Technische Hinweise zur Netzwerkkonfiguration

Technische Hinweise für einen reibungslosen Betrieb der SIP-basierten foncloud TK-Anlage

Inhalt

1. Router

Für die Initiale Einrichtung des Telefons muss ein **DHCP-Server** vorhanden sein.

In dem DHCP-Server muss die **Option 66** deaktiviert werden. Sollte Ihr Router keine Einstellmöglichkeit für Option 66 bieten, ignorieren Sie diesen Hinweis einfach.

Ein vorhandenes **SIP ALG** ist zu deaktivieren.

Der **UDP-NAT Timeout** (UDP-Aging) sollte mehr als 60 Sekunden betragen. Wir empfehlen einen Wert von 180 Sekunden.

Es müssen keine extra **Portweiterleitung** erstellt werden.

1.1 Empfohlene Router

Kleine Umgebungen

Große Umgebungen

- Fritzbox (für maximal 8 laufende Gespräche gleichzeitig)
- TP-Link N Serie
- DrayTek Vigos Serie
- MikroTik
- Cisco 800er Serie und größer
- LANCOM

1.2 Black-List Router

- Technicolor ältere Modelle (aufgrund von NAT-Handling)
- BINTEC be.IP Serie

2. Firewall

Ein vorhandenes **SIP ALG** ist in jedem Fall zu deaktivieren.

Der **UDP-NAT Timeout** (UDP-Aging) sollte mehr als 60 Sekunden betragen. Wir empfehlen einen Wert von 180 Sekunden.

Beim Einsatz von **SonicWall Firewalls** muss der NAT Modus auf „Consistant-NAT" eingestellt werden.

2.1 Portfreigaben und IP-Adressfreigaben

- 5060 + 5061 UDP für Signalisierung
- 12000-13100 UDP für RTP (Gesprächsdaten)
- 3478 für Stun
- 123 UDP für NTP (Synchronisation der Uhrzeit)
- 80 TCP
- 443 TCP
- 2443 TCP

Für die Portfreigaben gilt zu beachten:

- Für jeden Hersteller definieren wir einen „Basisport"
- Ein Telefon wird sich über den Basisport + Nebenstelle registrieren

Abhängig vom Endgerätehersteller müssen **zusätzlich** folgende **UDP Ports** freigegeben werden:

- Snom und Grandstream: ab Port 10.000
- Yealink Tischtelefone: ab Port 20.000
- Gigaset DECT: fester Port 15.060
- Yealink DECT: fester Port 20.000

2.2 Beispiel für restriktive Firewallregeln

In diesem Beispiel wird für jedes Telefon eine eigene ausgehende Regel definiert.

Sie haben ein Telefon mit der Nebenstelle 100.

- Ein Snom Endgerät, wird sich über den Port 10.100 anmelden.
- Ein Yealink Tischtelefon wird Port 20.100 verwenden.
- Ein Gigaset DECT-Telefon wird den Port 15.060 verwenden.
- Ein Yealink DECT-Telefon wird den Port 20.000 verwenden.

2.3 Beispiel für einfache Firewallregeln

In diesem Beispiel wird eine einzelne ausgehende Freigabe für alle Telefone im Firmennetz erstellt.

Sie konfigurieren hierfür eine ausgehende Regel für das lokale Netzwerk mit den unter 2.1 genannten Ports.

3. Quality of Service – Maßnahmen für VoIP (QoS)

Vorwort

In diesem Abschnitt werden die unterschiedlichen Möglichkeiten für eine Priorisierung innerhalb der lokalen Netzwerke von Sprachpaketen beschrieben. Diese stellen keine grundsätzlichen Empfehlungen seitens foncloud dar, da foncloud die netzwerkseitigen Gegebenheiten des Kunden nicht kennt. Der Support von foncloud steht bei Bedarf aber beratend zur Verfügung, um die individuell passende Methode zu finden. Die Umsetzung der Priorisierung im lokalem Netzwerk erfolgt durch den Partner oder durch den Endkunden selbst.

Methoden zur Trennung von Datenströme und Sprachdaten werden im Abschnitt "Trennung von Netzen für Voip" beschrieben.

3.1 Einleitung

Warum Sprache überhaupt priorisiert werden sollte?

Standardmäßig werden in einem Netzwerk alle Datenpakete nach dem Best-Effort-Prinzip gleich behandelt. In einem Netzwerk können jedoch die einzelnen Datenpakete unterschiedlich schnell unterwegs sein. So lange hauptsächlich Nachrichten und Dateien übertragen werden, kommt es hierbei selten zu Übertragungsproblemen. Werden jedoch Echtzeitanwendungen, wie Voice over IP oder Videostreaming genutzt, dann wirken sich Verzögerungen oder Paketverluste auf die Übertragungseigenschaften zwischen den Teilnehmern negativ aus. Dies wird beispielsweise durch abgehackte Sprache oder fehlende Bild-Fragmente in einem Video spürbar.
Im Vergleich dazu fällt es kaum auf, wenn eine E-Mail ein paar (Milli-)Sekunden später beim Empfänger eintrifft.

Eine geringe Bandbreite, schlechte Übertragungseigenschaften und unterschiedliche Auslastung führen zum Verwerfen oder verzögerten Ausliefern von Datenpaketen. In der Konsequenz kommt es zu Störungen bei der Sprach- und Videoübertragung. Die Sprache wirkt verzerrt. Kratzen und knacken verschlechtert die Sprachqualität. Videobilder werden pixelig oder ruckelnd wiedergegeben.

3.2 Typische QoS-Maßnahmen

3.2.1 Priorisierung von VLAN´s

VLANs werden mit Switchen realisiert, die in gewisser Weise die Vorteile von Switching und Routing vereinen. Es gilt die Regel: Verbleibt der Netzwerkverkehr innerhalb eines VLANs, wird geswitcht, andernfalls wird in ein anderes VLAN geroutet. Wobei Switching schneller ist als Routing.

Um Daten verzögerungsfrei zu übertragen, weist man den Telefonen eine VLAN ID´s und eine Priorität zu.

Über die VLAN ID werden Telefone vom restlichem Netzwerk logisch getrennt. Die VLAN Priorität sorgt dafür, dass Pakete die im Voip-VLAN transportiert werden bevorzugt werden.

Entsprechende VLAN Einstellungen für die Telefone können über den foncloud Support eingerichtet werden.

Besonderheit

Damit dieses Verfahren funktioniert, müssen die Netzwerkkomponenten auf der gesamten Übertragungsstrecke in der Lage sein, die Datenpakete zu klassifizieren und zu priorisieren. Mit diesem Verfahren ist trotzdem keine Garantie der Bandbreite und Verzögerungszeit möglich. Eine Garantie ist nur mit verbindungsorientierten Maßnahmen möglich.

Vorteile

Telefone und sonstige IT Komponenten sind voneinander separiert. Die einzelnen VLANs können gegeneinander priorisiert werden. Telefonie wird somit im gesamten Netzwerk bevorzugt und auch bei großer Netzlast kann störungsfrei telefoniert werden.

3.2.2 DiffServ

DiffServ ist ein Verfahren zur Priorisierung von Datenverkehr für Echtzeitapplikationen über IP. Jedes Datenpaket wird einer Verkehrsklasse zugewiesen. Datenpakete einer höheren Verkehrsklasse werden gegenüber einer niedrigeren Verkehrsklasse bevorzugt behandelt. Bei DiffServ wird die Klassifizierung und Markierung der Datenpakete durch den Sender vorgenommen. Die Router auf dem Weg zum Empfänger werten diese Markierung aus.

4. Trennung von Netzen für VoIP

Vorwort

In diesem Abschnitt werden die unterschiedlichen Möglichkeiten zur Trennung von Daten und Sprache beschrieben. Diese stellen keine grundsätzlichen Empfehlungen seitens foncloud dar, da foncloud die netzwerkseitigen Gegebenheiten des Kunden nicht kennt. Der Support von foncloud steht bei Bedarf aber beratend zur Verfügung, um die ideale Konfiguration zu finden. Die Umsetzung erfolgt stets durch den Partner oder durch den Endkunden selbst.

Zu berücksichtigen ist weiterhin, dass Softphones und/oder Smartphone Voip Clients nicht über die unten genannten Methoden getrennt werden können. Hierfür bedarf es komplexer Regeln, ein sogenanntes Policy-Based Routing.

Die in diesem Dokument beschriebenen Maßnahmen dienen lediglich der Trennung, nicht aber der Priorisierung von Sprachpaketen. Siehe hierzu das Dokument "QOS für Voip". Eine Kombination aus Trennung und Priorisierung der Sprachdaten ist besonders in größeren Netzwerken zu empfehlen.

4.1 Physikalische Trennung

Bei der physikalischen Trennung von Daten und Sprachnetz existieren zwei voneinander getrennte Netzwerke. Jedes Netzwerk verfügt über eigene Router, Switche und Kabelwege zu den Telefonen.

Eine physische Trennung ist immer dann zu empfehlen, wenn der Endkunde besonders sensible Daten verarbeitet. Beispielsweise haben Steuerberater von Seiten Datev / Lexware die feste Vorgabe keine Fremdgeräte ins Netzwerk zu lassen, die nicht für die Datenverarbeitung benötigt werden. Das bedeutet, dass Steuerkanzleien, ein eigenes Netzwerk für VOIP Telefone (und andere Geräte wie z.B. Gäste Wlan ect.) betreiben müssen.

Zusammengefasst

- Hohes Maß an Sicherheit.
- Volle Kontrolle über bereitstehende Bandbreite.
- DHCP für Telefone möglich: ja
- Da alle Kabelwege voneinander getrennt aufgebaut werden, kann es zu keinen DHCP Konflikt mit mehreren DHCP Servern kommen.
- Nutzung von CTI möglich: nein

4.2 Logische Trennung über VLAN

Bei dieser Form der Datentrennung werden virtuelle Local Area Networks (VLAN´s) aufgebaut. Das Telefon erhält über das Provisioning eine VLAN ID. Ebenso ist es möglich, dem Daten Port des Telefons eine andere VLAN ID zu geben.

Prinzipiell ist VLAN auch ein wichtiger Sicherheitsbaustein für VoIP. Durch die Trennung der Netze in anwendungsspezifische Bereiche – also z. B. Telefonnetz (VoIP) und Datennetz – begrenzt man auch mögliche Angriffe auf einen kleinen Bereich.

Im Werkszustand verfügt das Telefon über keine VLAN ID. Damit sich das Telefon korrekt provisionieren kann, muss das Default VLAN in der Lage sein, folgende Dienste durchzulassen:

- DNS
- NTP
- HTTP

- HTTPS

Zusammengefasst

- Logische und virtuelle Trennung mit einer gemeinsamen physikalischen Infrastruktur.
- Nutzung CTI möglich: ja
- DHCP für Telefone möglich: ja

4.3 Trennung über separaten VoIP Router

Bei dieser Form der Datentrennung wird ein zusätzlicher VoIP-Router im bestehenden Computer Netzwerk betrieben. Er hat DHCP ausgeschaltet und bekommt eine feste IP Adresse aus dem bestehendem Netzwerk.

Die Telefone stehen im Werkszustand im DHCP Modus. Sie erhalten über das Computer-Netzwerk per DHCP eine zufällige IP-Adresse und laden über dieses Netzwerk initial das Provisioning (also die Config Dateien) sowie die Firmware. Über das Provisioning erhält das Telefon dann eine feste IP Adresse und den VOIP-Router als Standard-Gateway.

Ab diesem Moment kommuniziert das Telefon ausschließlich mit dem Voip-Router. Der Daten-Router wird ab dem Moment nur noch von dem im DHCP Modus befindlichen Computern verwendet.

Nachteilig bei dieser Lösung ist jedoch, dass im Vorfeld jedes Telefon eine feste IP Adresse definiert werden muss. Die IP Adressen sollten idealerweise nicht im DHCP Bereich des Daten Routers liegen, um zufällige Doppelvergaben zu vermeiden.

Erhält das Telefon keine IP Adresse, ist es über den Daten Router online. Eine Trennung der Sprachdaten von restlichen Datenstrom würde also nur dann stattfinden, wenn das Telefon eine feste IP Adresse hat.

Die Zuordnung eines Voip Routers kann natürlich auch über den DHCP Server selbst erfolgen, sofern dieser die Funktion beherrscht.

Zusammengefasst

- Einfache Integration in bestehende Netzwerke
- Nutzung CTI möglich: ja
- DHCP für Telefone möglich: nein