



## **DOSSIER ALL-IP**

Wissenswertes rund um die Umstellung  
auf VoIP im Unternehmen.

# ALL-IP – DIE NEUE ÄRA

Das umfassende Dossier zeigt IT-Fachhändlern auf, wie die Umstellung von herkömmlicher Telefonie auf All-IP – sprich VoIP – geplant und erfolgreich umgesetzt wird.

## Vorbereitungen für die neue Ära

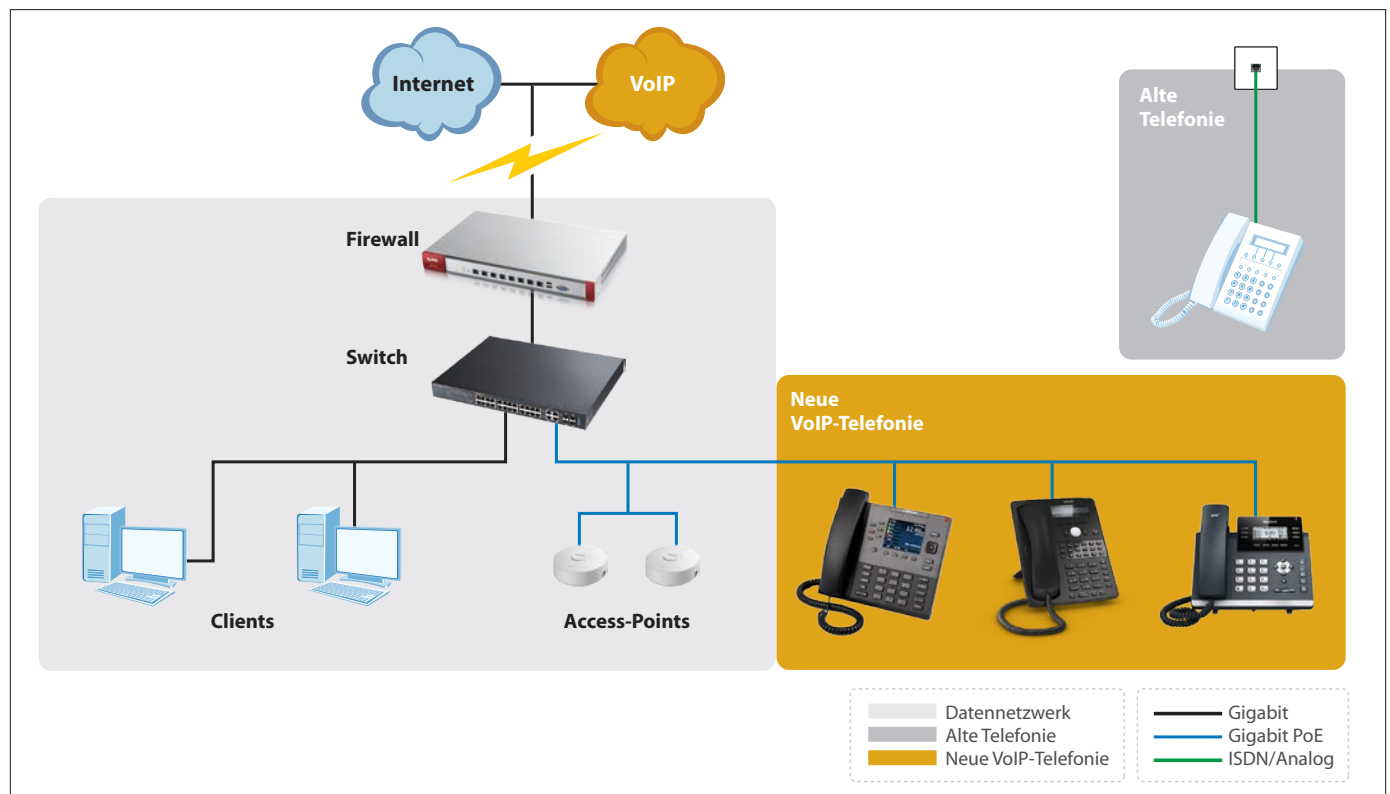
Die Ankündigung der Swisscom, die Analog- und ISDN-Anschlüsse per Ende 2017 abzuschalten, sorgt in einigen Kreisen für Unruhe. Die zuverlässige graue NT-Box wird durch VoIP-Technologie ersetzt. Der Internettelefonie haftet immer noch der schlechte Ruf an, unzuverlässig zu sein. Al-

## Planung und Umsetzung

Bevor etwas Neues geplant wird, muss der Ist-Zustand der jetzigen Infrastruktur analysiert und dokumentiert werden. Als zweiter Schritt ist ein Pflichtenheft für die neue Lösung zu erstellen. Erst danach ist eine seriöse Planung und erfolgreiche Umsetzung möglich. Nachfolgend wird im Detail in

## Abklärungen Telefonie

Was für Geräte (Telefon, Fax, Sprechanlagen, Konferenztelefone usw.) sind vorhanden? Ist eine Telefonanlage im Haus und soll diese noch weiterhin betrieben werden? Bestehen Verträge? Können die derzeitigen Geräte noch benutzt werden oder benötigt es neues Equipment? Welche Ruf-



All-IP verschmelzt Telefonie mit dem Datennetzwerk.

lerdings bestätigten in einer kürzlich von der Studerus AG durchgeführten Umfrage über 70% der Fachhändler, aktuell in Projekte mit All-IP involviert zu sein. Mit einer soliden Infrastruktur und richtig konfigurierten Netzwerkgeräten lässt sich eine gut funktionierende Nachfolgelösung realisieren.

Vielfach wird damit geworben, dass VoIP nur Vorteile gegenüber der alten Telefonie hat. Dies ist die halbe Wahrheit: Die neue Technologie verlangt mehr IT-Kenntnisse, andere Geräte und Kabel werden eingesetzt, es braucht komplexere Einstellungen und mehr Fehlerquellen sind vorhanden.

Form von Fragen aufgezeigt, welche Schritte dafür erforderlich sind.

## Netzwerkanalyse

Wie hoch ist die aktuelle Bandbreite der Internet-anbindung und wie stark die Auslastung? Sind die Netzwerkgeräte (Firewall, Switches) zeitgemäss und für die Nutzung mit VoIP zu gebrauchen? Sind überall bereits Netzkabel vorhanden? Wenn ja, welche Kategorie? Sollen die Geräte per PoE gespeist werden? Sind PoE-Switches vorhanden? Ist eine zweite Internetverbindung oder eine Backup-Lösung (LTE-Router etc.) vorhanden? Ist die Ausstattung für die Zukunft gerüstet?

nummern sollen übernommen werden? Wie viele Endgeräte werden in naher Zukunft noch benötigt? Sollen auch Telefone anderer Standorte mit eingebunden werden? Müssen spezielle Funktionen wie Music-on-Hold, Konferenzschaltung, CTI-Anbindungen oder Videotelefonie abgedeckt werden?

## Anforderungen Internetanbindung

Bei der Planung der Internetanbindung ist zu beachten, dass während der Hauptarbeitszeit der Internetanschluss zu maximal 50% ausgelastet sein sollte. Ein einzelnes VoIP-Gespräch benötigt lediglich eine Bandbreite von 100 Kbps. Die Anforderung

an die Qualität der Netzwerkverbindung ist dagegen sehr hoch. Mit QoS (Quality-of-Service) im ganzen Netzwerk und einer zuverlässigen WAN-Anbindung wird sichergestellt, dass keine Engpässe entstehen können. Eine redundante Anbindung mit zwei oder mehreren günstigen Anschlüssen von verschiedenen Internet Providern kann eine Alternative zu einem Business-Anschluss mit SLA (Service-Level-Agreement) sein. ZyXEL Firewalls unterstützen mehrere WAN-Ports, die kombiniert werden können. Ist eine hohe Redundanz gefordert, empfiehlt sich eine Backup-Lösung mit einem ZyXEL LTE-Router.

### Ausreichende Sicherheit

Heute kann auf die Sicherheit einer Firewall mit entsprechenden Services wie IDP, Content-Filter und Anti-Virus nicht verzichtet werden. Bei der Konfiguration der ZyXEL USG sind die Vorgaben des VoIP-Anbieters zu berücksichtigen. Die Einstellung der SIP-ALG und der NAT-Optionen sind matchentscheidend, um den schweizerischen Ansprüchen an die Telefonie zu genügen. Wie bei der Netzwerk-Infrastruktur ist auch hier QoS ein wichtiger Punkt. Je nach Wichtigkeit der Telefonie für ein Unternehmen bietet sich bei der Firewall eine redundante Lösung mit High-Availability-Mode (HA-Mode) an.

### Netzwerk als Rückgrat

Wer beim Netzwerk spart, handelt sich gerade bei VoIP fast zwangsläufig Ärger ein. End-to-End-QoS ist unabdingbar für einen zuverlässigen Betrieb. Gemanagte Gigabit-Switches bilden das solide Rückgrat eines stabilen Netzwerkes. Vernünftigerweise werden heute alle VoIP-Telefone per PoE gespeist. Damit sind zusätzliche Netzteile und Kabel am Arbeitsplatz überflüssig. Dies ist aus ästhetischen und ökologischen Gründen sinnvoll, denn mittlerweile ist PoE eine kostengünstige Lösung. Fast alle PoE-Switches verfügen über einen Lüfter. Für die Platzierung im Büro eignet sich das lüfterlose Modell GS1900-8HP von ZyXEL. Um bestehende Netzkabel für VoIP zu verwenden, müssen diese mindestens der

Standard-Kategorie 5e entsprechen. Es macht heute wenig Sinn, bei Neuinstallationen Kabel unter der Kategorie 6 zu verwenden.

### Mögliche VoIP-Varianten

Standard-SIP-Accounts bieten sich vor allem für einzelne Anschlüsse an. Für grössere Firmen eignen sich proprietäre Lösungen wie zum Beispiel Skype for Business. Das typische Schweizer KMU mit zwei bis dreissig Mitarbeitenden ist normalerweise

für jeden Geschmack und jeden Einsatzzweck das richtige Produkt verfügbar ist. Dank der Kompatibilität mit verschiedenen Lösungen können diese Marken auch gemischt eingesetzt werden. Bei kabellosen Telefonen empfiehlt sich die Verwendung der bewährten DECT-Technologie. Hier existieren Single-Cell-Geräte von snom und Yealink für die Verwendung in SOHO (Small-Office, Home-Office)-Umgebungen. Bei hohen Ansprüchen sind die professionellen Multi-Cell-DECT-Geräte von Mitel



Auf diese renommierten VoIP-Telefon-Brands setzt Studerus: Mitel, snom und Yealink

mit einer Virtual-PBX (Private-Branch-Exchange) – auch Hosted-TVA (Teilnehmervermittlungsanlage) genannt – am besten aufgehoben. Hat ein KMU erst kürzlich in eine lokale PBX investiert, ergibt es Sinn, diese – falls möglich – VoIP-fähig zu machen: Entweder mit einem Update durch den Hersteller oder mit einer Erweiterung durch einen VoIP-Gateway.

### Unterschiede bei VoIP-Telefonen

Aktuelle Endgeräte unterscheiden sich in der Handhabung kaum von herkömmlichen Telefonen und fördern so die Akzeptanz beim Benutzer. Die Geräte der verschiedenen Hersteller differenzieren sich lediglich im Design und bei der Haptik; die Grundfunktionen sind bei allen Herstellern vorhanden. Um ihren Kunden eine Auswahl zu bieten, führt die Firma Studerus AG Telefone der bekannten Brands Mitel, snom und Yealink. So ist sichergestellt, dass

und snom die richtigen Produkte.

### Projektunterstützung

Die Migration von herkömmlicher Telefonie auf All-IP stellt hohe Anforderungen an alle Beteiligten. Daher empfiehlt es sich, mit einem kompetenten Partner wie der Studerus AG zusammenzuarbeiten. Unsere erfahrenen Techniker sind in der Lage, auch anspruchsvolle Projekte von der Netzwerkanalyse über die Planung bis hin zur Implementation zu begleiten. Erfahrungsgemäss funktionieren Lösungen mit Produkten aus einer Hand reibungsloser, trotzdem ist eine frühzeitige Planung unabdingbar. ▼

**Sind Sie ready für All-IP? Eine ausführliche Checkliste finden Sie hier:**  
[www.studerus.ch/checkliste\\_all-ip](http://www.studerus.ch/checkliste_all-ip)

# VOIP MIT ZYXEL USG

Die Next-Generation ZyWALLs und USGs funktionieren mit VoIP. Zentral sind die Konfiguration der Firewall und Switches, die Parameter des VoIP-Providers und die PBX-Settings.

## ZyXEL USG als Sündenbock?

Gibt es Probleme mit VoIP und wird eine USG eingesetzt, war bislang der Fall klar: Die USG ist der Sündenbock. Die Realität zeigt, dass in 95% aller Fälle, bei denen der Studerus Support zum Thema VoIP mit Firewall kontaktiert wird, der Fehler wo anders liegt. Der Einsatz einer Next-Gen. ZyWALL/USG ab 110er-Modell wird empfohlen.

## VoIP ohne NAT

Jede eingerichtete NAT-Regel WAN-to-LAN auf der Firewall birgt ein gewisses Risiko. Kann man das vermeiden, sollte man es tun. Elegant lässt sich dies bei der Anbindung einer lokalen PBX an den SIP-Provider lösen, indem eine ständige Verbindung von der PBX durch die Firewall zum Provider besteht. Eingehende Calls nutzen so die gleiche Session wie ausgehende (siehe Grafik).

## PBX hinter USG

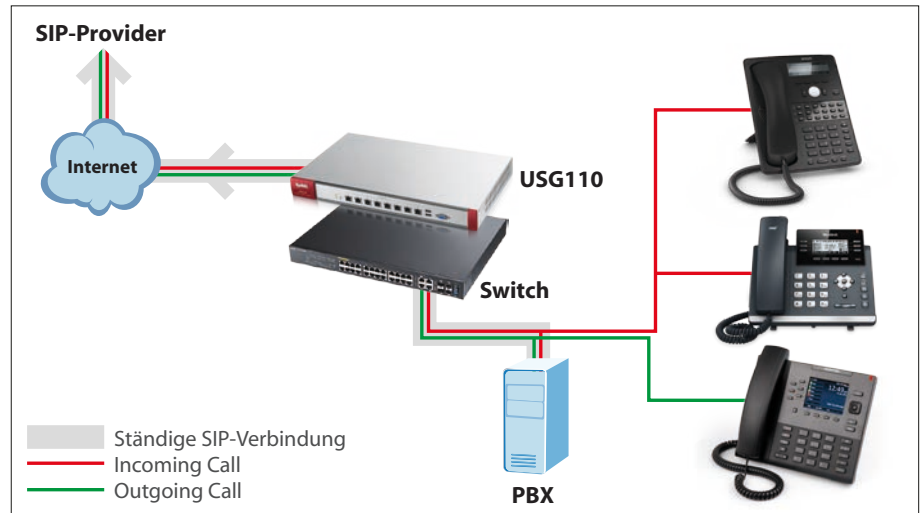
Die Next-Gen. ZyWALLs & USGs unterstützen den Betrieb einer IP-Telefonanlage. Der KB-3505 zeigt die maximale Anzahl SIP-Clients bei aktiviertem SIP-ALG.

## WAN-Anschluss bei VoIP

Damit bei der Business-Telefonie die Qualität gewährleistet ist, sollte für die VoIP-Anbindung ein dedizierter WAN-Anschluss verwendet werden. Ein synchroner Anschluss (gleicher Up-/Download) mit ausreichender Bandbreite bietet ebenfalls eine gute Basis. Das Aktivieren von «Höchste Priorität für SIP-Traffic» im Bandbreiten-Management stellt sicher, dass VoIP gegenüber anderen Protokollen bevorzugt wird.

## Simpler Router vs. Firewall

Es ist plausibel, dass sich VoIP mit einem simplen Router rascher implementieren lässt als mit einem komplexeren Gateway. Ein Schadenfall bei VoIP ist jedoch oft sehr teuer und rechtfertigt den grösseren Konfigurationsaufwand. Sicherheit muss gerade auch bei VoIP Priorität haben. Firewall-Regeln sollen so eng wie möglich gefasst sein und IP- oder Port-Ranges sind klar zu definieren. Ein «any» gilt es zu vermeiden.



Durch die ständige Verbindung von der PBX zum VoIP-Provider ist keine eingehende NAT-Regel auf der Firewall notwendig. Für die Sicherheit ein grosses Plus!

## SIP-ALG ja/nein?

Der SIP-ALG hilft die SIP-Pakete durch die Network-Address-Translation (NAT) zu schleusen. Bei dieser Funktion muss beachtet werden, was der VoIP-Provider für Einstellungen vorgibt.

## USG und BCon-VoIP

Bei der ZyXEL USG kommt es bei aktiviertem SIP-ALG zu Problemen mit dem Swisscom Business Connect VoIP-Service. Wir empfehlen bei BCon-VoIP den SIP-ALG zu deaktivieren und die UDP-Verbindungen auf 180 oder den Maximalwert auf 300 Sekunden hochzusetzen.

## VoIP durch VPN-Tunnel

Ist der Voice-Stream im gleichen VPN-Tunnel wie der Datentransfer, stehen diese in gewisser Konkurrenz zueinander. Die Firewall als Gateway kann nicht verhindern, dass aggressive Protokolle die Gesprächsqualität beeinflussen. Voice ist anfällig auf Paketverlust, weil wie bei UDP üblich verlorene Pakete nicht erneut gesendet werden. Geht beispielsweise das Invite-Paket verloren, wird das Gespräch gar nicht erst aufgebaut. In diesem Szenario ist auch das Monitoring nur bedingt möglich.

## Ready für All-IP

Im neuen Kurs «Ready für All-IP» wird

Know-how zu VoIP im Einsatz mit Switch und Firewall vermittelt. Migrationsmöglichkeiten, Sprachqualitäts-Optimierung mittels Quality-of-Service, Anforderungen an Firewall und Switch sind nur ein paar der Themeninhalte.

## Projektunterstützung

Wir sind interessiert, dass Sie Projekte mit unseren Produkten fachgerecht umsetzen können. Unsere Spezialisten befassen sich immer wieder mit denselben Schwierigkeiten und können Ihnen eine kompetente Unterstützung bieten. Die Projektleitung gegenüber dem Endkunden bleibt bei Ihnen als Fachhändler. Wir unterstützen Ihre Techniker und transferieren das Know-how, damit Sie die Wartung der Installation nach Projektabschluss problemlos übernehmen können. Projektanfragen richten Sie bitte an [info@studerus.ch](mailto:info@studerus.ch) ■

## CHECKLISTE

- WAN-Anbindung Up-/Download ausreichend?
- Provider-IP-/Port-Vorgaben erfüllt?
- IP-/Port-Ranges so eng wie möglich definiert?
- NAT-Optionen überprüft?
- SIP-ALG nach Vorgabe des Providers?
- SIP-Priorisierung gesetzt?
- UDP Session-Time-Out auf 300 Sekunden?
- SIP-Traffic von Internet-Anbieter priorisiert?



# TIPPS UND TRICKS

In diesem Interview stellen wir einem erfahrenen Studerus Netzwerktechniker häufige Fragen zu VoIP/All-IP. Hier seine Antworten und nützlichen Informationen.



**Stefan Rieger**  
Leiter Support

## Ein häufiges Problem: «Ich höre den Anrufer, er mich aber nicht.»

Bei VoIP kommen zwei Protokolle zum Einsatz, bei SIP werden u. a. die Anrufinformationen zwischen der anrufenden und angerufenen Person ausgetauscht. Die Sprachübertragung erfolgt dann mit RTP über ein eigenes Protokoll. Die IPs und auch Verbindungspoints der Audioübertragung werden im SIP-Protokoll definiert. Befindet sich die angerufene Person nun hinter einer Firewall, kann der Audiostream der anrufenden Person am WAN-Port der Firewall blockiert werden. Damit SIP-/RTP-Protokolle korrekt über eine Firewall funktionieren können, muss entweder der Provider oder die Firewall die IPs für die Audioverbindung korrigieren, die im SIP angegeben sind. Die Firewall kann die Korrektur mit Hilfe der SIP-ALG-Einstellung vornehmen. Nimmt der VoIP-Provider die SIP-/RTP-Korrektur vor, sollte die SIP-ALG deaktiviert und der UDP-Session-Timer der Firewall auf 180 Sek. eingestellt werden. Die Ursache einer einseitigen Audioverbindung ist also immer auf der Seite zu suchen, auf der nichts gehört wird. In der Regel wird das Problem durch eine Firewall-Einstellung für die Protokolle SIP/RTP verursacht, die nicht richtig auf den genutzten VoIP-Anbieter eingestellt ist.

## Was tun gegen schlechte Gesprächsqualität?

Da sich die VoIP-Sprachübertragung die Leitung mit anderen Datendiensten teilt, kann z. B. ein grosser Datei-Download die

Sprachqualität von VoIP stark beeinflussen. Es ist wichtig, managbare Komponenten mit QoS-Option auf dem Weg vom VoIP-Endgerät zum Internetanschluss einzusetzen, um eine konstante Sprachqualität zu erreichen. Diese Komponenten sind besonders zu beachten, wenn VoIP-Service und Internetanschluss von unterschiedlichen Providern bezogen werden. Hier liegt die Qualität der Sprachübertragung ab Internetanschluss in den Händen des Providers. Wird eine Leitung durch andere Datendienste zu stark ausgelastet, ist eine hohe Sprachqualität nur schwer zu erreichen. Denkbar wäre, für VoIP eine eigene, separate Internetanbindung zu nutzen.

## Wie misst man eine schlechte Gesprächsqualität?

Mit dem Tool Wireshark werden die VoIP-Datenpakete aufgezeichnet und analysiert. Damit kann nicht nur die Qualität gemessen, sondern auch Ursachen von Störungen gefunden werden. Ist man damit nicht vertraut, besteht die Möglichkeit, sich in einem Kurs das notwendige Know-how anzueignen (<https://www.studerus.ch/de/training/detail/net-analyse>).

## Ist ein Durchschleifen des LAN über das VoIP-Telefon zum PC sinnvoll?

Dies ist stark von der lokalen Verkabelungssituation abhängig. Bestehen genug UGV-Anschlüsse, empfehlen wir, PC und VoIP-Telefon auf einer eigenen Leitung anzuschliessen und nicht zu schlaufen. Wird der PC via VoIP-Telefon geführt, ist das Setup der Netzwerkkonfiguration aufwändiger und komplexer.

## Sind Lösungen mit Softphones zu empfehlen?

Um Softphones erfolgreich einsetzen zu können, muss ein klarer Mehrwert für die

User vorhanden sein. Sonst wird eine reine Software-Lösung kaum als Ersatz für das gewohnte Telefon akzeptiert. Technisch ist zu beachten, dass die Softphone-Software bei der Nutzung von CPU/Memory auf dem PC bevorzugt behandelt werden muss, um eine optimale Qualität zu erreichen. Es ist auch zu bedenken, dass ein PC-Absturz gleichzeitig bedeutet, kein Telefon mehr verfügbar zu haben.

## Ist Telefonie über WLAN empfehlenswert?

Die Anforderungen an die WLAN-Installation für den Einsatz mit VoIP sind um ein Vielfaches höher als für die normale Datennutzung. Es braucht bis zu doppelt so viele APs, um die für VoIP notwendige Dichte in der Signalabdeckung und -stärke zu erreichen. Sehr oft kollidieren die für VoIP-über WLAN notwendigen Einstellungen mit den Anforderungen für die normale Datennutzung: Für VoIP ist eine geringe Bandbreite mit hoher Stabilität und sehr kurzer Latenz notwendig, für die normale Datenübertragung hingegen braucht es einen möglichst hohen Datendurchsatz pro Client, und die Anforderungen an die Latenz sind geringer. Zudem verfügen die VoIP-Endgeräte über eine geringere Akkulaufzeit als diejenigen der klassischen DECT-Telefone. Der Betrieb für einen Arbeitstag kann ohne Nachladen des Akkus oft nicht erreicht werden. Daher ist eine Lösung via DECT oft kosteneffizienter und einfacher, als das WLAN für VoIP fit zu machen. ■