Dest port	Protocol	Info
2023-02-02 16:06:24,262339	sipsorcery_v4.0.79.1	10.0.50.118	4901	10.0.50.118	4900	SIP/SDP	Request: INVITE sip:699@10.0.50.118:4900;transport=tcp
2023-02-02 16:06:24,263545	XPhone Call Controller	10.0.50.118	4900	10.0.50.118	4901	SIP	Status: 100 Trying
2023-02-02 16:06:26,028960	XPhone Call Controller	10.0.50.118	62750	10.0.50.118	4901	SIP/SDP	Request: INVITE sip:+4989840798699@10.0.50.118:4901;transport=tcp
2023-02-02 16:06:26,011917		10.0.50.118	30012	192.168.178.28	65268	STUN	Binding Request user: 3a39ca0c:cHPTSdgupcMw88V0
2023-02-02 16:06:26,209342		93.228. 65268		10.0.50.118	30012	STUN	Binding Request user: cHPTSdgupcMw88V0:3a39ca0c
2023-02-02 16:06:26,209483		10.0.50.118	30012	93.228. 65268		STUN	Binding Success Response XOR-MAPPED-ADDRESS: 93.228. 65268
2023-02-02 16:06:26,247820		192.168.178.28	65268	10.0.50.118	30012	STUN	Binding Request user: cHPTSdgupcMw88V0:3a39ca0c
2023-02-02 16:06:26,247885		10.0.50.118	30012	192.168.178.28	65268	STUN	Binding Success Response XOR-MAPPED-ADDRESS: 192.168.178.28:65268
2023-02-02 16:06:26,029203	XPhone Call Controller	10.0.50.118	4900	10.0.50.118	4901	SIP/SDP	Status: 183 Session Progress
2023-02-02 16:06:26,127829		10.0.50.118	4901	10.0.50.118	62750	SIP	Status: 100 Trying
2023-02-02 16:06:26,127970		10.0.50.118	4901	10.0.50.118	62750	SIP	Status: 180 Ringing
2023-02-02 16:06:27,041445		10.0.50.118	30012	93.228. 65268		STUN	Binding Request user: 3a39ca0c:cHPTSdgupcMw88V0
2023-02-02 16:06:27,045080		93.228. 65268		10.0.50.118	30012	STUN	Binding Success Response XOR-MAPPED-ADDRESS: 93.228. 30012
2023-02-02 16:06:27,231016		93.228. 65268		10.0.50.118	30012	STUN	Binding Request user: cHPTSdgupcMw88V0:3a39ca0c
2023-02-02 16:06:27,231083		10.0.50.118	30012	93.228. 65268		STUN	Binding Success Response XOR-MAPPED-ADDRESS: 93.228. 65268

Die **roten** Pakete gehören zum 1. Call Leg. In diesem Fall ist das der Call-Leg auf dem Loopback Adapter. Die Pakete in **rosa** gehören zum 2. Call Leg, diese gehen vom XPhone Server in Richtung Gegenstelle (das kann der Connect Client sein oder auch das Handy bei Verwendung von Softphone Mobile). Die **blauen** Pakete sind die nun relevanten. Was Sie im Screenshot sehen ist ein Gutfall bei dem die Binding Request Pakete von der Gegenstelle mit einem Binding Success beantwortet werden.

Die Wireshark Analyse ist nun abgeschlossen.

Wenn Sie sich bis hierher eingelese haben, dann haben Sie vermutlich einen Schlechtfall und möchten diesen Lösen. Im Folgenden finden Sie die uns bisher bekannten Fehlerbilder. Sie können entweder Ihr Trace mit diesen vergleichen oder die Schritte im Ablaufdiagramm weiter durchgehen.

Zurück zum [Ablaufdiagramm Netzwerkanalyse](#)

5. BEKANNTE FEHLERBILDER

MOBILE APP ANMELDUNG NICHT MÖGLICH

Wenn die Tests im WebApi Test Tool erfolgreich sind, die Mobile App Anmeldung jedoch nicht möglich ist, überprüfen Sie die **Grundkonfiguration** und werfen Sie einen Blick auf folgenden KB-Artikel:
<https://support.c4b.de/hc/de/articles/8809009914268-Warum-kann-ich-mich-in-der-Mobile-App-nicht-anmelden->

KEINE GERÄTE IN DER MOBILE APP VERFÜGBAR

Bei IOS werden Geräte in der Mobile App angezeigt, bei Android nicht.

Wichtig: Sollten bei IOS UND Android keine Geräte verfügbar sein, scheint etwas mit der **Grundkonfiguration** nicht zu stimmen und muss an anderer Stelle behoben werden.

Sollte es nur bei Android zu dem beschriebenen Verhalten kommen, prüfen Sie bitte die Punkte des folgenden Artikels:

<https://support.c4b.de/hc/de/articles/8809119345180-Warum-sehe-ich-keine-Ger%C3%A4te-in-der-MobileApp->

FEHLENDE BINDING SUCCESS MELDUNGEN IM WIRESHARK

Im Wireshark sieht man, dass die STUN Binding Requests versendet werden, jedoch sieht man keine Binding Success Meldungen:

No.	Time	Protocol	User-Agent	#Source	Destination	Info
2758	2022-12-05 14:59:49,610593	SIP/SDP	sipsorcery_v4.0.79.1	127.0.0.1	127.0.0.1	Request: INVITE sip: [REDACTED]@127.0.0.1:4901;transport=tcp
2765	2022-12-05 14:59:49,612007	SIP	XPhone Call Controller	127.0.0.1	127.0.0.1	Status: 100 Trying
2776	2022-12-05 14:59:49,624317	SIP/SDP	XPhone Call Controller	127.0.0.1	127.0.0.1	Status: 183 Session Progress
2887	2022-12-05 14:59:49,620648	SIP/SDP	XPhone Call Controller	192.168.101.12	192.168.101.10	Request: INVITE sip: [REDACTED]@192.168.101.10:5060
2933	2022-12-05 14:59:49,645316	STUN		192.168.101.12	172.20.10.2	Binding Request user: 8b708ebc:BUmkOSgeYbP7L5rF
2936	2022-12-05 14:59:49,648206	SIP		192.168.101.10	192.168.101.12	Status: 180 Ringing
5427	2022-12-05 14:59:54,665315	STUN		192.168.101.12	172.20.10.2	Binding Request user: 8b708ebc:BUmkOSgeYbP7L5rF
6767	2022-12-05 14:59:57,331167	SIP/SDP		192.168.101.10	192.168.101.12	Status: 200 OK (INVITE)
6768	2022-12-05 14:59:57,332208	SIP		192.168.101.12	192.168.101.10	Request: ACK sip: [REDACTED]@192.168.101.10:5060;transport=udp
6769	2022-12-05 14:59:57,333041	STUN		192.168.101.12	172.20.10.2	Binding Request user: 8b708ebc:BUmkOSgeYbP7L5rF
6875	2022-12-05 14:59:57,354160	SIP/SDP	XPhone Call Controller	127.0.0.1	127.0.0.1	Status: 200 OK (INVITE)
6881	2022-12-05 14:59:57,354688	SIP		127.0.0.1	127.0.0.1	Request: ACK sip: [REDACTED]@127.0.0.1:4901;transport=tcp
9756	2022-12-05 15:00:02,374697	STUN		192.168.101.12	172.20.10.2	Binding Request user: 8b708ebc:BUmkOSgeYbP7L5rF
12...	2022-12-05 15:00:07,377613	STUN		192.168.101.12	172.20.10.2	Binding Request user: 8b708ebc:BUmkOSgeYbP7L5rF
13...	2022-12-05 15:00:09,112671	SIP		127.0.0.1	127.0.0.1	Request: BYE sip: [REDACTED]@127.0.0.1:4901;transport=tcp
13...	2022-12-05 15:00:09,133468	SIP	XPhone Call Controller	127.0.0.1	127.0.0.1	Status: 200 OK (BYE)
13...	2022-12-05 15:00:09,112948	STUN		192.168.101.12	172.20.10.2	Binding Request user: 8b708ebc:BUmkOSgeYbP7L5rF
13...	2022-12-05 15:00:09,178382	SIP	XPhone Call Controller	192.168.101.12	192.168.101.10	Request: BYE sip: [REDACTED]@192.168.101.10:5060;transport=udp
13...	2022-12-05 15:00:09,179495	SIP		192.168.101.10	192.168.101.12	Status: 200 OK (BYE)

Typische Ursache

- Keine Routen zwischen den Netzwerken
- Firewall fängt Pakete ab

Mögliche Lösung

- **Pin Hole Puncher** aktivieren (Hintergrund: Der XCC im Standard pingt nur einen Kandidaten an. Wenn dieser nicht erreichbar ist, aus welchem Grund auch immer, kann man mit dem Pin Hole Puncher dafür sorgen, dass der XCC alle RTP Endpunkte des Clients anpingt und ggf. die nötigen Ports in der Firewall öffnet.)
- Firewall Trace starten und die Routen prüfen auf denen Pakete abgefangen werden könnten
- Wireshark Trace auf Desktop Client und XCC starten und prüfen ob die bidirektionalen Pakete auch auf beiden Seiten ankommen

Hilfestellung

Prüfen ob XCC Pakete das Netzwerk verlassen:

- WAN Schnittstelle des Kunden tracen und prüfen ob der XCC nach extern über die vordefinierte Portrange (im Standard des XCCs ist das die Port Range 30000-33000) kommuniziert
 - Falls dies nicht passiert, läuft schon auf dem Weg vom XCC zur Firewall etwas schief. So etwas zu tracen ist schwer, im Normalfall hilft es jedoch die Pakete Schritt für Schritt zu verfolgen, tracen Sie also am besten jede mögliche Schnittstelle, die den UDP Traffic des XCCs manipulieren könnte (Firewall / Switches / Loadbalancer etc.)

- Falls die Pakete auf der WAN Schnittstelle ins öffentliche Netz versendet werden, sind Sie mit diesem Schritt fertig und können nun zur Prüfung der Client UDP Pakete gehen

Prüfen ob Client UDP Pakete im Firmennetz/ XCC ankommen:

Damit Sie den Netzwerk-/ Firewall-Admin unter die Arme greifen können, geben wir Ihnen hier einmal ein paar Tipps an die Hand, um Probleme mit der UDP Port Range zu analysieren. Was benötigen Sie für den Test:

- Ein Firewall Log, welches wiedergibt, aufgrund welcher Regeln Pakete abgewiesen/zugelassen werden
- Ein TCP Dump/Trace der Firewall, hiermit lässt sich eine falsche Umleitung der Pakete erkennen
- Den WebApi Tester (<https://wonderful-wave-0fef5e603.2.azurestaticapps.net/>)
- Zugriff auf die XCC Konsole

Vorgehen:

- Aktivieren Sie ein Trace auf der Firewall auf der WAN Schnittstelle der Firewall, welche den Übergang ins Internet darstellt, hier müssen die Pakete der Mobile App ankommen
- Führen Sie nun einen UDP Port Test via WebApi Tester durch, eine genaue Beschreibung zur Vorgehensweise finden Sie in der Hilfe des WebApi Tester <https://wonderful-wave-0fef5e603.2.azurestaticapps.net/help.html>
- Überprüfen Sie anschließend die Firewall Logs auf die vordefinierten RTP Ports (im Standard des XCCs ist das die Port Range 30000-33000)
- Falls Pakete blockiert werden:
 - überprüfen Sie bitte Ihr Port-Forwarding
 - oder das NAT der Firewall, dieses darf den Port welchen der XCC für die ausgehende Kommunikation verwendet nicht abändern, heißt wenn der XCC Port 33000 verwendet, muss dieser Port auch von extern für den Mobile Client erreichbar sein

Mögliche weitere "Fehlerquellen":

- Es kam schonmal vor, dass ein Destination NAT in der Firewall eingerichtet war, dieses muss natürlich auf den XCC zeigen, damit der Payload zustande kommen kann
- Manche Kunden aktivieren gerne ALG-Firewalls (Application Layer Gateway Firewalls) welche ggf. den Traffic blocken können (sei es SIP oder STUN)

Sollten Sie nach allen Anstrengungen kein UDP Paket vom Client auf der WAN Schnittstelle des Kunden finden, kann es sein, dass der Client gar nicht bis zur WAN Firewall des Kunden kommt. Hier kann es mehrere Ursachen geben.

Ein paar bekannte Beispiele aus unserer Erfahrung sind:

- Firewall auf Softphone Mobile Seite (in einem Funknetz welches nicht von Kunden verwaltet wird und welches ggf. recht restriktive ausgehende Firewall-Regeln besitzt)
- Antivirens Scanner
- VPN Tunnel blockiert/ verwirft die Pakete schon auf dem Mobile Gerät

Um das Verhalten zu prüfen befolgen Sie bitte den folgenden Schritt " Prüfen ob Client Pakete versendet"

Prüfen ob Client Pakete versendet:

Bitte gehen Sie folgende Schritte durch, um zu verifizieren ob der Client UDP Pakete an den XCC sendet.

- Überprüfen Sie, falls vorhanden, die Firewall der Netzwerkverbindung auf Client Seite via der vorhin erwähnten Firewall Log/ TCP Dump Methode
 - hier kann wieder auf den Zielport des XCCs oder die Portrange gefiltert werden (oder ggf. auf den verwendeten Port des Porttesters)
 - sollte nichts auf der Firewall ankommen, gibt es entweder Netzwerkkomponenten im Netz die die UDP Pakete blockieren, oder das Gerät blockiert diese selbst. Beide dieser möglichen Fehlerquellen, können wir leider nicht tracen oder mit XPhone-Bordmitteln erkennen, hier ist eine Analyse Ihrerseits/ des Dienstleisters/ der Admins gefragt
- Sollte es keine Firewall geben, wie bei Mobilfunk Netzen, muss ggf. Kontakt mit dem Provider aufgebaut werden. An der Stelle müssen Sie diesen Fragen, weshalb versendete UDP Pakete nicht an der öffentlichen IP-Adresse des XCCs ankommen.

FEHLENDE ÖFFENTLICHE ODER PRIVATE KANDIDATEN IM WIRESHARK

Im Wireshark prüft man den SDP Header aus dem INVITE und dem Session Progress des XCC's (IP Adresse 127.0.0.1, kann bei ausgelagertem XCC abweichen). In unserem Beispiel wird vom Freeswitch (siehe roter Rahmen) nur ein Kandidat versendet. Dieser hat eine private IP Adresse.

No.	Time	Protocol	User-Agent	#Source	Destination	Info
2776	2022-12-05 14:59:49.624317	SIP/SDP	XPhone Call Controller	127.0.0.1	127.0.0.1	Status: 183 Session Progress
<						
> Frame 2776: 1782 bytes on wire (14256 bits), 1782 bytes captured (14256 bits) on interface \Device\NPF_{...} id 1						
> Null/Loopback						
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1						
> Transmission Control Protocol, Src Port: 4901, Dst Port: 4900, Seq: 361, Ack: 1900, Len: 1738						
✓ Session Initiation Protocol (183)						
> Status-Line: SIP/2.0 183 Session Progress						
> Message Header						
✓ Message Body						
✓ Session Description Protocol						
Session Description Protocol Version (v): 0						
> Owner/Creator, Session Id (o): FreeSWITCH 1670217503 1670217504 IN IP4 192.168.101.12						
Session Name (s): FreeSWITCH						
> Connection Information (c): IN IP4 192.168.101.12						
> Time Description, active time (t): 0 0						
> Session Attribute (a): msid-semantic: WMS wwa9gFPYT263laTH7cYmlvpHXT6Qlnhs						
> Media Description, name and address (m): audio 31286 UDP/TLS/RTP/SAVPF 96 97						
> Media Attribute (a): rtpmap:96 opus/48000/2						
> Media Attribute (a): fmtp:96 useinbandfec=1; maxaveragebitrate=64000; maxplaybackrate=48000; sprop-maxcapture=48000; stereo=1						
> Media Attribute (a): rtpmap:97 telephone-event/48000						
> Media Attribute (a):ptime:20						
> Media Attribute (a): fingerprint:sha-256 1A:82:D0:30:B4:59:FA:42:3C:8A:F5:51:3F:C8:83:44:9E:C3:CB:95:DD:5D:47:4E:92:4E:B0:7F:5E:48:09:63						
> Media Attribute (a): setup:active						
Media Attribute (a): rtcp-mux						
> Media Attribute (a): rtcp:31286 IN IP4 192.168.101.12						
> Media Attribute (a): ice-frag:BUmkOSgeYbP7L5rF						
> Media Attribute (a): ice-pwd:Vr4YA48AkeiGy93Uo1EmBN2f						
> Media Attribute (a): candidate:1925634062 1 udp 2130706431 192.168.101.12 31286 typ host generation 0						
Media Attribute (a): end-of-candidates						

Dieses Bild sorgt dafür, dass eine Kommunikation außerhalb des Netzes nicht möglich ist, da der XCC nur über eine interne IP-Adresse erreichbar ist.

Typische Ursache

- STUN Server wird nicht erreicht und daher schickt der Freeswitch oder der Client nur private Kandidaten

Mögliche Lösung

- Firewall prüfen
- Prüfen ob der jeweilige Client (Desktop oder Mobile) den STUN Server erreicht ([WebApi-Tester](#))
- Prüfen ob der STUN Server vom XPhone Server aus erreichbar ist z.B. mit dem [WebApi-Tester](#) oder dem STUN Test in der Adminoberfläche:

Telefonie & Meetings > Netzwerk

NAT-Typen Erkennung

Die "NAT-Typen Erkennung" ist ein Werkzeug, welches ermitteln kann hinter welchem NAT-Typen der XPhone Connect sollten.

Die Überprüfung der "Erreichbarkeit dieses STUN-Servers" überprüft, ob der XPhone Call Controller (lokal oder ausg.)

SIP Gate

NAT-Typen erkennen

Erreichbarkeit dieses STUN-Servers überprüfen

Hinweis: In älteren V9 Versionen kann es sich auch noch um einen bekannten Bug handeln. Dieser wurde mit einem Patch für die V9.0.131 behoben und ist in V9.0.164 enthalten.

IP ADRESSEN DER PAKETE STIMMEN NICHT ÜBEREIN

Aufgrund diverser Konfigurationen kann es vorkommen, dass der XPhone Server zwei Netzwerkkarten hat und durch eine falsche / fehlende Konfiguration auf der falschen kommuniziert wird. So könnte dieses Thema im Wireshark aussehen:

Time	User-Agent	Source	Src port	Destination	Dest port	Protocol	Info
2023-01-26 15:26:11,662812	sipsorcery_v4.0.79.1	10.0.50.118	4901	10.0.50.118	4900	SIP/SDP	Request: INVITE sip:de_testcall@10.0.50.118:4900;transport=tcp
2023-01-26 15:26:11,665593	XPhone Call Controller	10.0.50.118	4900	10.0.50.118	4901	SIP	Status: 100 Trying
2023-01-26 15:26:11,670174	XPhone Call Controller	10.0.50.118	4900	10.0.50.118	4901	SIP/SDP	Status: 183 Session Progress
2023-01-26 15:26:11,797723	Netzwerkkarte 1	80.187.65.222	28953	10.0.50.121	30004	STUN	Binding Request user: NQRFr1pNjICiU5UF:9bef59e5
2023-01-26 15:26:11,682309		10.0.50.118	30004	172.20.10.2	61568	STUN	Binding Request user: 9bef59e5:NQRFr1pNjICiU5UF
2023-01-26 15:26:11,995552	Netzwerkkarte 2	80.187.65.222	28953	10.0.50.121	30004	STUN	Binding Request user: NQRFr1pNjICiU5UF:9bef59e5
2023-01-26 15:26:12,430787		80.1		10.0.50.121	30004	STUN	Binding Request user: NQRFr1pNjICiU5UF:9bef59e5
2023-01-26 15:26:13,220685		80.1		10.0.50.121	30004	STUN	Binding Request user: NQRFr1pNjICiU5UF:9bef59e5

Typische Ursache

- Multiple öffentliche IP-Adressen beim Kunden:
So kann es dazu kommen, dass der XCC aufgrund der Netzwerkeinstellungen mit Adresse A rausschickt, jedoch zuvor im STUN Request eine andere öffentliche IP Adresse B erhalten hat, welche dem Client übermittelt wird, welche diese Nutz > Datenströme finden nicht zusammen
- XCC besitzt mehrere Netzwerkkarten läuft das NAT so dass RTP und STUN auf die Primäre Adresse des XPhone Servers / XCCs geschickt werden, obwohl dieser eigentlich die sekundäre Adresse in den Konfigurationen stehen hat > So finden sich die beiden Maschinen ebenfalls nicht, da die IP/Port Kombination nicht stimmt

Mögliche Lösung

- Nur noch eine Netzwerkkarte verwenden
- Routing in der Firewall anpassen

GEBLOCKTER CALL (DURCH ACL) – 403 FORBIDDEN

Wird ein Anruf direkt abgeblockt, sieht das Ganze im Wireshark wie folgt aus:

Time	User-Agent	Source	Src port	Destination	Dest port	Protocol	Info
2023-01-26 15:04:17,764065	sipsorcery_v4.0.79.1	10.0.50.118	4901	10.0.50.118	4900	SIP/SDP	Request: INVITE sip:de_testcall@10.0.50.118:4900;transport=tcp
2023-01-26 15:04:17,765175	XPhone Call Controller	10.0.50.118	4900	10.0.50.118	4901	SIP	Status: 403 Forbidden
2023-01-26 15:04:17,765516		10.0.50.118	4901	10.0.50.118	4900	SIP	Request: ACK sip:de_testcall@10.0.50.118:4900;transport=tcp

Das 403 Forbidden zeigt schon auf den ersten Blick, dass an irgendeiner Stelle etwas geblockt wird. An diesem Punkt sollte man dann in das sogenannte "FS Log" zur genaueren Überprüfung sehen. Dieses finden Sie im Logordner des XCC unter einem Namen wie z.B.: "XCC_FS_2023_01_26_14_59_05.log" Nun schaut man zu dem Zeitpunkt des Tests und findet z.B. einen Eintrag wie diesen hier:

```
2023-01-26 15:04:17.755102 [DEBUG] sofia.c:10509 verifying acl "xcc_localnet" for ip/port 10.0.50.118:0.  
2023-01-26 15:04:17.755102 [WARNING] sofia.c:10622 IP 10.0.50.118 Rejected by acl "xcc_localnet"
```

An dieser Stelle werden die ACL's (Black und Whitelist) überprüft. In unserem Fall stößt der Server bei der 10.0.50.118 auf ein Problem.

Haben Sie einen ähnlichen Fall, werfen Sie bitte einen Blick in die [Konfiguration der Black und Whitelist](#).

GEBLOCKTE KANDIDATEN (DURCH ACL) – 488 NOT ACCEPTABLE HERE

Werden Kandidaten geblockt kann sich das wie folgt im Wireshark äußern:

Time	User-Agent	Source	Src port	Destination	Dest port	Protocol	Info
2023-02-02 13:13:23,020422	sipsorcery_v4.0.79.1	10.0.50.118	4901	10.0.50.118	4900	SIP/SDP	Request: INVITE sip:de_testcall@10.0.50.118:4900;transport=tcp
2023-02-02 13:13:23,022017	XPhone Call Controller	10.0.50.118	4900	10.0.50.118	4901	SIP	Status: 100 Trying
2023-02-02 13:13:23,025767	XPhone Call Controller	10.0.50.118	4900	10.0.50.118	4901	SIP	Status: 488 Not Acceptable Here
2023-02-02 13:13:23,026048		10.0.50.118	4901	10.0.50.118	4900	SIP	Request: ACK sip:de_testcall@10.0.50.118:4900;transport=tcp

Typische Ursache:

- Private / Öffentliche IP Adressen der angebotenen Kandidaten werden durch die ACLs geblockt

Mögliche Lösung:

Überprüfen der Kandidaten die uns angeboten werden:

```
> Owner/Creator, Session Id (o): IceLink-3.14.3.12044 7327698553850195968 1 IN IP4 127.0.0.1
  Session Name (s): Frozen Mountain
> Time Description, active time (t): 0 0
> Session Attribute (a): group:BUNDLE audio
> Media Description, name and address (m): audio 56290 UDP/TLS/RTP/SAVPF 96 9 0 8 97 98 99
> Connection Information (c): IN IP4 93.228.1.1
> Media Attribute (a): ice-ufrag:ab8aa0fc
> Media Attribute (a): ice-pwd:4666c573bac8409882e04a963070a1c3
> Media Attribute (a): mid:audio
> Media Attribute (a): candidate:a177363cad22b150a7941723204347d1 1 udp 2122294527 192.168.69.112 56290 typ host
> Media Attribute (a): candidate:68e969ff339a21abd50a25188a5a73fe 1 udp 1686086655 93.228.1.1 56290 typ srflx raddr 192.168.69.112 rport 56290
> Media Attribute (a): fingerprint:sha-256 33:A2:5A:E9:52:76:9D:4F:42:D3:EF:03:F3:5D:98:92:2F:C8:27:EF:95:9A:18:E8:DA:65:C4:C4:65:82:11:DB
```

Prüfen Sie nun in der Black und Whitelist in der Konfiguration des XCCs, ob einer / beide der Kandidaten geblockt wurden:

Private IP-Adressbereiche

Geben Sie hier zwingend den im Unternehmen konfigurierten privaten Adressbereich (ver Audio-Medien-Verbindung innerhalb des Firmennetzwerks bleibt.

Adressbereich LAN/VPN	IP-Adresse	Suffix		
	127.0.0.1	/ 8	+	-
	10.0.50.0	/ 24	+	-

Zugriffskontrolle über IP-Adressbereiche (Blacklist)

Die hier aufgelisteten Netzwerke werden nicht für die Medien-Kommunikation verwendet. Separation). Weitere Informationen und Beispiele finden Sie in der Dokumentation.

Adressbereich WAN/LAN	IP-Adresse	Suffix		
	0.0.0.0	/ 8	+	-
	10.0.0.0	/ 8	+	-
	192.168.0.0	/ 16	+	-
	93.0.0.0	/ 8	+	-

In diesem Fall wurde die private und die öffentliche IP Adresse des Clients geblockt. Dadurch wird natürlich vom XCC abgebrochen.

Haben Sie einen ähnlichen Fall, werfen Sie bitte einen Blick in die [Konfiguration der Black und Whitelist](#).

6. TICKETERSTELLUNG

Wenn der Artikel bei der Ursachenfindung nicht helfen konnte, steht es unseren Partnern natürlich frei ein Ticket bei unserem Support zu eröffnen. Je besser Tickets mit solch komplexen aufbereitet werden, desto schneller ist eine Lösung auffindbar.

Bitte teilen Sie uns so viele Informationen wie möglich mit:

- XID des Kunden
- Wie äußert sich das Fehlerbild?
- Seit wann tritt der Fehler auf und was hat sich geändert?
- Sind alle User von dem Verhalten betroffen?
- Tritt der Fehler extern oder intern auf?
- Funktioniert Softphone Desktop?
- Ist der XCC ausgelagert?

Folgende Logfiles werden benötigt:

- Logordner SIP Trunk
- Logordner XCC
- Logordner Festnetzgateway (sofern ein Office Device im Szenario involviert ist)
- ungefilterter Wireshark von Loopback und Ethernet Adapter
- Mobile App Logs (bei Problemen mit Signalisierung) Anleitungen zur Loggerstellung finden Sie hier:
<https://support.c4b.de/hc/de/articles/5669195253404>

Bei der Szenario Beschreibung zu den Logfiles benötigen wir folgende Informationen:

- Schritt für Schritt Anleitung des Testablaufs
- beteiligte Devices
- beteiligte Rufnummern
- ein grobes Netzwerkdiagramm der Kundenumgebung
- Uhrzeit des Tests

Copyright und Rechtliche Hinweise

C4B Com For Business AG

Untere Point 8

82110 Germering | Germany

+49 (89) 840798 - 0

E-Mail: support@c4b.de

Website: www.c4b.com

Copyright © C4B Com For Business AG.

Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieses Handbuchs oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch die C4B Com For Business AG nicht gestattet. In dieser Dokumentation enthaltene Informationen können ohne vorherige Ankündigung geändert und ergänzt werden.

Keine Gewährleistung. Dieses Handbuch wird Ihnen wie vorgelegt zur Verfügung gestellt. Die C4B Com For Business AG übernimmt keine Gewährleistung bezüglich der Genauigkeit oder Nutzung dieses Handbuchs. Jeglicher Gebrauch des Handbuchs oder der darin enthaltenden Informationen erfolgt auf Risiko des Benutzers. Das Handbuch kann Ungenauigkeiten technischer oder anderer Art sowie typografische Fehler enthalten.

Die Lizenzrechte für eine weltweite, zeitlich unlimitierte Nutzung der installierten wav-Dateien des XPhone Connect Servers liegen bei C4B Com For Business AG. Eine Nutzung durch Partner und Kunden der C4B Com For Business AG ist im Rahmen der bestimmungsgemäßen Verwendung des Standardprodukts XPhone Connect Server erlaubt. Eine weitere Verwendung, Verwertung oder Weiterverkauf außerhalb dieser Telekommunikationssysteme ist nicht gestattet, ebenso wenig wie eine Ausstrahlung über TV, Rundfunk oder Internet. Jegliche weitere Nutzung ist untersagt und nur ggf. in Rücksprache mit C4B Com For Business AG gestattet."

Microsoft®, Windows®, Word®, Excel®, Access®, Outlook®, Teams® und Skype® for Business sind eingetragene Warenzeichen der Microsoft Corporation.

Unify®, OpenScape®, OpenStage® und HiPath® sind eingetragene Warenzeichen der Unify GmbH & Co. KG.

XPhone™ ist ein eingetragenes Warenzeichen der C4B Com For Business AG.

Andere in dieser Dokumentation erwähnte Hard- und Softwarenamen sind Handelsnamen und/oder Marken der jeweiligen Hersteller.