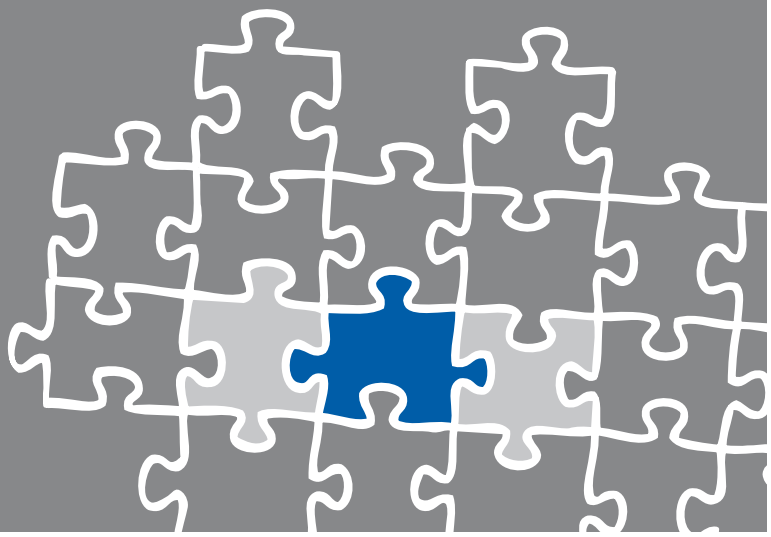
TechNote

XCAPI und Firewalls

Stand: 14. Juni 2011

XCAPI voiceoverIP



Zusammenfassung

Alle aktuellen Windows-Versionen schützen die Netzwerkschnittstellen mit einer Firewall, die einerseits den Computer vor unberechtigten Zugriffen von außen schützen soll, und andererseits dem Benutzer eine gewisse Kontrolle darüber geben kann, welche Programme ihrerseits auf das Netzwerk zugreifen dürfen. Die VoIP-Controller der XCAPI sind davon nicht ausgenommen und sind daher ebenso eingeschränkt, vor allem, was den eingehenden Datenverkehr von der PBX angeht.

Die meisten XCAPI-Installationen sind in ein lokales Netzwerk integriert, welches über einen Router mit dem Internet verbunden ist. Diese Router übernehmen oftmals ebenso eine Firewall-Funktion und blockieren eingehende Nachrichten von den VoIP-Providern.

XCAPI und Firewalls

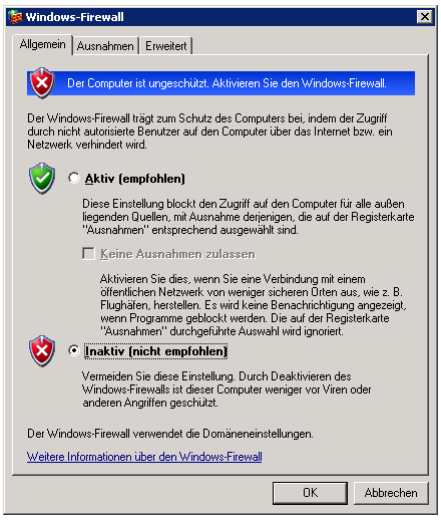
Damit die XCAPI problemlos mit der PBX oder dem VoIP-Provider kommunizieren kann, muss die Firewall überwunden werden. Die einfachste Methode besteht darin, die Firewall zu deaktivieren. Was im lokalen Netzwerk noch vertretbar ist, ist jedoch auf dem Router zum Internet unbedingt zu vermeiden. Daher gibt es in der XCAPI eine Möglichkeit, die Kommunikation auf eine bestimmte Gruppe von Ports festzulegen, die wiederum fest in der Firewall konfiguriert werden können.

Im Folgenden wird eine einfache und in der Praxis häufig verwendete Lösung beschrieben:

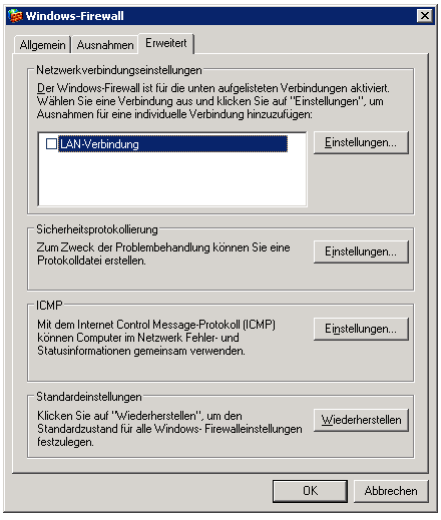
Firewall-Konfiguration: XCAPI - PBX

Die XCAPI ist auf einem Rechner im LAN installiert und muss lediglich mit einer PBX kommunizieren, die im gleichen Subnetz erreichbar ist. Wenn aus Sicht der Sicherheit nichts dagegen spricht, kann im Betriebssystem, auf dem die XCAPI läuft, die Firewall deaktiviert werden. Dadurch können alle TCP- und UDP-Pakete ungehindert zwischen der XCAPI und der PBX (und zu allen anderen Netzwerkgeräten) übertragen werden. In der Windows-Systemsteuerung können unter `Windows-Firewall` alle relevanten Einstellungen vorgenommen werden.

Möglichkeit 1: Firewall deaktivieren Häufig wird bei Problemen mit der Firewall nur die Einstellung `Aktiv` auf `Inaktiv` gesetzt.



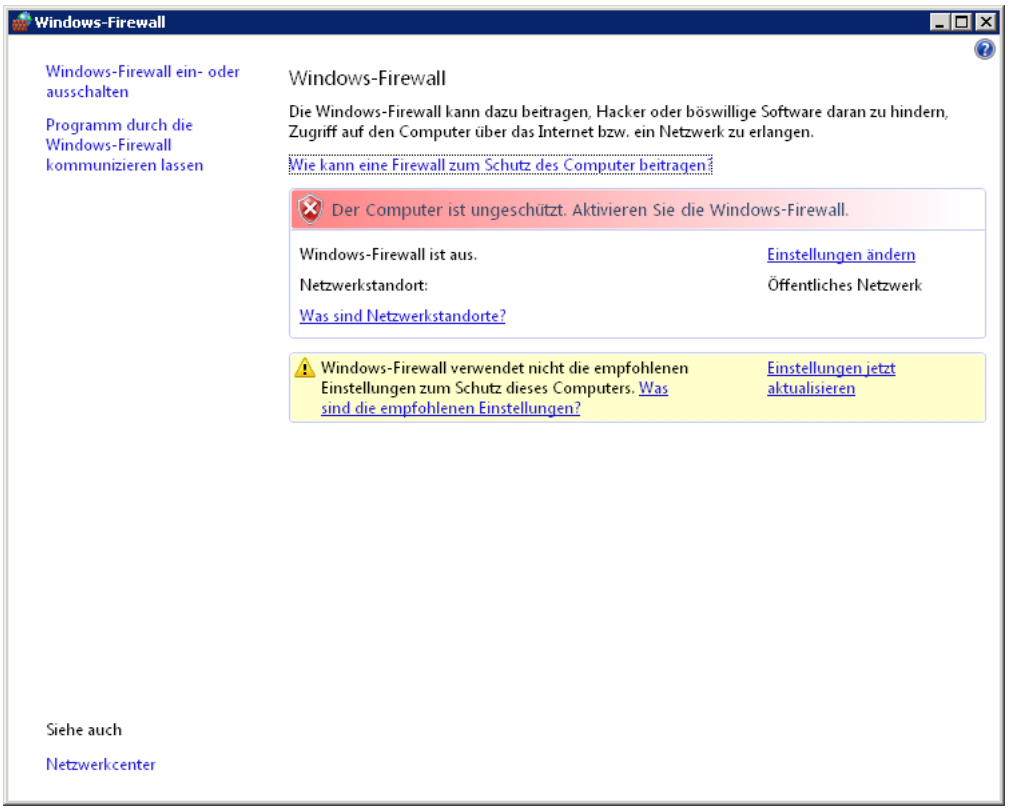
Es sind jedoch auch die Einstellungen im Reiter `Erweitert` zu beachten, da diese im Regelfall noch immer die Kommunikation behindern. Aus diesem Grund muss in den `Netzwerkverbindungseinstellungen` des `Erweitert`-Reiters ebenso die Netzwerkschnittstelle (z. B. LAN-Verbindung 1, etc.) deaktiviert werden, die die XCAPI nutzen soll.



Erweiterte Firewall-Einstellungen beachten

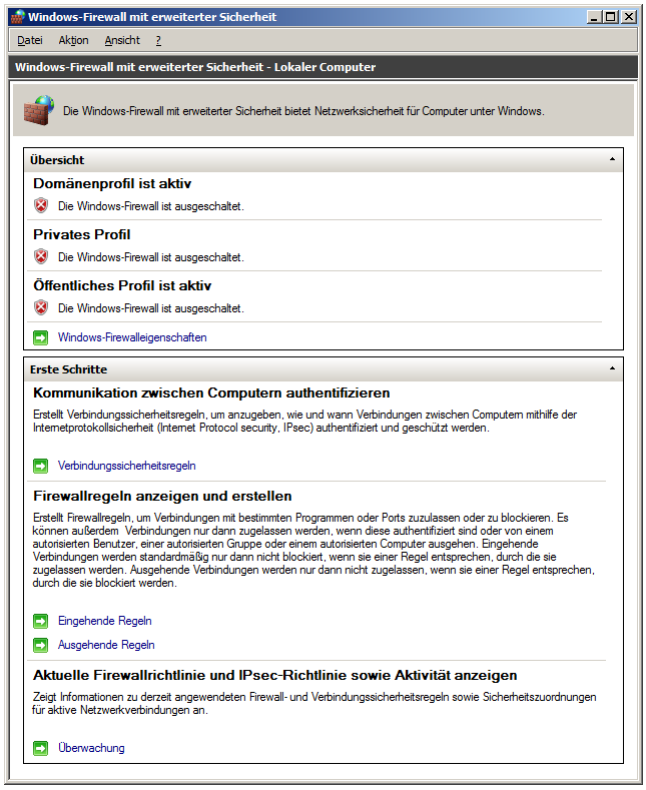
Diese Einstellungen reichen nur auf Systemen bis Windows Server 2003, welcher nach einer Standard-Installation ausnahmsweise immer mit deaktivierter Firewall läuft und daher in den meisten Fällen keine Probleme bereitet.

Auch in Windows-Versionen ab Server 2008 gibt es die `einfache Ansicht`, in der die Firewall deaktiviert werden kann:

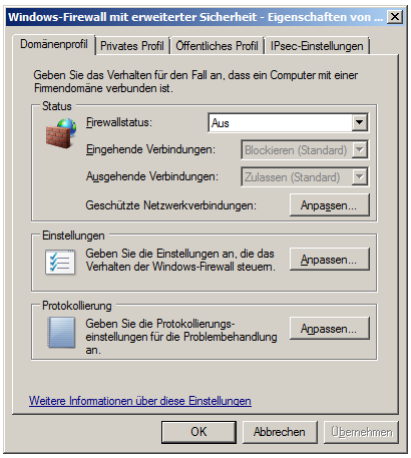


Windows-Systeme ab Vista haben noch eine weitere Firewall-Konfiguration, die ebenfalls zu beachten ist:

In der Windows-Systemsteuerung befindet sich unter `Verwaltung` das Konfigurationsprogramm für die `Windows-Firewall mit erweiterter Sicherheit`.



Hier wird über Profile geregelt, ob eine Verbindung genutzt werden darf, oder nicht - abhängig davon, welches Netzwerkprofil für die Netzwerkkarte ausgewählt wurde, die die XCAPI nutzen soll. Hier können gezielt einzelne oder auch alle Profile deaktiviert werden, um eine einwandfreie Kommunikation zuzulassen.



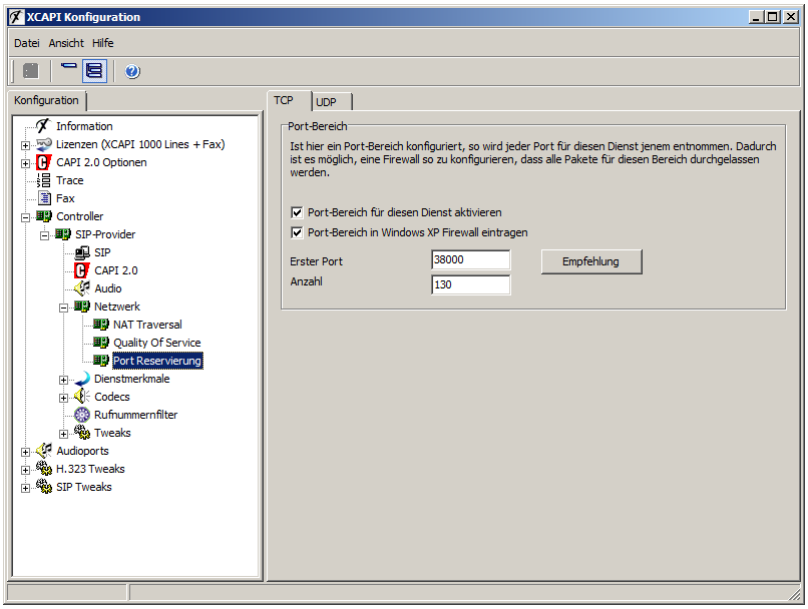
Firewall-Konfiguration: XCAPI - Router - VoIP-Provider

Die sichere, dafür mit etwas Konfigurationsaufwand verbundene Variante, kann sowohl im Intranet als auch für externe Verbindungen zu VoIP-Providern genutzt werden. Die Firewall des XCAPI-Rechners und/oder des Routers wird nur auf bestimmten Ports geöffnet, die die XCAPI für die Signalisierung und die RTP-Daten benötigt. Die für die VoIP-Kommunikation wichtigen Pakete können somit ungehindert zwischen XCAPI und Gegenstelle ausgetauscht werden, während die Firewall weiterhin das lokale Netzwerk und die restlichen Funktionen des Betriebssystems schützt.

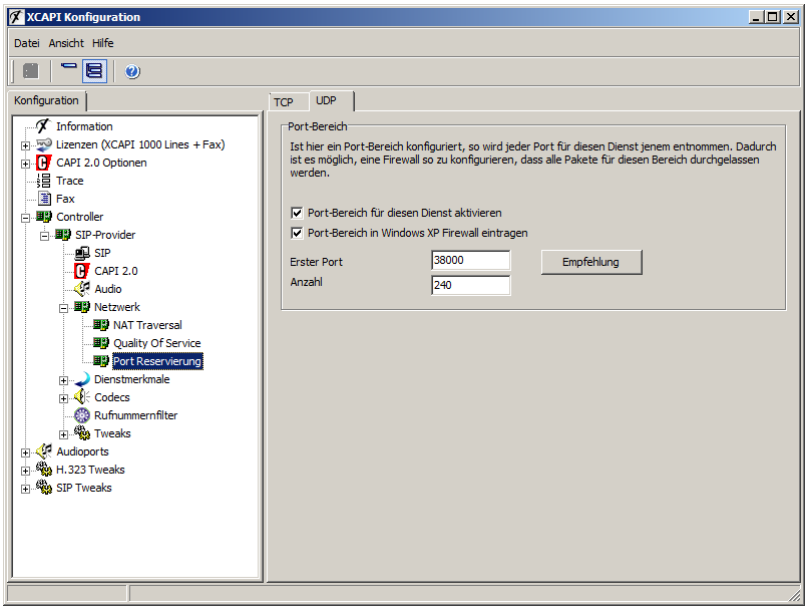
Möglichkeit 2: Port-Bereich definieren

Während die VoIP-Signalisierung in den meisten Fällen über standardisierte Ports läuft (z.B. `5060` für SIP und `1720` für H.323), werden erst während des Rufaufbaus zwischen der XCAPI und dem Teilnehmer festgelegt, welche Ports für die RTP-Daten genutzt werden. Das stellt den Firewall-Administrator vor das nächste Problem, da unter diesen Voraussetzungen eigentlich alle Ports freigeschaltet werden müssten. Es ist sehr wahrscheinlich, dass die RTP-Daten bei jedem Ruf über einen anderen Port geleitet werden. Um dieser Problematik zu entgehen, kann in der XCAPI-Konfiguration ein Port-Bereich festgesetzt werden, den die XCAPI ausschließlich nutzt. Dementsprechend muss der Administrator lediglich diesen Port-Bereich in der Firewall freigeben, was das Sicherheitsrisiko einschränkt.

Um die XCAPI auf einen bestimmten Port-Bereich festzulegen, müssen Sie in der Experten-Ansicht den Konfigurationseintrag des VoIP-Controllers erweitern und unter `Netzwerk` das Menü `Port-Reservierung` öffnen.



Hier können Sie für TCP und UDP zunächst den `Port-Bereich` für das entsprechende Protokoll aktivieren. Mit Hilfe der Schaltfläche `Empfehlung` wird automatisch ein Port-Bereich vorgeschlagen. Falls der Bereich nicht in Ihre Planung passt, können Sie auch anhand der Vorgaben einen eigenen Bereich festlegen. Hierbei ist zu beachten, dass der Bereich die gleiche Anzahl an Ports umfasst, wie der Vorschlag der XCAPI.



Anpassung der Ports bei Erweiterung der XCAPI-Lizenzen

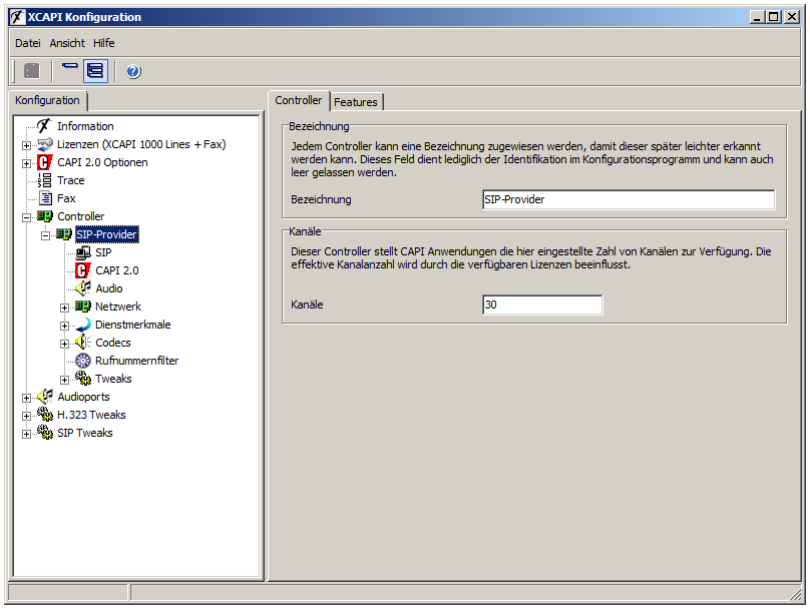
Die Anzahl der Ports wird aus verschiedenen Parametern der Controller-Konfiguration - wie etwa die Anzahl der zur Verfügung stehenden Kanäle - berechnet. Je mehr parallele Rufe der Controller bearbeiten kann, desto größer ist die Anzahl der benötigten RTP-Ports. Das sollten Sie auch beachten, wenn Sie nachträglich die Anzahl der Kanäle erhöhen. In diesem Fall muss die Anzahl der Ports in der Port-Reservierung ebenso erhöht werden.

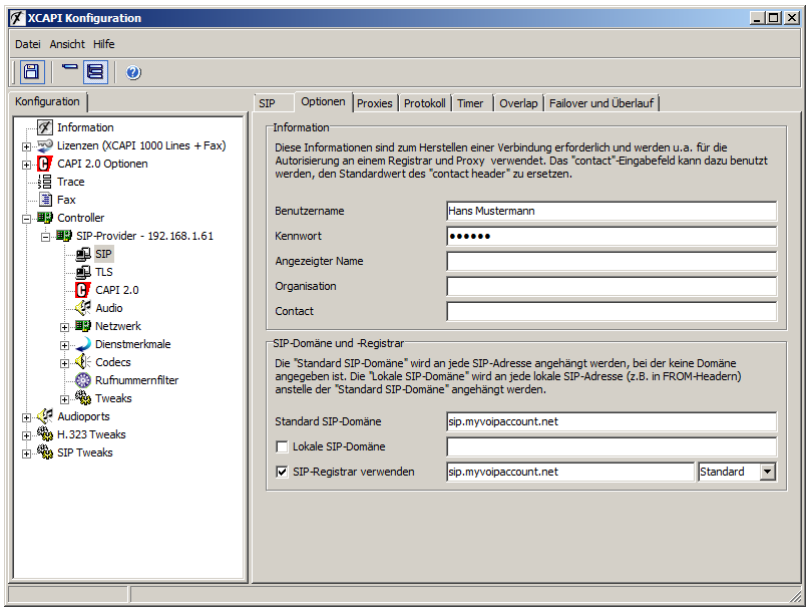
Nachdem die XCAPI auf eine bestimmte Reihe von Ports festgelegt wurde, müssen diese Ports noch in der Firewall freigegeben werden. Wird die XCAPI auf Windows XP genutzt, kann das automatisch durch das Konfigurationsprogramm geschehen. Bei neueren Systemen kann es sein, dass Sie diese Ports manuell in die Firewall-Konfiguration eingeben müssen.

Definierten Port-Bereich in `lokaler` Firewall eintragen

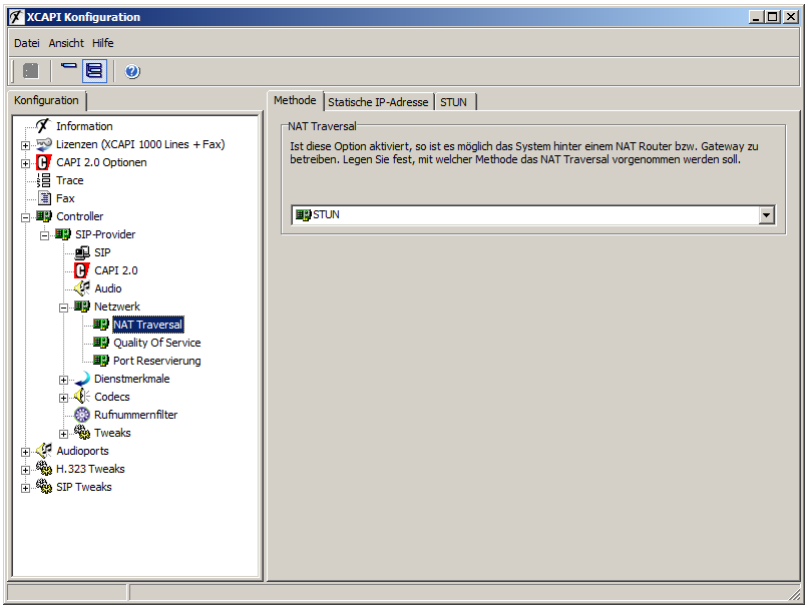
Hier finden Sie eine Beispielkonfiguration einer SIP-Anbindung:

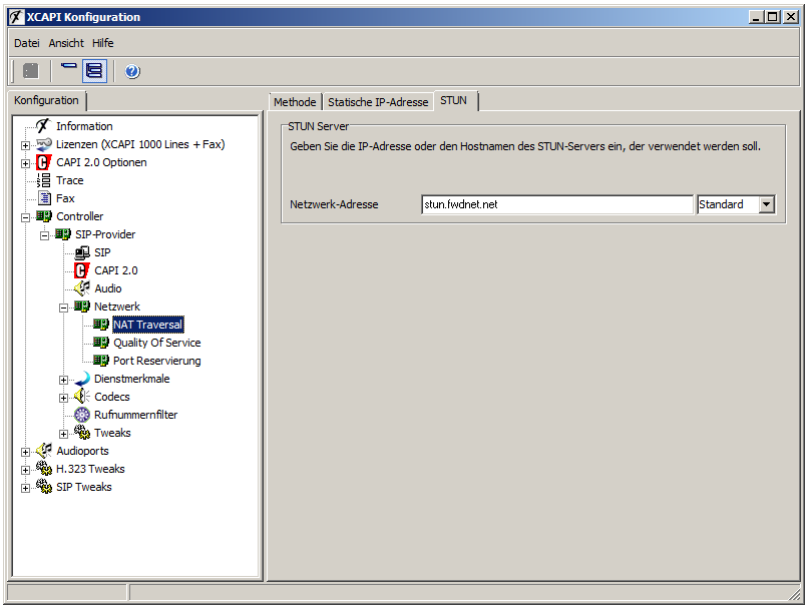
Wir haben einen SIP-Controller konfiguriert, der sich an einem SIP-Provider registrieren soll und 30 Kanäle parallel nutzen kann.





Der SIP-Provider erfordert den Einsatz eines STUN-Servers, da wir uns in einem lokalen Netzwerk befinden.





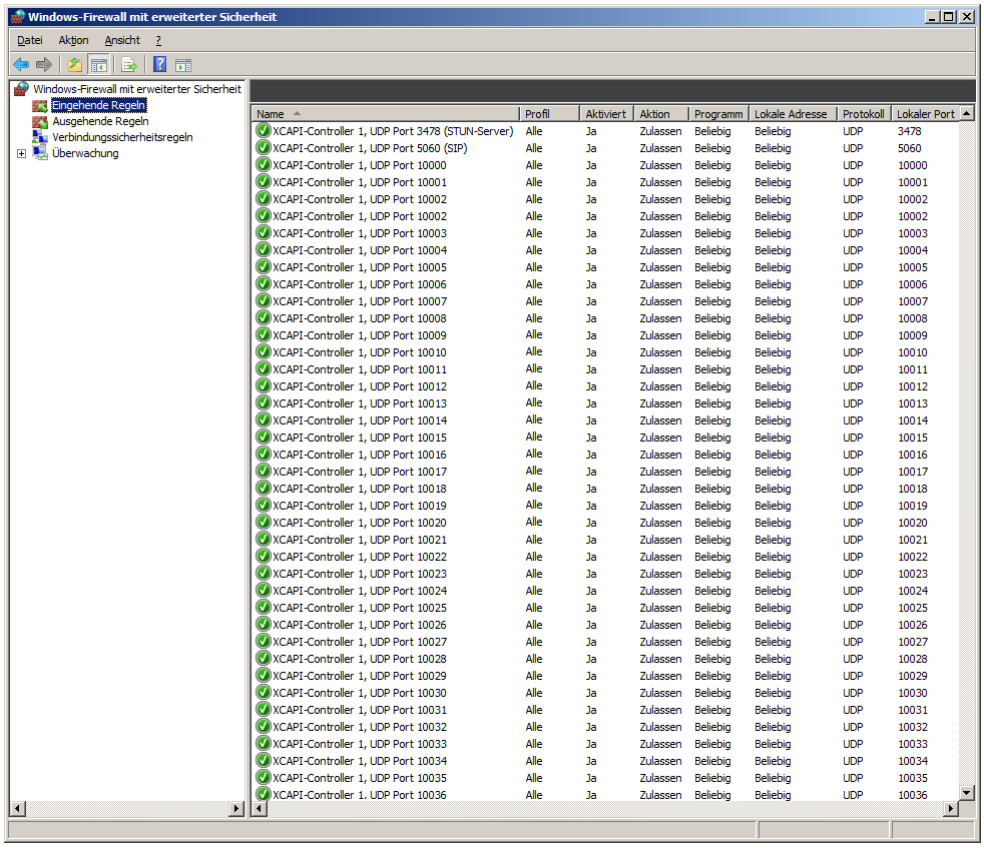
Die Empfehlung für die Port-Reservierung beginnt mit dem Wert `10000` als erster Port und einer Anzahl von `100` Ports für TCP und `180` Ports für UDP.

Zunächst sollte geprüft werden, ob TCP überhaupt benötigt wird, da SIP oftmals nur über UDP genutzt wird und RTP-Daten generell nur per UDP übertragen werden. In unserem Beispiel unterstützt unser SIP-Provider lediglich UDP, daher können wir darauf verzichten, die Ports für TCP freizuschalten.

Unter diesen Voraussetzungen ergeben sich folgende benötigte Ports:

- `5060/UDP` für die SIP-Signalisierung.
- `3478/UDP` für den STUN-Server.
- `10000-10179/UDP` (insgesamt `180` Ports) für die Port-Reservierung.

Diese Ports müssen zunächst in der lokalen Firewall des XCAPI-Rechners freigeschaltet werden, damit die Pakete überhaupt bis zur XCAPI vordringen können. Weiterhin muss im Router, der das lokale Netzwerk mit dem Internet verbindet, eine Port-Weiterleitung für die einzelnen Ports auf die entsprechenden Zielports zur IP-Adresse der XCAPI eingerichtet werden.



Definierten Port-Bereich in `globaler` Firewall eintragen

Die XCAPI teilt dem SIP-Provider jetzt während des Rufaufbaus mit, dass die RTP-Daten an einen der `180` Ports zwischen `10000` und `10179` geschickt werden können. Der Router wird die RTP-Pakete entgegennehmen und an die XCAPI im lokalen Netzwerk weiterleiten.

Mit diesem Wissen können Firewall-bedingte Probleme auch wesentlich leichter diagnostiziert werden:

Wenn nur Port `5060` freigegeben wurde und somit die Signalisierung zwischen XCAPI und Provider funktioniert, kann es sein, dass bei einem ausgehenden Ruf von der XCAPI die Audiodaten nur einseitig hörbar sind. Die Daten von der XCAPI werden eventuell von der lokalen Firewall und von der im Router in Richtung Provider durchgelassen, aber die Richtung vom Provider zur XCAPI wird durch den Router geblockt. Wenn dieses Phänomen beobachtet wird, sollten Sie noch einmal die Konfiguration aller beteiligter Firewalls prüfen.

Haftungsausschluss

Copyright © 2011 TE-SYSTEMS GmbH

Alle Rechte vorbehalten

Kein Teil dieses Dokuments oder das Dokument als Ganzes dürfen ohne vorherige schriftliche Genehmigung von TE-SYSTEMS GmbH in irgendeiner Form reproduziert werden.

Die in diesem Dokument gemachten Angaben entsprechen dem Kenntnisstand zum Zeitpunkt der Erstellung. Die TE-SYSTEMS GmbH behält sich das Recht vor, Veränderungen ohne vorherige Ankündigung vorzunehmen.

Bei der Zusammenstellung von Texten und Abbildungen sowie bei der Erstellung der Software wurde mit größter Sorgfalt vorgegangen. Dennoch kann für die Richtigkeit, Aktualität und Vollständigkeit des Inhalts, eine Wirtschaftlichkeit oder die fehlerfreie Funktion von Software für einen bestimmten Zweck keinerlei Gewähr übernommen werden. Die TE-SYSTEMS GmbH schließt daher jegliche Haftung für Schäden aus, die direkt oder indirekt aus der Verwendung dieses Dokuments entstehen.

Marken

Alle verwendeten Namen von Produkten und Dienstleistungen sind Marken oder eingetragene Marken (auch ohne gesonderte Kennzeichnung) der jeweiligen privaten oder juristischen Personen und unterliegen als solche den gesetzlichen Bestimmungen.

Drittrechte

Third Party Disclaimer and Limitations

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes source code derived from the RSA Data Security, Inc. MD2, MD4 and MD5 Message Digest Algorithms.

This product includes source code derived from the RFC 4634 Secure Hash Algorithm software.

TE-SYSTEMS GmbH

Geschäftsführer Andreas Geiger
Oliver Körber

Anschrift Max-von-Laue-Weg 19
38448 Wolfsburg

Telefon 05363 8195-0
Fax 05363 8195-999
freecall 0800 8379783

E-Mail info@te-systems.de
Internet www.te-systems.de
www.xcapi.de